**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

**ФАКУЛЬТЕТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**Управление мобильными устройствами**

Реферат на тему:

«Криптография в LTE технологиях»

Работу выполнил

студент группы N3347

**Изображение выглядит как игра

Автоматически созданное описание**Конищев В.А.

Проверил: Таранов С.В.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Санкт-Петербург

2020 г.

Оглавление

[Криптография в сетях LTE 3](#_Toc45126081)

[Безопасность в сетях LTE 3](#_Toc45126082)

[Генерация векторов аутентификации 4](#_Toc45126083)

[Защита сообщений протокола RRC 7](#_Toc45126084)

[Список использованной литературы: 9](#_Toc45126085)

# Криптография в сетях LTE

## Безопасность в сетях LTE

* Защита абонентов.
* Защита передаваемых сообщений.
* Шифрование сообщений.
* Аутентификация и абонента, и сети.

Защита абонента заключается в том, что в процессе обслуживания его скрывают временными идентификаторами.

Для закрытия данных в сетях LTE используется потоковое шифрование методом наложения на открытую информацию псевдослучайной последовательности (ПСП) с помощью оператора XOR (исключающее или). В этих сетях для обеспечения безопасности внутри сети применяется принцип туннелирования соединений. Шифрации можно подвергать пакеты S1 и X2 при помощи IPsec ESP, а также подвергаются шифрации сигнальные сообщения этих интерфейсов.

В момент подключения или активизации абонентского оборудования (UE) в сети, сеть запускает процедуру аутентификации и соглашения о ключах AKA (Authentication and Key Agreement). Целью этой процедуры является взаимная аутентификация абонента и сети и выработка промежуточного ключа KASME. Работа механизма AKA занимает доли секунды, которые необходимы для выработки ключа в приложении USIM и для установления соединения с Центром регистрации (HSS). Вследствие этого, для достижения скорости передачи данных сетей LTE необходимо добавить функцию обновления ключевой информации без инициализации механизма AKA. Для решения этой проблемы в сетях LTE предлагается использовать иерархическую ключевую инфраструктуру. Здесь также, как и в сетях 3G, приложение USIM и Центр аутентификации (AuC) осуществляет предварительное распределение ключей. Когда механизм AKA инициализируется для осуществления двусторонней аутентификации пользователя и сети, генерируются ключ шифрования CK и ключ общей защиты, которые затем передаются из ПО USIM в Мобильное оборудование (ME) и из Центра аутентификации в Центр регистрации (HSS). ME и HSS, используя ключевую пару (CK;IK) и ID используемой сети, вырабатывает ключ KASME. Установив зависимость ключа от ID сети, Центр регистрации гарантирует возможность использования ключа только в рамках этой сети. Далее KASME передается из Центра регистрации в устройство мобильного управления (MME) текущей сети, где он используется в качестве мастер-ключа. На основании KASME вырабатывается ключ KNAS-ENC, который необходим для шифрования данных протокола NAS между мобильным устройством (UE) и MME, и KNAS, необходимый для защиты целостности. Когда UE подключается к сети, MME генерирует ключ KeNB и передает его базовым станциям. В свою очередь, из ключа KeNB вырабатывается ключ KUP-enc, используемый для шифрования пользовательских данных протокола U-Plane, ключ KRRC-enc для протокола RRC (Radio Resource Control - протокол взаимодействия между Мобильными устройствами и базовыми станциями) и ключ KRRC-int, предназначенный для защиты целостности.

**Алгоритм аутентификации и генерации ключа представлен на рис. 1:**

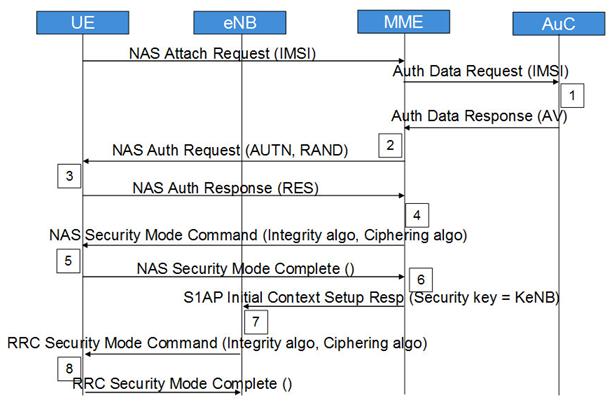


Рис. 1 Диаграмма аутентификации и генерации ключа

## Генерация векторов аутентификации

Для генерации векторов аутентификации используется криптографический алгоритм с помощью однонаправленных функций (f1, f2, f3, f4, f5) когда прямой результат получается путем простых вычислений, а обратный результат не может быть получен обратным путем, то есть не существует эффективного алгоритма получения обратного результата. Для этого алгоритма используется случайное 128 битное случайное число RAND, мастер-ключ K абонента, также 128 бит и порядковый номер процедуры SQN (Sequence Number). Счетчик SQN меняет свое значение при каждой генерации вектора аутентификации. Похожий счетчик SQN работает и в USIM. Такой метод позволяет генерировать каждый раз новый вектор аутентификации, не повторяя предыдущий уже использованный вектор аутентификации.

