Особенности доступа и управления мощностью в режиме TDD

Процедура доступа инициализируется мобильной станцией по каналу RACH в случайные моменты времени, что связано с возникновением конфликтов. Для того, чтобы снизить их вероятность и повысить пропускную способность канала RACH, в каждом фрейме дополнительно используется 8 ортогональных кодов.

Механизмы управления мощностью передачи в режиме временного дуплекса описаны в [18]. В TDD применяются следующие принципы управления мощностью:

- коды, расположенные в пределах одного и того же временного интервала (слота) и используемые для реализации одной услуги, передаются с одинаковой мощностью;
- при работе в режиме реального времени (например, передаче речевых сообщений) используется управление мощностью по схеме «замкнутой петли»;
- в приложениях, не требующих передачи в режиме реального времени, существуют опции использования обеих схем управления мощностью: как «замкнутой петли», так и «разомкнутой»;
- начальный уровень мощности передатчика устанавливается путем определения оценки потерь на распространение сигналов на трассе до обслуживающей БС.

Механизмы обеспечения информационной безопасности в сетях 3G

Обеспечение секретности в системе подвижной связи – важнейший вопрос как для ее пользователей, заинтересованных в конфиденциальности, так и для операторов, которые стремятся предотвратить случаи мошенничества, наносящие ущерб их доходам.

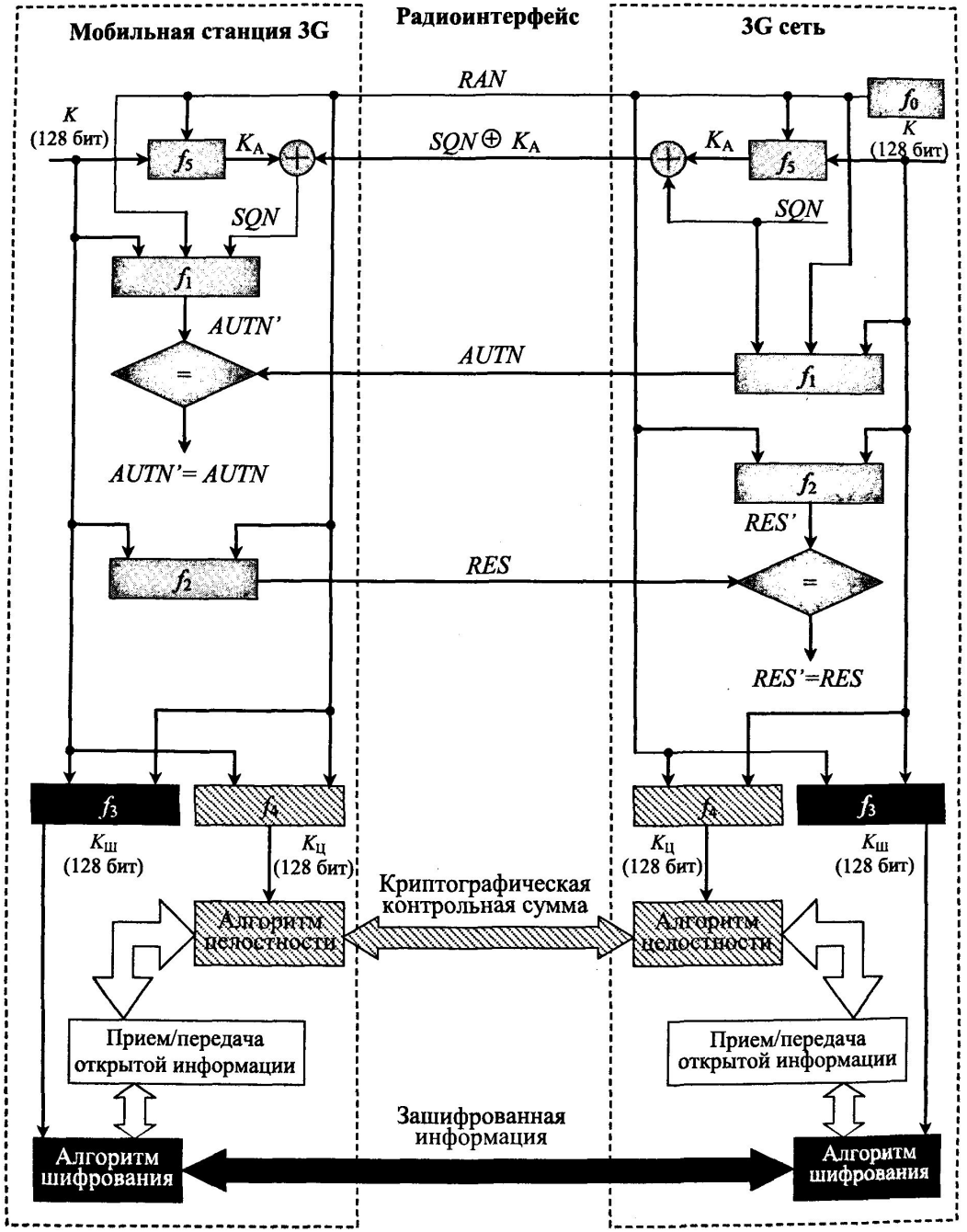
В этом разделе проведен анализ механизмов безопасности систем сотовой связи 3G, разрабатываемых в рамках партнерских проектов 3GPP и 3GPP2 – UMTS и cdma2000. Обе соответствуют требованиям совместимости с системами 2G/2,5G и унаследовали некоторые их особенности. Несмотря на ряд отличий, в них применяются похожие схемы аутентификации и распределения ключей. Важным преимуществом систем 3G является свободный доступ к информации об алгоритмических основах их безопасности. Засекреченность таковых в случае с GSM помогала поддерживать иллюзию безопасности, но не позволяла выявлять и своевременно исправлять слабые стороны ее реализации.

