[19] 中华人民共和国国家知识产权局

[12] 发明专利说明书

专利号 ZL 03141257.2

[51] Int. Cl.
H04Q 7/20 (2006.01)
H04Q 7/38 (2006.01)
H04Q 7/32 (2006.01)
H04L 9/32 (2006.01)
H04L 12/16 (2006.01)

[45] 授权公告日 2007 年 1 月 24 日

[11] 授权公告号 CN 1297155C

[22] 申请日 2003.6.10 [21] 申请号 03141257.2

[73] 专利权人 华为技术有限公司
地址 518057 广东省深圳市科技园科发路华为用服大厦
[72] 发明人 邹锋哨

[56] 参考文献
CN1259811A 2000.7.12 H04L9/14
WO02/078380A1 2002.10.3 H04Q7/38
WO00/02406A2 2000.1.13 H04Q7/38

审查员 赵 颖

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 宋志强 王 琦

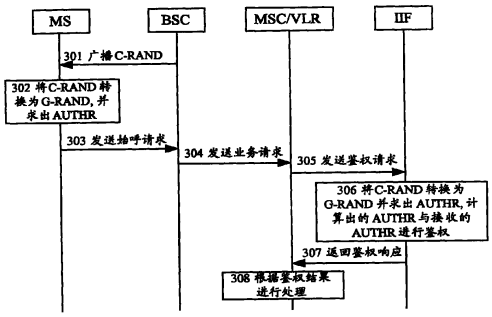
权利要求书 3 页 说明书 13 页 附图 3 页

[54] 发明名称

全球移动通信系统用户漫游到码分多址网络的鉴权方法

[57] 摘要

本发明公开了一种全球移动通信系统(GSM)用户漫游到码分多址(CDMA)网络的鉴权方法，该方法中，互通和互操作功能实体(IIF)保存需要漫游到 CDMA 网络的 GSM 用户移动台(MS)的身份密钥(Ki)；通过一定算法进行适配，将 CDMA 鉴权参数与 GSM 鉴权参数进行互相转换，使用 CDMA 鉴权流程和 GSM 的鉴权算法进行鉴权。 本发明的鉴权方法在开展 GSM 用户漫游到 CDMA 网络的新业务时，使用原有 GSM 用户的 SIM 卡进行鉴权，避免了运营商向 GSM 用户发放新的用户识别模块，同时，不需要修改现有的 GSM 网络设备和 CDMA 网络设备，实现简便，增强了业务的可运营性。



1、一种全球移动通信系统 GSM 用户漫游到码分多址 CDMA 网络的鉴权方法，其特征在于，该方法包括:

1）互通和互操作功能实体 IIF 保存需要漫游到 CDMA 网络的 GSM 用户移动台 MS 的身份密钥 Ki；CDMA 网络对 GSM 用户的鉴权方式包括：广播查询鉴权和独特查询鉴权，其中，

2）广播查询鉴权过程，包括以下步骤:

21）MS 接收 CDMA 的基站控制器 BSC 广播的 CDMA 鉴权随机数 C-RAND，将 C-RAND 转换为 GSM 鉴权随机数 G-RAND，再根据 G-RAND 和 MS 中保存的 Ki 计算出符号响应 SRES 和密钥 C Kc; 再将 SRES 转换为 CDMA 鉴权结果，发送给 BSC;

22）BSC 将 C-RAND 和 CDMA 鉴权结果发送给 CDMA 的移动交换中心 MSC/拜访位置寄存器 VLR;

23）MSC/VLR 向 IIF 发送包含 C-RAND 和 CDMA 鉴权结果的鉴权请求;

24）IIF 将收到的 C-RAND 转换为 G-RAND，再根据 G-RAND 和 IIF 中保存的该 MS 的 Ki 计算出 SRES 和 Kc；再将 SRES 转换为 CDMA 鉴权结果，将转换出的 CDMA 鉴权结果和收到的 CDMA 鉴权结果进行比较，完成广播查询鉴权;

3）独特查询鉴权过程，包括以下步骤:

31）CDMA 的 MSC/ VLR 为没有带鉴权参数的 GSM 的 MS 向 IIF 发送鉴权请求;

32）IIF 根据鉴权请求，生成 C-RAND，并转换为 G-RAND，再根据 G-RAND 和 IIF 中保存的该 MS 的 Ki 计算出 SRES 和 Kc；再将 SRES 转换为 CDMA 鉴权结果;

33）IIF 向 MSC/ VLR 返回包含 C-RAND 和 CDMA 鉴权结果的鉴权响应;

34）MSC/ VLR 保存 CDMA 鉴权结果，并通过 BSC 向 MS 发送包含 C-RAND

的独特查询鉴权请求;

35）MS 将收到的 C-RAND 转换为 G-RAND，再根据 G-RAND 和 MS 中保存的 Ki 计算出 SRES 和 Kc；再将 SRES 转换为 CDMA 鉴权结果，并将鉴权结果随鉴权响应通过 BSC 返回给 MSC/VLR;

36） MSC/VLR 将收到的 CDMA 鉴权结果和步骤 34）中保存的 CDMA 鉴权结果进行比较，完成独特查询鉴权。

2、如权利要求 1 所述的鉴权方法，其特征在于，所述的步骤 34）进一步包括：MSC/ VLR 收到 IIF 返回的鉴权响应后，先通过 BSC 指配业务信道，业务信道指配成功后，再发送独特查询鉴权请求。

3、如权利要求 2 所述的鉴权方法，其特征在于，所述的指配业务信道的方法为：MSC/ VLR 向 BSC 发送指配请求；BSC 根据该指配请求指配业务信道；并向 MSC/ VLR 返回指配响应。

4、如权利要求 1 所述的鉴权方法，其特征在于：步骤 21）-步骤 24）中所述的 CDMA 鉴权随机数为广播鉴权随机数; 步骤 32)-步骤 36)中所述的 CDMA 鉴权随机数为独特查询鉴权随机数。

