v. 2.0

Криптография

Лекция 9. Защищенные сетевые соединения.

Дмитрий Яхонтов

“Кочерга”, 2019

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)

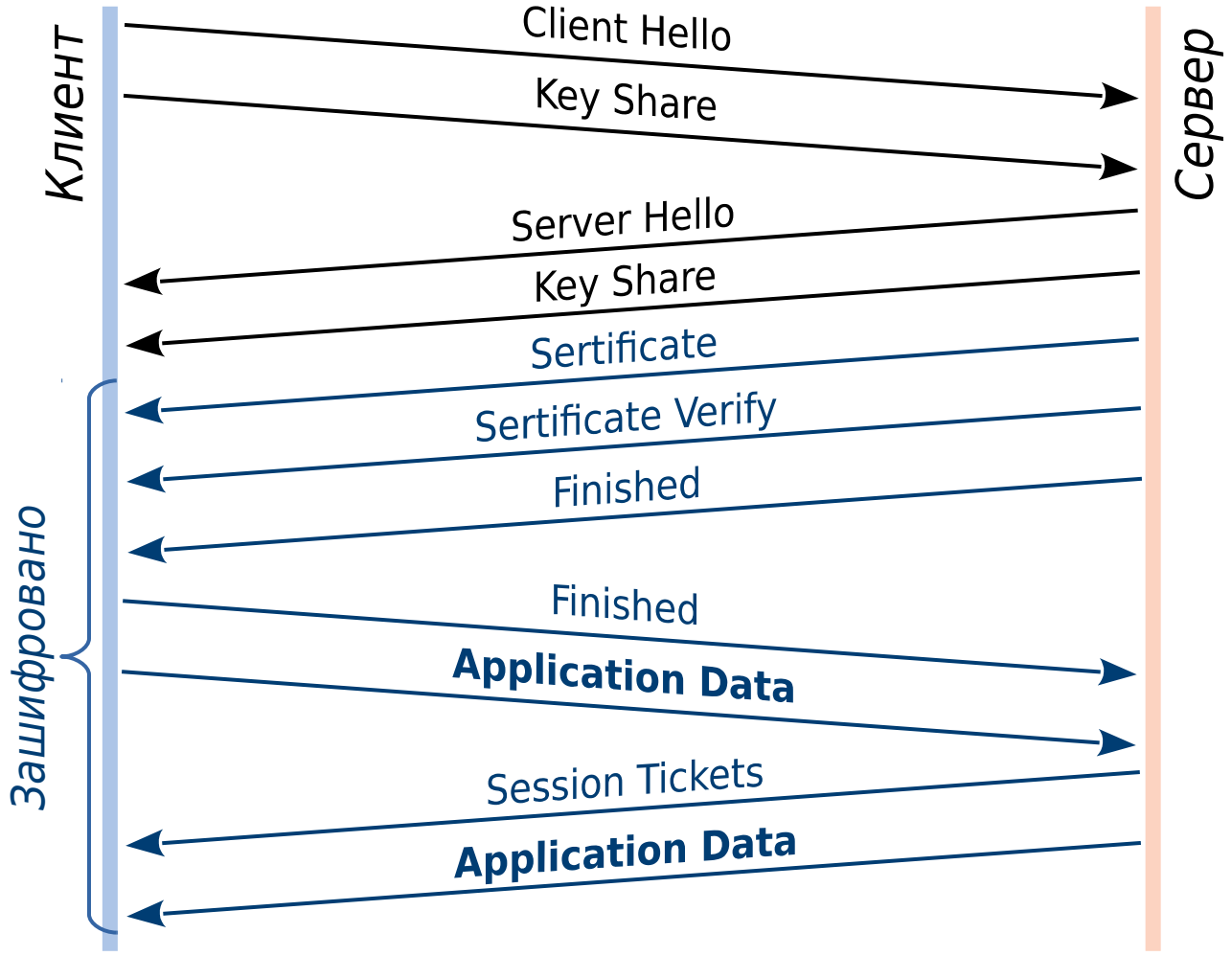
SSL/TLS — протокол представительского (L6) и сеансового (L5) уровней, который обеспечивает:

- аутентификацию
- шифрование
- контроль целостности

для произвольного прикладного (L7) протокола.

