v. 2.0

Криптография

Лекция 11. Беспроводные соединения.

Дмитрий Яхонтов

“Кочерга”, 2019

Стандарты Wi–Fi

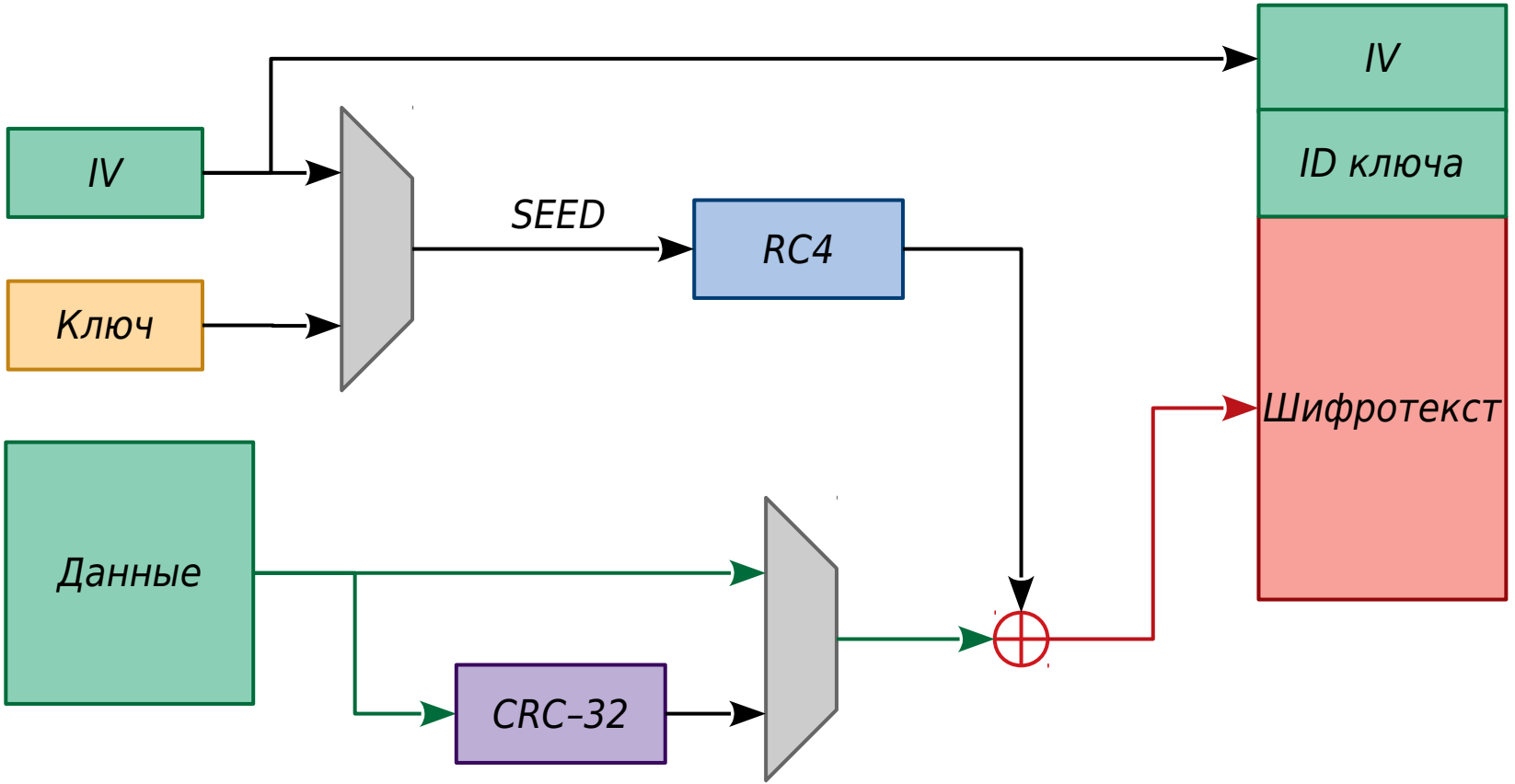
IEEE 802.11 — набор стандартов беспроводной связи

1997	*1999*	*2003*	*2009*	*2014*	*???*
2.4 ГГц *1–2 Мбит/с*	*2.4 ГГц* *5.5–11 Мбит/с*	*2.4 ГГц* *54 Мбит/с*	*2.4 / 5 ГГц* *150 Мбит/с* *MIMO*	*5 ГГц* *433 Мбит/с*	*60 ГГц* *7 Гбит/с*

