

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 9/32 (2006.01)

H04Q 7/38 (2006.01)



[12] 发明专利说明书

专利号 ZL 200410084842.6

[45] 授权公告日 2008 年 4 月 23 日

[11] 授权公告号 CN 100384120C

[22] 申请日 2004.9.30

[21] 申请号 200410084842.6

[73] 专利权人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

[72] 发明人 谢红 王金城 朱东铭 顾炯炯

[56] 参考文献

WO03/084257A1 2003.10.9

US2004/0153667A1 2004.8.5

CN1430835A 2003.7.16

US2003/0200433A1 2003.10.23

WO03/105436A1 2003.12.18

CN1474586A 2004.2.11

3GPP TS 33.102 v5.4.0. 3GPP, 全文.

2004

3GPP2 S. R0086 - A, Version: 1.0 IMS Security Framework. 3GPP2, 全文. 2004

审查员 江红

[74] 专利代理机构 北京德琦知识产权代理有限公司

代理人 王琦 程殿军

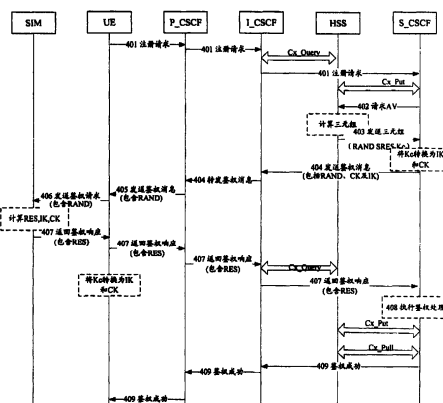
权利要求书 3 页 说明书 12 页 附图 7 页

[54] 发明名称

IP 多媒体子系统中对终端用户标识模块进行鉴权的方法

[57] 摘要

本发明公开了一种在 IP 多媒体子系统中对终端用户标识模块进行鉴权的方法，该方法首先由 IMS 系统在收到 UE 发送来的注册请求后，确定针对该 UE 的三元组鉴权向量，所述三元组鉴权向量至少包含 RAND 和 SRES，保留三元组中的 SRES，并将 RAND 下发到 UE；UE 将所述 RAND 传送到自身的终端用户标识模块；终端用户标识模块计算 RES，并将 RES 通过 UE 返回给 IMS 系统；IMS 系统判断 UE 返回的 RES 是否与自身保存的 SRES 相等，如果是，则鉴权通过，否则，鉴权失败。本发明方案解决了现有技术中必须通过 ISIM 才能实现鉴权的问题。通过本发明方案实现了在 IMS 系统中通过 SIM 及 USIM 模块等对 UE 的鉴权，大大降低了 IM 业务的推广难度，且对现有网络的改动很小。



1、一种在 IP 多媒体子系统中对终端用户标识模块进行鉴权的方法，其特征在于，该方法包括以下步骤：

a. IP 多媒体子系统 IMS 在收到移动终端 UE 发送来的注册请求后，由所述 IMS 系统中的归属用户服务器 HSS 或服务-呼叫状态控制功能 S-CSCF 确定针对该 UE 的三元组鉴权向量，所述三元组鉴权向量至少包含随机数 RAND 和符号响应 SRES，保留三元组中的 SRES，并将 RAND 下发到 UE；

b. UE 将所述 RAND 传送到自身的终端用户标识模块；其中，所述终端用户标识模块为 SIM 模块或 USIM 模块；

c. 终端用户标识模块根据 RAND 计算 RES，并将 RES 通过 UE 返回给 IMS 系统；

d. IMS 系统中的 S-CSCF 判断 UE 返回的 RES 是否与自身保存的 SRES 相等，如果是，则鉴权通过，否则，鉴权失败。

2、根据权利要求 1 所述的方法，其特征在于，所述步骤 a 中，所述 IMS 系统确定针对 UE 的三元组鉴权向量包括：S-CSCF 判断自身是否存有针对该 UE 的三元组鉴权向量，如果是，则执行后续步骤；否则，

向 HSS 请求针对该 UE 的三元组鉴权向量；HSS 在收到 S-CSCF 发送来的鉴权向量请求后，确定针对该 UE 的三元组鉴权向量，并发送给 S-CSCF。

3、根据权利要求 2 所述的方法，其特征在于，当所述 UE 中的终端用户标识模块为用户标识模块 SIM 时，所述 HSS 直接确定针对该 UE 中 SIM 模块的三元组鉴权向量。

4、根据权利要求 2 所述的方法，其特征在于，当所述 UE 中的终端用户标识模块为用户服务标识模块 USIM 时；

所述 HSS 确定针对 UE 的三元组鉴权向量包括：HSS 首先确定针对 USIM 模块的五元组鉴权向量，并将所述五元组鉴权向量转换为三元组鉴权向量。

5、根据权利要求 4 所述的方法，其特征在于，所述三元组鉴权向量进一步

包括：全球移动通信网使用的加密密钥 Kc；所述五元组鉴权向量包括：RAND、预期响应 XRES、完整性密钥 IK、加密密钥 CK 和鉴权令牌 AUTN；

所述将五元组鉴权向量转换为三元组鉴权向量为：丢弃五元组中的 AUTN，保留 RAND，将 XRES 转换为 SRES，并将 IK 和 CK 转换为 Kc。

6、根据权利要求 4 所述的方法，其特征在于，所述步骤 c 中，所述终端用户标识模块根据 RAND 计算 RES 包括：USIM 模块根据是否收到 AUTN 判断是否需要将五元组转换为三元组，如果没有收到 AUTN，则确定需要将五元组转换为三元组，根据 RAND 计算出 XRES，将 XRES 转换为 SRES；如果收到 AUTN，则不执行转换，并结束本处理流程。

7、根据权利要求 1 所述的方法，其特征在于，所述步骤 a 中，IMS 系统将 RAND 下发到 UE 为：S_CSCF 通过代理呼叫状态控制功能 P_CSCF 将 RAND 下发到 UE；

步骤 c 中，所述终端用户标识模块将 RES 通过 UE 返回给 IMS 系统为：终端用户标识模块将 RES 发送给 UE，UE 再将所述 RES 通过 P_CSCF 发送给 S_CSCF。

8、根据权利要求 7 所述的方法，其特征在于，所述系统启用一致性保护和保密性保护；所述三元组中进一步包括 Kc；

所述步骤 a 进一步包括：IMS 系统中的 S_CSCF 将三元组中的 Kc 转换为 CK 和 IK，并将所述 CK 和 IK 发送给 P_CSCF；

所述步骤 c 进一步包括：终端用户标识模块计算 Kc，并将所述 Kc 上传给 UE；

该方法进一步包括：UE 将终端用户标识模块上传的 Kc 转换为 IK 和 CK；UE 和 P_CSCF 将所述 IK 和 CK 作为后续会话中的密钥。

9、根据权利要求 7 所述的方法，其特征在于，所述系统启用一致性保护和保密性保护；

所述步骤 a 进一步包括：IMS 系统中的 S_CSCF 将三元组中的 Kc 直接发送

给 P_CSCF;

所述步骤 c 进一步包括: 终端用户标识模块计算 K_c , 并将所述 K_c 上传给 UE;

