(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2007 年11 月8 日 (08.11.2007)

PCT

(10) 国际公布号
WO 2007/124657 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01)

(21) 国际申请号: PCT/CN2007/000914

(22) 国际申请日: 2007 年3 月21 日 (21.03.2007)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200610035298.5
2006 年4 月29 日 (29.04.2006) CN
200610084992.6
2006 年5 月29 日 (29.05.2006) CN
200610091433.8
2006 年6 月12 日 (12.06.2006) CN

(71) 申请人 (对除美国外的所有指定国): **华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **刘文宇(LIU, Wenyu)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **徐杰(XU, Jie)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

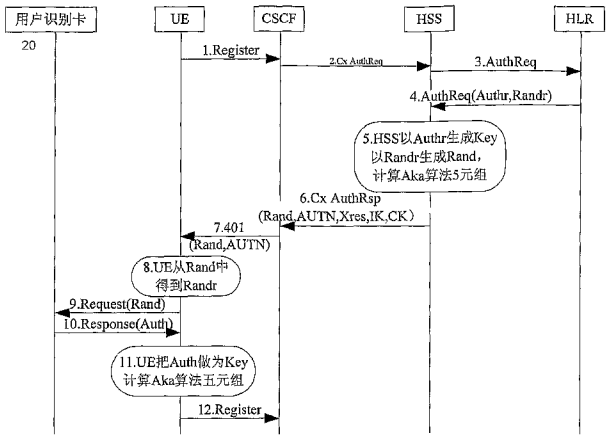
(74) 代理人: **北京集佳知识产权代理有限公司(UNITALEN ATTORNEYS AT LAW)**; 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU,

[见续页]

(54) Title: A METHOD, SYSTEM AND DEVICE FOR AUTHENTICATING

(54) 发明名称: 一种用于鉴权的方法、系统及装置



20 SUBSCRIBER IDENTITY CARD
5 HSS GENERATES THE KEY FROM THE Authr, GENERATES THE Rand FROM THE Randr, AND COMPUTES THE FIVE NUMBER GROUP OF THE Aka ARITHMETIC
8 THE UE ACQUIRES THE Randr FROM THE Rand
11 THE UE USES THE Auth AS THE KEY AND COMPUTES THE FIVE MUNBER GROUP OF THE Aka ARITHMETIC

(57) Abstract: A method, system and device for authenticating is disclosed. The method comprises the third entity generates the second authenticating data and the second random data, and transfers the second random data to the second entity; the second entity transfers the first random data obtained from the second random data to the first entity; the first entity generates the first authenticating data according to the first random data and transfers the first authenticating data to the second entity; the second entity generates the third authenticating data according to the first authenticating data and the second random data, and transfers the third authenticating data to the third entity; the third entity determines whether the authentication is successful by comparing whether the second authenticating data is consistent with the third authenticating data. The invention can make the authentication progress between the user terminal and IMS network on the safe side.

[见续页]

WO 2007/124657 A1

LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：
— 包括国际检索报告。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(57) 摘要：

本发明公开一种用于鉴权的方法、系统及装置，该方法包括：第三实体生成第二鉴权数据及第二随机数，并把所述第二随机数发给第二实体；所述第二实体将根据所述第二随机数得到的第一随机数发送给第一实体；所述第一实体根据所述第一随机数所生成第一鉴权数据，并把所述第一鉴权数据发给所述第二实体；所述第二实体根据所述第一鉴权数据及所述第二随机数生成第三鉴权数据，并把所述第三鉴权数据发送给所述第三实体；所述第三实体通过对比所述第二鉴权数据和所述第三鉴权数据的一致性来判断鉴权是否成功。本发明可使用户终端与 IMS 网络之间的鉴权过程更加安全可靠。

一种用于鉴权的方法、系统及装置

本申请要求申请日为 2006 年 4 月 29 日、申请号为 200610035298.5、发明名称为“一种用于鉴权的系统、装置及方法”的中国专利申请，申请日为 2006 年 6 月 12 日、申请号为 200610091433.8、发明名称为“一种用于鉴权的系统、装置及方法”的中国专利申请以及申请日为 2006 年 5 月 29 日、申请号为 200610084992.6、发明名称为“一种用于鉴权的系统、装置及方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及无线通信网络领域，尤其涉及一种用于鉴权的方法、系统及装置。

背景技术

随着向下一代网络（NGN，Next Generation Network）的演进，基于 IP 的网络架构必将使移动网络面临 IP 网络固有的一些安全问题。移动通信网络最终会演变成开放式的网络，能向用户提供开放式的应用程序接口，以满足用户的个性化需求。网络的开放性以及无线传播的特性，安全问题将成为整个移动通信系统的核心问题之一。