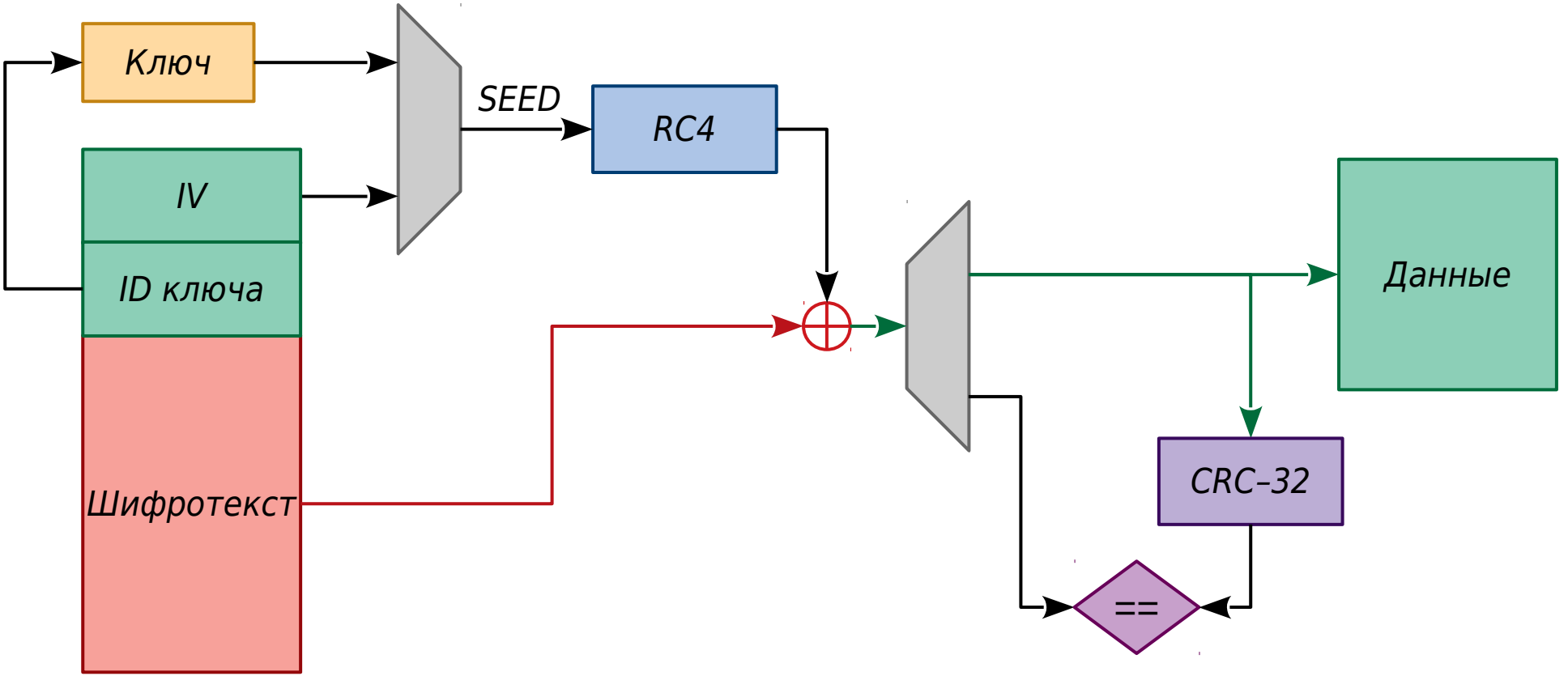
Протокол обеспечения безопасности WEP
(Wired Equivalent Privacy)

- В основе — потоковый шифр RC4
- Начальное значение (Seed) для генератора гаммы —
  ключ + случайный вектор инициализации (IV)
- IV передаётся в открытом виде
- Контроль целостности — контрольная сумма CRC–32
- **WEP–40**
  Seed 64 бита = Ключ 40 бит + IV 24 бита
- **WEP–104**
  Seed 128 бит = Ключ 104 бита + IV 24 бита