5、如权利要求 1 所述的鉴权方法，其特征在于：所述的将 C-RAND 转换为 G-RAND 的方法为：将 C-RAND 进行运算后填入 G-RAND；或将 C-RAND 和国际移动用户识别码 IMSI 或/和电子序列号 ESN 进行运算后填入 G-RAND。

6、如权利要求 5 所述的鉴权方法，其特征在于：所述的将 C-RAND 转换为 G-RAND 的方法为：将 C-RAND 填入 G-RAND 的固定位置，将 G-RAND 剩余位置用预定数字或/和 IMSI 填满；或将 G-RAND 的剩余位置用预定数字或/和 ESN 填满。

7、如权利要求 1 所述的鉴权方法，其特征在于：所述的根据 G-RAND 和 MS 中保存的 Ki 计算出 SRES 和 Kc 的方法，与所述的根据 G-RAND 和 IIF 中保存的该 MS 的 Ki 计算出 SRES 和 Kc 的方法相同，为：用 G-RAND 和 Ki 通过 A3/A8 算法计算出 SRES 和 Kc。

8、如权利要求 1 所述的鉴权方法，其特征在于：所述的将 SRES 转换为 CDMA 鉴权结果的方法为：将在 SRES 的固定位置取出 CDMA 鉴权结果；或将 SRES 进行运算后，在固定位置取出 CDMA 鉴权结果；或将 SRES 和 Kc 或/和 IMSI 或/和 ESN 进行运算后，在固定位置取出 CDMA 鉴权结果。

全球移动通信系统用户漫游到码分多址网络的鉴权方法

技术领域

本发明涉及移动通信系统的鉴权技术，特别涉及一种全球移动通信系统（GSM）用户漫游到码分多址（CDMA）网络的鉴权方法。

背景技术

在移动通信系统中，移动台要接入系统，首先要进行鉴权，通过鉴权的合法用户才能接入网络。

其中,GSM 网络对 GSM 用户的鉴权，包括通用鉴权算法 A3/A8 以及对 MS 和网络唯一的参数身份密钥（Ki）；当 SIM 卡生成时，将生成 Ki 并写在卡中；在 HLR/AuC 中对 GSM 用户开户时，需保存与 SIM 卡中保存相同的 Ki；Ki 不能通过空口传递。

网络侧通过以下步骤对 MS 进行鉴权:

1、HLR/AuC 将生成随机数 RAND，并根据 Ki 和 RAND 经过 A3/A8 算法计算出符号响应（SRES）和密钥 C（Kc）；

2、网络侧通过鉴权请求消息，将随机数 RAND 发送给 MS;

3、MS 收到 RAND 后，同样根据 RAND 和 Ki 经过 A3/A8 算法计算出 SRES 和 Kc，并将 SRES 返回给网络侧，Kc 不需要在空口传递;

SRES = A3 (RAND，Ki)；Kc = A8 (RAND，Ki);

其中 SRES 为 32 位(bit)，Kc 为 64 位(bit)，RAND 为 128 位(bit)，Ki 为 32 位(bit)。

4、网络侧收到 MS 发送的 SRES 后，将其与自身计算的 SRES 进行比较，相同则 MS 为合法用户，否则非法。

另外，CDMA 网络对 CDMA 用户鉴权的方法，包括一个通用的用户鉴

权与语音加密算法（CAVE）以及对移动台（MS）和网络唯一的参数鉴权密钥（AKey）；当 R-UIM 卡生成时，生成 AKey 并写在卡中；在 HLR/AC 中对 CDMA 用户开户时，需保存与 R-UIM 卡中保存相同的 AKey；通过共享加密数据（SSD）更新流程，可根据 AKey 和鉴权随机数（RANDSSD）生成 SSD，而 SSD 是 CDMA 鉴权最重要的参数之一，只能动态生成。AKey 和 SSD 不能通过空口传递。

当用户第一次接入系统时，必须首先进行 SSD 更新，以保证 HLR/AC 与 R-UIM 卡中的 SSD 保持一致；否则，鉴权将无法成功；

在 SSD 更新成功之后，用户再次接入系统时，网络需对用户进行鉴权；由于 HLR/AC 与 R-UIM 卡中的鉴权参数完全一致，经过同样的算法，应能计算出相同的结果；否则，表明该用户为非法用户。

网络对用户的鉴权有两种方式：

一种是广播查询鉴权，该方式要求基站（BS）系统支持广播查询鉴权，其对 MS 进行鉴权的过程为：

1、网络侧通过控制/寻呼信道向本小区下所有 MS 周期性地广播 RAND。

2、 MS 需要接入系统时，如位置登记、始呼、寻呼响应等，使用当前控制/寻呼信道上 RAND 计算鉴权结果（AUTHR），并在初始接入消息中发送给网络侧。

3、网络侧根据 RAND 计算出 AUTHR，并与 MS 发送上来的 AUTHR 进行比较，相同则 MS 为合法用户，否则非法。

网络侧计算 AUTHR 的算法与 MS 计算 AUTHR 的算法相同，为：

AUTHR = CAVE(RAND，SSD_A，ESN，AUTHDATA)；其中 AUTHR 为 18 位(bit)，RAND 为 32 位(bit)，SSD_A 为 SSD 前 64 位(bit)，ESN 为电子序列号，AUTHDATA 为鉴权数据，接入类型不同时使用的数据也不同，如在呼叫时根据移动识别号码 (MIN)与被叫号码计算，在位置登记或寻呼响应时则仅根据 MIN 计算。

另一种是独特查询鉴权方式，用该方式对 MS 进行鉴权的过程为：

1、网络侧生成独特查询随机数（RANDU），并用该 RANDU 计算出该用户的鉴权结果（AUTHU）；并将向 MS 发送独特查询随机数（RANDU）。

2、MS 收到 RANDU 后也根据 RANDU 计算 AUTHU 并返回给网络侧。

3、最后，网络侧将自身计算的 AUTHU 与 MS 发送的 AUTHU 进行比较，相同则 MS 为合法用户，否则非法。

这种鉴权方式可由 MSC 在控制信道或业务信道上发起；其算法如下：

AUTHU = CAVE (RANDU，SSD_A， ESN，MIN)；其中 AUTHU 为 18 位(bit)，RANDU 为 32 位(bit)，SSD_A 为 SSD 前 64 位(bit)， ESN 为电子序列号，MIN 为移动识别号码。

