Защита информации в мобильных сетях третьего поколения (стандарт UMTS)

Реферат по курсу «Защита информации»,
выполнил Борздый Ю.В., группа 116, ФРТК МФТИ

Предпосылки

К середине 90х годов GSM сети получили широкое распространение во всём мире и сделали мобильную телефонную связь неотъемлемой частью жизни людей. Было очевидно, что с развитием технологий требования к мобильным сетям будут усложняться и ужесточаться, и поэтому уже в 1998 году стартовал 3GPP — международный проект по разработке стандарта мобильной связи третьего поколения.

С самого начала было очевидно, что механизмы защиты передаваемой информации следует переработать в новом стандарте, поскольку соответствующие системы GSM стали к концу 90х уязвимы для атак злоумышленников и с трудом удовлетворяли некоторым законодательным нормам. Во-первых, для зашифровки передаваемых данных использовался простой поточный шифр, который к этому времени стал доступен для взлома как минимум спецслужбами за разумное время. Во-вторых, с другой стороны, авторизованные государством спецслужбы должны легко иметь доступ к передаваемой информации, но в GSM такие механизмы не были учтены при создании, и их пришлось достраивать уже после утверждения стандарта. В-третьих, аутентифицировался только пользователь сетью, а не наоборот. Это оставляло злоумышленнику возможность повлиять на выработку сессионного ключа и тем самым получить доступ к информации. Однако, основные принципы политики безопасности GSM (шифрование радиосигнала, использование модуля идентификации пользователя, определённая свобода выбора механизмов оператором и т.д.) оправдали себя и легли в основу механизмов защиты информации UMTS — стандарта третьего поколения.

Взаимная аутентификация в UMTS

Перед началом обмена информацией каждая сторона должна убедиться в том, что общается именно с тем, кто ей нужен, а не со злоумышленником, имитирующем собеседника с целью перехвата этой информации. В случае канала радиосвязи мобильных сетей такими сторонами являются Абонент (User Equipment конечного пользователя) и Сеть (передаточный узел провайдера мобильной связи). Основные понятия, которыми оперируют в этом вопросе это:

- домашнее окружение и аутентификационный центр;
- идентификационные модули пользователя (USIM или UICC);
- регистры местоположения пользователя (VLR).

В дополнение к принципам, использованным в GSM, UMTS также реализует:

- аутентификацию домашнего окружения по отношению к пользователю;
- соглашение о ключе целостности (IK) между пользователем и обслуживающей сетью;
- взаимное подтверждение “свежести” ключей шифрования и аутентификации между пользователем и обслуживающей сетью.

Главным заметным новшеством является алгоритм аутентификации и согласования ключей, приведённый вкратце ниже.

Аутентификация и выработка ключа

Каждое понятие определено стандартом и выполняет строго определённые функции. Аутентификационный центр (AuC) и USIM хранят по копии основного ключа абонента, на основе которого строится общение абонента с сетью. По запросу обслуживающей сети AuC производит таблицу из n (обычно n=5) пятикомпонентных аутентификационных векторов. Компонентами каждого вектора являются: случайное число RAND, ожидаемый ответ XRES, ключ шифрования CK, ключ целостности IK и маркер аутентификации AUTN, из которых последние 4 компоненты получаются из RAND, K и порядкового номера вектора SQN.