该方法进一步包括: P_CSCF 及 UE 将自身收到的 K_c 转换为 CK 和 IK; UE 和 P_CSCF 并将所述 IK 和 CK 作为后续会话中的密钥。

10、根据权利要求 8 或 9 所述的方法, 其特征在于, 当所述终端用户标识模块为 USIM 模块;

步骤 c 中, 所述终端用户标识模块计算 K_c 进一步包括: USIM 模块判断是否收到 AUTN, 如果没有收到 AUTN, 则确定需要将五元组转换为三元组, 根据 RAND 计算出 IK 和 CK, 并将 IK 和 CK 转换为 K_c , 之后将所述 K_c 发送给 UE。

IP 多媒体子系统中对终端用户标识模块进行鉴权的方法

技术领域

本发明涉及对移动终端的鉴权技术，更确切地说是涉及在 IP 多媒体子系统（IMS）中对终端用户标识模块进行鉴权的方法。

背景技术

随着多媒体业务的发展，目前已出现了针对移动终端的多媒体业务。现在为移动终端提供多媒体业务的 IMS 系统如图 1 所示，该系统起初是在第三代网络（3G）已有的分组域之外叠加的一个子域，这个子域专门用于支持 IP 多媒体业务。在条件成熟的情况下，IMS 系统也可服务于终端局域网（WLAN）等其他方式接入的用户。

IMS 系统主要由呼叫控制实体和媒体网关部件构成，在各个部件之间主要使用会话发起协议（SIP）传输控制信令。呼叫控制部件主要完成呼叫控制、地址转换、计费、隐蔽移动终端（UE）的移动性等功能，是 IMS 系统中的关键部件；媒体网关部件则是为与现有公共开关电话网络（PSTN）网络兼容而引入的。另外，IMS 系统中的归属用户服务器（HSS）是归属网络中用于保存 IMS 用户签约信息的设备。

IMS 系统的安全包括用户在 IMS 系统的鉴权和 SIP 消息的保护。IMS 系统的安全架构如图 2 所示。其中，UE 与归属网之间的鉴权及安全联盟（SA: Security Association）协商采用 IMS 鉴权密钥协议（AKA）双向认证机制，SIP 消息的加密和完整性保护采用的是逐跳处理方式。

具体来说，在 IMS 系统中，为实现对 IP 多媒体（IM）用户的鉴权，3GPP 协议组织使用了专门的 IMS 用户标识模块（ISIM）模块作为用户侧的鉴权模块，并使用了通用移动通信系统（UMTS）的 AKA 机制。IMS 系统对用

户的鉴权处理过程如图 3 所示，对应以下步骤：

步骤 301、UE 在需要使用 IMS 业务时，依次通过代理 - 呼叫状态控制功能（P_CSCF）及查询 - 呼叫控制功能（I_CSCF）将注册请求发送给服务呼叫状态控制功能（S_CSCF）。

步骤 302、S_CSCF 在收到注册请求后，如果自身存在针对该用户的五元组鉴权向量（AV），则直接利用该鉴权向量对用户进行鉴权，即进入步骤 304；如果没有，则向 HSS 请求 AV。

这里，五元组 AV 包括：随机数（RAND）、鉴权令牌（AUTN）、全球移动通信网使用的加密密钥（CK）、完整性密钥（IK）及预期响应（XRES）。

步骤 303、HSS 收到 S_CSCF 的请求后，确定五元组 AV，并发送给 S_CSCF。

当然，为提高效率，HSS 一般会按顺序向 S_CSCF 发送多组五元组 AV。

步骤 304、S_CSCF 保留 HSS 发送来的五元组 AV 中的 XRES，将 RAND、AUTN、CK 及 IK 放在鉴权考验（Auth_Challenge）消息中，并将该消息通过 I_CSCF 发送给 P_CSCF。

如果 HSS 发送多组五元组 AV，则 S_CSCF 可以按顺序选择一组五元组 AV，其他五元组 AV 则留在针对该用户的下一次鉴权中使用。

步骤 305、P_CSCF 保留 S_CSCF 通过 Auth_Challenge 消息发送来的 CK 和 IK，并将 RAND 和 AUTN 下发到 UE。

如果系统启动了一致性保护和保密性保护，则 P_CSCF 将在后续的会话中使用保存下来的 IK 和 CK 作为密钥。

步骤 306、UE 将收到的 RAND 和 AUTN 发送到 ISIM。

步骤 307、ISIM 对收到的 AUTN 进行验证，并在验证通过后根据 RAND 计算响应（RES），然后将计算出的 RES 作为鉴权响应发送给 UE，并由 UE 将该 RES 返回给 S_CSCF，同时 ISIM 还根据 RAND 计算出 IK 和 CK，并将 IK 和 CK 发送给 UE。

ISIM 对收到的 AUTN 进行验证包括确定 AUTN 中包含的 MAC 值是否合法，以及确定 SQN 是否可接受。其中，ISIM 对 SQN 是否可接受的验证即为验证是否需要再同步。

UE 具体会通过 P_CSCF 和 I_CSCF 将 RES 发送给 S_CSCF，并保留 IK 和 CK，以作为后续会话中的密钥。

步骤 308 ~ 309、S_CSCF 将 UE 发送来的鉴权响应中的 RES 与自身保存的 XRES 进行比较，如果相等，则确定鉴权通过，并通过 I_CSCF 及 P_CSCF 向 UE 发送鉴权成功消息；否则，确定鉴权失败。

上述处理过程要求使用单独的 ISIM 模块完成 IM 域的鉴权，也就是说，目前所设置的 ISIM 模块是专门用于实现 IM 域的鉴权的，而目前能够用于 3G 的终端用户标识模块都是不包含 ISIM 模块的，因此这些终端用户标识模块无法通过上述过程完成 IM 域的鉴权。比如，用户目前大多使用基于 GSM/GPRS 网络的用户标识模块（SIM）卡，即使部分网络升级到了 3G 网络，由于 UE 实现了双模应用，因此用户仍然可以通过 SIM 卡接入 3G 系统，这种情况下，由于 SIM 卡中没有 ISIM 模块，因此无法通过上述处理过程完成 IM 域的鉴权。再比如，目前已出现的针对 3G 的 UICC 卡，一般只包含了用于 CS 域和 PS 域鉴权的 USIM 模块，这样也就无法通过上述处理过程完成 IM 域的鉴权。

如果不用上述基于 ISIM 模块的处理过程完成对 IM 域的鉴权，而是希望通过 USIM 模块实现鉴权，则会出现因 USIM 模块在实现 CS 域或 PS 域鉴权的同时对 IM 域进行鉴权而引起频繁再同步的问题。所谓再同步是指：USIM 模块中保存了 SQN_{MS} ，如果 HSS/HLR 下发的五元组中的 SQN 比 USIM 模块中保存的 SQN_{MS} 旧，而下发的 SQN 是以 HSS/HLR 保存的 SQN_{HE} 为准的，这说明 SQN_{HE} 比 SQN_{MS} 旧，故将引发 USIM 模块会用自身的 SQN_{MS} 去同步 HSS/HLR 中的 SQN_{HE} 。