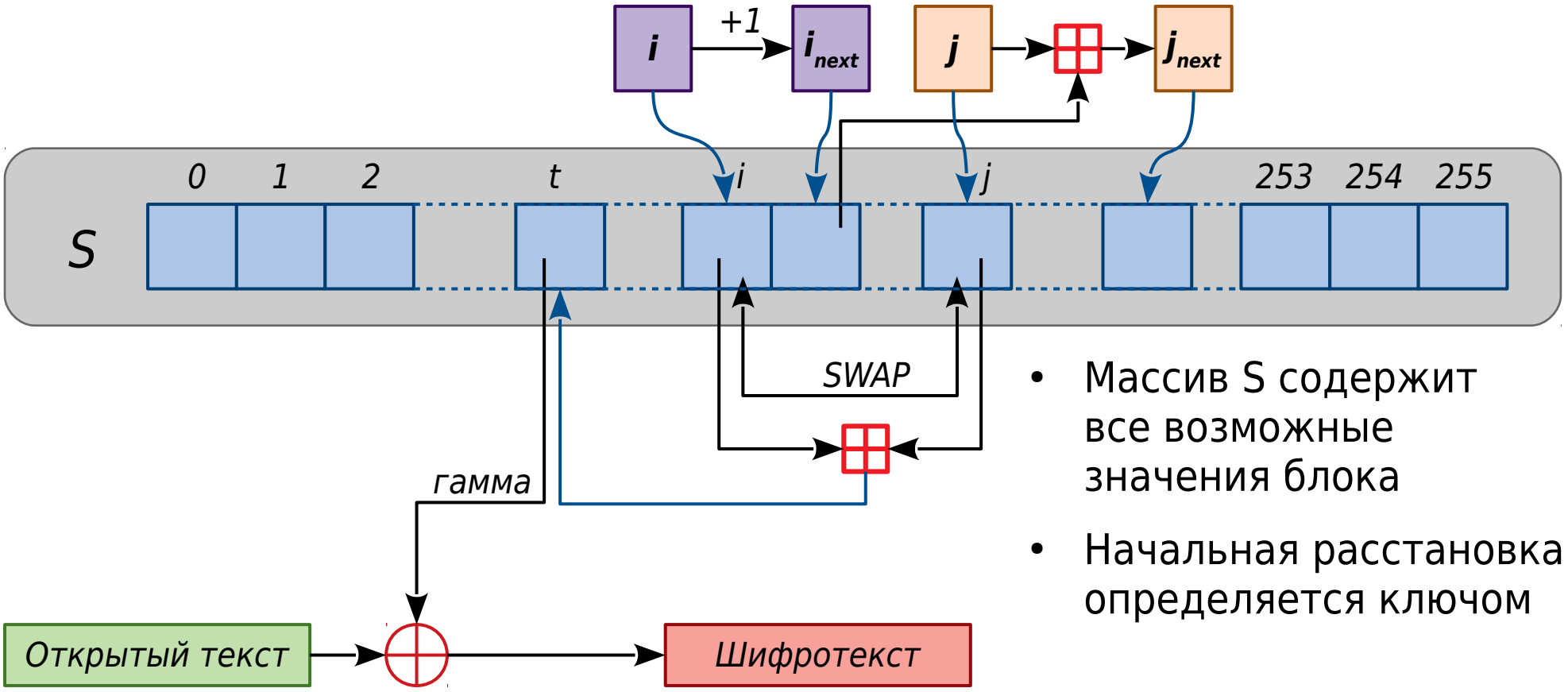
Шифрование в WEP



Дешифровка в WEP

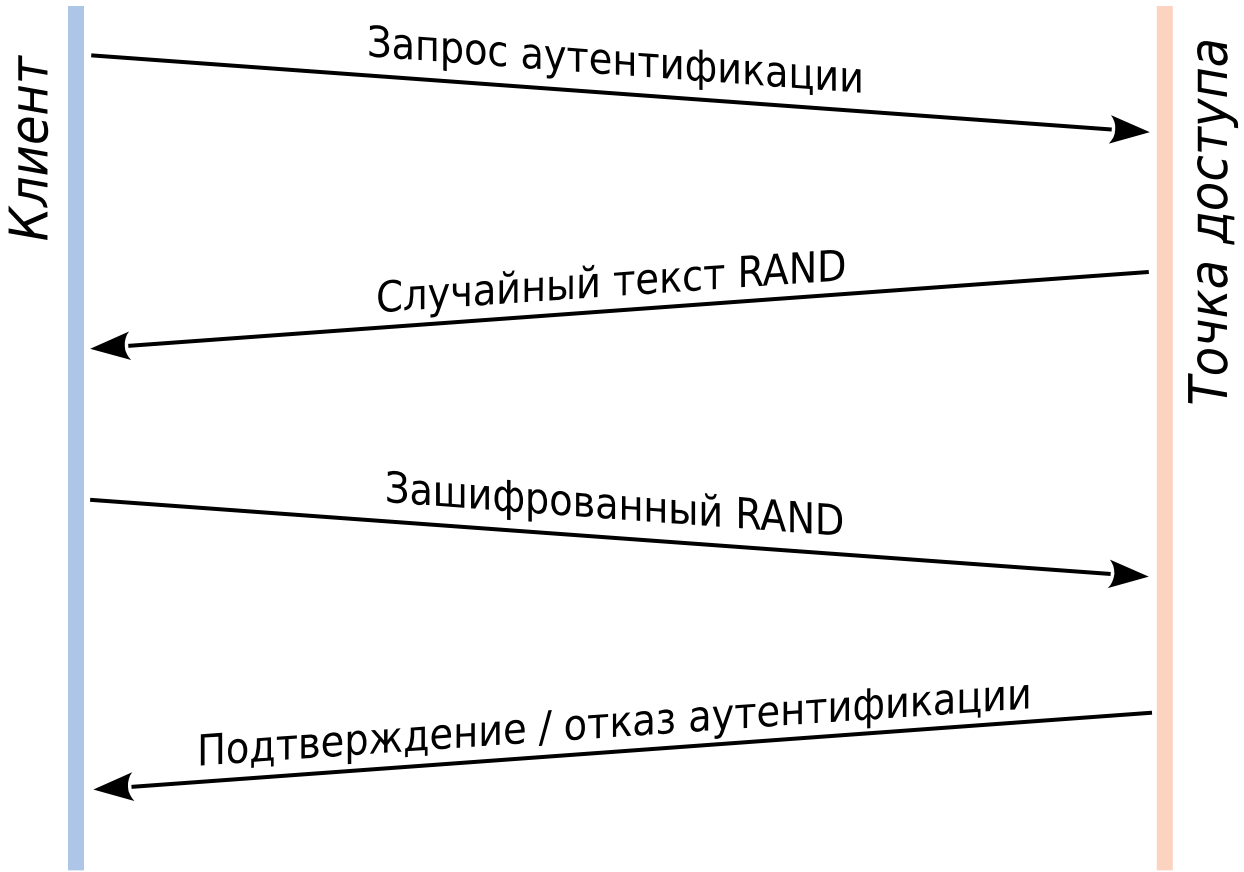


Шифр RC4



- Массив S содержит все возможные значения блока
- Начальная расстановка определяется ключом

Аутентификация в WEP



Уязвимости WEP

- Алгоритм шифрования RC4 недостаточно стойкий
- Малая длина ключа — 40 / 104 бита
- Ключ задаётся в виде строки ASCII–символов, использование только буквенно–цифровых символов сокращает пространство ключей