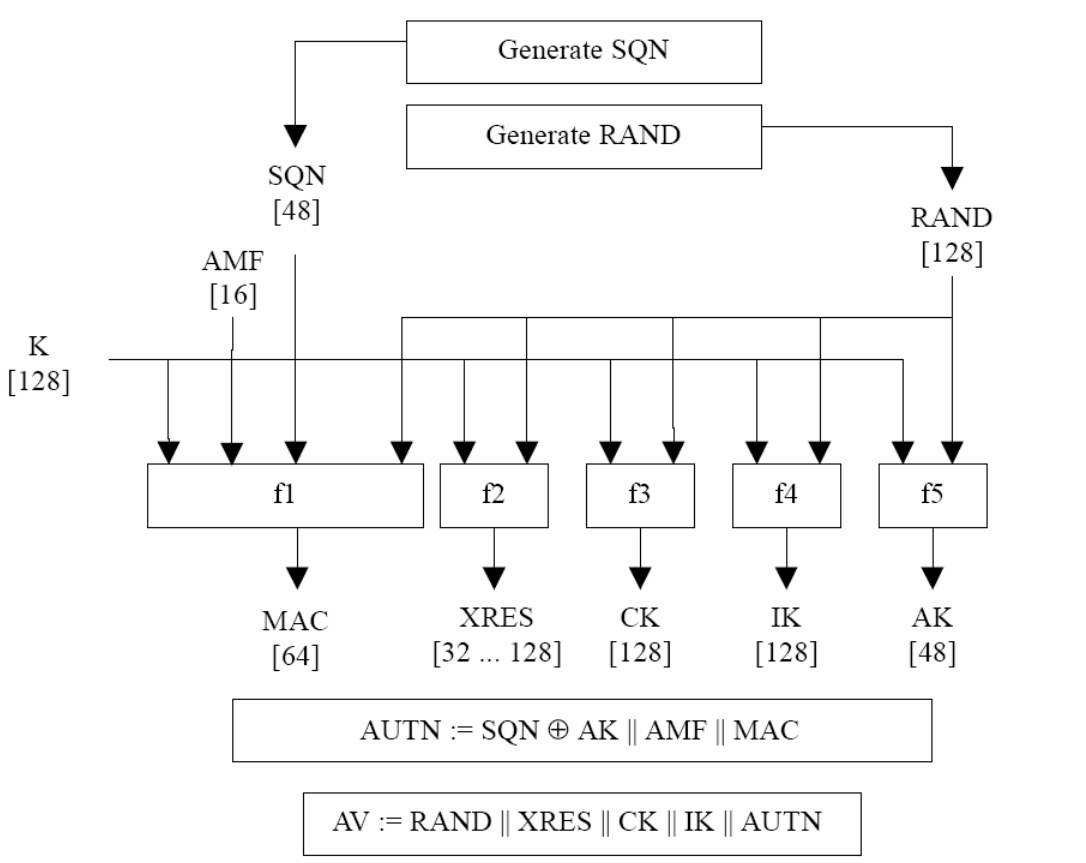

Рисунок 1. Генерация аутентификационных векторов

Обслуживающая сеть (а конкретно — её VLR) выбирает следующий (i-тый) аутентификационный вектор из упорядоченной таблицы и посылает RAND(*i*) и

AUTN(*i*) пользователю. USIM проверяет, производит ли AUTN(*i*) валидный маркер аутентификации и, если да, генерирует и посылает ответ RES(*i*), который обслуживающая сеть сравнивает с XRES(*i*). USIM также вычисляет CK и IK, которые используются, соответственно, для шифрования и поддержки целостности потока данных на уровне эфира.

Криптографические алгоритмы в UMTS

Процесс разработки

Когда возникает необходимость разработать новый алгоритм шифрования, можно сделать это тайно и явно. Преимущество тайных методик защиты информации состоит в том, что задача криптоаналитика усложняется незнанием им не только ключа, но и непосредственно алгоритма. Такой подход хорошо применим в системах для внутреннего пользования (государственных, внутрикорпоративных), но не пользуется популярностью на рынке. Потенциальный покупатель должен принимать на веру то, что система достаточно надёжна, что в основе этой надёжности лежит именно вычислительная сложность задачи подбора ключа, а не секретность алгоритма шифрования, и что не существует каких-либо обходных путей, позволяющих тому же разработчику легко определить ключ и дешифровать информацию на выходе системы в процессе её эксплуатации. Публикация же алгоритма шифрования позволяет проводить независимые исследования его надёжности и привлекать к ним гораздо больше разных исследовательских групп, чьим результатам потенциальные клиенты будут доверять больше.

В рамках 3GPP выла создана группа разработчиков и группа тестировщиков, последние проверяли полученный шифр на криптоустойчивость и соответствие требованиям.

Требования

В рамках общей концепции стандарта функции, отвечающие за шифрование и целостность определили как f8 и f9. С учётом специфики используемого канала и передаваемых данных, а так же технологических возможностей по производству обслуживающих схем, для f8 и f9 были определены следующие требования:

- f8 должна представлять собой поточный шифр;
- f9 должна быть функцией умножения/суммирования;
- обе функции должны удовлетворительно считаться на небольших чипах с низким энергопотреблением;
- не должно быть ограничений по замене этих функций на терминалах (в абонентском оборудовании);
- распространение сетевого оборудования должно быть в соответствии с Вассенарскими соглашениями.