具体来说，为提高网络的存取效率，针对 CS 域的 VLR、针对 PS 域的

SGSN, 以及针对 IM 域的 S_CSCF 在索取鉴权向量时都会索取多组, 每次只使用其中一组进行鉴权处理, 并自行缓存剩余的鉴权向量。在这种情况下, 如果各个域的操作频度不同, 比如, SGSN 和 VLR 先后向 HSS 获取了 5 组鉴权元组, 在各自使用了一组之后, 可能由于用户在 CS 域的操作很频繁, 使得 SGSN 中已缓存的 4 组剩余鉴权向量将比 USIM 模块中的 SQN_{MS} 旧, 此时 USIM 模块中保存的 SQN_{MS} 以 VLR 下发的 SQN 为准, 这样, USIM 模块就会用自身的 SQN_{MS} 去同步 HSS/HLR 中的 SQN_{HE} , 进而导致 SGSN/VLR 当前缓存的所有鉴权向量失效。从上述例子可见, 如果不同域的操作频度相差较大, 则必然会引起频繁的再同步。

为解决上述频繁再同步的问题, 可以用 HSS 来替代现网中的所有 HLR, 因为 HSS 可以将下发的 SQN 划分为 CS 域、PS 域和 IM 域, 这样, USIM 模块可以分别对各个域内的 SQN 进行比较, 只要能够保证 HSS 下发给每个域的鉴权元组所对应的 SQN 是有序的, 就不会导致不必要的再同步过程。由于每个域中都只有一个网络实体用于缓存鉴权元组, 比如, CS 域中有 VLR 缓存、PS 域中有 SGSN 缓存, IM 域中则有 S_CSCF 缓存, 因此通过 HSS 对 SQN 的划分可以解决再同步问题。

但是, 由于目前的网络处于初始阶段, 大规模替换 HLR 基本上是不可能的, 更为合理的解决方案是在现网的基础上叠加一个或多个专门提供 IM 业务的 HSS, 而现有的 HLR 保持不变, 继续提供 CS 和 PS 域的业务, HSS 则通过与现网中 HLR 的交互获取用户的 CS/PS 信息。这种组网情况下, 新增的 IM 域和已有的 CS/PS 域可以共享 USIM, 且 IM 域的 HSS 能够从用户归属的 HLR 获取鉴权向量, 但由于 HLR 无法将下发的 SQN 划分为 CS 域、PS 域和 IM 域, 因此频繁再同步的问题仍然没有解决。

另外, 如果采用在现有网络上叠加建设 IMS 系统时, 由于需要对 SQN 进行校验, 因此需要现网的 HLR 与新增的 HSS 共享同一个 AUC, 对现网的影响较大。

从以上描述可知,要想 SIM 卡中实现 IM 业务,或者使用 USIM 卡实现 IM 业务且不会出现频繁再同步的问题,目前按照 3GPP 的建议方案就是将卡更换为包含 ISIM 模块的卡。根据目前的运营模式,如果用户想要升级 UE,可以通过各种途径实现,包括购置新机、通过 Java 或者手机制造商提供的接口升级等,这些升级具有很强的可操作性。但如果用户想要换卡,则必须到运营商授权的专门营业点进行更换,而为保证业务的持续性,新卡中的 IMSI 与旧卡中的 IMSI 必须保证一定的关联性,比如,必须归属同一个 HLR,因此,换卡在实际操作时必然非常繁琐。

综上所述,目前要想使用 IM 业务,则用户的终端用户标识模块中必须包含 ISIM 模块,显然这对终端用户标识模块的要求比较高,往往需要用户更换自身的 SIM 卡或 USIM 卡才能实现。而换卡在实际操作中非常繁琐,必然会大大降低 IM 业务的吸引力,增加运营商推广 IM 业务的难度。

发明内容

有鉴于此,本发明的主要目的在于提供在 IMS 系统中对终端用户标识模块进行鉴权的方法,以使用户不用更换自身的终端用户标识模块,即可使用 3G 系统中的 IM 业务。

为达到以上目的,本发明的技术方案是这样实现的:一种在 IP 多媒体子系统中对终端用户标识模块进行鉴权的方法,该方法包括以下步骤:

a. IP 多媒体子系统 IMS 在收到移动终端 UE 发送来的注册请求后,由所述 IMS 系统中的归属用户服务器 HSS 或服务-呼叫状态控制功能 S-CSCF 确定针对该 UE 的三元组鉴权向量,所述三元组鉴权向量至少包含随机数 RAND 和符号响应 SRES,保留三元组中的 SRES,并将 RAND 下发到 UE;

b. UE 将所述 RAND 传送到自身的终端用户标识模块;其中,所述终端用户标识模块为 SIM 模块或 USIM 模块;

c. 终端用户标识模块根据 RAND 计算 RES,并将 RES 通过 UE 返回给 IMS 系统;

d. IMS 系统中的 S_CSCF 判断 UE 返回的 RES 是否与自身保存的 SRES 相等, 如果是, 则鉴权通过, 否则, 鉴权失败。

所述步骤 a 中, 所述 IMS 系统确定针对 UE 的三元组鉴权向量包括: IMS 系统中的 S_CSCF 判断自身是否存有针对该 UE 的三元组鉴权向量, 如果是, 则执行后续步骤; 否则, 向归属用户服务器 HSS 请求针对该 UE 的三元组鉴权向量;

HSS 在收到 S_CSCF 发送来的鉴权向量请求后, 确定针对该 UE 的三元组鉴权向量, 并发送给 S_CSCF。

当所述 UE 中的终端用户标识模块为用户标识模块 SIM 时, 所述 HSS 直接确定针对该 UE 中 SIM 模块的三元组鉴权向量。

当所述 UE 中的终端用户标识模块为用户服务标识模块 USIM 时; 所述 HSS 确定针对 UE 的三元组鉴权向量包括: HSS 首先确定针对 USIM 模块的五元组鉴权向量, 并将所述五元组鉴权向量转换为三元组鉴权向量。

所述三元组鉴权向量进一步包括: Kc; 所述五元组鉴权向量包括: RAND、XRES、IK、CK 和 AUTN; 所述将五元组鉴权向量转换为三元组鉴权向量为: 丢弃五元组中的 AUTN, 保留 RAND, 将 XRES 转换为 SRES, 并将 IK 和 CK 转换为 Kc。

所述步骤 c 中, 所述终端用户标识模块根据 RAND 计算 RES 包括: USIM 模块根据是否收到 AUTN 判断是否将五元组转换为三元组, 比如判断是否需要启动 3G + Kc 模式, 如果没有收到 AUTN, 则启动 3G + Kc 模式, 并根据 RAND 计算出 XRES, 将 XRES 转换为 SRES; 如果收到 AUTN, 则不启动 3G + Kc 模式, 并结束本处理流程。

所述步骤 a 中, IMS 系统将 RAND 下发到 UE 为: S_CSCF 通过 I_CSCF 及 P_CSCF 将 RAND 下发到 UE;

步骤 c 中, 所述终端用户标识模块将 RES 通过 UE 返回给 IMS 系统为: 终端用户标识模块将 RES 发送给 UE, UE 再将所述 RES 通过代理呼叫状态

控制功能 P_CSCF 及 I_CSCF 发送给 S_CSCF。

所述系统启用一致性保护和保密性保护；且所述三元组中进一步包括 Kc；

所述步骤 a 进一步包括：IMS 系统中的 S_CSCF 将三元组中的 Kc 转换为 CK 和 IK，并将所述 CK 和 IK 通过 I_CSCF 发送给 P_CSCF；