- Один ключ для всех участников сети
- Односторонняя аутентификация
- Некриптостойкая функция контроля целостности (CRC-32)
- Атака FMS *(Fluhrer–Mantin–Shamir),* корреляционная атака по слабым векторам инициализации, требует ~500 000 кадров
- Атака Кляйна, улучшенная версия FMS, требует ~100 000 кадров

Система стандартов WPA
(Wi–Fi Protected Access)

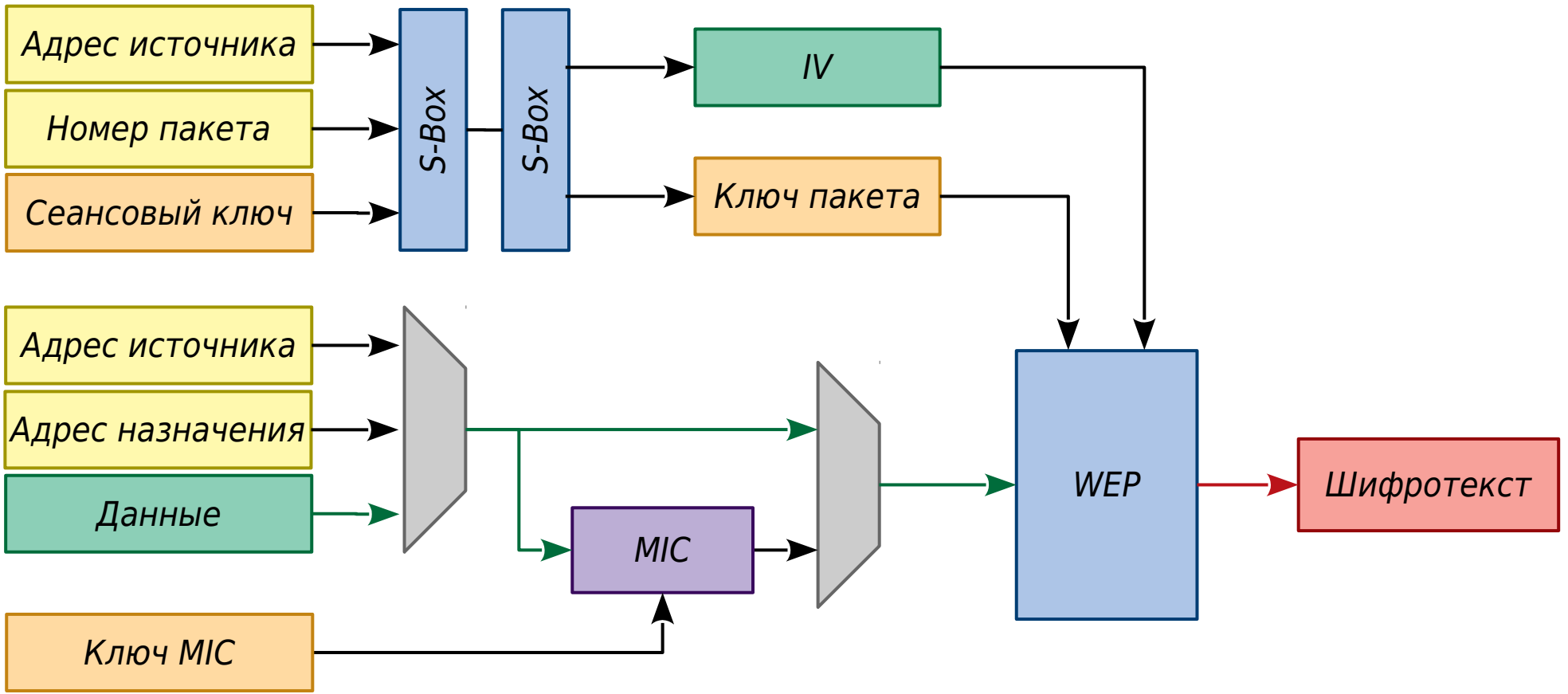
Протокол аутентификации EAP
(Extensible Authentication Protocol)