目前，通过网络侧增加一个互通和互操作功能实体（IIF）可以支持 GSM 注册用户使用 CDMA 网络中的业务以及 CDMA 注册用户使用 GSM 网络中的业务，IIF 主要完成 GSM 网络和 CDMA 网络之间的互通和互操作功能；参见图 1，图 1 为 IIF 与 GSM 网络和 CDMA 网络的连接结构示意图。

其中，CDMA 的美国国家标准学会 41 系列协议（ANSI-41）核心网 110 中，CDMA 鉴权中心（AC）111 通过 H 接口与归属位置寄存器（HLR）113 相连，短消息中心（MC）112 通过 N 接口与 HLR 相连，MC112、HLR113、访问位置寄存器（VLR）114、移动交换中心（MSC）115 分别通过 Q 接口、D 接口、D 接口、和 E 接口与 IIF 相连。

GSM 移动应用部分（MAP）核心网 130 中，GSM 短消息业务中心（SMS-SC）132 与 GSM 短消息业务-互通 MSC（SMS-IWMSC）131、GSM 短消息业务-关口 MSC（SMS-GMSC）133 分别相连，GSM 鉴权中心（AuC）135 通过 H 接口与 HLR134 相连，SMS-IWMS131、CSMS-GMSC133、HLR134、VLR136、MSC137、服务 GPRS 支持节点（SGSN）138 分别通过 E 接口、E 接口、D 接口、D 接口、E 接口、Gr 接口与 IIF 相连。

IIF120 处于 GSM MAP 核心网和 ANSI-41 核心网之间，执行 ANSI-41

信令和 GSM MAP 信令的转换。

当 GSM 注册用户使用双模终端漫游到 CDMA 网络，称 GSM 注册用户处于 CDMA 外地模式；此时，对于 CDMA 网络，IIF 可看作该 GSM 注册用户的 CDMA HLR；而对于 GSM 网络，IIF 可看作为服务于这个 GSM 注册用户的 GSM VLR。

处于 CDMA 外地模式的 GSM 用户需要被 CDMA 网络鉴权，鉴权成功后，GSM 用户才被允许接入 CDMA 网络，获得使用网络资源的权利。对于允许 GSM 用户使用 CDMA 网络资源的业务，鉴权是最关键的设计之一。

上述的 GSM 网络鉴权方法和 CDMA 网络鉴权方法，在 GSM 网络通过 IIF 与 CDMA 网络连接时，都不能对漫游到 CDMA 网络的 GSM 用户进行鉴权。因此，出现了 GSM 用户漫游到 CDMA 网络的鉴权方法，该方法为：

由于 IIF 具备 CDMA HLR 功能，所以，需在 IIF 或 AC 上需注册 GSM 用户的 CDMA 鉴权签约数据 A-Key，一般通过在 GSM 终端上插入标准 CDMA R-UIM 卡，或在终端使用能同时存储 Ki 和 A-Key 的新类型双模卡来实现。这样，CDMA 外地模式下的 GSM 用户使用 CDMA 标准鉴权流程，包括 SSD 更新和鉴权；鉴权过程中不需要与归属网络 GSM HLR 参与交互。

参见图 2，图 2 为现有技术 GSM 用户漫游到 CDMA 网络鉴权的流程示意图。GSM 用户终端插入了 CDMA R-UIM 卡，该用户同时也是 CDMA 用户。在 HLR/AC 中对 CDMA 用户开户时，保存与 R-UIM 卡中保存相同的 AKey；通过 SSD 更新流程，可根据 AKey 和 RAND 生成 SSD。当用户第一次接入系统时，必须首先进行 SSD 更新，以保证 HLR/AC 与 R-UIM 卡中的 SSD 保持一致。这样，GSM 用户漫游到 CDMA 网络时鉴权的基本流程包括以下步骤：

步骤 201，MS 根据 SSD 和 RAND 计算 AUTHR；

步骤 202，MS 将 AUTHR 发送给 CDMA 网络的 MSC/VLR；

步骤 203， MSC/VLR 向 IIF 发送鉴权请求（AUTHREQ）消息；

步骤 204，IIF 收到鉴权请求消息后，向 CDMA 网络的 AC 转发鉴权请求；

步骤 205，CDMA 网络的 AC 根据 SSD、RAND 计算 AUTHR，并与 IIF 送上来的 AUTHR 进行比较；若不相同，则表明为非法用户，否则为合法用户；

步骤 206，CDMA 网络的 AC 向 IIF 返回包含鉴权结果的鉴权响应（authreq）消息；

步骤 207，IIF 将鉴权结果转发给 CDMA 网络的 MSC/VLR；

步骤 208，MSC/VLR 根据鉴权结果进行处理，将合法用户接入，非法用户清除。

上述 GSM 用户漫游到 CDMA 网络的鉴权方法中，需要在 GSM 终端上发放新用户识别模块，一般通过在 GSM 终端上插入标准 CDMA R-UIM 卡，或在终端使用能同时存储 Ki 和 A-Key 的新类型双模卡来实现。因此，运营商需要再次发放用户识别模块给申请了漫游到 CDMA 网功能的 GSM 用户。这种使用户享受新业务的业务分发方式比较复杂，需要用户配合，不利于业务的推广。

发明内容

有鉴于此，本发明的目的在于提供一种全球移动通信系统（GSM）用户漫游到码分多址（CDMA）网络的鉴权方法，在开展GSM用户漫游到CDMA网络的新业务时，避免运营商向GSM用户发放新的用户识别模块，增强业务的可运营性。

为达到上述目的，本发明的技术方案具体是这样实现的：

一种全球移动通信系统（GSM）用户漫游到码分多址（CDMA）网络的鉴权方法，该方法包括：

1）互通和互操作功能实体（IIF）保存需要漫游到 CDMA 网络的 GSM 用户移动台（MS）的身份密钥（Ki）；CDMA 网络对 GSM 用户的鉴权方式包括：广播查询鉴权和独特查询鉴权，其中，