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

Рукопожатие TLS 1.3



Цели рукопожатия:

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

Приветствие

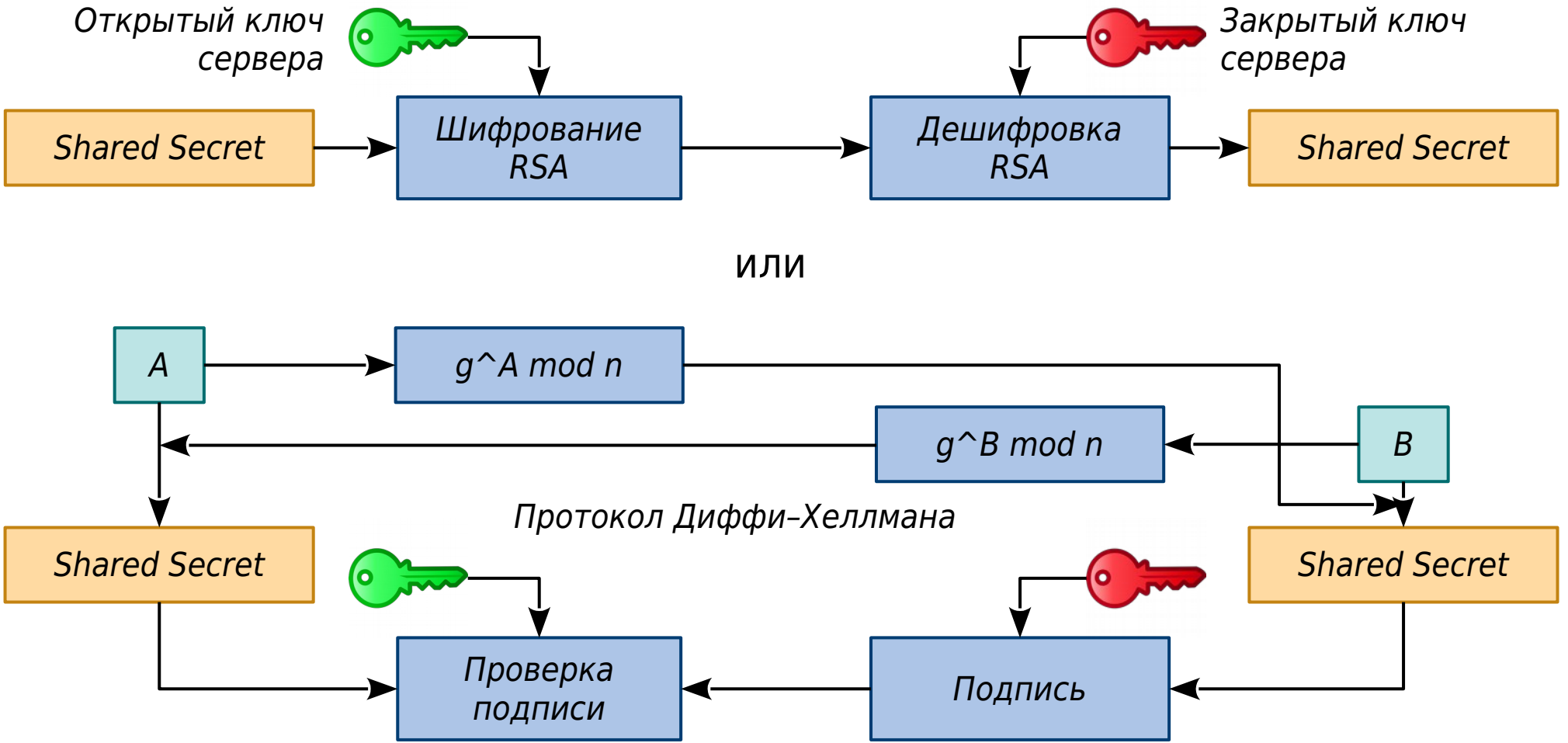
Client Hello — приветствие клиента:

- случайное число Client Nonce
- ~~*session ID при повторном подключении (если первый раз — это поле пустое)*~~
- session Ticket
- список всех поддерживаемых алгоритмов шифрования
- список поддерживаемых версий протокола
- (extension) имя сервера, для доступа к разным сайтам на одном IP

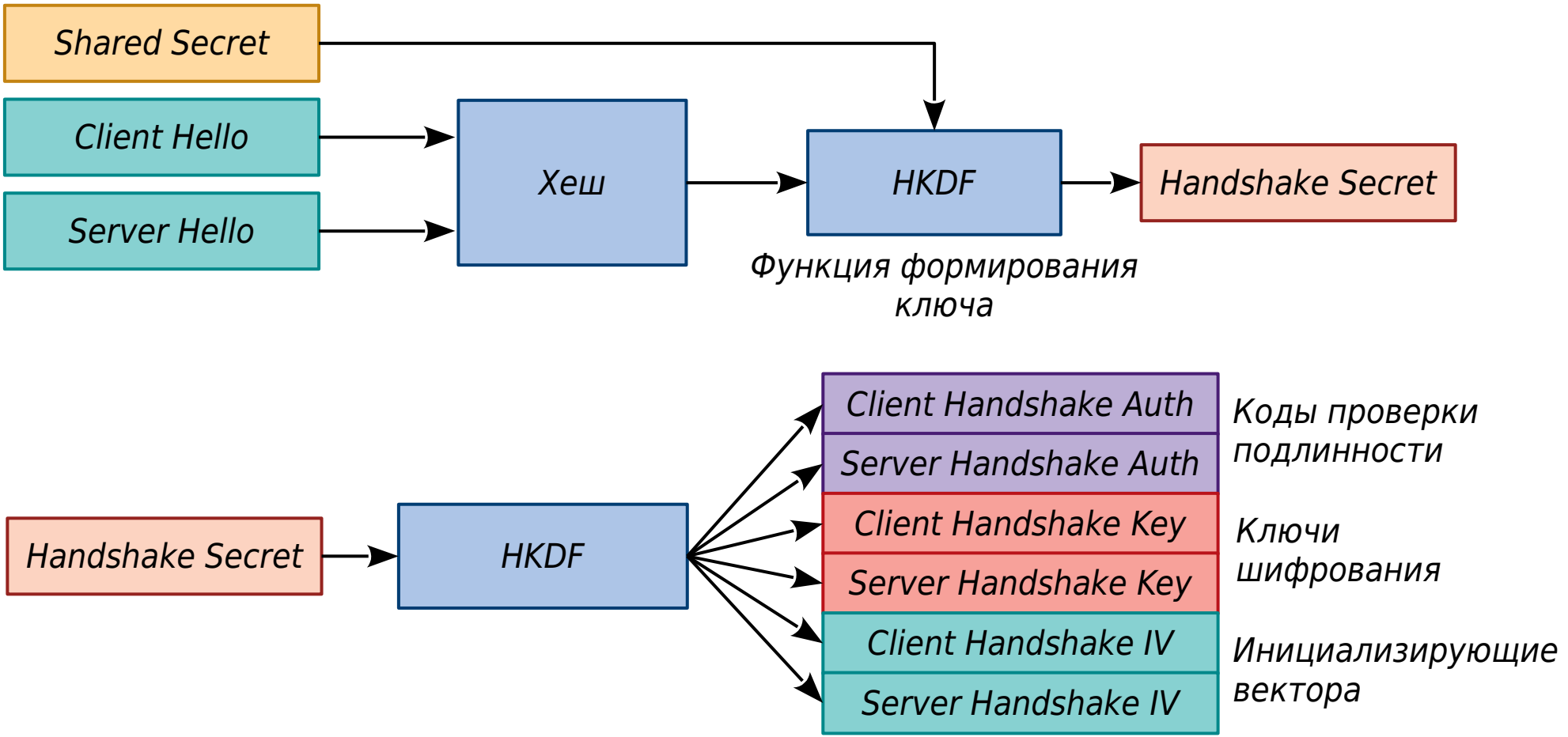
Server Hello — приветствие сервера:

- случайное число Server Nonce
- ~~*session ID для ускорения последующих подключений*~~
- выбранный набор алгоритмов
- выбранная версия протокола

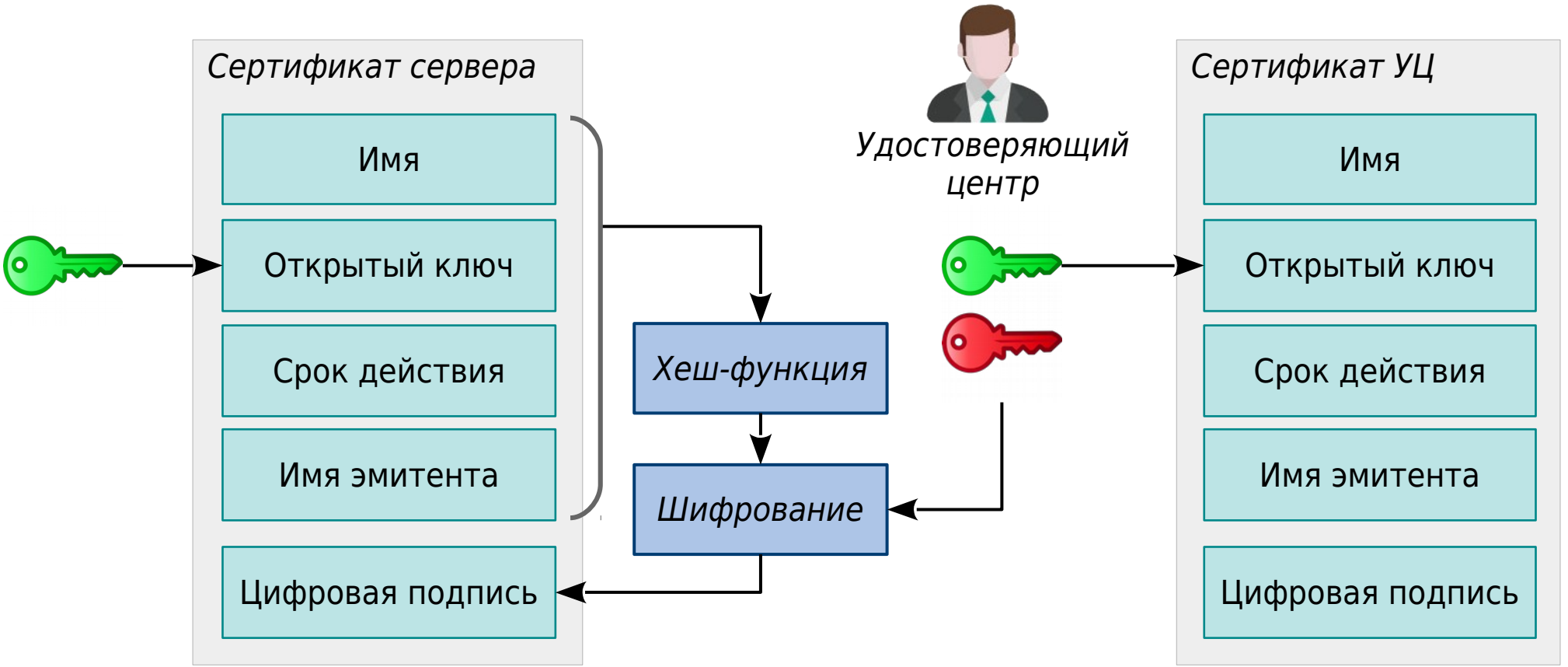
Генерация общего секрета



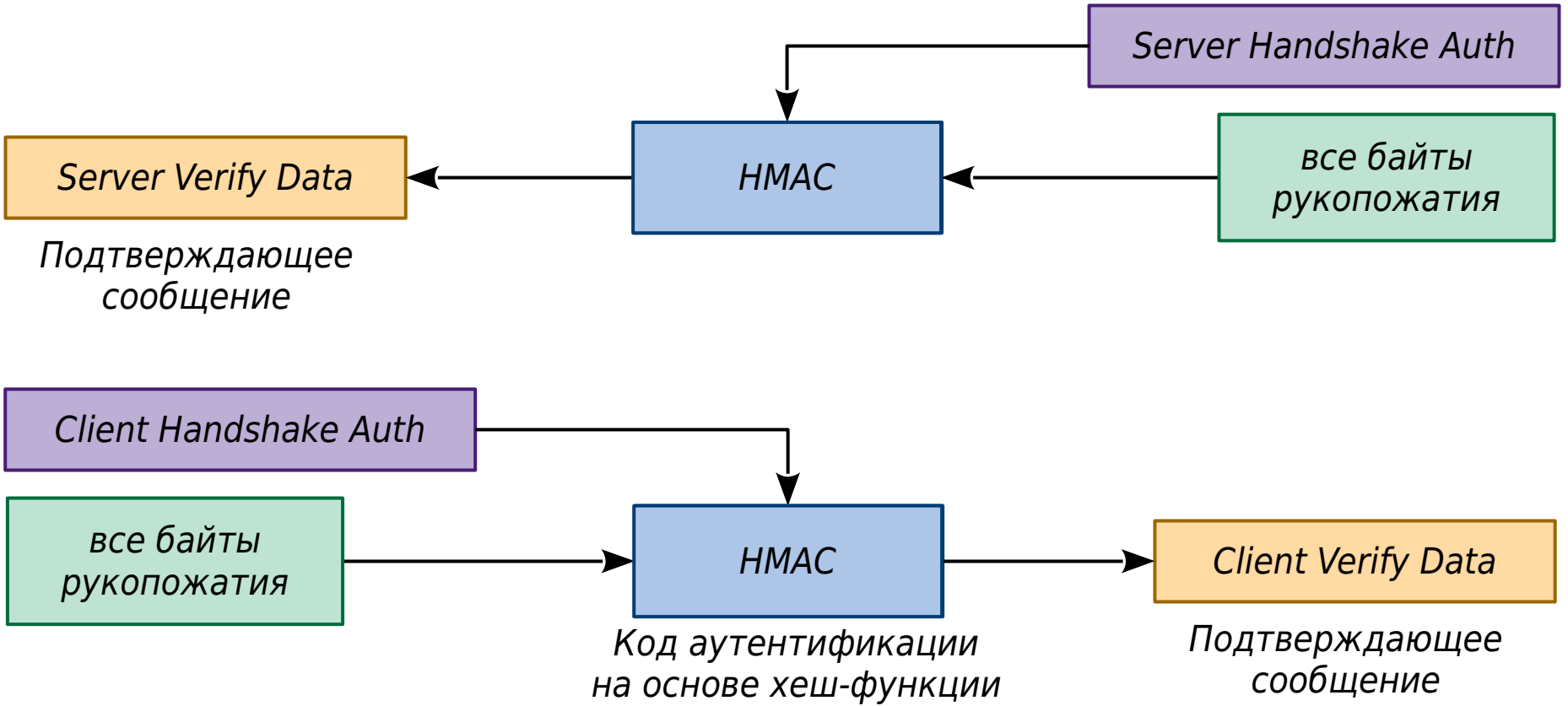