EAP используется для выбора метода аутентификации и передачи ключей.
В стандарте WPA описано более 100 возможных методов аутентификации.

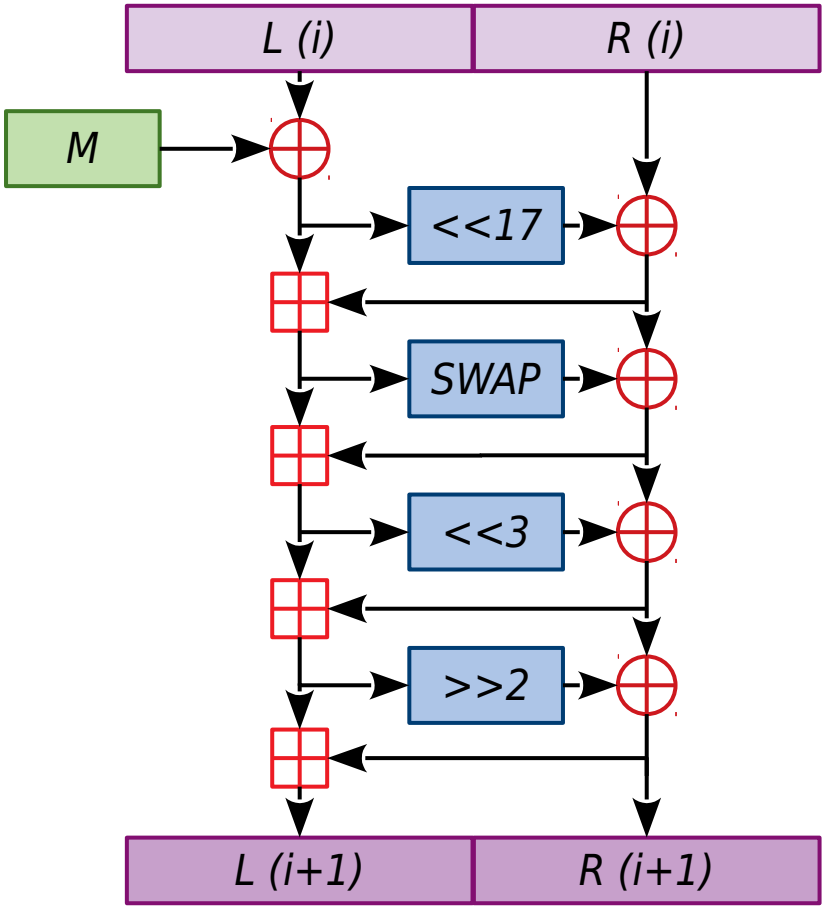
- LEAP *(Lightweight EAP)* — облегченный протокол “запрос—отклик”, односторонняя аутентификация по паролю
- EAP–TLS *(Transport Layer Security)* — по сертификатам
- EAP–POTP *(One–Time Password)* — по одноразовому паролю
- EAP–SIM *(Subscriber Identity Module)* — по SIM–карте
- EAP–GTC *(Generic Token Card)* — по аппаратному токену
- EAP–PSK *(Pre–Shared Key)* — по статическому секретному ключу

Используется сервер аутентификации, который может быть
тем же устройством, что и точка доступа, либо отдельным.