2）广播查询鉴权过程，包括以下步骤：

21）MS 接收 CDMA 的基站控制器（BSC）广播的 CDMA 鉴权随机数（C-RAND），将该鉴权随机数（C-RAND）转换为 GSM 鉴权随机数（G-RAND），再根据 G-RAND 和 MS 中保存的 Ki 计算出符号响应（SRES）和密钥 C（Kc）；再将 SRES 转换为 CDMA 鉴权结果，发送给 BSC；

22）BSC 将鉴权随机数（C-RAND）和 CDMA 鉴权结果发送给 CDMA 的移动交换中心（MSC）/拜访位置寄存器（VLR）；

23）MSC/VLR 向 IIF 发送包含鉴权随机数（C-RAND）和 CDMA 鉴权结果的鉴权请求；

24）IIF 将收到的鉴权随机数（C-RAND）转换为 GSM 鉴权随机数（G-RAND），再根据 G-RAND 和 IIF 中保存的该 MS 的 Ki 计算出 SRES 和 Kc；再将 SRES 转换为 CDMA 鉴权结果，将转换出的 CDMA 鉴权结果和收到的 CDMA 鉴权结果进行比较，完成广播查询鉴权；

3）独特查询鉴权过程，包括以下步骤：

31）CDMA 的 MSC/ VLR 为没有带鉴权参数的 GSM 的 MS 向 IIF 发送鉴权请求；

32）IIF 根据鉴权请求，生成鉴权随机数（C-RAND），并转换为 GSM 鉴权随机数（G-RAND），再根据 G-RAND 和 IIF 中保存的该 MS 的 Ki 计算出 SRES 和 Kc；再将 SRES 转换为 CDMA 鉴权结果；

33）IIF 向 MSC/ VLR 返回包含鉴权随机数（C-RAND）和 CDMA 鉴权结果的鉴权响应；

34）MSC/ VLR 保存 CDMA 鉴权结果，并通过 BSC 向 MS 发送包含鉴权随机数（C-RAND）的独特查询鉴权请求；

35）MS 将收到的鉴权随机数（C-RAND）转换为 GSM 鉴权随机数（G-RAND），再根据 G-RAND 和 MS 中保存的 Ki 计算出 SRES 和 Kc；再将 SRES 转换为 CDMA 鉴权结果，并将鉴权结果随鉴权响应通过 BSC 返回给

MSC/VLR;

36） MSC/VLR 将收到的 CDMA 鉴权结果和步骤 34）中保存的 CDMA 鉴权结果进行比较，完成独特查询鉴权。

其中，所述的步骤 34）可以进一步包括：MSC/ VLR 收到 IIF 返回的鉴权响应后，先通过 BSC 指配业务信道，业务信道指配成功后，再发送独特查询鉴权请求。

所述的指配业务信道的方法可以为：MSC/ VLR 向 BSC 发送指配请求；BSC 根据该指配请求指配业务信道；并向 MSC/ VLR 返回指配响应。

步骤 21）-步骤 24）中所述的 CDMA 鉴权随机数可以为广播鉴权随机数；步骤 32）-步骤 36）中所述的 CDMA 鉴权随机数可以为独特查询鉴权随机数。

所述的将 C-RAND 转换为 G-RAND 的方法可以为：将 C-RAND 进行运算后填入 G-RAND；或将 C-RAND 和国际移动用户识别码（IMSI）或/和电子序列号（ESN）进行运算后填入 G-RAND。例如，该方法可以为：将 C-RAND 填入 G-RAND 的固定位置，将 G-RAND 剩余位置用预定数字或/和国际移动用户识别码（IMSI）填满；或将 G-RAND 的剩余位置用预定数字或/和电子序列号（ESN）填满。

所述的根据 G-RAND 和 MS 中保存的 Ki 计算出 RES 和 Kc 的方法，可以与所述的根据 G-RAND 和 IIF 中保存的该 MS 的 Ki 计算出 SRES 和 Kc 的方法相同，为：用 G-RAND 和 Ki 通过 A3/A8 算法计算出 SRES 和 Kc。

所述的将 SRES 转换为 CDMA 鉴权结果的方法可以为：将在 SRES 的固定位置取出 CDMA 鉴权结果；或将 SRES 进行运算后，在固定位置取出 CDMA 鉴权结果；或将 SRES 和 Kc 或/和国际移动用户识别码（IMSI）或/和电子序列号（ESN）进行运算后，在固定位置取出 CDMA 鉴权结果。

由本发明的技术方案可见，本发明的这种全球移动通信系统（GSM）用户漫游到码分多址（CDMA）网络的鉴权方法在开展GSM用户漫游到CDMA网络的新业务时，使用原有GSM用户的SIM卡进行鉴权，避免了运营商向GSM用户

发放新的用户识别模块，同时，不需要修改现有的GSM网络设备和CDMA网络设备，实现简便，增强了业务的可运营性。

附图说明

图 1 为 IIF 与 GSM 网络和 CDMA 网络的连接结构示意图；

图 2 为现有技术 GSM 用户漫游到 CDMA 网络鉴权的流程示意图；

图 3 为本发明第一较佳实施例的广播鉴权流程示意图；

图 4 为图 3 所示实施例中 MS 生成 AUTHR 的示意图；

图 5 为本发明第二较佳实施例的独特查询鉴权流程示意图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明进一步详细说明。

本发明是根据 GSM 网络鉴权参数与 CDMA 网络鉴权参数比较的结果，通过一定算法进行适配，将CDMA 鉴权参数与 GSM 鉴权参数进行互相转换，进行鉴权。

参见表一，表一 GSM 网络鉴权参数与 CDMA 网络鉴权参数比较。

		GSM	CDMA
随机数	标识	RAND	RANDU
	长度	128 位(bit)	32 位(bit)
鉴权结果	标识	SRES，注：Kc 不需要传递	AUTHU
	长度	32 位(bit)	18 位(bit)