所述步骤 c 进一步包括：终端用户标识模块计算 Kc，并将所述 Kc 上传给 UE；

该方法进一步包括：UE 将终端用户标识模块上传的 Kc 转换为 IK 和 CK；UE 和 P_CSCF 将所述 IK 和 CK 作为后续会话中的密钥。

所述系统启用一致性保护和保密性保护；

所述步骤 a 进一步包括：IMS 系统中的 S_CSCF 将三元组中的 Kc 直接通过 I_CSCF 发送给 P_CSCF；

所述步骤 c 进一步包括：终端用户标识模块计算 Kc，并将所述 Kc 上传给 UE；

该方法进一步包括：P_CSCF 及 UE 将自身收到的 Kc 转换为 CK 和 IK；UE 和 P_CSCF 并将所述 IK 和 CK 作为后续会话中的密钥。

所述终端用户标识模块为 USIM 模块；

步骤 c 中，所述终端用户标识模块计算 Kc 进一步包括：USIM 模块判断是否收到 AUTN，如果没有收到 AUTN，则确定需要将五元组转换为三元组，比如需要启动 3G+Kc 模式后，根据 RAND 计算出 IK 和 CK，并将 IK 和 CK 转换为 Kc，之后将所述 Kc 发送给 UE。

本发明方案通过 IMS 系统使用三元组鉴权向量对终端用户标识模块进行鉴权，在实现了使用现有的 SIM 模块或 USIM 模块进行鉴权的同时，还避开了 USIM 模块对 SQN 的校验，继而使得在现网基础上新建的 HSS 不需要与现网中的 HLR 共享同一个 AUC，也就是说，可以针对 HSS 单独设置 AUC，从而使得在现网中增加 HSS 时，不需要因鉴权问题升级任何已有的

现网设备。

通过本发明方案,使得使用诸如 SIM 模块、USIM 模块之类的用户不需要升级或换卡即可享受 IM 业务,大大降低了 IM 业务的推广难度。

另外,本发明方案所涉及的所有修改和改造都是在 IM 域的相关网络实体中实现的,对于目前的 GSM、GPRS 以及 UMTS 中的所有设备都没有任何的额外要求,使得在现有网络上叠加一个专门用于提供 IM 域的 IMS 系统成为可能。

附图说明

图 1 为目前的 IMS 系统结构示意图;

图 2 为 IMS 的安全架构示意图;

图 3 为现有技术中 IMS 系统通过 ISIM 对 UE 进行鉴权的消息流时序图;

图 4 为本发明中 IMS 系统通过 SIM 对 UE 进行鉴权的消息流时序图;

图 5 为本发明中 IMS 系统通过 SIM 对 UE 进行鉴权的另一种方案的
消息流时序图;

图 6 为本发明中 IMS 系统通过 USIM 对 UE 进行鉴权的消息流时序图;

图 7 为本发明中 IMS 系统通过 USIM 对 UE 进行鉴权的另一种方案的
消息流时序图。

具体实施方式

由于图 3 所示处理过程需要验证 AUTN,对于 SIM 模块及 USIM 模块来说,验证 AUTN 会带来频繁再同步的问题,因此,本发明的核心思想在于:S_CSCF 在需要对 UE 进行鉴权时,利用不包含 AUTN 的三元组鉴权向量进行鉴权来避开对 SQN 的校验。这样,HSS 发送给 S_CSCF 的鉴权向量也应该为三元组。

下面分别以 SIM 和 USIM 作为终端用户标识模块为例,结合附图对本发明方案作详细的说明。

图 4 所示为 SIM 卡接入 IM 域的鉴权处理过程，对应以下步骤：

步骤 401、UE 在需要使用 IMS 业务时，依次通过 P_CSCF 及 I_CSCF 将注册请求发送给 S_CSCF。

步骤 402、S_CSCF 在收到注册请求后，判断自身是否存在针对该用户的三元组 AV，如果存在，则直接利用该 AV 对用户进行鉴权，即进入步骤 404；如果不存在，则向 HSS 请求 AV。

这里，三元组 AV 包括：RAND、符号响应 SRES 和 Kc。

步骤 403、HSS 在收到 S_CSCF 的请求后，确定针对该 SIM 模块的三元组 AV，并发送给 S_CSCF。

由于 SIM 本身就支持三元组 AV，因此 HSS 可以直接确定针对该 SIM 的三元组 AV。

另外，为提高效率，HSS 一般会按顺序向 S_CSCF 发送多组三元组 AV。

步骤 404、S_CSCF 保留 HSS 发送来的三元组 AV 中的 SRES，使用标准算法将 Kc 转换为 CK 和 IK，之后将 RAND 及转换得到的 CK 和 IK 通过 Auth_Challenge 消息发送给 P_CSCF。

如果 HSS 发送的是多组三元组 AV，则 S_CSCF 可以按顺序选择一组 AV，其他 AV 则留在针对该用户的下一次鉴权中使用。

步骤 405、P_CSCF 保留 S_CSCF 通过 Auth_Challenge 消息发送来的 CK 和 IK，并将 RAND 下发到 UE。

如果系统启动了一致性保护和保密性保护，则 P_CSCF 将在后续的会话中使用保存下来的 IK 和 CK 作为密钥。

步骤 406、UE 将收到的 RAND 传送给 SIM。

步骤 407、SIM 在收到 RAND 后，根据 RAND 计算出 RES 和 Kc，并将 RES 作为鉴权响应通过 UE 返回给 S_CSCF，同时将 Kc 上传给 UE。

UE 具体会依次通过 P_CSCF 和 I_CSCF 将 SIM 返回的鉴权响应发送给 S_CSCF。

步骤 408 ~ 409、S_CSCF 将 UE 发送来的鉴权响应中的 RES 与自身保存的 SRES 进行比较,如果相等,则确定鉴权通过,并通过 I_CSCF 及 P_CSCF 向 UE 发送鉴权成功消息;否则,确定鉴权失败。

通过上述处理过程即可实现对 SIM 的鉴权。当然,如果系统启动了一致性保护和保密性保护,则 UE 还需要将 SIM 发送来的 Kc 转换为 IK 和 CK,以作为后续会话的一致性密钥和完整性密钥。

在上述处理过程中, S_CSCF 与 UE 使用的转换算法可以是 3GPP TS 33.102 中给定的三元组和五元组转换算法,从而提高通用性。

对于针对 SIM 卡鉴权的过程来说,还可以通过图 5 所示过程实现。该过程与上述图 4 所示过程相比,图 5 中的步骤 501 ~ 503,以及步骤 506 ~ 509 与图 4 中的相应步骤相同,其主要区别在于:

在步骤 504 中, S_CSCF 不对 Kc 进行转换,而是直接将 Kc 通过 Auth_Challenge 消息发送给 P_CSCF。

在步骤 505 中, P_CSCF 保留的是 S_CSCF 通过 Auth_Challenge 消息发送来的 Kc。当然,如果系统启动了一致性保护和保密性保护,则 P_CSCF 还需要使用标准算法将该 Kc 转换为 CK 和 IK,并在后续的会话中使用保存下来的 IK 和 CK 作为密钥。