Управление ключами и шифрование TKIP
(Temporal Key Integrity Protocol)



Функция контроля целостности MIC
(Message Integrity Check)



- Хеш-функция с длиной вектора 64 бита
- Начальное состояние задаётся ключом
- В каждом раунде замешивается 32 бита
- Последние 2 раунда — финализация

Уязвимости WPA

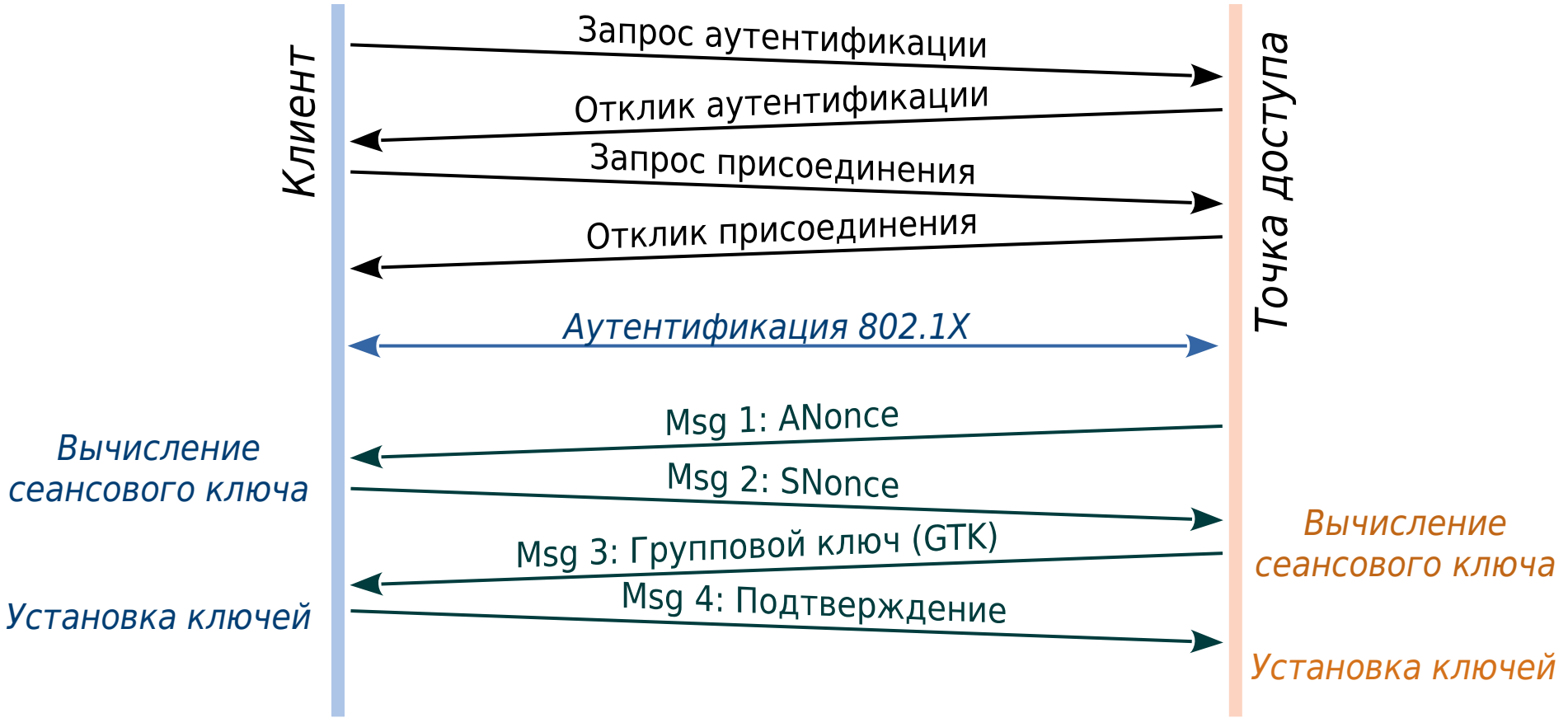
- Алгоритм шифрования — всё ещё RC4
- Доступ к мастер–ключу дает возможность расшифровать все данные этой сети в прошлом и будущем
- Функция контроля целостности MIC подвержена коллизиям
- Возможность инъекции пакетов (ошибка реализации QoS)
- Атака с предсказанием групповых ключей для некоторых моделей оборудования (слабый генератор псевдослучайных чисел)