表 一

由表一可见，若使用 CDMA 鉴权流程，无法完全承载 GSM 鉴权参数；因此，可考虑通过一定算法进行适配，通过算法 Fa 将 CDMA 的 32bit 的 RAND 或 RANDU（简称 C-RAND）转换为 128bitRAND（简称 G-RAND）；并通过算法 Fb 将 GSM 的 32bitSRES 转换为 CDMA 的 18bit 的 AUTHR 或

AUTHU（简称 C-AUTH）；对应关系表示如下：

G-RAND = Fa(C-RAND)

C-AUTH = Fb(SRES)

算法 Fa 和 Fb 还可以用户信息作为入参，如 MIN、ESN、被叫号码中某几个字节（无被叫号码时可用全 1 表示），但不仅限于这几个参数；

其中，算法 Fa 可以将 C-RAND 进行运算后填入 G-RAND；或将 C-RAND 和国际移动用户识别码（IMSI）或/和电子序列号（ESN）进行运算后填入 G-RAND。

例如：将 C-RAND 填入 G-RAND 的固定位置，将 G-RAND 剩余位置用预定数字或/和国际移动用户识别码（IMSI）填满；或将 G-RAND 的剩余位置用预定数字或/和电子序列号（ESN）填满。

算法 Fb 可以将在 SRES 的固定位置取出 CDMA 鉴权结果；或将 SRES 进行运算后，在固定位置取出 CDMA 鉴权结果；或将 SRES 和 Kc 或/和国际移动用户识别码（IMSI）或/和电子序列号（ESN）进行运算后，在固定位置取出 CDMA 鉴权结果。

本发明中，IIF 作为 GSM 注册用户在 CDMA 外地模式下的 HLR/AC，其中保存 Ki 和鉴权算法 A3/A8。在 IIF 中对需要漫游到 CDMA 网络的 GSM 用户开户时，将国际移动用户识别码（IMSI）和 Ki 的关系保存在 IIF 的数据库中。

本发明的鉴权方法包括：广播查询鉴权过程和独特查询鉴权过程。以下对两个鉴权过程分别举一个较佳实施例进行详细说明。

第一较佳实施例为一个广播查询鉴权始呼流程。本实施例在鉴权流程上与普通 CDMA 广播鉴权流程没有差别，但在鉴权算法上采用 GSM 的鉴权算法，并新增了 Fa 和 Fb 两个函数。参见图 3，图 3 为本发明第一较佳实施例的广播鉴权流程示意图；该流程包括以下步骤：

步骤 301，BSC 通过寻呼/控制信道广播广播鉴权随机数 C-RAND。

步骤 302，MS 对于收到的 C-RAND 先通过算法 Fa 将 C-RAND 转换为

G-RAND，并用 G-RAND 和 MS 保存的 Ki 通过 MS 的 SIM 卡中 A3/A8 算法计算出 SRES 和 Kc，然后用算法 Fb 将 SRES 转换为鉴权结果 AUTHR。

步骤 303，MS 向 BSC 发送包含 AUTHR 的始呼请求。

步骤 304，BSC 收到始呼请求后，向 MSC/VLR 发送业务请求（CM Service Request），其中包含 C-RAND 和 AUTHR。

步骤 305，MSC/VLR 收到业务请求后，向 IIF 发送鉴权请求 AUTHREQ，其中包含 C-RAND 和 AUTHR。

步骤 306，IIF 收到鉴权请求消息后，首先通过 Fa 算法将 C-RAND 转换为 G-RAND，并用 G-RAND 和 IIF 中保存的该 MS 的 Ki 通过 A3/A8 算法计算出 SRES 和 Kc，然后通过算法 Fb 将 SRES 转换为 AUTHR，并比较计算出来的 AUTHR 与 MSC/VLR 在鉴权请求中送上来的 AUTHR 是否相等；若相等，则表明为合法用户，允许接入；否则，为非法用户，拒绝接入。

步骤 307，IIF 向 MSC/VLR 返回包含是否允许用户接入信息的鉴权响应（authreq）。

步骤 308，MSC/VLR 收到鉴权响应消息后，根据是否允许用户接入信息继续呼叫处理或清除呼叫。

其中，步骤 302 是 MS 生成 AUTHR 的过程；步骤 306 中包含了 IIF 生成 AUTHR 的过程。图 4 为图 3 所示实施例中 MS 生成 AUTHR 的示意图；其包含三个算法：先在 MS 中的移动设备（ME）中通过算法 Fa 将 32 位的 C-RAND 转换为 128 位的 G –RAND、然后用该 G –RAND 和 Ki 通过 SIM 卡中的算法 A3/A8 计算出 32 位和 Kc、最后在 ME 中通过算法 Fb 将 32 位的 SRES 转换为 18 位的 AUTHR。IIF 中生成 AUTHR 的算法与图 4 所示相同，只是所用的 Ki 和 A3/A8 算法是预先存储在 IIF 中的。

本实施例中 Fa 采用了一种较简单的算法：将 C-RAND 填入 G-RAND 前 32 位，G-RAND 其他位可填写为全 1。Fb 的算法也比较简单：从 32 位的 SRES 中，取出前 18 位作为 AUTHR。在实际应用中，算法 Fa、Fb 可以将

MIN、ESN、被叫号码中某几个字节（无被叫号码时可用全 1 表示）作为入参，使用较复杂的算法进行转换。

本实施例为始呼流程，位置登记、寻呼响应的鉴权处理流程与此类似。

第二较佳实施例为一个独特查询鉴权始呼流程。本实施例在鉴权流程上与普通 CDMA 独特鉴权流程没有差别，但在鉴权算法上采用 GSM 的鉴权算法，并新增了 Fa 和 Fb 两个函数。参见图 5，图 5 为本发明第二较佳实施例的独特鉴权流程示意图；该流程包括以下步骤：