上述结合图 4 及图 5 对通过 SIM 鉴权的过程进行了描述,对于通过 USIM 进行鉴权的过程来说,则如图 6 所示,对应以下步骤:

步骤 601、UE 在需要使用 IMS 业务时,依次通过 P_CSCF 及 I_CSCF 将注册请求发送给 S_CSCF。

步骤 602、S_CSCF 在收到注册请求后,判断自身是否存在针对该用户的三元组 AV,如果存在,则直接利用该 AV 对用户进行鉴权,即进入步骤 604;如果不存在,则向 HSS 请求三元组 AV。

这里,三元组 AV 包括: RAND、SRES 和 Kc。

步骤 603、HSS 在收到 S_CSCF 的请求后,确定与该 USIM 对应的五元

组 AV，该五元组 AV 包括 RAND、XRES、IK、CK 和 AUTN，再使用标准转换算法将该五元组 AV 转换为相应的三元组 AV，该三元组 AV 包括 RAND、SRES 和 Kc，然后将所得的三元组 AV 下发给 S_CSCF。

由于 USIM 本身不支持三元组 AV，因此 HSS 需要首先确定 USIM 所支持的五元组 AV，再将其转换为相应的三元组 AV。主要转换工作为：保留原有的 RAND，丢弃 AUTN，将 XRES 转换为 SRES，以及将 IK 和 CK 转换为 Kc。

另外，为提高效率，HSS 一般会确定多个五元组 AV，并将每个五元组 AV 转换为相应的三元组 AV，然后再将转换得到的三元组 AV 按顺序发送给 S_CSCF。

步骤 604、S_CSCF 保留 HSS 发送来的三元组 AV 中的 SRES，使用标准算法将 Kc 转换为 CK 和 IK，之后将 RAND 及转换得到的 CK 和 IK 通过 Auth_Challenge 消息发送给 P_CSCF。

当然，如果 HSS 发送的是多组三元组 AV，则 S_CSCF 可以按顺序选择一组 AV，其他 AV 则留在针对该用户的下一次鉴权中使用。

步骤 605、P_CSCF 保留 S_CSCF 通过 Auth_Challenge 消息发送来的 CK 和 IK，并将 RAND 下发到 UE。

如果系统启动了一致性保护和保密性保护，则 P_CSCF 将在后续的会话中使用保存下来的 IK 和 CK 作为密钥。

步骤 606、UE 将收到的 RAND 传送给 USIM。

步骤 607、USIM 在收到 RAND 后，在根据 AUTN 确定需要将五元组转换为三元组后，利用 RAND 计算出 XRES、IK 及 CK，然后再使用转换算法将 XRES 转换为 RES，将 IK 和 CK 转换为 Kc，并将所述 RES 作为鉴权响应通过 UE 返回给 S_CSCF，同时将转换得到的 Kc 上传给 UE。

其中，USIM 根据 AUTN 确定需要将五元组转换为三元组，可以是根据 AUTN 确定需要启动 3G + Kc 模式。USIM 根据 AUTN 确定是否需要启动 3G

+ Kc 模式具体为：USIM 判断是否收到 AUTN，如果收到 AUTN，则不启动 3G + Kc 模式，并按照原有处理逻辑进行处理；如果没有收到 AUTN，则启动 3G + Kc 模式，之后执行所述后续处理过程。

UE 具体会依次通过 P_CSCF 和 I_CSCF 将 USIM 返回的鉴权响应发送给 S_CSCF。

步骤 608 ~ 609、S_CSCF 将 UE 发送来的鉴权响应中的 RES 与自身保存的 SRES 进行比较，如果相等，则确定鉴权通过，并通过 I_CSCF 及 P_CSCF 向 UE 发送鉴权成功消息；否则，鉴权失败。

当然，如果系统启动了一致性保护和保密性保护，则 UE 还需要将 USIM 发送来的 Kc 转换为 IK 和 CK，以作为后续会话的一致性密钥和完整性密钥。

同样，上述处理所使用的转换算法可以是 3GPP TS 33.102 中给定的三元组和五元组转换算法，从而提高通用性。

对于针对 USIM 卡鉴权的过程来说，还可以通过图 7 所示过程实现。该过程与上述图 6 所示过程相比，其主要区别与上述 SIM 卡鉴权过程中图 4 与图 5 所示流程之间的区别相同。也就是说，S_CSCF 可以对 Kc 不作转换，而是直接发送给 P_CSCF，如果系统启动了一致性保护和保密性保护，则 P_CSCF 还需要使用标准算法将该 Kc 转换为 CK 和 IK，并将其作为后续会话中的密钥。