WPA2 и его отличия от WPA

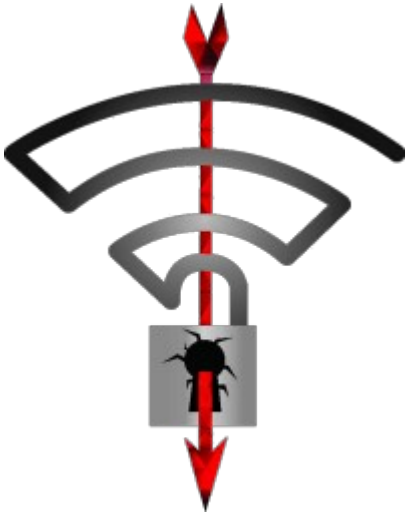
- Вместо RC4 используется алгоритм AES-128 в режиме CTR
- Вместо MIC используется MAC–функция на основе AES
- Нет необходимости генерировать новые ключи для каждого пакета

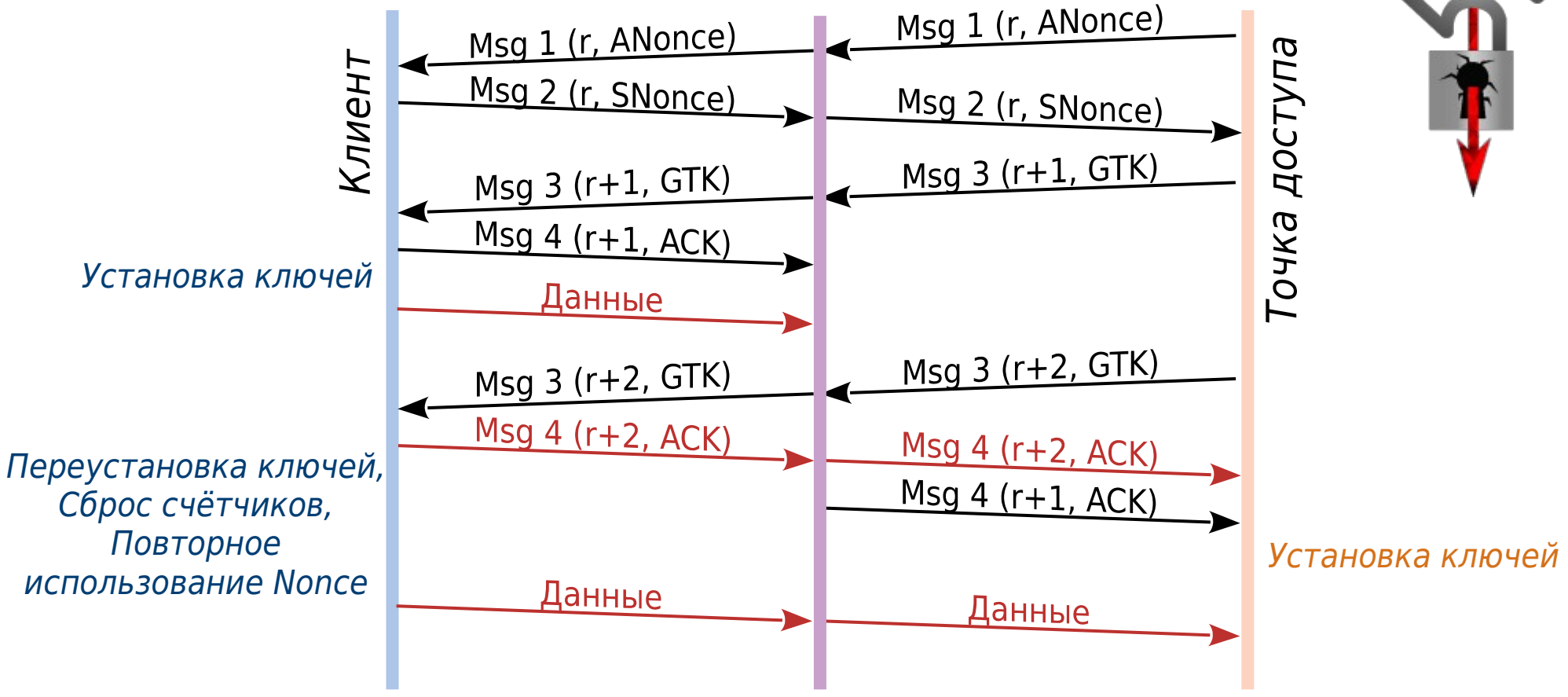
- WPA2 не совместим с WPA на уровне аппаратуры
- WPA2 требует большей вычислительной мощности и энергопотребления