步骤 501，MS 接入，且未带鉴权参数，MSC/VLR 为该 MS 向 IIF 发送鉴权请求（AUTHREQ）。

步骤 502，IIF 收到鉴权请求消息后，发现无鉴权参数，则生成随机数 RANDU（C-RAND），并通过 Fa 算法将 C-RAND 转换为 G-RAND，用 G-RAND 和 IIF 中保存的该 MS 的 Ki 通过 A3/A8 算法计算出 SRES 和 Kc；再通过 Fb 算法将 SRES 转换为 CDMA 鉴权结果（AUTHU）。

步骤 503，IIF 向 MSC/VLR 返回鉴权响应（authreq），其中包含 RANDU、AUTHU，指示 MSC/VLR 发起独特查询鉴权；

步骤 504，MSC/VLR 收到鉴权响应消息后，发现包含 RANDU 和 AUTHU，则保存 AUTHU。

步骤 505，MSC/VLR 向 BSC 发送指配请求（Assignment Request）指配业务信道

步骤 506，BSC 收到指配请求后，指配业务信道，并返回指配响应（Assignment Response）；

步骤 507，业务信道指配成功之后，MSC/VLR 向 BSC 发送独特查询鉴权请求（Authentication Request），其中包含 RANDU。

步骤 508，BSC 将收到的独特查询鉴权请求（Authentication Request）发送给 MS。

步骤 509，MS 收到独特查询鉴权请求消息后，获得随机数 RANDU

（C-RAND），并通过算法 Fa 将 C-RAND 转换为 G-RAND，并通过 SIM 卡中 A3/A8 算法计算出 SRES 和 Kc,然后通过算法 Fb 将 SRES 转换为 AUTHU。

步骤 510，MS 向 BSC 返回独特鉴权响应，其中包含 AUTHU。

步骤 511，BSC 将收到的包含 AUTHU 的独特查询鉴权响应返回给 MSC/VLR。

步骤 512，MSC/VLR 收到独特查询鉴权请求响应后，获得 AUTHU，并与在步骤 504）保存的 AUTHU 进行比较，判断结果是否一致，若一致，则表明为合法用户；否则，为非法用户。

步骤 513，MSC/VLR 将判断结果通过鉴权状态报告（ASREPORT）上报给 IIF。

步骤 514，IIF 收到鉴权状态报告后，根据判断结果决定是否允许用户接入，并将包含是否允许接入信息的鉴权状态报告响应（asreport）中返回给 MSC/VLR。

步骤 515，MSC/VLR 收到鉴权状态报告响应消息后，根据是否允许接入信息继续接入处理或清除用户接入。

其中，步骤 502 是 IIF 生成 AUTHU 的过程；步骤 509 是 MS 生成 AUTHU 的过程。本实施例中，步骤 509 的 MS 生成 AUTHU 的过程，与图 3 中步骤 302 的 MS 生成 AUTHR 的过程相同；步骤 502 中 IIF 生成 AUTHU 的过程，与图 3 中步骤 306 的 IIF 生成 AUTHR 的过程相同；算法 Fa 和 Fb 也可以与第一较佳实施例相同。

本实施例为始呼流程，寻呼响应的鉴权处理流程与此相似。

上述两个实施例中，对于漫游到 CDMA 网络的 GSM 用户，IIF 禁止进行 SSD 更新操作。

另外，本发明还可以有以下的实施方法：和上述两个实施例相同，首先，IIF 中保存需要漫游到 CDMA 网络的 GSM 用户移动台（MS）的身份密钥（Ki），IIF 也具备执行 GSM A3/A8 算法运算的能力。然后，在 SSD 更

新流程中，利用 Ki 产生 SSD。最后，在广播查询鉴权和独特查询鉴权流程中，GSM 的 MS 象一个普通 CDMA 终端一样被 CMSC 或 AuC 鉴权。

其中，利用 Ki 产生 SSD 的方法与上述两个鉴权流程中，利用 Ki 产生 AUTHR 或 AUTHU 的方法相似。

利用 Ki 产生 SSD 的过程包括以下步骤：

1、IIF 产生随机数 RANDSSD，并通过 Fa 算法转换为 G-RAND，用 G-RAND 和 IIF 中保存的进行 SSD 更新的 GSM MS 的 Ki，通过 A3/A8 算法计算出 SRES 和 Kc；再通过 Fb 算法将 SRES 转换为 SSD。

2、IIF 将 RANDSSD 通过 CDMA 的 MSC/VLR 发送给 GSM 的 MS。

3、GSM 的 MS 用通过算法 Fa 将 RANDSSD 转换为 G-RAND，并通过 SIM 卡中 A3/A8 算法计算出 SRES 和 Kc,然后通过算法 Fb 将 SRES 转换为 SSD。

4、GSM 的 MS 产生确认 SSD 更新信息通过 CDMA 的 MSC/VLR 发送给 IIF。

这样，GSM 的 MS 就可以象一个普通 CDMA 终端一样用 SSD 参数，被 CMSC 或 AuC 鉴权了。

由上述三个实施例可见，本发明的这种全球移动通信系统（GSM）用户漫游到码分多址（CDMA）网络的鉴权方法在开展 GSM 用户漫游到 CDMA 网络这个新业务时，不针对 GSM 外地模式用户增加新鉴权流程，不更换或修改 GSM 用户识别模块 SIM，使用原有 GSM 用户的 SIM 卡进行鉴权，避免了运营商向 GSM 用户发放新的用户识别模块，同时，不需要修改现有的 GSM 网络设备和 CDMA 网络设备，实现简便，增强了业务的可运营性。