Основные алгоритмы обеспечения безопасности информации в 3G

f_0	Функция генерирования параметров вызова (Random challenge generating function)
f_1	Функция аутентификации сети (Network authentication function)
f_2	Функция аутентификации пользователя (User challenge-response authentication function)
f_3	Функция генерирования ключа шифрования (Cipher key derivation function)
f_4	Функция генерирования ключа проверки целостности (Integrity key derivation function)
f_5	Функция генерирования ключа анонимности (Anonymity key derivation function)

В системах сотовой связи третьего поколения используется схема взаимной аутентификации мобильной станции и сети (рис. 7.35). Приняв вызов от МС, сеть инициирует процедуру аутентификации. Ее центр аутентификации генерирует случайное число *RAND* с помощью функции f_0, а затем параметр аутентификации *AUTN* (функция f_1). Для этого помимо числа *RAND* используется предварительно распределенный секретный ключ *K* и номер передаваемой последовательности данных *SQN*. Для предотвращения определения местоположения абонента *SQN* суммируется по модулю 2 с ключом анонимности K_A, генерируемым функцией f_5. После этого «кортеж» параметров *RAND*, $SQN \oplus K_A$ и *AUTN* передается мобильной станции по радиоканалу.

Для осуществления аутентификации сети в модуле идентичности абонента МС вычисляется номер переданной последовательности $SQN \oplus K_A \oplus K_A$. Затем по принятому *RAND* и предварительно распределенному *K* с помощью функции f_1, определяется *AUTN'*. В случае совпадения вычисленного и принятого значений (*AUTN'=AUTN*) МС «признает» сеть своей, а при расхождении – отклоняет ее.