以上所述仅为本发明方案的较佳实施例，并不用以限定本发明的保护方案。

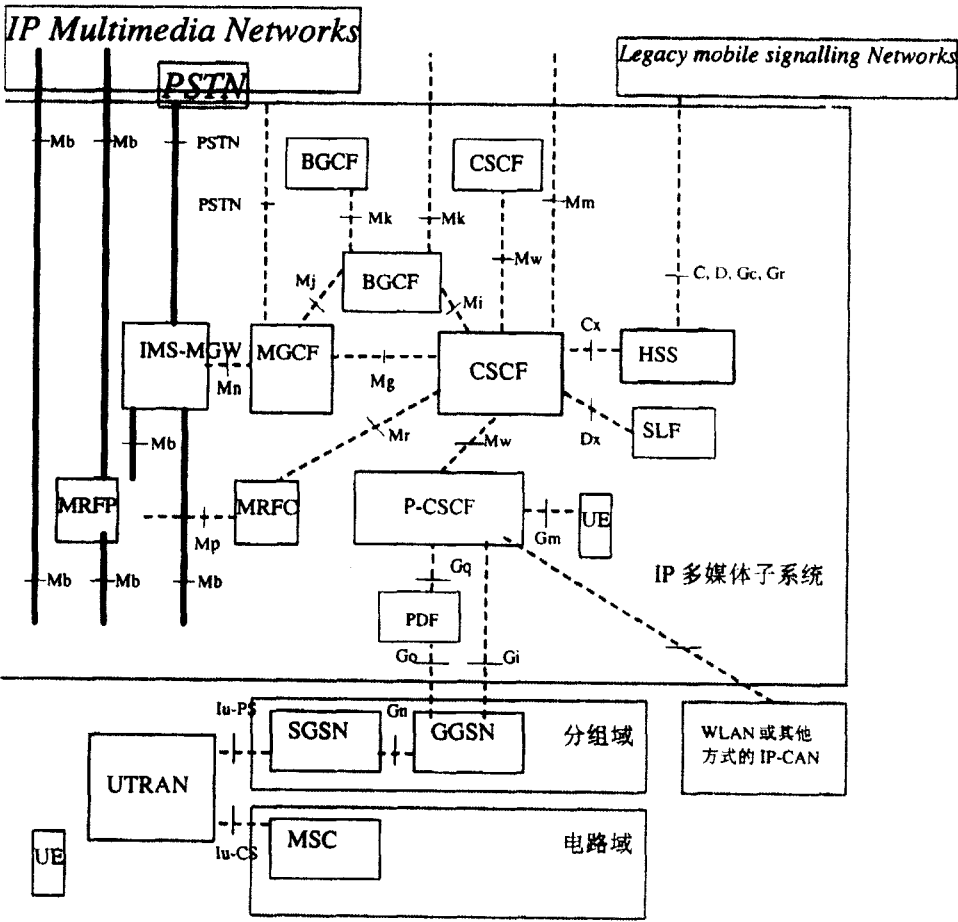


图 1

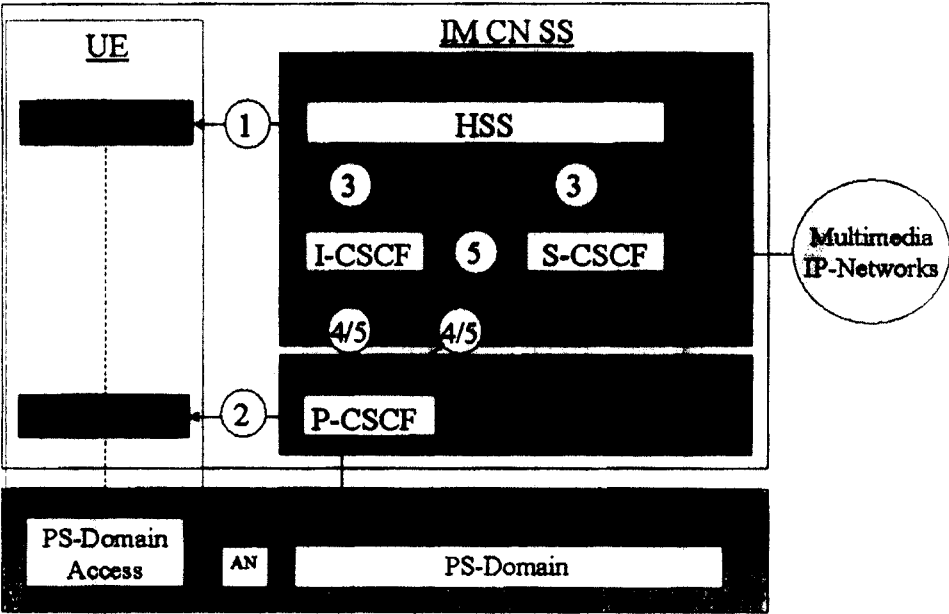