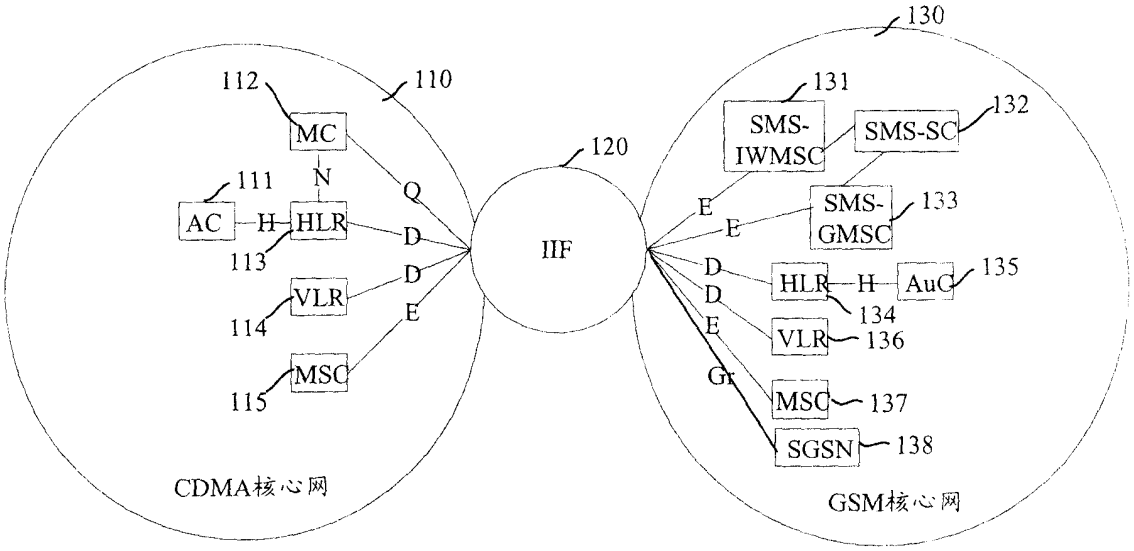

130
112
110
131
MC
SMS-IWMSC
SMS-SC
132
120
N
111
Q
E
AC
H
HLR
D
IIF
SMS-GMSC
133
E
113
D
D
HLR
H
AuC
135
VLR
134
E
VLR
136
Gr
MSC
137
115
SGSN
138
CDMA核心网
GSM核心网

图 1

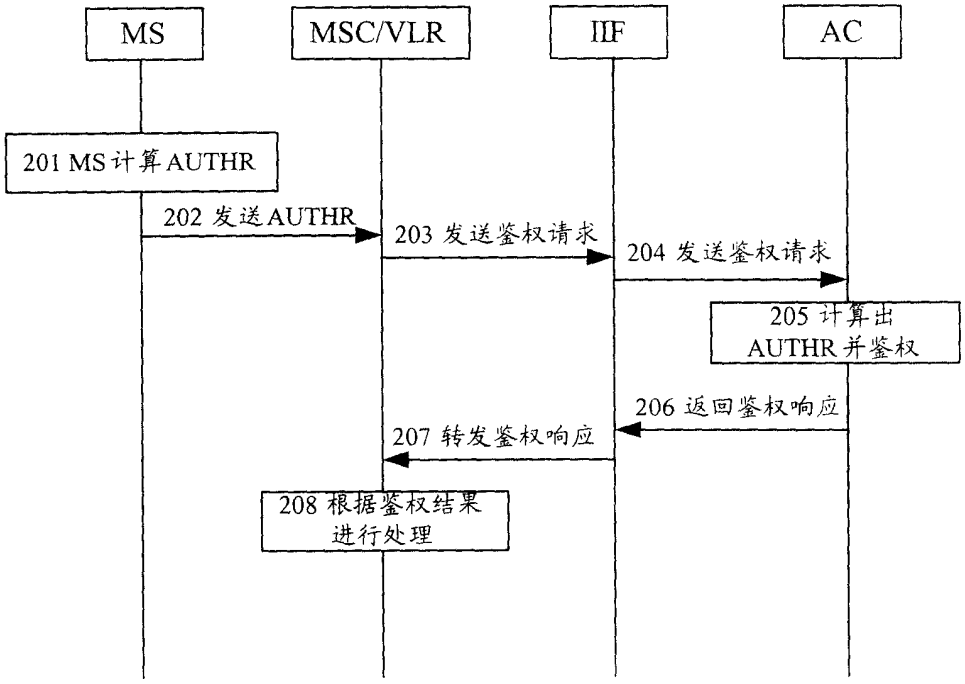

MS
MSC/VLR
IIF
AC
201 MS计算AUTHR
202 发送AUTHR
203 发送鉴权请求
204 发送鉴权请求
205 计算出AUTHR并鉴权
206 返回鉴权响应
207 转发鉴权响应
208 根据鉴权结果进行处理

图 2

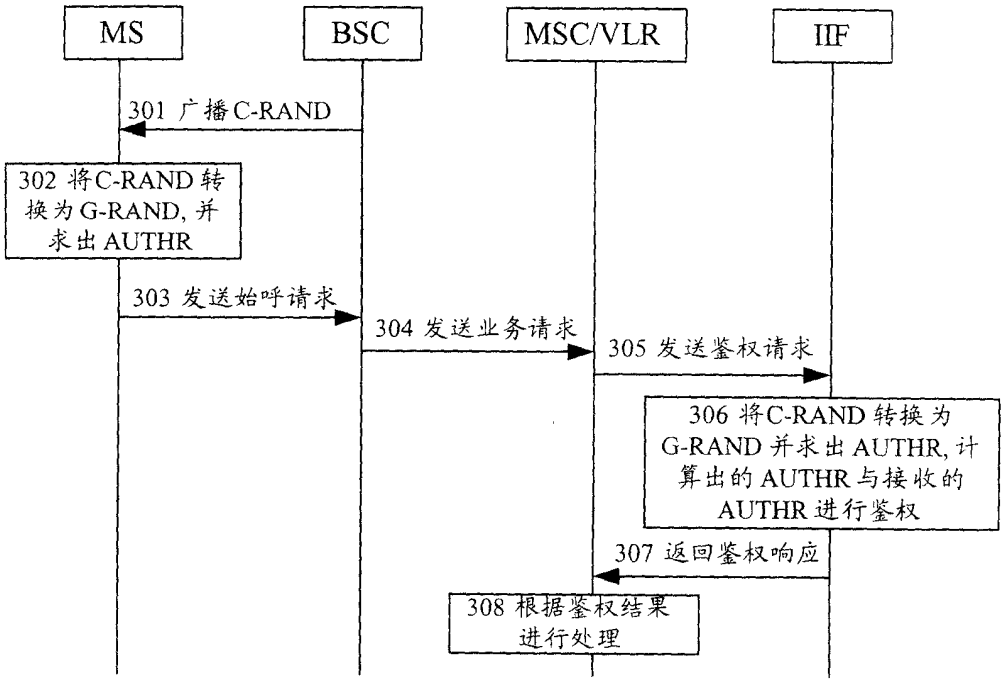

MS
BSC
MSC/VLR
IIF
301 广播C-RAND
302 将C-RAND转换为G-RAND, 并求出AUTHR
303 发送始呼请求
304 发送业务请求
305 发送鉴权请求
306 将C-RAND转换为G-RAND并求出AUTHR, 计算出的AUTHR与接收的AUTHR进行鉴权
307 返回鉴权响应
308 根据鉴权结果进行处理