Мобильная станция 3G
Радиоинтерфейс
3G сеть
RAN
K
(128 бит)
f_5
K_A
SQN ⊕ K_A
K_A
f_5
f_0
K
(128 бит)
SQN
SQN
f_1
AUTN'
=
AUTN
f_1
AUTN'= AUTN
f_2
RES'
f_2
RES
=
RES'=RES
f_3
f_4
f_4
f_3
$K_Ш$
(128 бит)
$K_Ц$
(128 бит)
$K_Ц$
(128 бит)
$K_Ш$
(128 бит)
Криптографическая
контрольная сумма
Алгоритм
целостности
Алгоритм
целостности
Прием/передача
открытой информации
Прием/передача
открытой информации
Зашифрованная
информация
Алгоритм
шифрования
Алгоритм
шифрования

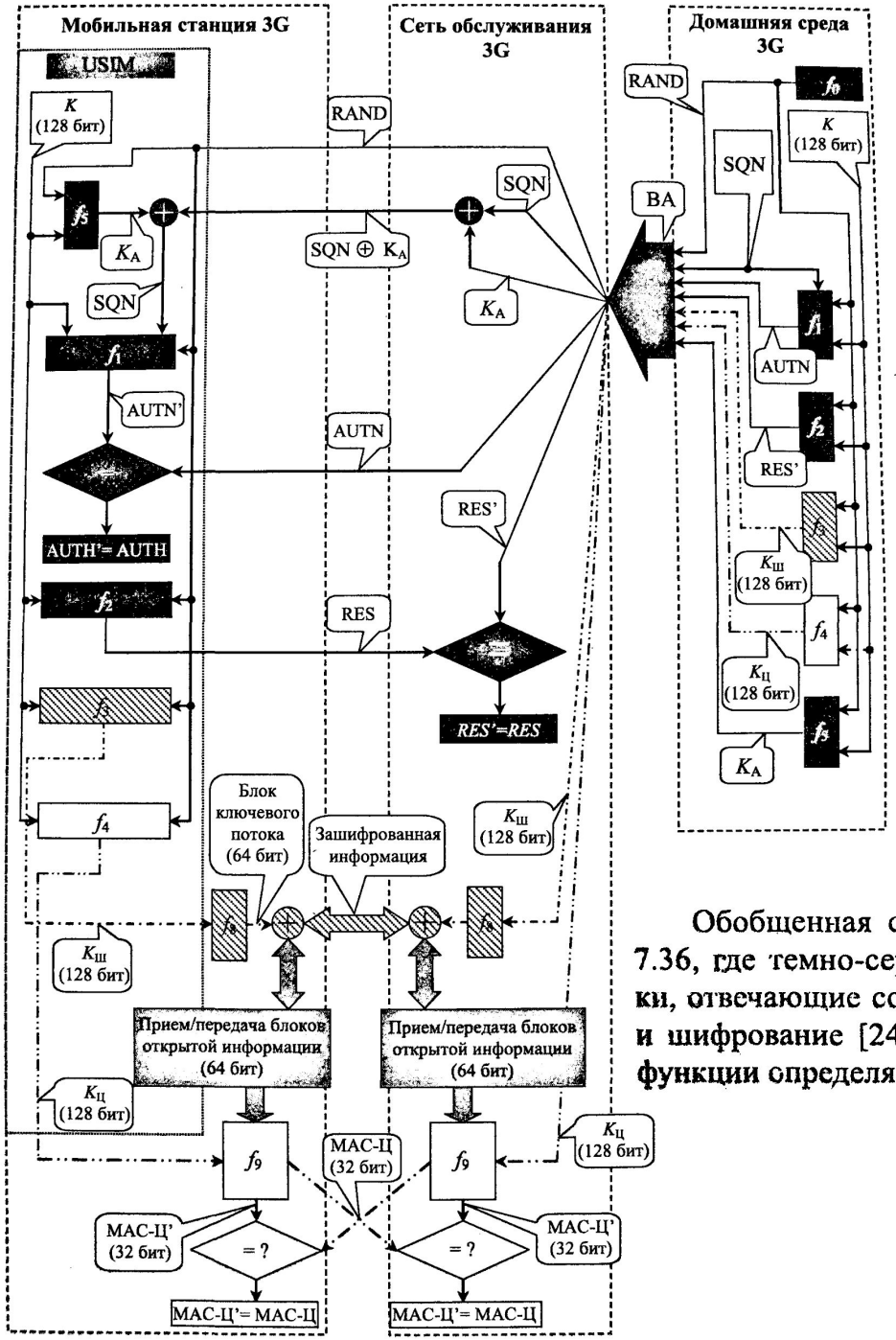
Процедура аутентификации МС сетью напоминает аналогичную процедуру в GSM. МС вычисляет параметр *RES* («отклик» – response) с помощью функции f_2, на вход которой поступает секретный ключ *K* и принятое число *RAND*. Параметр *RES* передается в сеть, которая производит аналогичные вычисления, получает *RES'* и сравнивает его с *RES*. Если два значения равны, сеть признает МС «своей». Таким образом, в 3G предусмотрены процедуры подтверждения достоверности, как самой МС, так и непосредственно сети. Модуль идентичности пользователя 3G в случае фрода (попытке обмана) может отклонить услуги сети, в которой ему предстоит регистрироваться. Такая возможность отсутствовала в системе GSM.