Рукопожатие в WPA2



Атака с переустановкой ключа
(KRACK — Key Reinstallation Attack)





WPA3

- Использование 192–битного шифрования вместо 128–битного
- Новая процедура рукопожатия “Dragonfly”
- Одновременная аутентификация равных (Simultaneous Authentication of Equals) — протокол обмена ключами, основанный на ECDH с использованием для аутентификации предустановленных ключей (PSK) и MAC–адресов устройств
- Совершенная прямая секретность (Perfect Forward Secrecy)
- Индивидуальные ключи для клиентов в открытых сетях
- Протокол настройки IoT–устройств “Easy Connect”

Уязвимости WPA3

Семейство атак DragonBlood *(CVE-2019-9494)*

- Атака по побочному каналу на основе кеша.
  Алгоритм кодирования пароля содержит условные переходы,зависящие от пароля. Код, запущенный на устройстве, которое авторизуется в сети, может определить, какие из переходов выполнялись, определяя промахи и попадания кеша.

- Тайминг–атака
  Время выполнения рукопожатия зависит от пароля и MAC-адресов устройств. Возможна удалённая атака: точные измерения временых задержек позволяют сократить пространство возможных паролей.

Downgrade–атака

- WPA3 поддерживает режим совместимости с WPA2
  Атакующий может инициировать переход в режим совместимости, а затем воспользоваться уязвимостями WPA2.

Дополнительные материалы

- Key Reinstallation Attacks
  https://www.krackattacks.com
  KRACK — описание, демо, FAQ
- Key Reinstallation Attacks:
  Forcing Nonce Reuse in WPA2
  https://papers.mathyvanhoef.com/ccs2017.pdf
  Статья с подробным описанием атаки
- Dragonblood: A Security Analysis
  of WPA3’s SAE Handshake
  https://papers.mathyvanhoef.com/dragonblood.pdf
  Статья с подробным описанием Dragonblood

Wi-Fi Protected Setup (WPS) и его дыры

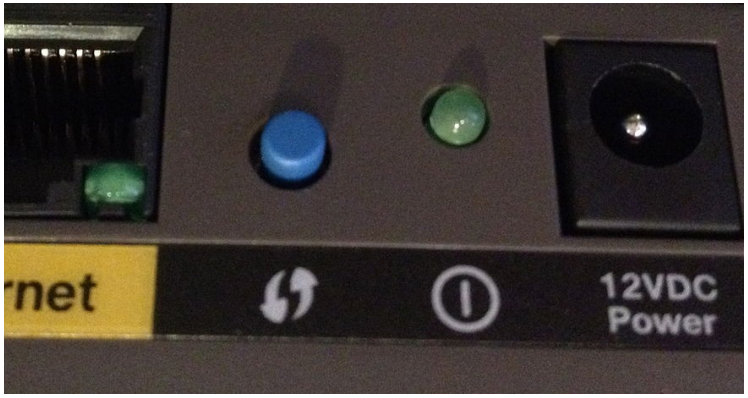
Автоматическая настройка Wi-Fi–соединения без необходимости задавать параметры руками

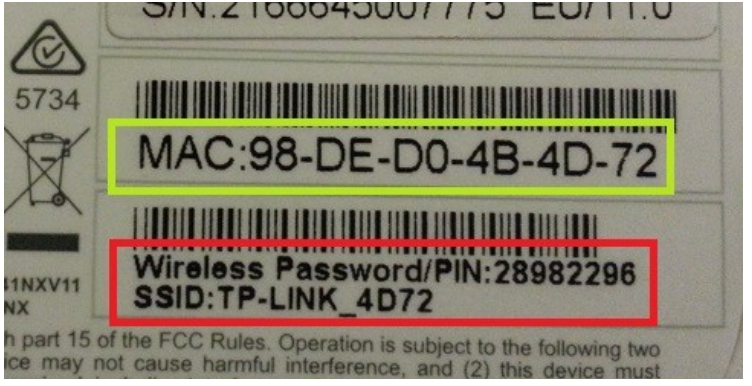
- по кнопке (нажать на обоих устройствах)
- по PIN–коду (8 цифр, ввести на клиенте)

Стойкость PIN–кода — 10^7
(восьмая цифра — контрольная сумма).

Точка доступа проверяет PIN–код блоками по 4 цифры, то есть код можно подобрать всего за 11 000 попыток.

Слабые алгоритмы генерации случайных чисел для функции проверки PIN позволяют провести оффлайн–атаку (WPS Pixie Dust)





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