图 3

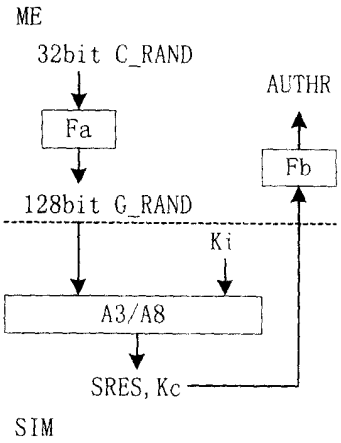

ME
32bit C_RAND
Fa
128bit C_RAND
Ki
A3/A8
SRES, Kc
SIM
AUTHR
Fb

图 4

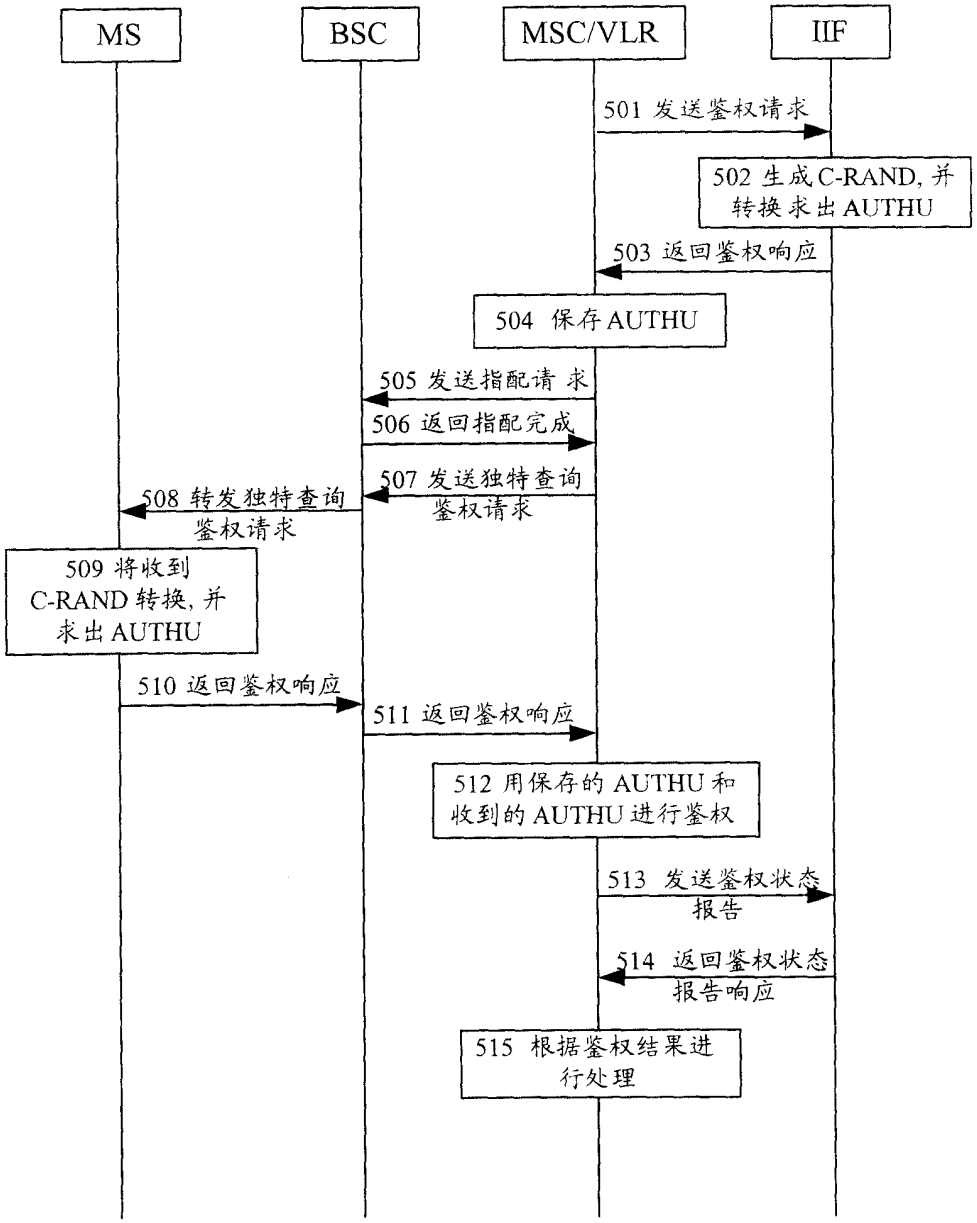

MS
BSC
MSC/VLR
IIF
501 发送鉴权请求
502 生成C-RAND, 并转换求出AUTHU
503 返回鉴权响应
504 保存AUTHU
505 发送指配请 求
506 返回指配完成
507 发送独特查询鉴权请求
508 转发独特查询鉴权请求
509 将收到C-RAND转换, 并求出AUTHU
510 返回鉴权响应
511 返回鉴权响应
512 用保存的AUTHU和收到的AUTHU进行鉴权
513 发送鉴权状态报告
514 返回鉴权状态报告响应
515 根据鉴权结果进行处理

图 5