Для обеспечения криптографической защиты информации в канале связи сеть и МС, используя функции f_3 и f_4, генерируют ключи шифрования и проверки целостности. Входными параметрами при этом являются числа *RAND* и *K*. Длина каждого ключа – 128 бит. После этого стороны могут осуществлять потоковое шифрование передаваемых данных. Проверка целостности сообщений проводится путем формирования и проверки криптографических контрольных сумм.

Механизмы обеспечения безопасности в системе UMTS

В UMTS определены основные функциональные группы по обеспечению секретности, каждая из которых соответствует определенным угрозам и решает определенные задачи в сфере безопасности [23].

1. Защита от вторжений на линии радиодоступа к сети, обеспечивающая для пользователей конфиденциальный доступ к услугам 3G. Она включает защиту от подслушивания информации о международном номере мобильной станции IMSI (International Mobile Subscriber Identity), аутентификацию пользователя и сети, а также конфиденциальность соглашения о шифрах.
2. Защита домена сети, обеспечивающая конфиденциальный обмен служебной информацией между узлами в домене провайдера.
3. Защита домена пользователей, которая обеспечивает безопасный доступ к оборудованию пользователя (например, аутентификацию пользователь – модуль USIM на основе PIN-кода).
4. Защита домена приложений, которая обеспечивает конфиденциальный обмен информацией между приложениями пользователя и провайдера (например, между USIM и сетью).



Обобщенная схема архитектуры безопасности UMTS приведена на рис. 7.36, где темно-серым цветом, белым цветом и штриховкой помечены участки, отвечающие соответственно за аутентификацию, целостность информации и шифрование [24]. Применяемые в UMTS криптографические алгоритмы и функции определяются спецификацией 3GPP TS 33.200 [25].

Аутентификация в системе UMTS. Идентификатором подвижного абонента при осуществлении процедуры его аутентификации сетью является международный идентификационный номер – International Mobile Station Identity (IMSI) number или временный номер TMSI, используемый во избежание передачи IMSI через радиоэфир. Назначаемый текущим гостевым регистром VLR и будучи действительным только в зоне действия последнего, TMSI уникальным образом идентифицирует мобильную станцию.

Архитектура безопасности основана на использовании процедуры взаимной аутентификации между оборудованием пользователя и сетью, называемой UMTS-*аутентификацией и ключевым соглашением*. Помимо аутентификации, данная процедура включает генерирование ключей шифрования и защиты целостности.

Аутентификация осуществляется в два этапа. На первом этапе т.н. *вектор аутентификации* (ВА), содержащий основные криптографические ключи и параметры, необходимые для аутентификации, передается в сеть домашней средой. При передаче он надежно защищается от перехвата и модификации. Целостность и конфиденциальность вектора аутентификации обеспечивается протоколом MAPsec, который в качестве главного элемента содержит т.н. центр администрирования ключей (Key Administration Centre) и функционирует на базе криптографических схем с открытым ключом [26,27].

