

GSM-WCDMA 鉴权原理

前言

- 在现有的**2G**和**3G**移动网络中，只有具有有效的**IMSI**号码的**MS**才有权得到服务。鉴权，即识别有效用户**IMSI**的过程。它是移动网络安全管理的一部分，用来实现移动网络的保密性、数据完整性
- 由于**WCDMA**网络提供了较**GSM**更为丰富的业务，网络必须提供更为安全的鉴权机制。

基本原理

- 在现有**GSM**网络和将来的**WCDMA**网络中，鉴权是由**MS**、**VLR/SGSN**、**HLR/AUC**协同工作完成，都是由**MS**和**AUC**分别计算出鉴权参数，由**VLR/SGSN**比较双方的计算结果，完成网络对**MS**合法性的验证；
- **WCDMA**增加了**MS**对网络合法性的验证功能，从而实现**MS**与网络双向认证；

*** GSM鉴权原理之鉴权参数***

- SIM卡上的鉴权参数
 - IMSI号码（唯一识别SIM卡的号码）
 - 鉴权密钥Ki（长度为16B，IMSI为Ki的索引，即一个IMSI号码唯一地对应于一个Ki值，但一个Ki值可能被多个IMSI使用）。
 - 安全算法（A3）；
- SIM卡上的与鉴权无关的参数
 - 序号（唯一识别SIM卡，且包括生产厂商信息、操作系统版本等）
 - SIM卡状态（闭锁/解锁）
 - PIN以及用户接入控制等级
 - 临时的网络数据（如TMSI、LAI、KC、被禁止的PLMN）
 - 业务相关数据
- AUC上的鉴权参数
 - 用户数据（IMSI，用来对移动签约者身份进行识别）；
 - 鉴权密钥Ki（注意：该值与用户SIM卡上的Ki值是一致的）；
 - 密码密钥（即密钥K4）：K4是Ki的密钥，用来对Ki进行加密和解密，长度为8B。
 - 密钥序号：是K4的索引（数据库中的外密钥），用来获取K4，若其值为0，表明Ki没有用K4加密（即当前的Ki值为解密后的值）。
 - 安全算法（A3和A8）；
 - 用于生成随机数的随机数发生器