3GPP（3G Partnership Project）网络接入安全机制有三种：根据临时身份（TMSI，Temporary Mobile Subscriber Identity）识别，使用永久身份（IMSI，International Mobile Subscriber Identity）识别，认证和密钥协商（AKA，Authentication and Key Agreement）。AKA 机制可完成移动终端（MS，Mobile Station）和网络的相互认证，并建立新的加密密钥和完整性密钥。

在 IP 多媒体子系统（IMS，Internet Multiedia Subsystem）的注册流程中使用的鉴权算法就是 AKA 鉴权算法，该算法根据密钥、随机数以及相关参数生成一个认证向量 AV，该认证向量 AV 是一个五元组，包括随机数 RAND、认证令牌 AUTN、认证应答 XRES、加密密钥 CK 及消息完整性密钥 IK。用于用户对网络认证、网络对用户认证或 IP 安全性（IPSEC，IP Securty）的建立等。

下面结合图 1 来说明 AKA 鉴权算法。3GPP 为 3G 系统定义了 12 种安全算法：f0-f9、f1*和 f5*，应用于不同的安全服务。身份认证与密钥分配方案中移动用户登记和认证参数的调用过程与 GSM（Global System Mobile）网络基本相同，不同之处在于 3GPP 认证向量 AV 是五元组，并实现了用户对网络的认证。AKA 利用 f0 至 f5*算法，这些算法仅在鉴权中心（AC，Authentication Center）和用户终端的身份识别卡（如 SIM，Subscriber Identity Module）中执行。其中，f0 算法仅在 AC 中执行，用于产生随机数 RAND；f1 算法用于产生消息认证码（AC 中为 MAC-A，用户身份识别卡中为 XMAC-A）；f1*是重同步消息认证算法，用于产生 MAC-S；f2 算法用于产生期望的认证应答（AC 中为 XRES，SIM 卡中为 RES）；f3 算法用于产生加密密钥 CK；f4 算法用于产生消息完整性密钥 IK；f5 算法用于产生匿名密钥 AK，该匿名密钥 AK 用于对序列号（SQN，Sequence number）加解密，以防止被位置跟踪；f5*是重同步时的匿名密钥生成算法。AKA 由访客位置寄存器（VLR，Visited Location Register）发起，在 AC 中产生认证向量 AV=(RAND, XRES, CK, IK, AUTN)和认证令牌 AUTN = SQN ⊕ AK || AMF || MAC-A。VLR 发送 RAND 和 AUTN 至用户（比如 SIM）。用户计算 XMAC-A = f1K (SQN || RAND || AMF)，若该 XMAC-A 等于 AUTN 中的 MAC-A，并且 SQN 在有效范围，则认为对网络鉴权成功；并分别用 f2、f3、f4 计算 RES、CK、IK，发送 RES 至 VLR。VLR 验证 RES，若与先前所产生的认证向量中的 XRES 相符，则认为对用户终端鉴权成功；否则，拒绝用户终端的接入。当 SQN 不在有效范围时，SIM 和 AC 利用 f1*算法进入重新同步程序，VLR 向 HLR/AC 请求新的认证向量 AV。

如图 2 所示，为现有的一种 IMS 鉴权流程示意图。其中：

1、用户设备（UE，User Equipment）向 IMS 网络中的服务 CSCF（S-CSCF，Serving Call Server Control Function）发送注册请求（REGISTER）；

2、S-CSCF 向归属用户服务器（HSS，Home Subscriber Server）请求鉴权数据（Cx-Authentication）；

3、HSS 根据 AKA 算法得出认证向量 AV 的 5 元组（RAND、AUTN、XRES、CK 及 IK），并发送给 S-CSCF（Cx-Authentication Resp）;

4、S-CSCF 把五元组中的 RAND、AUTN、CK 及 IK 发给代理 CSCF（P-CSCF），P-CSCF 把包括所述认证令牌 AUTN 和随机数 RAND 的认证请求发给 UE，请求 UE 产生认证数据（401 Unauthorized）;

5、UE 接收到所述认证请求后，首先计算 XMAC，并与 AUTN 中的 MAC 进行比较，若不同，则向 VLR 发送拒绝认证消息，并放弃该过程。同时还要验证接受到的序列号 SQN 是否在有效的范围内，若不在，MS 向 VLR 发送同步失败消息，并放弃该过程。上述两项均通过后，用户终端用 f2 计算出 RES，用 f3 计算出 CK，用 f4 算法计算出 IK，并根据 IK、CK 与 P-CSCF 建立 IP 安全（IPSEC）隧道，并把 RES 发送给 IMS 网络（REGISTER）;