На втором этапе сеть обслуживания выполняет процедуру «вызов–ответ» для взаимного установления подлинности между модулем идентичности абонента USIM (UMTS Subscriber Identity Module) (в cdma2000 он называется UIM – User Identity Module) и сетью. Отвечающие за выполнение процедур аутентификации и ключевого соглашения модули размещены в USIM и в центре аутентификации. В этих модулях используются криптографические функции $f_0 \div f_5$. Для их реализации оператор UMTS может выбрать любой алгоритм, описанный в спецификациях [28], однако 3GPP с этой целью разработан набор алгоритмов MILENAGE [29, 30] на базе симметричного блочного шифра Rijndael. Основные криптографические функции и алгоритмы, определенные для UMTS, приведены в табл. 7.18.

Для взаимной аутентификации сети и USIM используется предварительно распределенный 128-битовый секретный ключ K, размещаемый в USIM и в центре аутентификации домашней среды. Важнейшим условием безопасности информации в системе является сохранение в тайне ключа K на протяжении всего срока службы USIM.

Функция генерирования случайного числа RAND f_0 локально размещается в центре аутентификации домашней сети. Значение RAND не должно повторяться в течение всего срока службы USIM. В противном случае знание значения RAND, использованного в одном из предшествующих сеансов, теоретически позволяет восстановить отклик RES и влечет за собой нарушение конфиденциальности передаваемой информации.

Процедура аутентификации и ключевого соглашения инициируется сетью, которая передает мобильной станции сообщение вызова, содержащее случайное число RAND и символ установления подлинности AUTN. Суть этой процедуры заключается в установлении подлинности вызова, получаемого МС, который можно сгенерировать только зная секретный ключ K. С учетом существующих ограничений на время установления соединения используется т.н. процедура с вызовом и ответом при использовании кодов аутентификации, минимизирующая вычислительные затраты. Последнее достаточно важно, поскольку функции f_1 и f_2 выполняются в самом USIM [25].

Алгоритмы/функции безопасности UMTS и cdma2000

Алгоритм (функция)	**Назначение**	
	UMTS	**cdma2000**
f_0	Функция генерирования случайного числа	
f_1	Функция аутентификации сети	
f_2	Функция аутентификации пользователя	
f_3	Функция генерирования ключа шифрования $K_{Ш}$	
f_4	Функция генерирования ключа целостности $K_{Ц}$	
f_5	Функция генерирования ключа анонимности $K_{А}$	
f_6	Алгоритм шифрования, обеспечивающий конфиденциальность данных, передаваемых между домашней средой и сетью обслуживания	–
f_7	Алгоритм целостности, предназначенный для обеспечения контроля целостности данных на участке домашняя среда – сеть обслуживания	–

f_8	Алгоритм шифрования, предназначенный для шифрования данных, передаваемых на участке сеть обслуживания – мобильная станция	–
f_9	Алгоритм целостности, предназначенный для обеспечения контроля целостности данных на участке сеть обслуживания – мобильная станция	–
f_{11}	–	Функция генерирования ключа K_{AU} аутентификации UIM
UMAC	–	Алгоритм аутентификации UIM
ESP_AES	–	Алгоритм шифрования
EHMAC	–	Усовершенствованный алгоритм обеспечения целостности HMAC

Получив вызов, USIM проверяет подлинность сети, вычисляя значение

$$AUTN' = f_1(K, SQN, RAND)$$

и производя его сравнение с AUTN, переданным в векторе аутентификации (см. рис. 7.36). Если два значения равны, подлинность сети считается установленной.

После этого вычисляется ответ RES с использованием функции f_2 в USIM

$$RES = f_2(K, RAND),$$

необходимый для доступа мобильной станции в сеть. Одновременно вычисляются ключи шифрования и обеспечения целостности $K_{Ш}$ и $K_{Ц}$,

$$K_{Ш} = f_3(K, RAND) \text{ и } K_{Ц} = f_4(K, RAND),$$

после чего сравниваются значения RES с RES′, также содержащимся в векторе аутентификации. В случае RES=RES′ подлинность оборудования пользователя считается установленной.