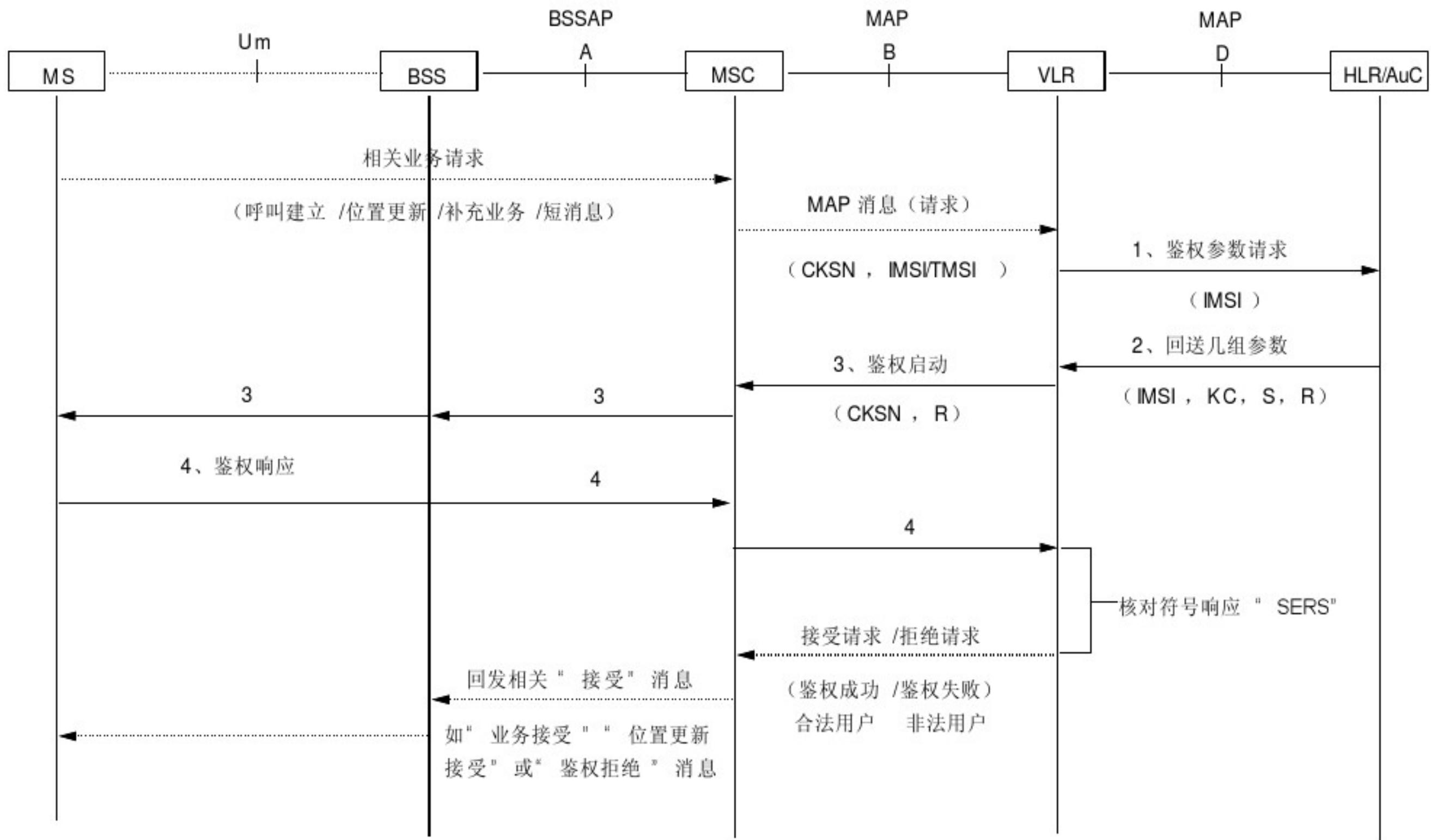
GSM鉴权原理之鉴权参数

- 鉴权三元组(Triplet Vector)
- GSM用于用户鉴权的三个主要参数组成的向量，包括
 - RAND (Random Challenge 随机数)：
 - 由随机数发生器产生，长16B，主要作为计算三元组中其他两个参数的基础。
 - SRES (Signed Response 符号响应)：
 - 对RAND和鉴权密钥Ki利用A3算法计算得出，长4B，用来判断鉴权是否通过，
 - Kc (Cipher Key 密码密钥)：
 - 对RAND和Ki 做A8算法计算得出，长8B，用于空间无线信道加密的密钥
- CKSN (Ciphering Key Sequence Number)
 - CKSN (加密密钥序列号) 被用来保证MS与VLE或MS与SGSN之间的GSM鉴权信息 (Kc) 的一致性，作为临时签约数据存储在VLR (或SGSN) 上。

鉴权三元组的相关说明

- 鉴权三元组的存储位置
 - 鉴权三元组有条件地存储在HLR和VLR（和SGSN）中。当AUC计算出一些三元组后，将这些三元组传送给HLR，并存储在HLR中；若某一MS已登记，其所在的VLR/SGSN也将从HLR装载至少一个三元组。
- 鉴权三元组的复用度
 - 这里所说的GSM中的复用度概念指的是HLR中的鉴权三元组的复用度，对于VLR有相应的复用度概念。
 - 鉴权三元组的复用度是指n个鉴权三元组所组成集合的可重用的次数。设协议规定复用度为m，则当AUC计算出N组鉴权数据组成一个集合后，存储在HLR的数据库中，当HLR接到VLR发送的鉴权数据请求时，直接从数据库中检索出对应鉴权数据集合发送给VLR，该鉴权数据集合可最多发送m次。发送m次后，该集合数据失效，AUC需要重新计算。
 - 在HLR中建立鉴权数据的复用度，目的在于减少AUC的计算负荷，同时，可以对于实时性要求比较高的鉴权数据请求，可以比较迅速地给予响应

GSM鉴权流程



WCDMA鉴权原理之鉴权参数

- USIM卡上的鉴权参数
 - IMSI号码（唯一识别SIM卡的号码）
 - 鉴权密钥Ki（长度为16B，IMSI为Ki的索引，即一个IMSI号码唯一地对应于一个Ki值，但一个Ki值可能被多个IMSI使用）
 - 鉴权和加密算法（f1、f2、f3、f4、f5、f1*、f5*、UIE、UIA）
 - OP或OPc
 - SQNMS
- AUC上的鉴权参数
 - 用户数据（IMSI，用来对移动签约者身份进行识别）；
 - 鉴权密钥Ki（注意：该值与用户SIM卡上的Ki值是一致的）；
 - 密码密钥（即密钥K4）：K4是Ki的密钥，用来对Ki进行加密和解密，长度为8B。
 - 密钥序号：是K4的索引（数据库中的外密钥），用来获取K4，若其值为0，表明Ki没有用K4加密（即当前的Ki值为解密后的值）。
 - 鉴权和加密算法（f1、f2、f3、f4、f5、f1*、f5*）
 - 用于生成随机数的随机数发生器
 - AMF
 - OP或OPc
 - SQNHE