Помимо этих трех исходных величин: SQN, RAND и К в алгоритме f1 участвует поле управления аутентификацией Authentication Management Field (AMF), а в алгоритмах f2 – f5 исходные параметры – RAND и К, что и продемонстрировано на рис. 3, 4. На выходах соответствующих функций получают Message Authentication Code (MAC) - 64 бита; XRES – eXpected Response, результат работы алгоритма аутентификации <32 – 128 бит>; ключ шифрации СК, генерируемый с использованием входящих (K,RAND)->f3->CK; ключ целостности IK, сгенерированный с использованием входящего (K,RAND)->f4->IK; и промежуточный ключ Anonymity Key (AK), генерируемый с помощью (K,RAND)->f5->AK - 64 бита.

При обслуживании абонента сетью LTE ключи CK и IK в открытом виде в ядро сети не передают. В этом случае HSS генерирует KASME с помощью алгоритма KDF (Key Derivation Function), для которого исходными параметрами являются CK и IK, а также идентификатор обслуживающей сети и SQNÅAK. Вектор аутентификации содержит RAND, XRES, AUTN и KASME, на основе которого происходит генерация ключей шифрации и целостности, используемых в соответствующих алгоритмах.

Когда мобильная станция получает из ядра сети три параметра (RAND, AUTN и KSIASME, где KSI – Key Set Identifier, индикатор установленного ключа, однозначно связанный с KASME в мобильной станции).

После чего используя RAND и AUTN, USIM на основе алгоритмов безопасности, тождественных хранящимся в HSS, производит вычисление XMAC, RES, CK и IK.

Затем в ответе RES UE передает в ММЕ вычисленное RES, которое должно совпасть с XRES, полученным из HSS. Так сеть аутентифицирует абонента. Вычислив XMAC, UE сравнивает его с МАС, полученным ею в AUTN. При успешной аутентификации абонентом сети (МАС = ХМАС) UE сообщает об этом в ответе RES. Если аутентификация сети не удалась (МАС ≠ ХМАС), то UE направляет в ММЕ ответ CAUSE, где указывает причину неудачи аутентификации.

При успешном завершении предыдущего этапа ММЕ, eNB и UE производят генерацию ключей, используемых для шифрации и проверки целостности получаемых сообщений. В LTE имеется иерархия ключей, которая приведена на рис. 4

Векторы аутентификации (рис. 2, 3):

* Ключи IK и CK генерируются и в центре аутентификации, и в USIM;
* Ключ AK генерируется только в центре аутентификации;
* Ответ XRES генерируется только в центре аутентификации, а RES генерируется в USIM;
* Код MAC генерируется только в центре аутентификации, а соответствующий ему параметр XMAC генерируется в USIM;
* Маркер AUTH генерируется только в центре аутентификации.

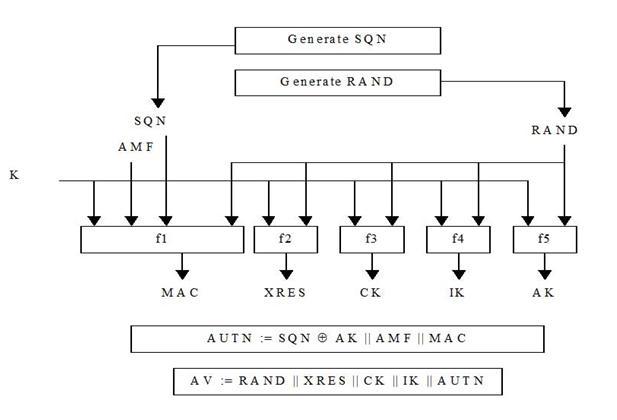


Рис. 2. Создание векторов на передающей стороне

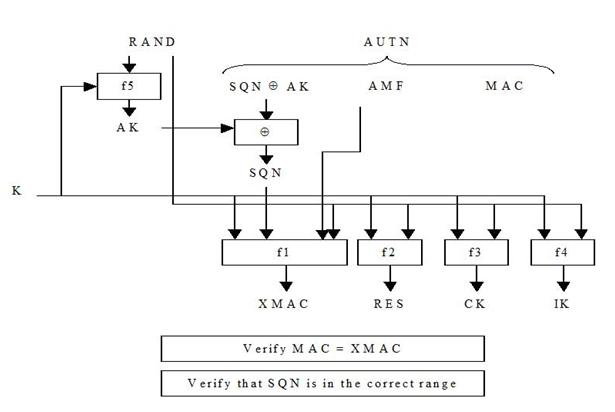


Рис. 3. Преобразование векторов на приемной стороне (в USIM)

