**Федеральное агентство связи**

Сибирский Государственный Университет Телекоммуникаций и Информатики

**Межрегиональный центр переподготовки специалистов**

**ЭКЗАМЕНАЦИОННАЯ РАБОТА**

# По дисциплине: Линии радиосвязи и методы их защиты

**Выполнил**: Таращенко А.В.

**Группа**: ЗБТП-81

**Билет: 4**

**Проверила**: Шевнина И.Е.

Новосибирск, 2018 г

Билет № 4

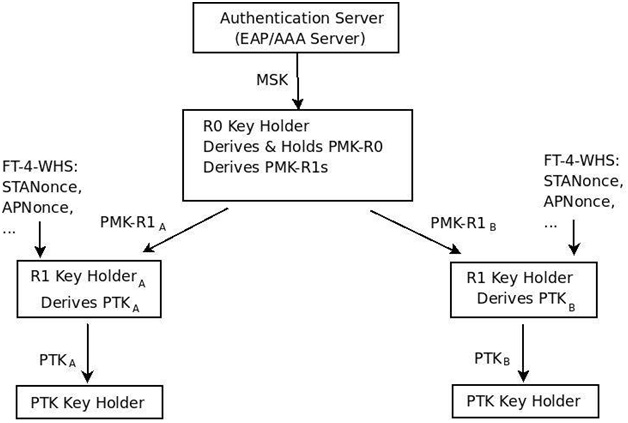
1. **Алгоритм WEP: схема шифрования и дешифрования.**
2. **Иерархия ключей в стандарте 802.11i.**
3. Алгоритм «четырех рукопожатий» в стандарте 802.11i.

### 3. Основные принципы работы стандарта WiFi 802.11r.

802.11r формирует трехуровневую референсную архитектуру,  которая делит [сеть доступа стандарта WiFi](http://wi-life.ru/texnologii/wi-fi/wi-fi-standarty) на зоны мобильности (mobility zones). Зона мобильности определяется как группа Точек Доступа WiFi , которые соединяются и управляются центральным устройством управления (чаще всего это контроллер сети WiFi). Обычно  соседние точки доступа, покрывающие определенную географическую зону, группируются в одну зону мобильности.

Когда мобильное устройство, отвечающее стандарту WiFi 802.11r,  пересекает границу зоны мобильности оно в первый раз выполняет аутентификацию, используя протокол EAP. Результирующий MSK используется мобильным устройством и контроллером для получения ключа, называемого PMK-R0.  PMK-R0 далее применяется для вычисления ключей PMK для каждой точки доступа. Такие ключи называются PMK-R1. В заключении контроллер отправляет ключи PMK-R1 на соответствующие точки доступа. Контроллер зоны мобильности, который хранит ключ PMK-R0, называется Хранителем ключа R0 (R0 Key Holder/R0KH). В то же время точки доступа, на которые отправлены ключи PMK-R1, называются Хранители ключа R1 (R1 Key Holder/R1KH).

**Иерархия ключей, которую ввел стандарт 802.11r, приведена на рисунке ниже:**



Точки Доступа WiFi, которые поддерживают 802.11r, передают информацию о поддержке 11r во фреймах Beacon и Probe response, путем включения специального элемента MDIE (Mobility Domain Information Element), описанном в стандарте 11r. В течении начальной ассоциации в зоне мобильности мобильное устройство, поддерживающее стандарт 802.11r,  и точка доступа, выполняющая обмен в рамках аутентификации открытой системы (Open System Authentication), следуют процедуре Fast Transition Reassociation Exchange, которая отличается от 802.11 Reassociation Exchange включением MDIE в Reassociation Request для обозначения желания мобильного устройства использовать 802.11r. Более того, элемент FTIE (Fast Transition Information Element) включается во фрейм-ответ Reassociation Response, отправляемый точкой доступа. Элемент FTIE переносит идентификатор R0KH-ID, а также идентификатор текущей точки доступа: R1KH-ID. После успешной 802.1Х аутентификации точка доступа и мобильное устройство запускают четырехсторонний процесс взаимодействия для обеспечения роуминга (FT four-way handshake), который отличается от взаимодействия в 802.11i в части переноса дополнительных элементов MDIE и FTIE, необходимых для извлечения PMK-R1 и PTK.

Обмены данными для выполнения последовательных хендоверов внутри мобильного домена WiFi несколько отличаются. 802.11r нацелен  на уменьшение задержек путем создания механизма обмена и управления ключами поверх процесса реассоциации 802.11. Процессы аутентификации (Authentication Exchange) и ассоциации (Association exchange) используются для выполнения протокола быстрого обмена (FT Protocol), который обеспечивает мобильным устройствам и точкам доступа Wi-Fi согласовать PMK-R1 и извлечь ключи PTK. FT Protocol замещает четырехсторонный процесс (FT four-way handshake) и уменьшает общее количество сообщений для выполнения полной реассоциации до четырех!

Когда мобильное устройство, поддерживающее [технологию WiFi](http://www.wi-life.ru/texnologii/wi-fi/texnologiya-ieee80211), принимает решение о пре-ассоциации с Точкой Доступа WiFi поверх среды обмена (distribution system) это мобильное устройство и целевая точка доступа выполняют специальный процесс обмена данными: Over the DS FT Protocol. Текущая точка доступа WiFi, с которой ассциировано мобильное устройство, перенаправляет фреймы между мобильным устройством и целевой точкой доступа. Протокол FT поверх DS использует новый процесс обмена FT Request/Response для замены процессов аутентификации и ассоциации на согласование кодов (ciphersuites) и извлечение ключей PTK на мобильном устройстве и точке доступа. 802.11r уменьшает количество сообщений для установления свежих PTK до четырех сообщений, вовлекая в процесс только мобильное устройство и точку доступа (и DS в случае пре-ассоциации). FT Protocol позволяет выполнять безопасный обмен данными между мобильным устройством и точкой доступа.  
  
Подробнее о [безопасности в сетях WiFi](http://www.wi-life.ru/texnologii/wi-fi/wi-fi-strategiya-bezopasnosti).

Можно найти исследования, которые показывают, что быстрый обмен 802.11r через радиоканал требует 40-50 мс (без учета времени сканирования, т.к. это очень вариативный показатель). Это значительно более быстрая технология, чем использование традиционной схемы хендоверов 802.11i, требующей EAP-аутентификации на каждом хендовере.  
  
Важно помнить, что поддержка 802.11r зависит не только от Wi-Fi инфраструктуры, но и от пользовательских мобильных устройств.