В процессе выполнения процедуры аутентификации может использоваться генерируемый функцией f_5 ключ анонимности $K_A = f_5(K, RAND)$. Он необходим для сокрытия *SQN* (Sequence Number) – номера передаваемой последовательности данных, являющегося составной частью вектора аутентификации. Сокрытие *SQN*, усложняющее несанкционированное отслеживание местоположения абонента [29, 30], реализуется путем суммирования по модулю два двоичного значения *SQN* и значения ключа K_A (рис. 7.36). Ясно, что функция f_5 должна выполняться раньше, нежели функция f_1.

Обеспечение конфиденциальности информационного обмена в UMTS. На участке оборудование пользователя – контроллер сети радиодоступа RNC (уровень протоколов MAC и RLC) задача обеспечения конфиденциальности возлагается на функцию симметричного потокового шифрования f_8 [31]. Опция шифрования активируется контроллером RNC. При этом базовая сеть передает в сеть радиодоступа UTRAN ключ шифрования, совместно используемый базовой сетью и оборудованием пользователя.

В архитектуре безопасности UMTS предусмотрена опция выбора алгоритма шифрования из 16 вариантов. Указатель на используемый алгоритм содержится в идентификаторе алгоритма шифрования UEA (т.е. *UMTS encryption algorithm*). Указатель на стандартный алгоритм обозначается как UEA1, а ссылка на «пустой алгоритм», соответствующий отсутствию шифрования, – как UEA0.

Криптографическим ядром стандартного алгоритма является симметричный блочный шифр KASUMI [32]. Размер шифруемого блока данных – 64 бита, длина ключа шифрования – 128. Шифр функционирует в режиме обратной связи, где функция f_8 используется для генерирования блоков ключевого потока, побитно суммируемых по модулю 2 с блоками открытого текста.

Зона обслуживания оператора в UMTS разделена на домены секретности, границы которых защищены шлюзами SEG (Security & Encryption Gateway). Ключи между шлюзами распределяются в соответствии с протоколом IKE (Internet Key Exchange) на базе алгоритмов асимметричного шифрования с открытым ключом, например RSA или Диффи-Хеллмана (Diffie-Hellman) [27, 33].

7.7.2.3. Обеспечение целостности информации в UMTS распространяется на передачу данных между мобильной станцией и контроллером радиосети. В архитектуре безопасности системы UMTS выделяют 16 алгоритмов обеспечения целостности, указываемые в идентификаторе UIA. Стандартный алгоритм имеет обозначение UIA1. Стандартная функция целостности f_9 также реализована на базе блочного шифра KASUMI. Наряду с защищаемыми данными на ее вход поступает 128 битовый ключ целостности $K_{Ц}$, после чего вычисленное значение МАС-Ц включается отправителем в передаваемое сообщение (рис. 7.36). Его получатель вычисляет МАС-Ц′. В случае идентичности вычисленного значения МАС-Ц′ и полученного МАС-Ц целостность данных считается подтвержденной.