WCDMA鉴权原理之鉴权五元组

- 五元组（Quintet Vector）组成
- **RAND** (**Random Challenge** 随机数)：
 - 由随机数发生器产生，长16B，主要作为计算五元组中其他参数的基础。
- **XRES** (**Expected Response** 期望响应)：
 - 是UMTS对鉴权请求的期望响应，长4—16字节
- **CK** (**Cipher Key** 加密密钥)：
 - 长16字节：用来实现实存取数据的完整性（**Access link data confidentially**），以加密被认为是机密的信令信息元素。（即对某些逻辑信道进行加密），针对不同的网络类型（CS: **Circuit Switch**和PS: **Packet Switch**），分别对应了一个CK: CKCS和CKPS。
- **IK** (**Integrity Key** 完整性密钥)：
 - 长16字节；用来实现用来实现连接数据存取的保密性（**Access link data confidentially**）。因为大多数发送给MS和网络的控制信令信息都被认为是敏感数据，必须进行完整性保护。针对不同的网络类型（CS: **Circuit Switch**和PS: **Packet Switch**），分别对应了一个IK: IKCS和IKPS。
- **AUTN** (**Authentication Token** 鉴权标记)，长16字节，包括以下内容
 - SQN^AK，其中SQN（序列号）与AK（匿名密钥）分别长6字节；USIM将验证AUC产生的SQN是否是最新的，并作为鉴权过程的一个重要组成部分。
 - AMF（鉴权管理域）长2字节。
 - MAC（消息鉴权编码）长8字节；MAC-A用来验证RAND、SQN、AMF的数据完整性并提供数据源；MAC-S则由USIM发送给AUC作为重新同步过程中鉴权的数据源。

鉴权五元组的生命周期

- 在UMTS中，鉴权五元组由HLR/AUC产生，发送给VLR/SGSN，VLR/SGSN将其按序排列，需要时利用authentication request消息将五元组中的部分参数传送给MS，每个五元组只能被使用一次（但是，若VLR/SGSN已经向MS发送了authentication request，但没有收到MS返回的User authentication response 或 User authentication reject消息时，会重发这个五元组，直到收到MS的响应，鉴权完毕后，将该五元组删除；同时，为了避免重发导致MS的再同步，MS需要保存最近的RAND、RES、CK、IK等鉴权参数）
- CK和IK存储在USIM以及VLR/SGSN上，由VLR/SGSN以security mode command（安全模式命令）敲(7)透鳴NC，以便进行信道加密。USIM也可以应UE（user equipment：用户设备）的要求，将CK和IK发送给UE，即UE中将保持一份CK和IK的拷贝。VLR/SGSN必须保证24小时内至少更新CK和IK一次。

WCDMA鉴权参数说明之AMF

- AMF(Authentication management field)
- 鉴权管理域 AMF目前用于计算MAC-S和MAC-A，也是AUTN的组成部分之一。以下是将来AMF的可能应用：
 - 支持多种鉴权算法和密码
 - 变换SQN验证参数
 - 设置限制IK和和CK的有效时间的阈值

WCDMA 鉴权参数说明之 SQN

- **SQN(Sequence number)** 序列号是鉴权五元组的一个组成部分，它类似五元组的计数器，是实现MS对网络合法性验证的一个重要参数
- **SQN**由AUC在计算每个五元组时，使用专门的发生器产生，并通过HLR在下发五元组的时候下发，HLR同时保存一个最新的SQNHE
- MS将保存接受的最新的SQNMS，通过比较收到的SQN与SQNMS以确保收到的下一组五元组是最新的（fresh）