Вычисление сеансовых ключей рукопожатия



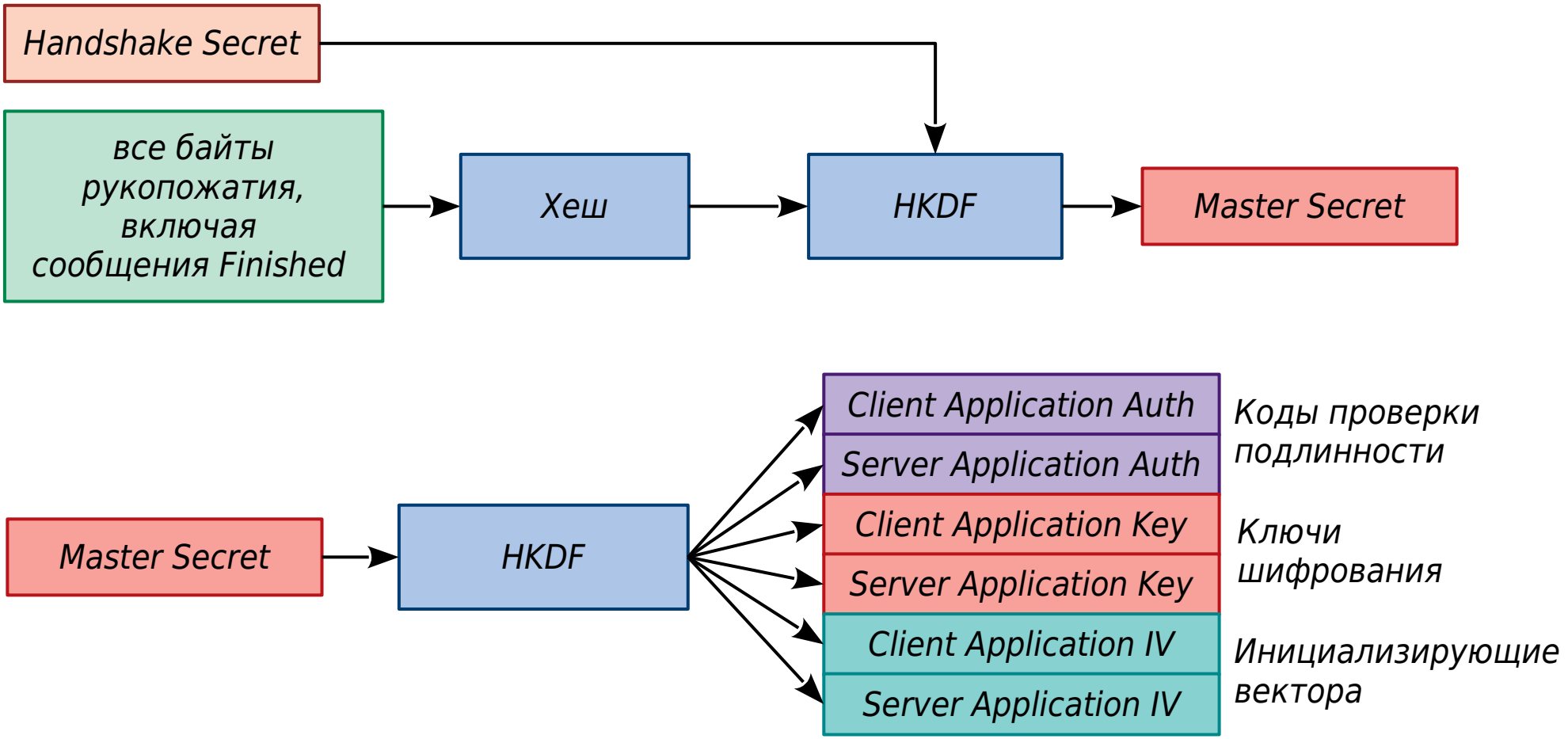
Сертификаты



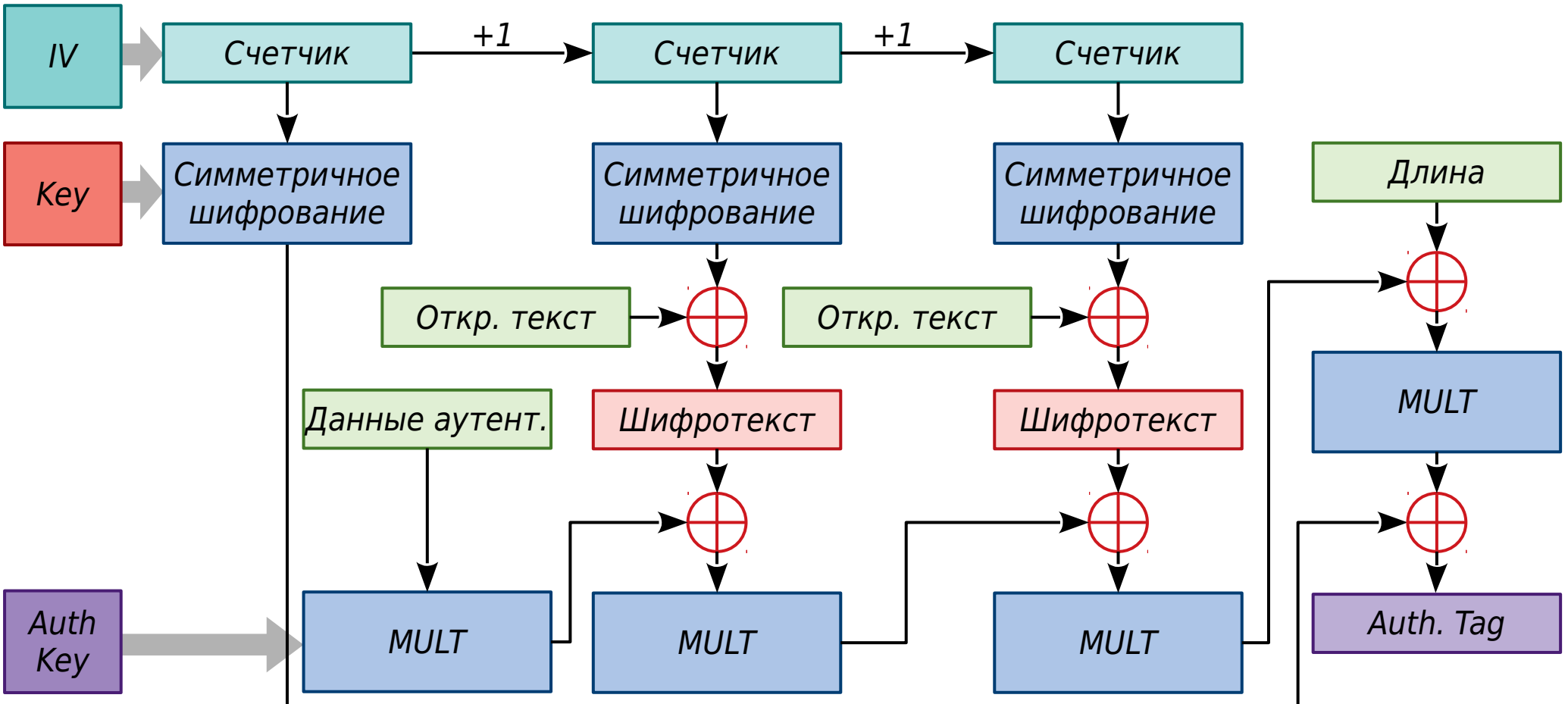
Завершение рукопожатия



Вычисление сеансовых ключей



Шифрование трафика прикладного уровня
(GCM — Galois/Counter Mode)