6、S-CSCF 对比 UE 上报的 RES 和从 HSS 获取的 XRES，如果两者相同则认为鉴权成功，同时与 HSS 交换用户数据，否则认证失败;

7、当认证成功后，IMS 网络向 UE 返回鉴权成功消息（200OK）。

由于 UE 与 HSS 计算 CK 用的都是同一种算法 f3，故而所得出的 CK 必定相同，这样 UE 与 IMS 网络经过相互身份认证和密码协商后，分别将该过程中的 CK、IK 作为以后 UE 和 RNC 的保密通信。

而在 CDMA2000 系统中，常采用蜂窝鉴权和语音加密（Cellular Authentication Voice Encription，CAVE）算法进行鉴权。

CAVE 算法无法根据一个随机数产生类似 AKA 算法的五元组认证向量，只能产生一个鉴权结果，也就是说，鉴权中心和用户终端根据同一个随机数计算出一个鉴权结果后，网络比较双方的结果是否符合；如果符合，则鉴权通过。参见下面的 CDMA2000 电路域鉴权流程:

如图 3 所示，是现有技术中进行注册时采用 CAVE 算法的鉴权流程。

1、基站子系统（BSS，Base Station Subsystem）中的移动终端（MS，Mobile Station）发起位置登记请求消息（Location Updating Request），在该消息中携带了 RANDC、RAND 及采用 CAVE 算法所生成的鉴权响应参数 AUTHR 和 COUNT 参数。

2、移动交换中心/访客位置寄存器（MSC/VLR，Mobile Services switching Center/Visited Location Register）向归属位置寄存器/鉴权中心（HLR/AC，Home Location Register/Authentication Center）发送鉴权请求消息 AUTHREQ，携带 RAND、AUTHR、COUNT 参数。

3、HLR/AC 采用 CAVE 算法生成鉴权响应参数 AUTHR，与用户端所传送过来的 AUTHR 进行比较，判断是否相同，以验证手机的合法性，并给 MSC/VLR 回送鉴权响应消息 authreq，返回鉴权结果。

4、MSC/VLR 收到 HLR/AC 的鉴权结果后，根据结果决定接入/拒绝后续业务。如果是鉴权成功，MSC/VLR 向 HLR/AC 发送 REGNOT 消息。

5、HLR/AC 返回位置登记响应消息 regnot。

6、MSC/VLR 向 BSS 返回位置登记接受消息（Location Updating Accept）。

如图 4 所示，是对共享保密数据（SSD，shared Secret Data）更新时的鉴权流程。SSD 是一组存储于用户终端半永久存储器中的 128 位的数据，网络端随时可以获得。SSD 被分成两上不同的子集，每个部分用来支持不同的过程。SSD 的前 64 位 SSD-A 用于支持鉴权过程，后 64 位 SSD-B 用于语音保密和信令信息加密。在该鉴权流程中：

1、MSC 发起鉴权请求消息 AUTHREQ。

2、如果 HLR/AC 判断鉴权失败，发起 SSD 更新流程。向 MSC 发送 authreq 消息，消息中带有用于计算 SSD 的随机数 RANDSSD、AUTHU 和用于计算 AUHTU 的随机数 RANDU。

3、MSC 给手机下发 SSD 更新请求消息（SSD Update Request），在该消息中携带有用于 SSD 更新的随机数 RANDSSD。

4、手机收到随机数 RANDSSD 后，产生一个 RANDBS 参数，并利用 CAVE 算法计算出一个 SSD 值和 AUTHBS 值。此时，手机要求验证网络侧的合法性，发送 Base Station Challenge 消息到 MSC，在该消息中携带有 RANDBS 参数。

5、MSC 向 HLR/AC 发送基站查询消息。

6、HLR/AC 将验证结果送给 MSC。

7、MSC 用与发给手机相同的 RANDSSD 参数计算出一个新的 SSD 值，且在从手机收到 RANDBS 参数后，与新的 SSD 一起利用 CAVE 算法算出 AUTHBS 参数，此时，给手机发送基站查询响应消息（Base Station Challenge Response），在该消息中携带有 AUTHBS 参数。

8、手机比较从网络侧收到的 AUTHBS 参数和它自己算出的 AUTHBS 值，如果两个值相同，则表示验证通过，更新原先手机中保存的 SSD 参数，向 MSC 上报 SSD 更新接受消息（SSD Update Response）；如果两个值不同，则手机放弃新的 SSD 值仍保留当前的值。