WCDMA鉴权参数之 OP&OPc

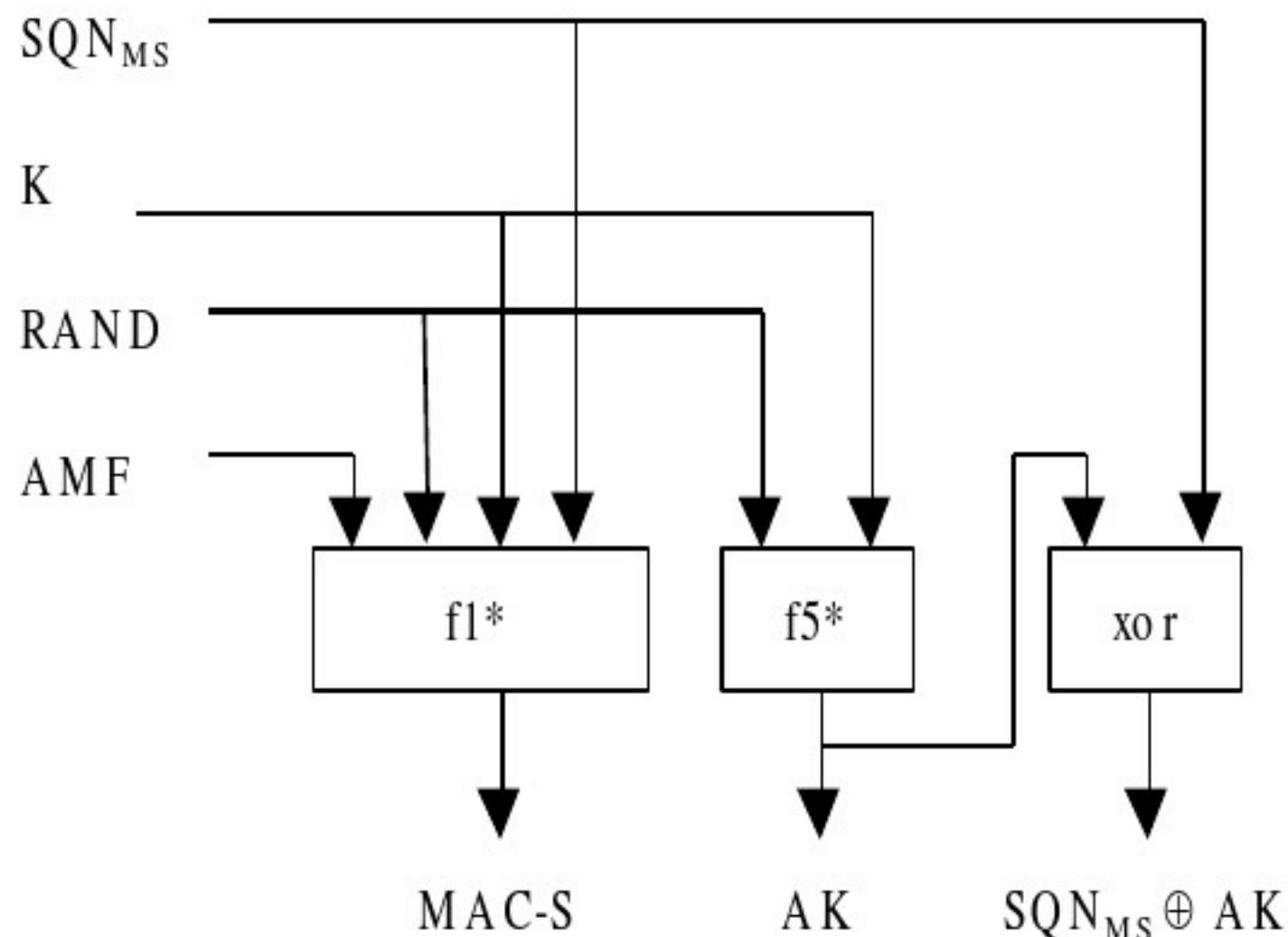
- OP(Operator Variant Algorithm Configuration Field)运营商可变算法配置域，长16B。该参数是使用**MILENAGE**鉴权算法引入的，是鉴权计算的一个输入参数。一个运营商的所有用户可以使用相同的OP，以区别其他运营商的用户。**HLR/AUC**和**USIM**卡都将保存OP，且应当保证其一致
- OPc是对OP以KI为密钥进行加密计算得到的结果。对于同一个运营商的不同用户，尽管OP是相同的，但OPc是不同的，对于同一用户，其OPc值是不变的。OPc是计算鉴权五元组的真正输入参数。因此，**HLR/AUC**和**USIM**卡可以选择保存OPc而不是OP，从而减少运算的耗费。

WCDMA鉴权参数之AK

- AK(Anonymity Key)匿名密钥
- 长6B
- 用于加密SQN，避免被被动攻击
- 如果不需要加密SQN，则AK=0

WCDMA鉴权参数之 AUTC

- AUTC(Resynchronisation Token)再同步标识符
 - 当MS对VLR/SGSN送来的AUTN验证后，认为同步失败时，返回“同步失败”消息给VLR/SGSN，此时，VLR/SGSN会向HLR/AUC发起一个重新同步请求，同时附上本参数。