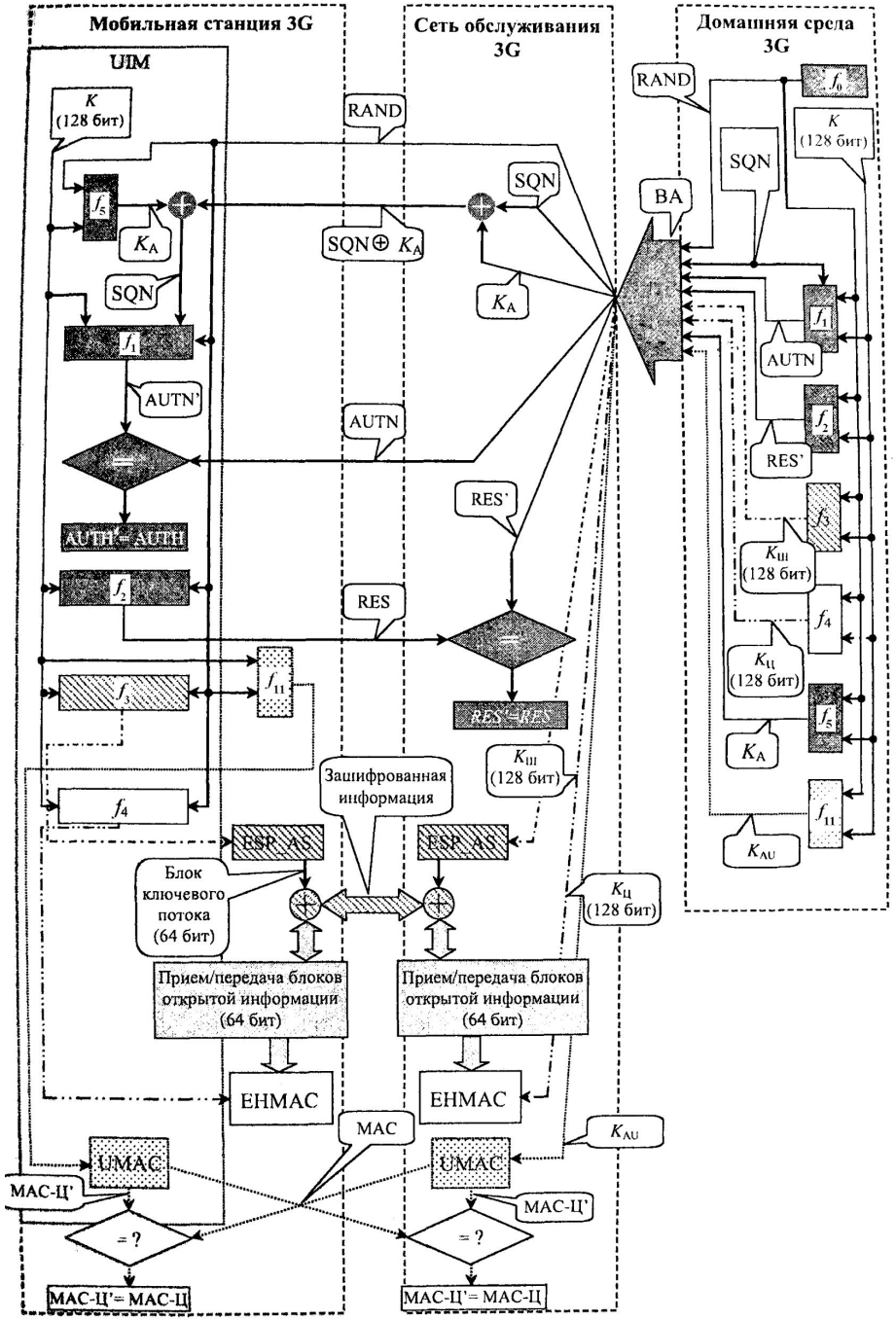
Механизмы обеспечения безопасности в системе cdma2000

Обобщенная архитектура безопасности cdma2000 приведена на рис. 7.37, где процедуры аутентификации, обеспечения целостности и шифрования выделены темно-серым цветом, белым цветом и диагональной штриховкой. Точечным узором помечены элементы UIM, отвечающие за аутентификацию. Алгоритмы безопасности, используемые в cdma2000, приведены в табл. 7.18 [34]. В cdma2000 предусмотрено использование как несъемного, так и съемного модуля идентичности (*removable*) R-UIM. В этом случае оператор может использовать собственный набор соответствующих алгоритмов.

Аутентификация в cdma2000. Идентификатор оборудования IMSN (TMSN) называется иначе, нежели аналогичный по назначению идентификатор UMTS. Процедура аутентификации в cdma2000 подобна двухэтапной процедуре аутентификации в UMTS с несколькими уточнениями. В частности, речь идет о необязательном дополнении процедуры аутентификации и ключевого соглашения функцией f_{11} генерирования ключа K_{AU} аутентификации модуля UIM и функцией UMAC, преобразующей с помощью K_{AU} тэг аутентификации сообщения (см. рис. 7.37). Кроме того, при передаче в сеть доступа вектора аутентификации целостность и конфиденциальность последнего взамен MAPsec обеспечивается близким, по сути, протоколом IPsec.