9、SSD 更新后，必然发起一次独特查询。MSC 向 BSS 发送独特查询消息（Authentication Request），在该消息中携带随机数 RANDU，要求进行独特查询。

10、手机用更新后的 SSD 和 RANDU 计算得到 AUTHU，通过独特查询响应消息（Authentication Response）上报给 MSC/VLR。

11、MSC 向 VLR 发送鉴权状态报告消息 ASREPORT，在该消息中携带有 SSD 更新的结果 SSDUPRT 和独特查询的结果 UCHALRPT。

12、VLR 回送鉴权状态报告响应消息 asreport。

13、MSC 向 HLR/AC 发送鉴权状态报告消息 ASREPORT，在该消息中携带有 SSD 更新的结果 SSDUPRT 和独特查询的结果 UCHALRPT。

14、HLR/AC 回送鉴权状态报告响应消息 asreport。

如图 5 所示，是为 IPV4 及 IPV6 网络定义的一种被称为“基于 CAVE 的 Early IMS”鉴权流程。但是这种鉴权流程对现有的鉴权流程有较大的修改，并且 S-CSCF、P-CSCF 也需要配合进行较大的修改。

另外，3GPP 标准组织提出的一种 EARLY IMS 的方案，该方案是接入网对终端鉴权后，利用接入网络与 IMS 网络的信任关系，由接入网络向 IMS 网络通知该用户获得的 IP 地址，IMS 网络接受该所述 IP 地址的终端注册。但是，在这种方案中，由于没有建立 IPSEC，故存在安全隐患，利用 IP 地址仿冒就可能实现破坏性的攻击，如仿冒用户进行去注册等操作。

发明内容

本发明实施例提供一种用于鉴权的方法、系统及装置，使用户终端与

IMS 网络之间的鉴权更加安全。

本发明实施例提供的一种用于鉴权的方法，包括如下步骤：

第三实体生成第二鉴权数据及第二随机数，并将所述第二随机数发送给第二实体；

所述第二实体将根据所述第二随机数得到的第一随机数发送给第一实体；

所述第一实体根据所述第一随机数生成第一鉴权数据，并将所述第一鉴权数据发送给所述第二实体；

所述第二实体根据所述第一鉴权数据及所述第二随机数生成第三鉴权数据，并将所述第三鉴权数据发送给所述第三实体；

所述第三实体通过对比所述第二鉴权数据和所述第三鉴权数据的一致性来判断鉴权是否成功。

本发明实施例还提出一种用于鉴权的方法，包括如下步骤：

第三实体生成第二鉴权数据及第二随机数，并将所述第二随机数发送给第二实体；

所述第二实体根据所述第二随机数得到多个第一随机数，并将所述多个第一随机数发送给第一实体；

所述第一实体根据所述多个随机数生成相对应的多个第一鉴权数据，并将所述多个第一鉴权数据发给所述第二实体；

所述第二实体将由所述多个第一鉴权数据组合成的第三鉴权数据发送给所述第三实体。

所述第三实体通过对比所述第三鉴权数据和所述第二鉴权数据的一致性来判断鉴权是否成功。

相应地，本发明实施例提供的一种用于鉴权的系统，包括第一实体、第二实体和第三实体，其中，所述第一实体与所述第二实体之间拥有信任机制，所述第二实体与所述第三实体之间可交换与第一随机数相关联的随机数；

所述第三实体用于根据由所述随机数获得的第一随机数利用第一算法生成第一鉴权数据，并将所述第一鉴权数据发送给所述第二实体，且依

据所述第一鉴权数据生成第二鉴权数据；并用于通过对比所述第二鉴权数据及第三鉴权数据进行鉴权；

所述第一实体用于根据所述第一随机数利用第一算法生成第一鉴权数据，并将所述第一鉴权数据发送给所述第二实体；

所述第二实体用于依据所述第一鉴权数据生成第三鉴权数据，并将所述第三鉴权数据发送给所述第三实体。

本发明实施例提供的一种用于鉴权的装置，包括用于与 S-CSCF 进行信息交互的 S-CSCF 接口模块，和用于进行第二算法运算的第二算法执行模块；还包括：

HLR 接口模块，用于与 HLR 进行信息交互，获取第一鉴权数据及第一随机数；

第二算法参数生成模块，用于从 HLR 接口模块处接收所述第一随机数及第一鉴权数据；并将由所述第一随机数及第一鉴权数据运算/组合获得的第二随机数和第一密钥传送给所述第二算法执行模块。