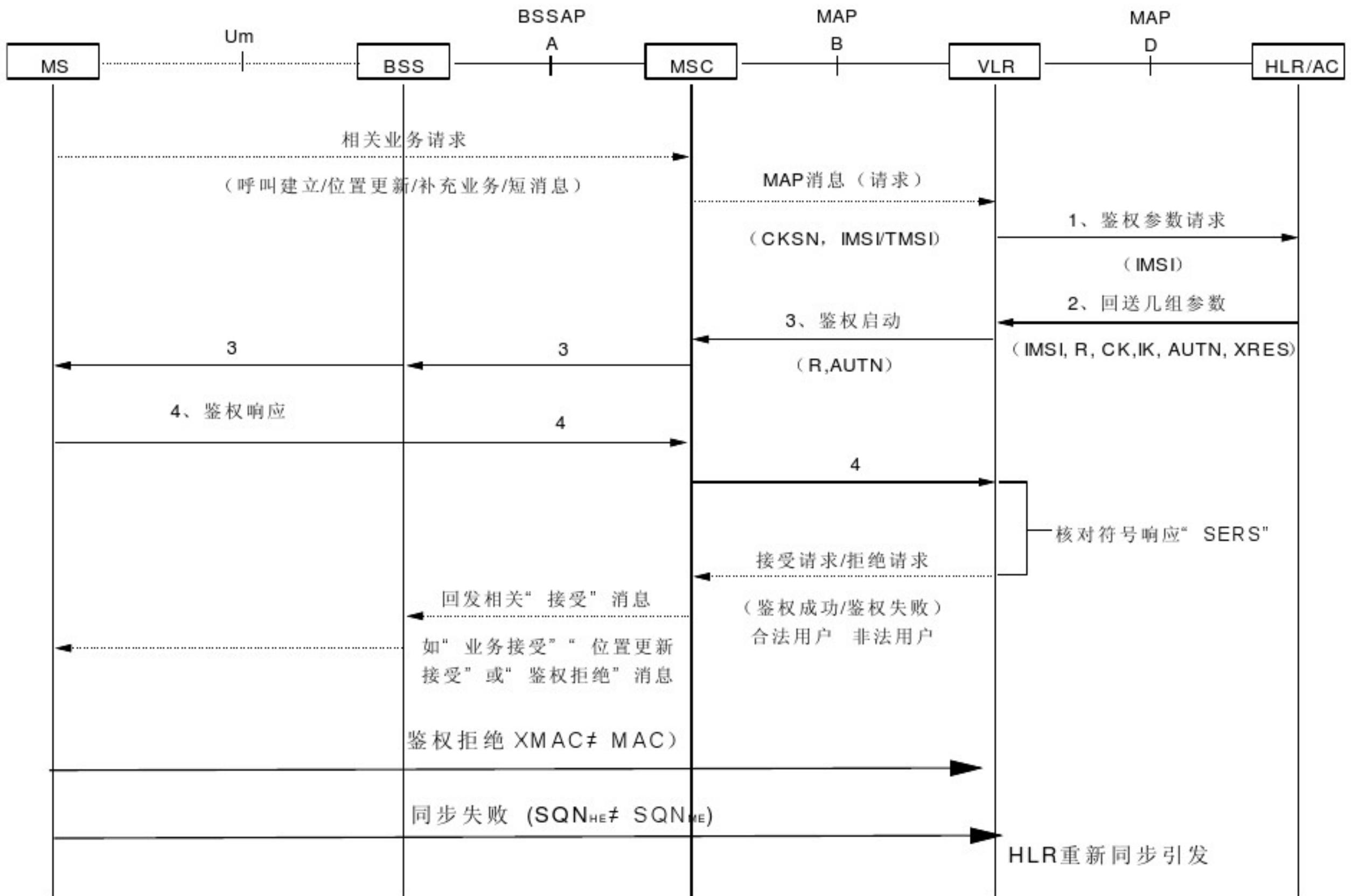


$$AUTC = SQN_{MS} \oplus AK \parallel MAC-S$$

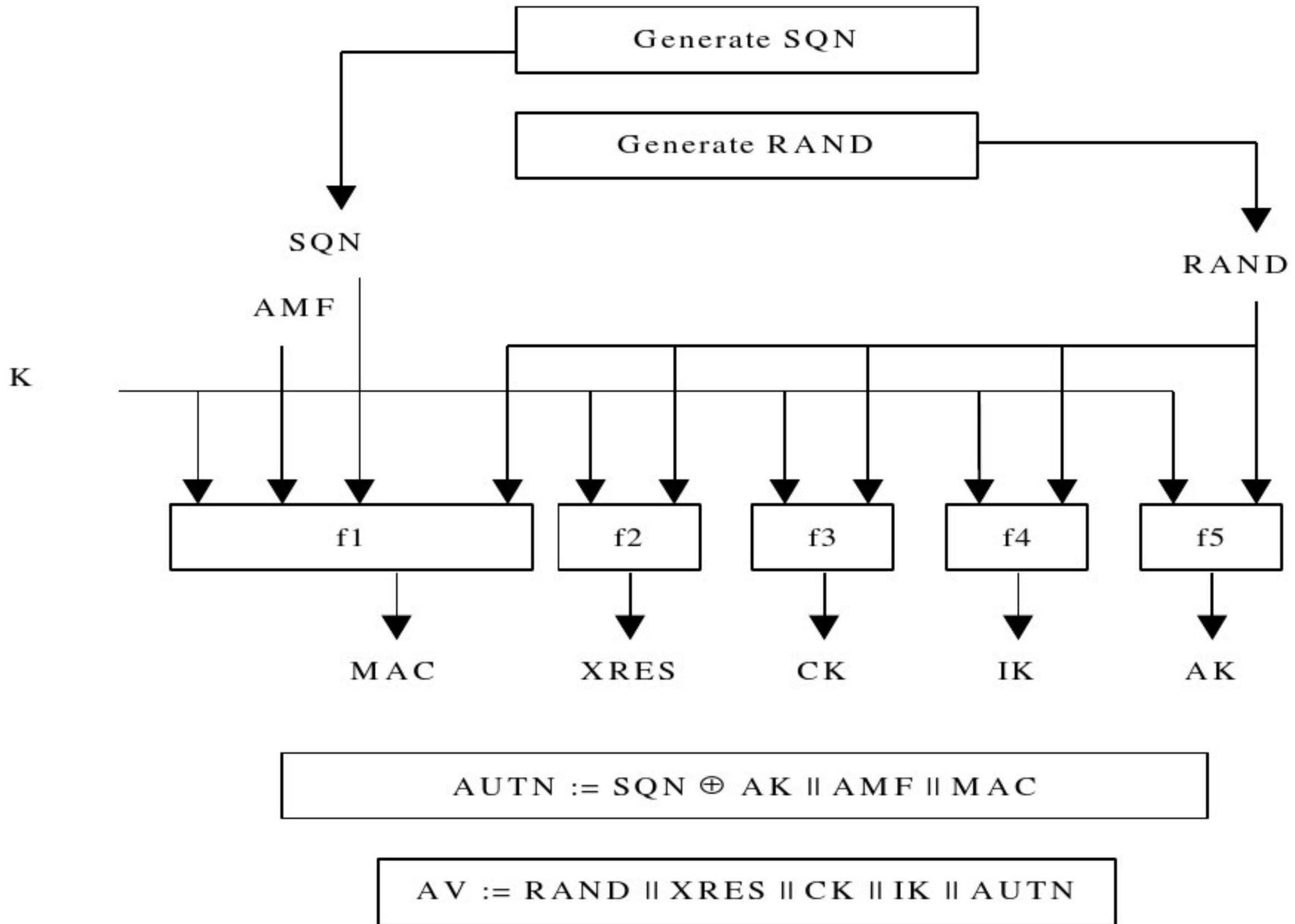
WCDMA鉴权参数之 KSI

- KSI (Key Set Identifier) 密钥集标识符是一个在鉴权过程中可以从CK和IK推导出的数字，它对应于GSM网络中的CKSN，由网络分配，并被VLR/SGSN将其与Authentication request message发送给MS，并与CK和IK一起存储在MS中。目的在于使得网络不调用鉴权算法就可以识别CK和IK，使得在后续的连接建立过程中，CK和IK的复用成为可能。
- KSI和CKSN的格式相同，占3bit，KSI共有7个值，其中，“111”表示某个密钥开始失效，如当删除CK和IK时，KSI被置为“111”。