Получив вектор аутентификации, UIM инициирует выполнение функции f_5, генерирующей ключ анонимности, и расшифровывает SQN. Полученное значение используется в качестве входа функции f_1, которая генерирует параметр AUTN′ аутентификации сети. После сравнения AUTN′ и AUTN для вычисления RES, $K_{Ш}$, $K_{Ц}$, и K_{AU} выполняются функции f_2, f_3, f_4 и f_{11}, соответственно. Затем значение RES передается в сеть для подтверждения подлинности абонента. Значения $K_{Ш}$ и $K_{Ц}$ передаются от UIM к терминалу, где они далее используются для обеспечения конфиденциальности и целостности данных.

7.7.3.2. Конфиденциальность в cdma2000. Конфиденциальность обмена данными на участке от мобильной станции до контроллера радиосети обеспечена применением стандарта шифрования AES [35] на основе симметричного блочного шифра Rijndael [36]. Последний зашифровывает блоки данных длиной 128-бит под управлением 128-битового ключа, длина которого при необходимости может быть уменьшена. При шифровании формируются блоки ключевого потока (рис. 7.37), используемые для потокового шифрования и расшифровывания данных.


Мобильная станция 3G
UIM
Сеть обслуживания 3G
Домашняя среда 3G
K (128 бит)
RAND
SQN
BA
f_0
f_1
f_2
f_3
f_4
f_5
f_{11}
K_A
SQN⊕ K_A
AUTN
AUTN'
RES
RES'
AUTH'= AUTH
RES'=RES
$K_{Ш}$ (128 бит)
$K_{Ц}$ (128 бит)
K_{AU}
Зашифрованная информация
ESP_AS
Блок ключевого потока (64 бит)
Прием/передача блоков открытой информации (64 бит)
EHMAC
MAC
UMAC
MAC-Ц'
= ?
MAC-Ц'= MAC-Ц

7.7.3.3. Целостность данных в cdma2000. Для обеспечения целостности переданной информации в системе используется код аутентификации сообщения (message authentication code – MAC), отвечающий за защиту от преднамеренной модификации. Длина кода определяется важностью сообщения, но не может быть менее 32 бит. Для защиты сообщений с наивысшим приоритетом используется UMAC (universal hashing MAC), вычисление которого требует использования не только ключа целостности $K_{Ц}$, но и ключа аутентификации K_{AU}. Преимущество UMAC в том, что его вычисление может быть осуществлено лишь непосредственно модулем идентичности абонента UIM (рис. 7.37). В случае предоставления домашней средой ключа аутентификации K_{AU} в виде составной части вектора аутентификации мобильная станция определяет UMAC и помещает его в соответствующий пакет данных.

Сравнительный анализ механизмов безопасности стандартов UMTS и cdma2000

В системах сотовой связи поколения 3G реализована достаточно мощная и продуманная архитектура безопасности информации, открытая для дальнейшего совершенствования. Проведем поэлементное сравнение механизмов обеспечения безопасности в стандартах cdma2000 и UMTS (табл. 7.19) [24].

Первое отличие заключается в возможности использования в cdma2000 как встроенного, так и съемного модуля идентичности абонента R-UIM. Применение последнего исключает использование утерянного терминала, снижает вероятность его хищения и компрометации, обеспечивает высокий уровень защиты хранимой в модуле конфиденциальной информации. Возможность использования съемных модулей проистекает из наличия в архитектуре безопасности cdma2000 алгоритма аутентификации UIM и функции генерирования ключа аутентификации. UMTS не имеет подобных механизмов аутентификации USIM, не считая возможности повторения процедуры аутентификации и ключевого соглашения. Напротив, в системе cdma2000 предусмотрена процедура подтверждения присутствия UIM без повторного запроса вектора аутентификации.