图 2

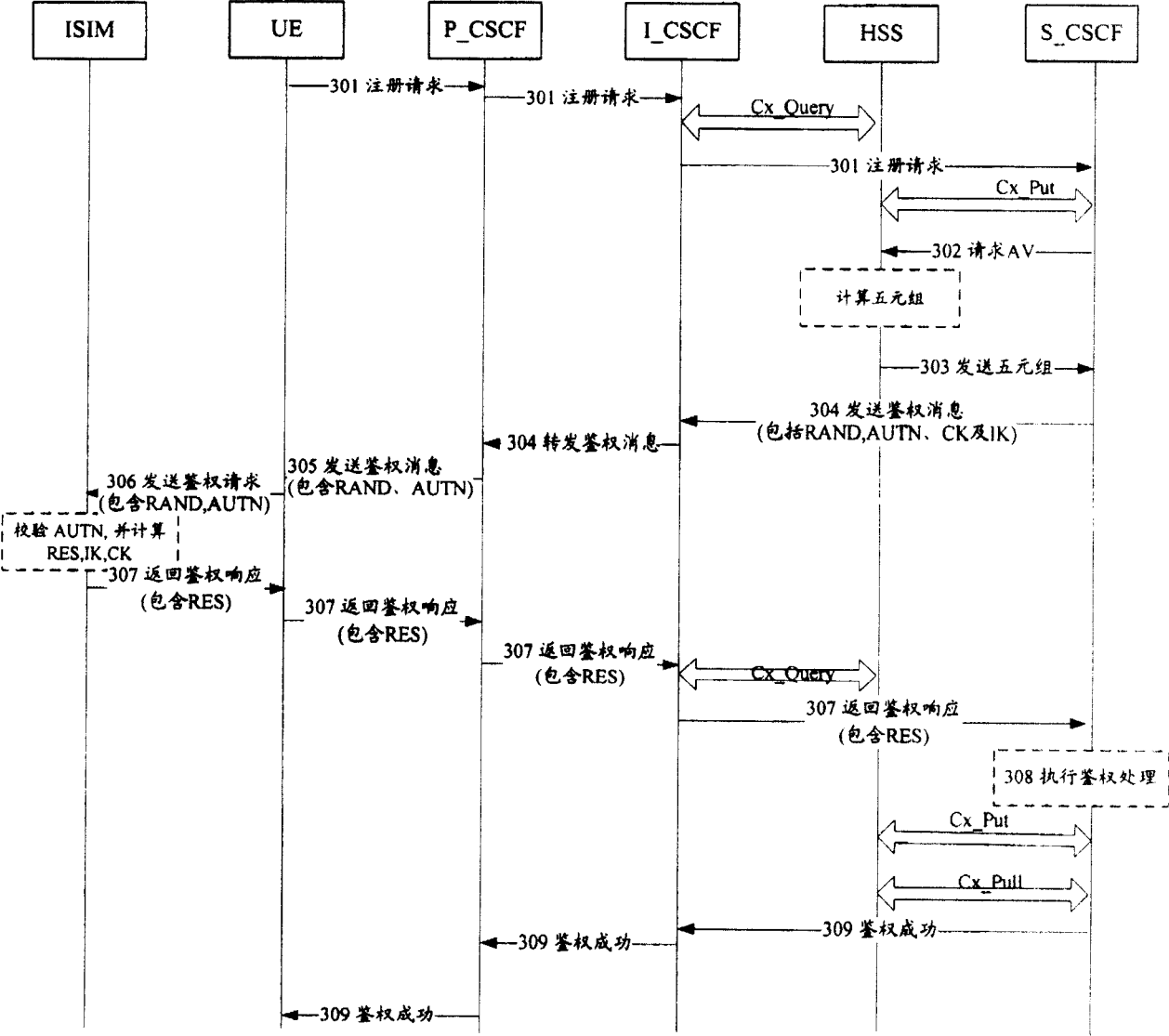


图 3

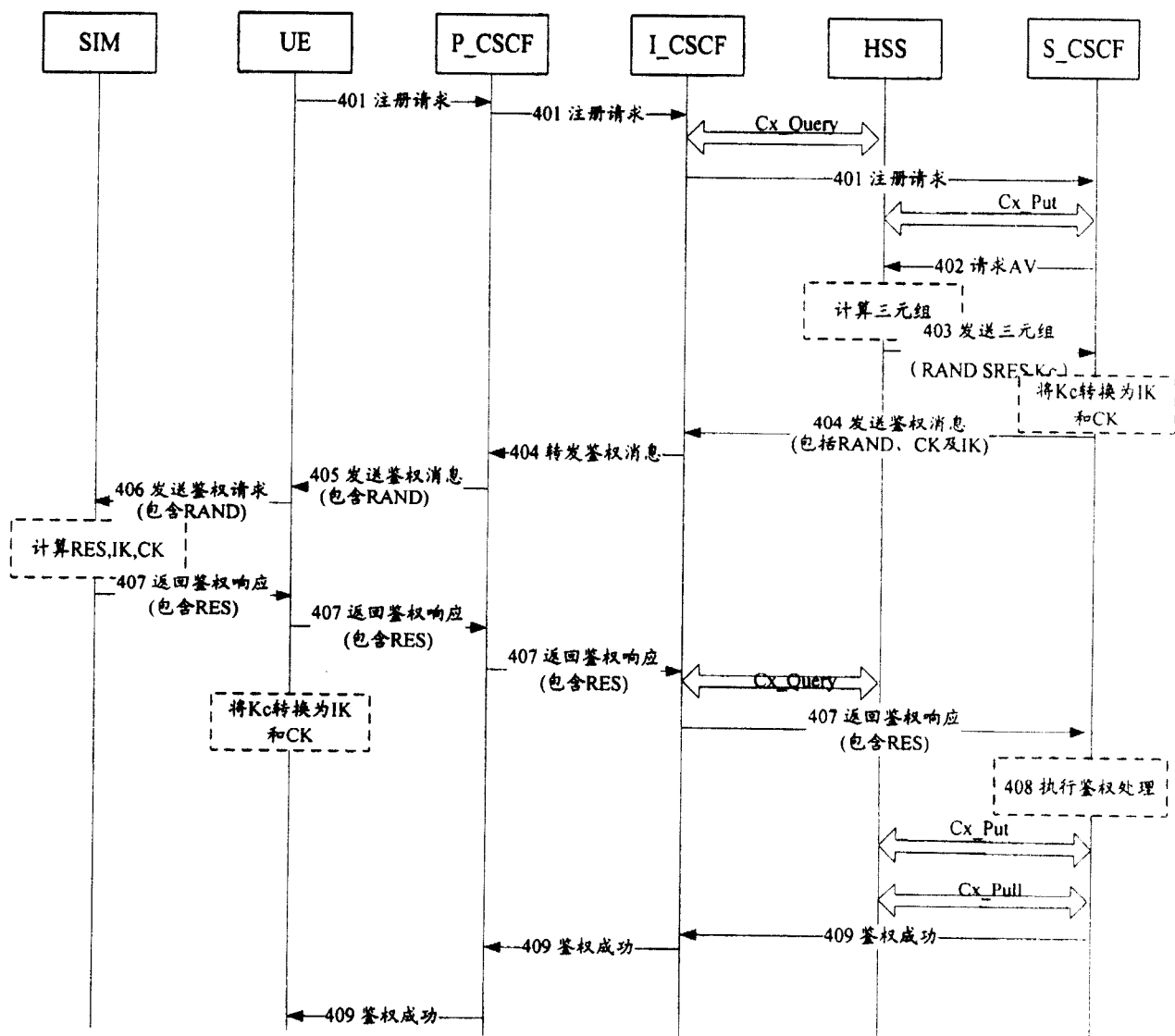


图 4