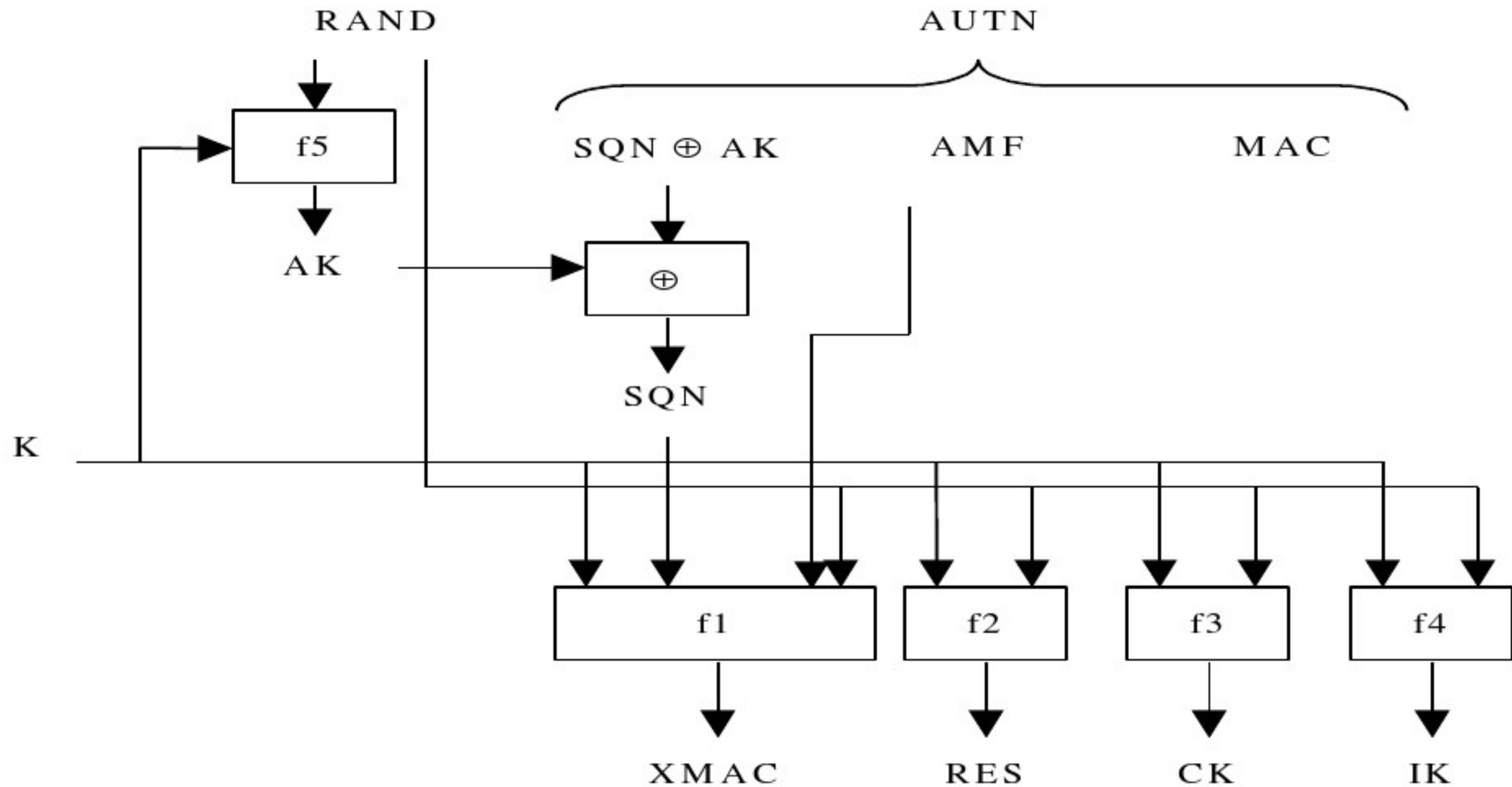
WCDMA鉴权流程



WCDMA之AUC计算鉴权五元组



WCDMA鉴权之USIM鉴权处理

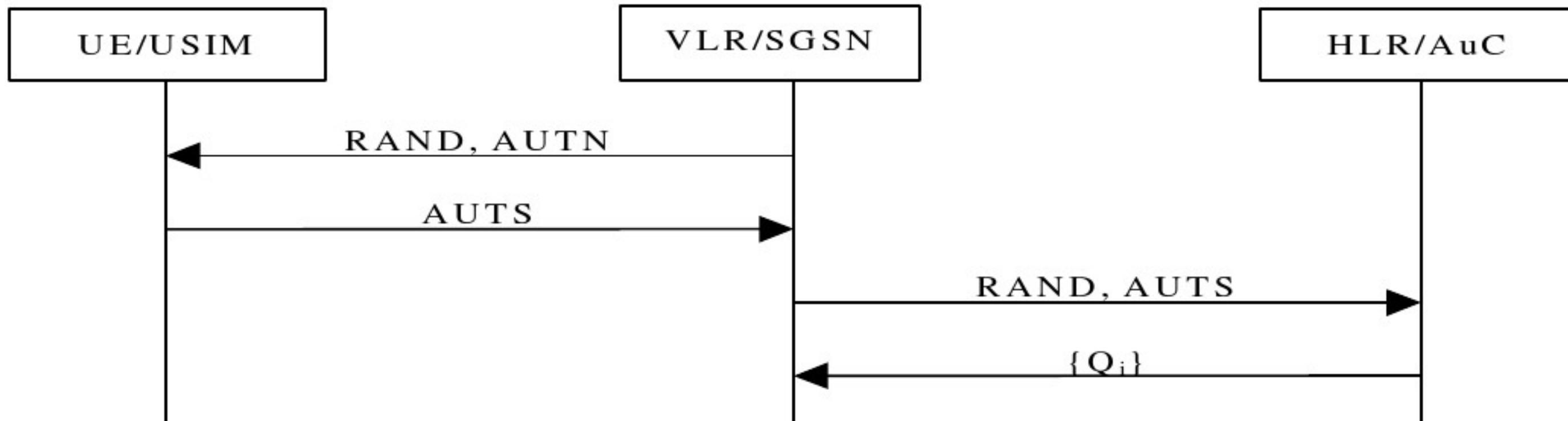


Verify $MAC = XMAC$

Verify that SQN is in the correct range

WCDMA鉴权之再同步过程

- 如果USIM认为SQN不在可用的范围内，则返回Synchronisation failure（同步失败），消息包含了AUTS参数
- HLR/AUC接到该请求后，完成以下操作：
- HLR/AUC验证AUTS，若AUTS被证明合法，则HLR/AUC将SQNHE的计数器值重置为与SQNMS相同。
- HLR/AUC发送鉴权数据响应并附带一些新的鉴权五元组给VLR/SGSN。（此时，为了减少HLR/AUC的计算负担，HLR/AUC可以只送一组鉴权向量给VLR/SGSN）。
- VLR/SGSN收到HLR/AUC送来的带有“同步失败标识”的鉴权数据响应后，将本地的旧的鉴权信息删除，MS也将根据这些新的鉴权参数进行鉴权。.



WCDMA对分割抑制标识

- 由于过长的**MAP**消息在传送过程中需要分割后才能传送，而鉴权五元组长**80**字节，若一次发送多个五元组可能造成过长的**MAP**消息，因此若**VLR/SGSN**发送的“鉴权数据请求”中包含有分割抑制标识（**Segmentation prohibited indicator**）时，**HLR/AUC**回送的“鉴权数据响应”会减少发送的鉴权五元组的个数，**VLR/SGSN**接着发送不带参数的鉴权数据请求以便接受未完的鉴权数据。