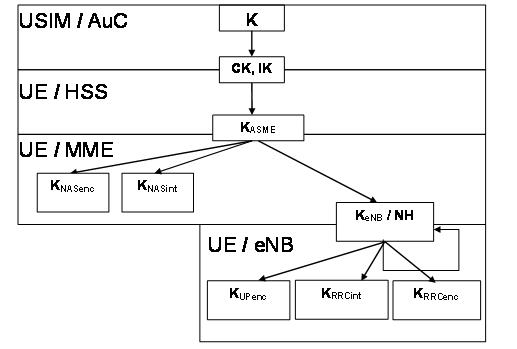


Рис. 4. Иерархия ключей в LTE

## Защита сообщений протокола RRC

Сигнальные сообщения протокола RRC (AS) также шифруют и обеспечивают их целостность. Пакеты трафика только шифруют. Эти операции производят в обслуживающей eNB и UE. Схема получения ключей шифрации и целостности для AS и UP трафика отличается от предыдущего случая тем, что исходным параметром здесь служит вторичный промежуточный ключ KeNB (256 бит). Этот ключ генерируют, также используя KDF, где входными параметрами являются: KASME, счетчик сигнальных сообщений NAS вверх, прежнее значение KeNB, идентификатор соты и номер частотного канала в направлении вверх. Следовательно, при каждой периодической локализации UE происходит изменение KeNB.  
Также KeNB меняется и при хэндовере; при этом в алгоритме генерации нового KeNB можно использовать дополнительный параметр NH (Next Hop), фактически счетчик числа базовых станций, по цепочке обслуживающих абонента. Все реализуемые процедуры безопасности в сети LTE продемонстрированы на рис. 5.

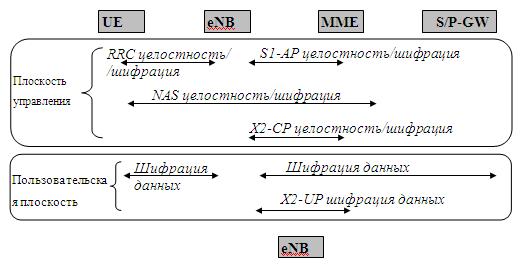


Рис. 5. Реализуемые процедуры безопасности в сети LTE

Алгоритм шифрации и дешифрации сообщений представлен на рис. 6.

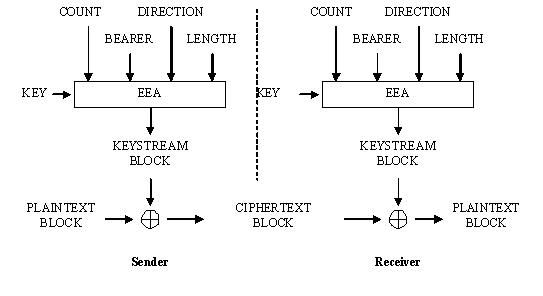


Рис. 6. Алгоритм шифрации в LTE

Исходными параметрами в этом алгоритме являются шифрующий ключ KEY (128 бит), счетчик пакетов (блоков) COUNT (32 бита), идентификатор сквозного канала BEARER (5 бит), указатель направления передачи DIRECTION (1 бит) и длина шифрующего ключа LENGTH. В соответствии с выбранным алгоритмом шифрации ЕЕА (EPS Encryption Algorithm) вырабатывается шифрующее число KEYSTREAM BLOCK, которое при передаче складывают по модулю два с шифруемым исходным текстом блока PLAINTEXT BLOCK. При дешифрации на приемном конце повторно совершают эту же операцию.  
Процедура защиты целостности сообщения состоит в генерации “хвоста“ МАС (Message Authentication Code) (32 бита), присоединяемого к передаваемому пакету. Алгоритм генерации МАС и проверки целостности полученного пакета путем сравнения ХМАС с МАС (они должны совпасть) отображен на рис. 7.

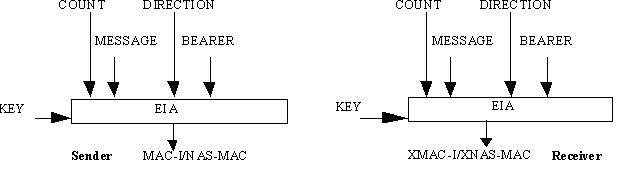


Рис. 7. Алгоритм проверки целостности в LTE

В алгоритме ЕIА (EPS Integrity Algorithm) использован ключ целостности KEY (128 бит), счетчик сообщений COUNT (32 бита), идентификатор сквозного канала BEARER (5 бит), указатель направления передачи DIRECTION (1 бит) и само сообщение MESSAGE.

## Список использованной литературы:

* http://www.osp.ru/nets/2012/06/13032673/
* [HEAVY READING, MAY 2012, WHITE PAPER AUTHENTICATION AS A SERVICE FOR LTE BASE STATIONS](http://www.symantec.com/en/ca/content/en/us/enterprise/white_papers/heavy-reading-authentication-as-a-service_WP.en-us.pdf)
* LTE Security Architecture.
* А.Н. Степутин, А.Д. Николаев. Мобильная связь на пути к 6G. В 2 томах. – 2-е изд. - Москва-Вологда: Инфра-Инженерия, 2018. – 804с. : ил.