Общий отчёт всех четырёх рабочих групп [3GPP TR 33.909] подтвердил соответствие разработанного алгоритма вышеупомянутым критериям.

MISTY

В 1994г. Мицуру Мацуи (Mitsuru Matsui) предложил линейный криптоанализ для DES, позволяющие за разумное время взламывать малораундовые реализации этого шифра. Данное обстоятельство привело его к разработке в 1997г. нового блочного шифра с 128-битным ключом, 64-битными блоками и варьируемым количеством итераций. Этот шифр, названный, MISTY, оказался гораздо более стойким, чем DES, и был использован в качестве ядра для f8.

Ключ в MISTY состоит из на 16 подключей: K0, ..., K7 и K8, ..., K15 – после каждой итерации подключи в группах циклически сдвигаются на 1. первые 8 ключей получаются простым разбиением главного ключа, а вторая группа получается путём зашифровывания первой группы с помощью элементарной итерации MISTY: K0, зашифрованный на K1 даёт K8 и т.д. последовательно.

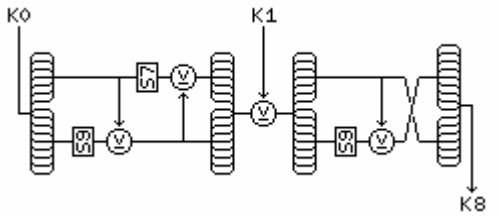

Рисунок 2. Получение второй группы подключей

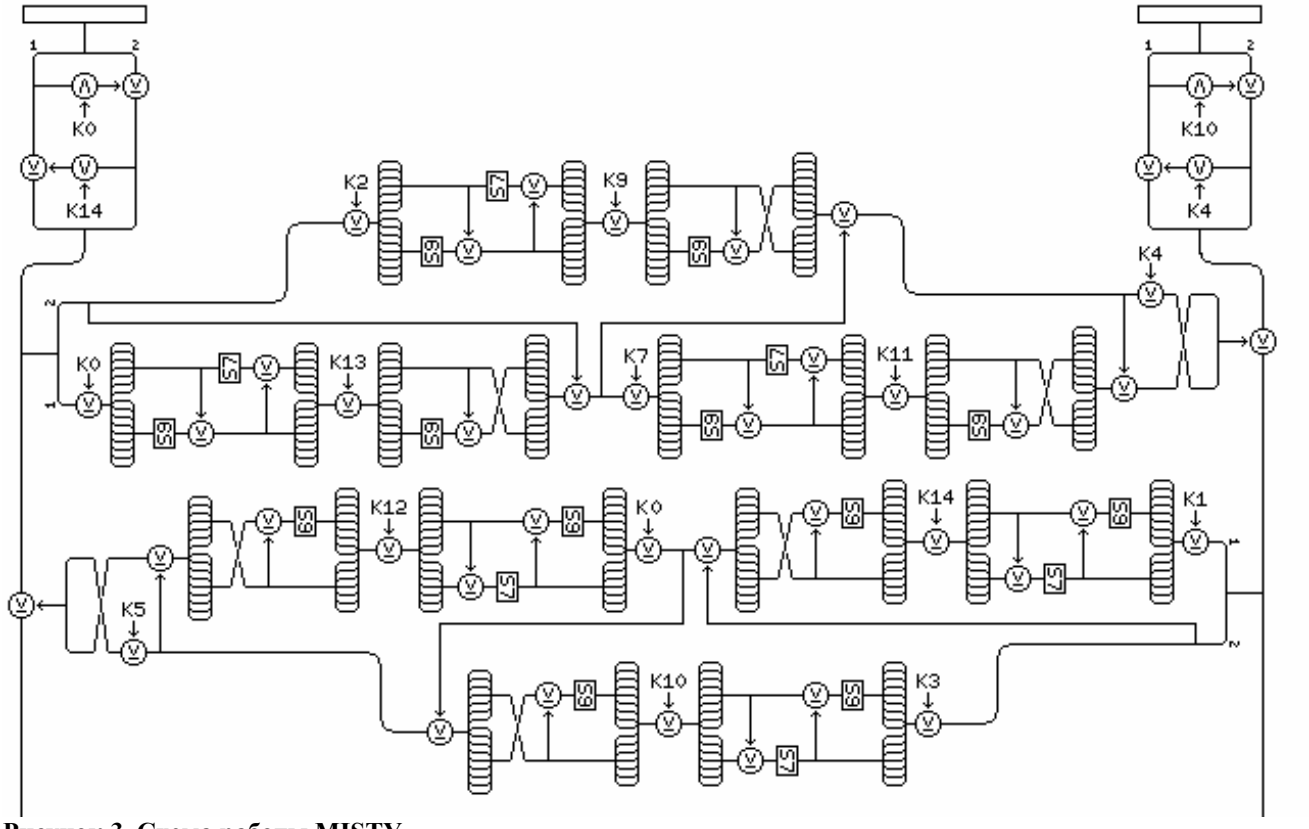

Рисунок 3. Схема работы MISTY