本发明实施例提供的另一种用于鉴权的装置，包括用于与 P-CSCF 进行信息交互的 P-CSCF 接口模块，以及用于进行第二算法运算的第二算法执行模块；还包括：

用户识别卡接口模块，用于与用户识别卡进行信息交互，将从网络收到的第二随机数发送给用户识别卡，并且接收用户识别卡所反馈的第一随机数及第一鉴权数据；

第二算法参数生成模块，用于从用户卡接口模块处接收所述第一随机数及第一鉴权数据，并将由所述第一随机数及第一鉴权数据运算/组合所获得的第二随机数和第一密钥传送给第二算法执行模块。

实施本发明实施例的用于鉴权的方法、系统及装置系统，在没有共享密钥的第二实体和第三实体之间需要鉴权时，可以通过与他们分别拥有信任机制的第一实体及第四实体，对第二实体与第三实体之间交换的随机数进行计算，产生共同的密钥或认证向量，从而实现鉴权过程。在应用面，本发明实施例在对 IMS 注册过程中，在终端侧和网络侧，同时采用 CAVE 算法，生成鉴权数据；并以该鉴权数据为密钥采用 AKA 算法，生成五元

组的认证向量，或者直接以多个鉴权数据组成一个五元组的认证向量，从而实现终端与网络的相互鉴权过程。这种鉴权的方式无需对现有网络进行大的修改，且能够在接入网与 IMS 网之间建立很好的 IPSEC，保证终端与网络之间通信的安全性，可以防御更多来自外界的攻击。

附图说明

图 1 是现有的 AKA 鉴权算法示意图；

图 2 是现有的一种 IP 多媒体子系统鉴权流程示意图；

图 3 是现有的进行注册时采用 CAVE 算法的鉴权流程示意图；

图 4 是现有的对共享保密数据更新时的鉴权流程示意图；

图 5 是现有的 IPV4 及 IPV6 网络定义的一种被称为“基于 CAVE 的 Early IMS”鉴权流程示意图；

图 6 是本发明用于鉴权的方法的第一实施例的流程图；

图 7 是本发明图 6 中所采用鉴权流程所基于的原理示意图；

图 8 是本发明用于鉴权的方法的第二实施例的流程图；

图 9 是本发明用于鉴权的方法的第三实施例的流程图；

图 10 是本发明 HSS 的第一实施例的结构示意图；

图 11 是本发明 HSS 的第二实施例的结构示意图；

图 12 是本发明一实施例中的用户终端的结构示意图。

具体实施方式

本发明实施例提供了一种用于鉴权的方法、装置及系统，下面结合附图进行详细说明。

如图 6 所示，是本发明用于鉴权的方法的第一实施例的流程图。

步骤 1：用户终端（UE）向呼叫会话控制功能（CSCF）发送注册请求，请求注册到该 IMS 网络；

步骤 2：CSCF 向归属用户服务器（HSS）请求鉴权数据；

步骤 3：HSS 向归属位置寄存器（HLR）请求鉴权数据；

步骤 4：HLR 生成随机数 Randr，并根据该随机数 Randr 采用 CAVE 算法生成鉴权数据 Authr，并将该鉴权数据 Authr 反馈给 HSS；

步骤 5：HSS 以 Authr 生成密钥并以 Randr 生成 Rand，采用 AKA 算

法计算出五元组的认证向量 AV（AUTN，Xres，IK，CK，Rand）;

步骤 6：HSS 把认证向量发给 CSCF;

步骤 7：CSCF 把认证向量中的随机数 Rand 及认证令牌 AUTN 发给用户终端;

步骤 8：用户终端从随机数 Rand 得到 Randr

步骤 9：用户终端把 Randr 发给用户识别卡（Card）;

步骤 10:用户识别卡根据随机数 Randr 用 CAVE 算法计算出鉴权数据 Authr，并把该鉴权数据 Authr 反馈给用户终端;

步骤 11：用户终端以 Authr 生成密钥并结合随机数 Rand，采用 AKA 算法计算出五元组的认证向量 AV;

步骤 12、用户终端把鉴权结果 Xres 发给 CSCF 用于后续的鉴权流程，CSCF 即可以通过比较来自用户终端的 Xres 与 HSS 中生成的 Xres 是否相同，来对用户终端进行鉴权，如果两者相同，则表示对终端鉴权成功。

在本实施例中，HSS 向 HLR 获取鉴权数据，然后把获取的鉴权数据作为终端的鉴权密钥，生成五元组的认证向量。终端将从网络收到的随机数发送给用户识别卡，并且把用户识别卡反馈的鉴权结果作为鉴权密钥，生成五元组的认证向量，从而实现终端与网络之间的鉴权过程。