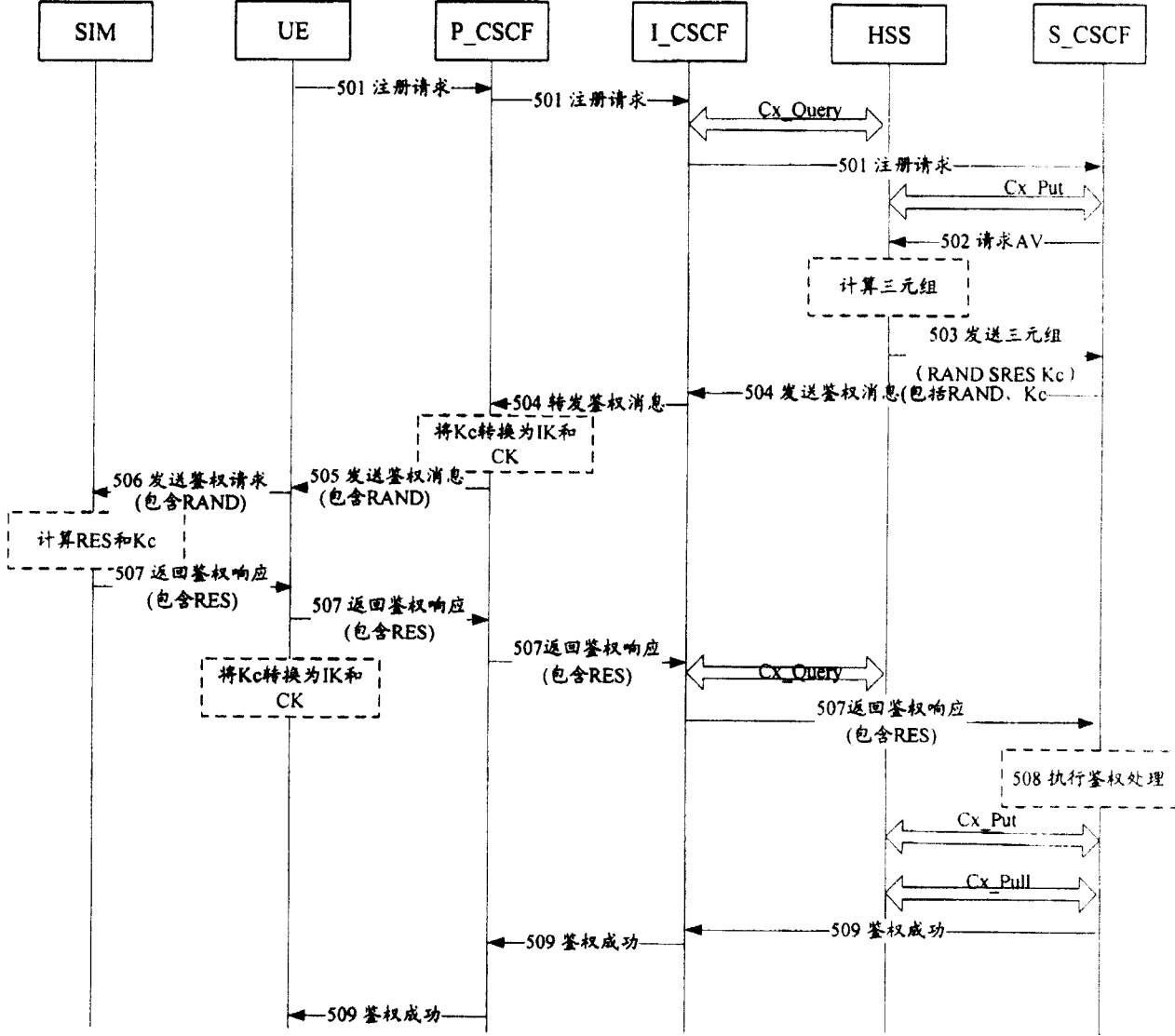


图 5

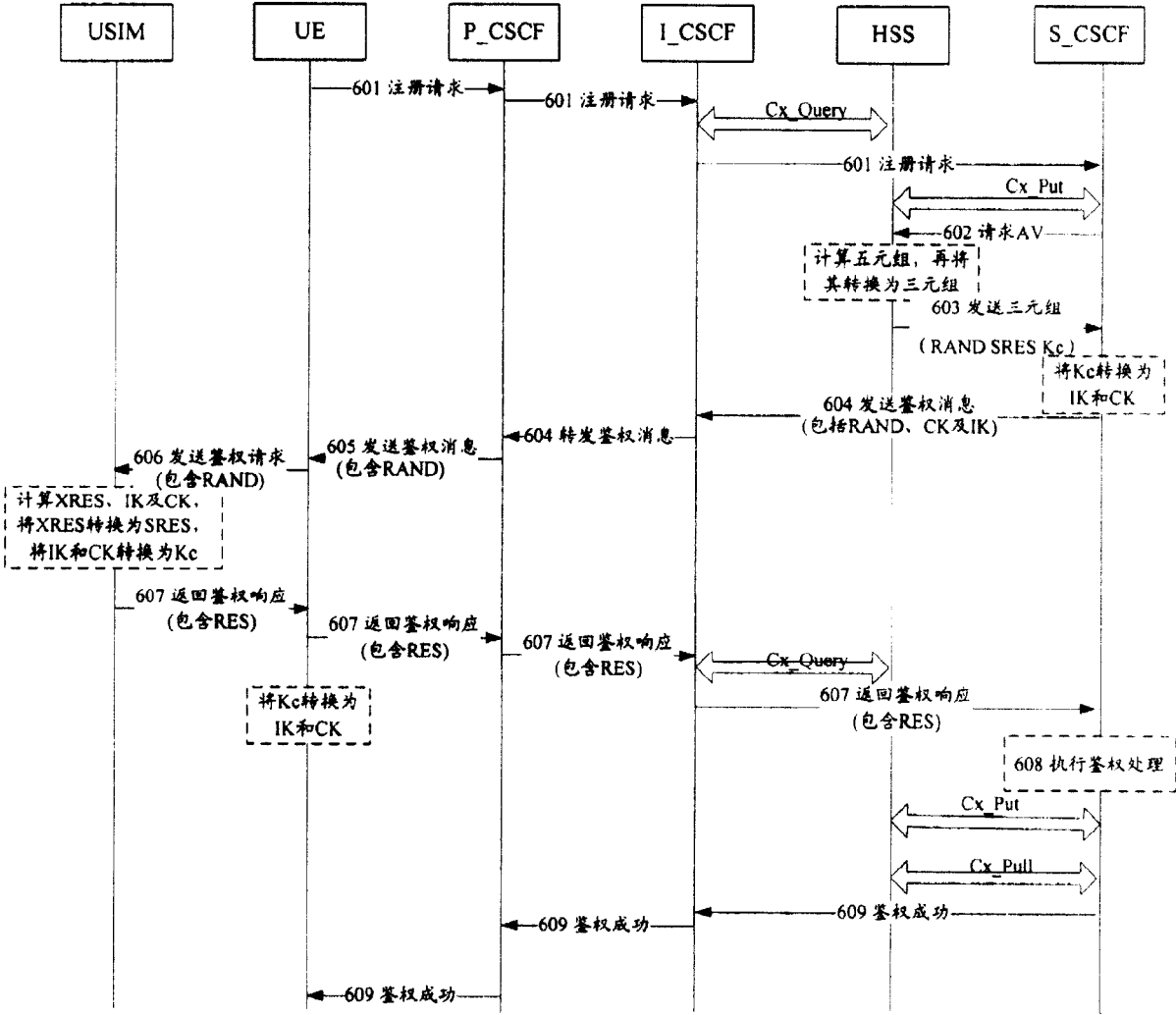


图 6

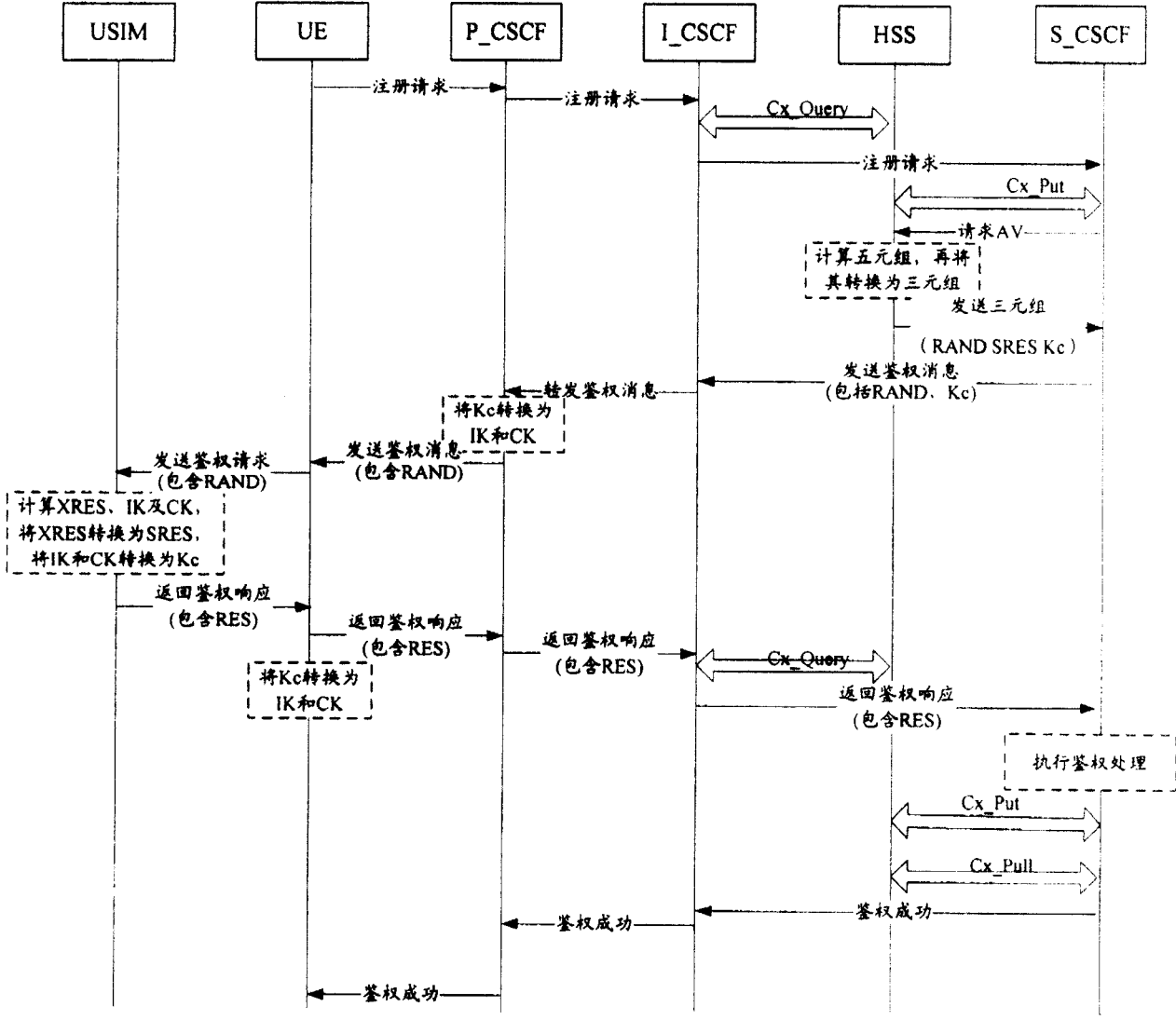


图 7