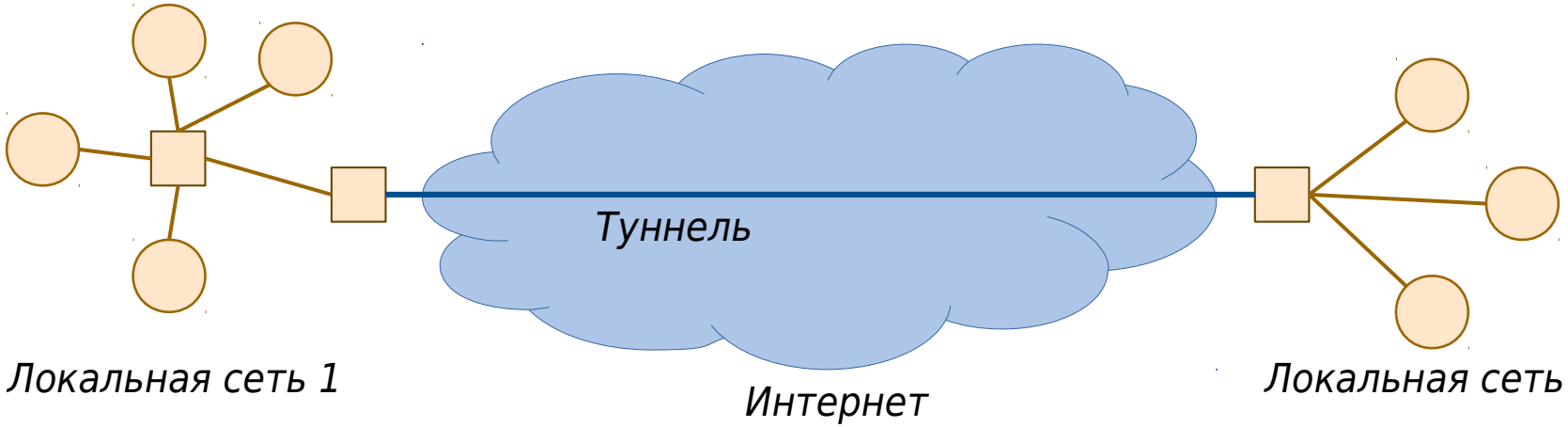
Что нового в TLS 1.3

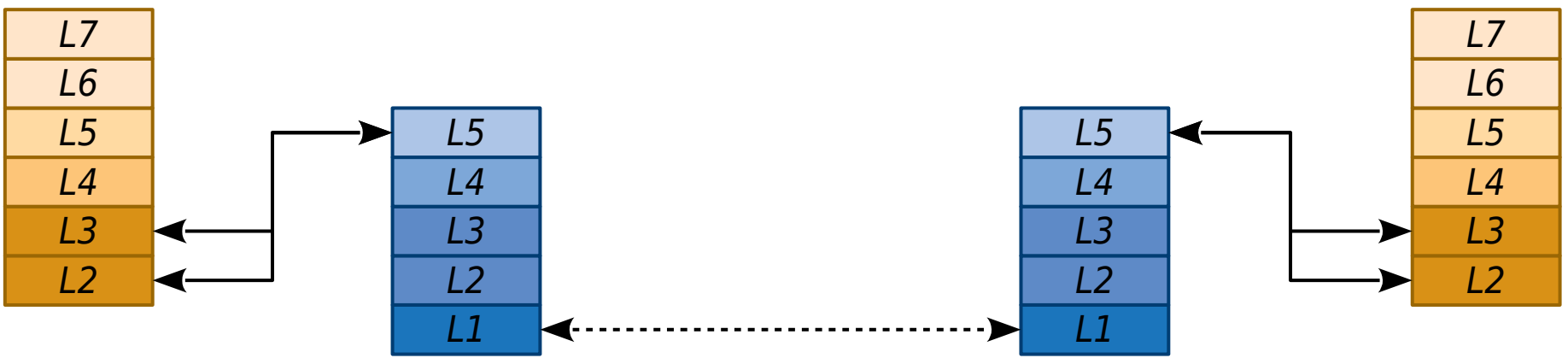
- Убрали поддержку слабых алгоритмов шифрования (3DES, ГОСТ 28147-89)
- Убрали поддержку слабых хеш–функций (MD5, SHA1)
- Убрали поддержку небезопасных режимов (в т.ч. режим “без шифрования”)
- Выкинули все слабые и редко используемые эллиптические кривые
- Вместо Session ID теперь одноразовые Session Tickets
- Добавили режим PSK (Pre–Shared Key)
- Рукопожатие за 1 запрос–ответ вместо 2 (и за 0 при использовании PSK)
- Отдельные ключи для шифрования рукопожатия
- Совершенная прямая секретность (Perfect Forward Secrecy)
- Убрали старые баги и добавили новые :)

Дополнительные материалы

- A Readable Specification of TLS 1.3
  https://www.davidwong.fr/tls13/
  Спецификация TLS, описанная понятным языком
- A Detailed Look at RFC 8446 (a.k.a. TLS 1.3)
  https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/
  Подробное описание истории протокола
  и различий между версиями
- The New Illustrated TLS Connection
  https://tls.ulfheim.net/
  https://tls13.ulfheim.net/
  Побайтный разбор протоколов TLS 1.2 и 1.3

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
  - @androidruberoid
- 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