在另外的一些实施例中，HLR 和 HSS 可以整合在一起，前面所述步骤 3 和步骤 4 即可以是内部实现过程，对外面没有表现，或者 Randr 可以由多个随机数组成，所述 Authr 可以是与所述多个随机数对应的多个鉴权数据。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以存储于一计算机可读取存储介质中，所述的存储介质，如：ROM/RAM、磁碟、光盘等。

如图 7 所示，是本发明图 6 中所采用鉴权流程所基于的原理示意图：

实体 A 和 B 之间需要鉴权，使用鉴权算法 2，但是 A 和 B 没有共享的密钥。

实体 X 和 Y 之间需要鉴权，使用鉴权算法 1，X 和 Y 有共享的密钥。

实体 X 和 A 之间已经建立了信任关系，实体 A 可以向实体 X 请求鉴权数据。

实体 B 和 Y 之间已经建立了信任关系，实体 B 可以向实体 Y 请求鉴权数据。

实体 A 和 B 通过交换来获得一个共同的挑战随机数。其工作原理如下所述:

（a）实体 Y 生成随机数并利用算法 1 和所述第一随机数生成第一鉴权数据;

（b）实体 B 以所述第一鉴权数据生成算法 2 所需的密钥，以所述第一随机数生成算法 2 所需的第二随机数（即挑战随机数），并以所述密钥和第二随机数利用算法 2 生成第二鉴权数据；并把该第二随机数和第二鉴权数据发送给所述实体 B;

（c）实体 B 把第二随机数发给所述实体 A，中间可能要通过一些实体（未画出）;

（d）实体 A 根据所述第二随机数得到所述第一随机数，并把所述第一随机数发送给所述实体 X;

（e）实体 X 根据所述第一随机数利用算法 1 生成第一鉴权数据，并发给所述实体 A;

（f）所述第实体 A 以所述第一鉴权数据生成密钥，并以所述第二随机数和所述密钥利用算法 2 生成第三鉴权数据，并把所述第三鉴权数据发送给所述实体 B;

（g）通过对比实体 B 中的所述第二鉴权数据和实体 A 中的所述第三鉴权数据的一致性来判断鉴权是否成功。

实体 A 和 B 都以各自获得的鉴权数据为密钥，由于 X 和 Y 使用共同的密钥和挑战随机数产生的鉴权数据，所以 A 和 B 活动的鉴权数据相同，也就是 A 和 B 获得了一个共同的密钥。

这样实体 A 和 B 就可以通过算法 2 进行鉴权了。

在上面的图 6 中，用户终端、HSS、用户识别卡、HLR 可以分被看作是实体 A、B、X、Y; CAVE 算法可以被看作是算法 1; AKA 算法可以被

看作是算法 2; 鉴权数据 Auth 可以被看作是实体 A、B 所获得的共同密钥，Randr 为第一随机数；Rand 为第二随机数；Authr 为第一鉴权数据；实体 A 及实体 B 中的 Xres 分别为第三鉴权数据及第二鉴权数据。

另外，在其他的实施例中，所述实体 Y 和实体 B 也可以由一个实体来实现，下称实体 BY（未画出），则其原理为：

（a）实体 BY 生成随机数并利用算法 1 和所述第一随机数生成第一鉴权数据;

（b）实体 BY 以所述第一鉴权数据生成算法 2 所需的密钥，以所述第一随机数生成算法 2 所需的第二随机数（即挑战随机数），并以所述密钥和第二随机数利用算法 2 生成第二鉴权数据;

（c）实体 BY 把第二随机数发给所述实体 A，中间可能要通过一些实体（图中未画出）;

（d）至（e）不变;

（f）所述第实体 A 以所述第一鉴权数据生成密钥，并以所述第二随机数和所述密钥利用算法 2 生成第三鉴权数据，并把所述第三鉴权数据发送给所述实体 BY;

（g）所述实体 BY 过对比所述第二鉴权数据和所述第三鉴权数据的一致性来判断鉴权是否成功。

如图 8 所示，是本发明用于鉴权的方法第二实施例的流程图。其中，

步骤 1：用户终端（UE）向呼叫会话控制功能（CSCF）发送注册请求，请求注册到该 IMS 网络;

步骤 2：CSCF 向归属用户服务器（HSS）请求鉴权数据;

步骤 3：HSS 向归属位置寄存器（HLR）请求鉴权数据；并连续请求 4 次分别对应步骤 3、3a、3b、3c;

步骤 4：HLR 根据 4 次请求，并采用 CAVE 算法，生成 4 次鉴权数据（分别包括 Rand1 及 Auth1、Rand2 及 Auth2、Rand 3 及 Auth3、Rand 4 及 Auth4），并分别在对应步骤 4、4a、4b、4c 中反馈给 HSS;