Обычно используются 8 Фейстелевских раундов, через каждые 2 раунда производится линейное преобразование выхода, зависящее, однако нелинейно от ключа. Для того, чтобы ядро удовлетворяло вышеуказанным требованиям стандарта, его слегка модифицировали, и был получен блочный шифр KASUMI [3GPP TS 35.202]

Поточный шифр f8

Подробное описание итогового шифра, полученного из KASUMI, даётся в [3GPP TS 35.201]. Для преобразования блочного MISTY в поточный KASUMI была использована комбинация обратной связи по выходу и режима счётчика. Схема работы f8 представлена на иллюстрации ниже.

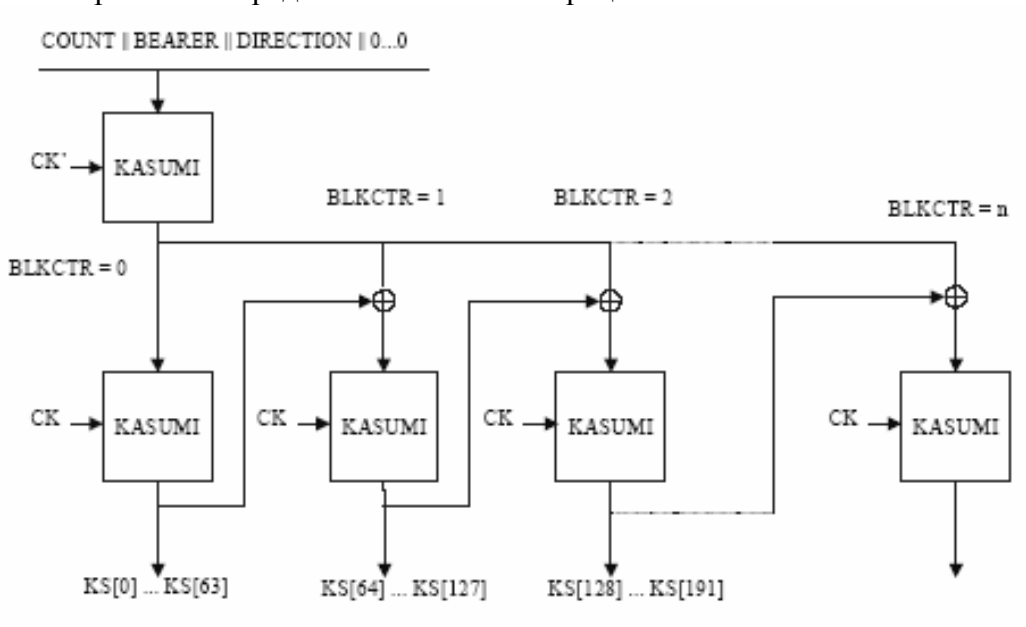

Рисунок 4. f8—KASUMI

Разумеется, невозможно было сделать KASUMI «абсолютно» поточным, но дискретность в 64 бит на практике совершенно незаметна. Для предотвращения атаки по известным фрагментам исходного текста инициирующий вектор зашифрован на другом ключе, $CK' = CK \oplus KM$, где KM – модификатор ключа. Это начальное шифрование также защищает от атаки по наложению, так как взломщик не может свободно ксориться с счётчиком блоков. Если бы не эта предосторожность, то можно было бы подобрать два различных начальных вектора таких, что при разных значениях счётчика блоков с некоторой вероятностью происходит наложение.