WCDMA之立即响应标识

- 当VLR/SGSN向HLR/AUC发送的“鉴权数据请求”中包含有立即响应标识（*Immediate response preferred indicator*）时，希望HLR/AUC能够立即给出响应。如果HLR的数据库中存有鉴权五元组，不论存有的鉴权组数是否满足VLR/SGSN的要求，HLR/AUC都将先发送这些鉴权五元组给VLR/SGSN。此时，返回给VLR/SGSN的鉴权数据可能少于VLR/SGSN所要求的组数。

WCDMA鉴权与GSM鉴权的兼容性

- 如果HLR和VLR/SGSN都是WCDMA，AuC将计算一些鉴权五元组，根据VLR\SGSN的要求下发五元组（但一次至多送5个）。作为临时签约数据，这些五元组有条件地存储在HLR和VLR/SGSN中。
- 如果HLR属于GSM，而VLR/SGSN属于WCDMA，则VLR/SGSN将从HLR传送过来的三元组中得出所需的五元组。其中，UTMS的五元组中的CK和IK可以从GSM中的Kc转换而来。
- 如果HLR是WCDMA，而VLR/SGSN属于GSM，HLR将首先计算出五元组，然后将五元组转换为三元组后，将三元组下发到VLR/SGSN。此时要求USIM也支持GSM的鉴权。

华为HLR/AUC特点

- 集成了HLR和AUC的功能
- 静态用户500万， 动态用户200万
- 兼容GSM和WCDMA网络鉴权
- 支持GSM多种鉴权算法， 包括XOR,COMP128-1,COMP128-2
- 支持WCDMA的MILENAGE鉴权算法
- 支持OP数据的加密性存贮
- 支持对“立即响应标识”的处理
- 不支持对”分割抑制标识”的处理
- 暂不支持对OPc数据的存储