步骤 5：HSS 把 4 个鉴权数据中的 32 位的 Rand1/2/3/4 合成 1 个 128 位的 Rand，并把 Auth1/2/3/4 分别对应（AUTN，Xres，IK，CK），生成

一个 5 元组的认证向量 AV;

步骤 6: HSS 把认证向量发给 CSCF;

步骤 7: CSCF 把认证向量中的随机数 Rand 及认证令牌 AUTN 发给用户终端;

步骤 7a: 用户终端把 128 位的 Rand 分解为 4 个 32 位的 Rand1、Rand2、Rand3 及 Rand4;

步骤 8: 用户终端把该 4 个随机数（Rand1、Rand2、Rand3 及 Rand4）分 4 次发给用户识别卡，用于请求鉴权结果，对应步骤 8、8a、8b、8c;

步骤 9: 用户识别卡根据 Rand1、Rand2、Rand3 及 Rand4 分别用 CAVE 算法计算出鉴权数据 Auth1、Auth2、Auth3 及 Auth4，并把鉴权数据结果反馈给用户终端，对应步骤 9、9a、9b、9c;

步骤 10: 用户终端把 Auth1、Auth2、Auth3 及 Auth4 分别对应为 AUTN、Xres、IK、CK，并结合原 128 位的 Rand，生成一个五元组的认证向量 AV;

步骤 11: 用户终端把鉴权结果 Xres 发给 CSCF 用于后续的鉴权流程，CSCF 即可以通过比较来自用户终端的 Xres 与 HSS 中生成的 Xres 是否相同，来对用户终端进行鉴权，如果两者相同，则表示对终端鉴权成功。

在本实施例中，HSS 能向 HLR 分多次获取鉴权数据，把多个随机数合成为一个随机数，把多次获得的数据对应到五元组的认证向量中。终端将从网络收到的随机数分解为多个随机数并发送给用户识别卡，并且把用户识别卡反馈的多个鉴权结果对应为五元组的认证向量。从而实现终端与网络之间的鉴权过程。

在另外的一些实施例中，HLR 和 HSS 可以整合在一起，前面所述步骤 3、3a、3b、3c 和步骤 4、4a、4b、4c 是内部实现，对外没有表现。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以存储于一计算机可读取存储介质中，所述的存储介质，如: ROM/RAM、磁碟、光盘等。

根据图 8 中的第二实施例，可以很容易地对图 7 中的鉴权系统模型进行一些适当修改，是本技术领域内的普通技术人员很容易想到的，在此不

进行详细说明，本发明所要求保护的是上述实施例中所涉及的方法、系统及装置（如 HSS、用户终端等）。

如图 9 所示，是本发明用于鉴权的方法第三实施例的流程图。其中，

步骤 1：用户终端（UE）向呼叫会话控制功能（CSCF）发送注册请求（Register），请求注册到该 IMS 网络；

步骤 2：CSCF 发送 CxAuthReq 消息向归属用户服务器（HSS）请求鉴权数据；

步骤 3：HSS 向归属位置寄存器（HLR）请求鉴权数据；

步骤 4：HLR 生成随机数 Randu，并根据该随机数 Randu 采用 CAVE 算法生成鉴权数据 Authu，并将该鉴权数据 Authu 反馈给 HSS；

步骤 4a：HSS 向 HLR 反馈鉴权状态报告，请求反馈共享加密数据（SSD）；

步骤 4b：HLR 向 HSS 反馈共享加密数据（SSD）；

步骤 5：HSS 生成一个随机数 Randr，利用 CAVE 算法根据 SSD 生成鉴权数据 AuthR、信令加密数据（Signaling Message Encryption Key, SMEKEY）和语音加密数据（CDMA Private Long Code Mask，CDMAPLCM），后两项统称为 Keys，HSS 以 AuthR 或/及 Keys 生成 AKA 算法的鉴权密钥，生成方式可以是使用 SMEKEY、CDMAPLCM 加上 AuthR 一起进行位运算得到。并且 HSS 利用 Randr 生成 AKA 算法的随机数 Rand，最后根据该随机数 Rand 及鉴权密钥采用 AKA 算法计算出 5 元组的认证向量 AV（Rand ，AUTN，Xres，IK，CK）；

步骤 6：HSS 把认证向量 AV 发给 CSCF；

步骤 7：CSCF 把认证向量 AV 中的随机数 Rand 及认证令牌 AUTN 发给用户终端；

步骤 8：用户终端从随机数 Rand 得到 Randr

步骤 9：用户终端把 Randr 发给用户识别卡（Card）；

步骤 10：用户识别卡根据随机数 Randr 用 CAVE 算法计算出鉴权数据 Authr，Keys 并把该鉴权数据 Authr 和 Keys 值反馈给用户终端；