Алгоритм проверки целостности в UMTS

Функция f9 представляет собой последовательную функцию умножения-накопления с KASUMI в ядре. К каждому отсылаемому сообщению прикрепляется MAC-I (32-хбитная псевдослучайная строка — выход f9), и такая же строка вычисляется принимающей стороной. Дело в том, что выход функции f9 практически непредсказуемым образом зависит от входных параметров, так что только правильное сочетание IK и счётчика гарантирует достоверность полученного сообщения.

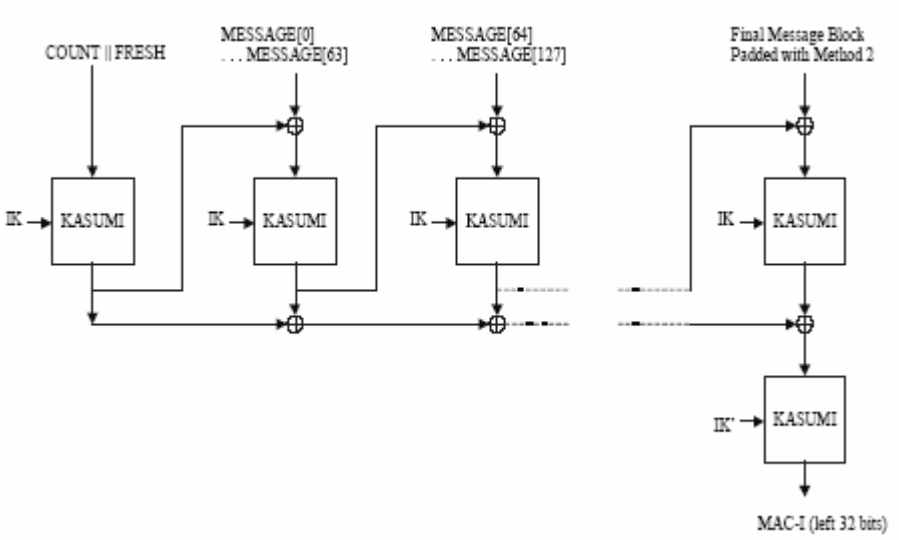

Рисунок 5. f9—генерация MAC-I

ЗАКЛЮЧЕНИЕ

UMTS стал первым массовым стандартом беспроводной связи, обеспечивающим серьёзный уровень защиты информации пользователя. Были использованы две принципиально новые вещи. Во-первых, была рассмотрена возможность атаки с помощью ложной базовой станции, чего не предусматривалось ранее. Во-вторых, благодаря публичности проводимых исследований, был проведён гораздо более детальны анализ криптостойкости и получены заслуживающие доверия результаты, подтверждающие, что эта стойкость соответствует современным требованиям. Немаловажным является и то обстоятельство, что оператор волен выбирать функцию-ядро системы безопасности. Эта функция порождает все f1-9 и может быть передана от обслуживающей сети терминалу абонента, данная возможность предусмотрена для осуществления роуминга.

Разумеется, описанные механизмы касаются только самого радиоканала, по которому можно передавать уже предварительно зашифрованную информацию. Например, протокол WAP использует собственное шифрование с открытым ключом, а интернет-протоколы, по которым осуществляется дистанционное управление банковским счётом или удалённый доступ к сети крупной корпорации, защищены дополнительно и независимо от канала, который занимают. Однако, защита радиоканала является важным предметом исследований, так как беспроводная связь играет всё большую роль в телекоммуникациях. Например, четвертым поколением мобильных сетей (4G) принято считать WLAN-сеть, охватывающую весь город и позволяющую, например, маршрутизировать вызовы через разных операторов. Можно предположить, что в 4G защита информации будет обеспечиваться подобно тому, как это делается в 3G, с возможным усложнением функции-ядра благодаря увеличению производительности оборудования.

ЛИТЕРАТУРА

[1] 3GPP Specifications, http://www.3gpp.org

[2] Kaisa Nyberg. *Cryptographic Algorithms for UMTS* — European Congress on Computational Methods in Applied Sciences and Engineering ECCOMAS 2004

[3] Stefan Putz, Roland Schmitz, Tobias Martin. Security Mechanisms in UMTS — Datenschutz und Datensicherheit 25 (2001)X.