步骤 11：用户终端以 Authr 或/及 Keys 生成 AKA 算法的鉴权密钥，

并结合随机数 Rand，采用 AKA 算法计算出五元组的认证向量 AV;

步骤 12、用户终端把鉴权结果 Xres 发给 CSCF 用于后续的鉴权流程，CSCF 即可以通过比较来自用户终端的 Xres 与 HSS 中生成的 Xres 是否相同，来对用户终端进行鉴权，如果两者相同，则表示对终端鉴权成功。

在本实施例中，HSS 向 HLR 获取鉴权数据，并把具有 CAVE 执行的能力通知给 HLR，HLR 就会把共享加密数据 SSD 发送给 HSS，HSS 就可以利用 CAVE 算法根据 SSD 计算鉴权数据（AuthR，Keys），然后把计算得到的鉴权数据合成为终端的鉴权密钥，生成五元组的认证向量。终端将从网络收到的随机数发送给用户识别卡，并且把用户识别卡反馈的鉴权结果做为鉴权密钥，生成五元组的认证向量，从而实现终端与网络之间的鉴权过程。

在另外的一些实施例中，HLR 和 HSS 可以整合在一起，前面所述步骤 3、步骤 4、步骤 4a 和步骤 4b 即可以是内部实现过程，对外面没有表现，或者 Randr 可以由多个随机数组成，所述 Authr，Keys 可以是与所述多个随机数对应的多个鉴权数据。

根据图 9 的第三实施例，可以很容易地对图 7 中的鉴权系统模型进行一些适当修改，是本技术领域内的普通技术人员很容易想到的，在此不再进行详细说明。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以存储于一计算机可读取存储介质中，所述的存储介质，如：ROM/RAM、磁碟、光盘等。

本发明的一种用于鉴权的系统主要包括有用户终端、用户识别卡、P-CSCF、S-CSCF、HSS 及 HLR 等。下面请进一步参照附图 10 至图 12 所示，对本发明涉及的主要装置进行详细的说明。

如图 10 所示，为本发明用于鉴权装置（HSS）的第一实施例的结构示意图。该 HSS 主要包括有依次连接的 HLR 接口模块 101、AKA 算法参数生成模块 102、AKA 算法执行模块 103 及 S-CSCF 接口模块 104。其中，HLR 接口模块 101 用于与 HLR 进行信息交互；AKA 算法参数生成模块

102 用于生成用于 AKA 算法的参数（如，随机数和密钥等）；AKA 算法执行模块 103 用于执行 AKA 算法；而 S-CSCF 接口模块 104 用于与 S-CSCF 进行信息交互。

首先，通过 HLR 接口模块 101 与 HLR 之间的信息交互，获取第一随机数及第一鉴权数据；接着，AKA 算法参数生成模块 102 从 HLR 接口模块 101 处获该第一随机数和第一鉴权数据，并进行组合或/及运算，得到 AKA 算法所需的第二随机数和一密钥，交由 AKA 算法执行模块 103 进行 AKA 算法计算，AKA 算法执行模块 103 将该第二随机数及密钥利用 AKA 算法进行计算获得计算结果（第二鉴权数据），该计算结果经由 S-CSCF 接口模块 104 传送给 S-CSCF。

如图 11 所示，为本发明用于鉴权装置（HSS）的第二实施例的结构示意图。其与图 10 所示的第一实施例的最大的区别在于，在 HLR 接口模块 101 与 AKA 算法参数生成模块 102 之间还设有一 CAVE 算法执行模块 105，该 CAVE 算法执行模块 105 用于执行 CAVE 算法。

在该实施例中，首先，通过 HLR 接口模块 101 与 HLR 之间的信息交互，此时获取的是用于 CAVE 算法的共享加密数据（SSD）；CAVE 算法执行模块 105 根据该共享加密数据利用 CAVE 算法进行运算，生成第一鉴权数据，同时输出用于 CAVE 运算的第一随机数；接着，AKA 算法参数生成模块 102 从 CAVE 算法执行模块 105 处获该第一随机数和第一鉴权数据，进行组合或/及运算，得到 AKA 算法所需的第二随机数和一密钥，交由 AKA 算法执行模块 102 进行 AKA 算法计算，AKA 算法执行模块 102 将该第二随机数及密钥利用 AKA 算法进行计算获得计算结果（第二鉴权数据），该计算结果经由 S-CSCF 接口模块 104 传送给 S-CSCF。

如图 12 所示，为本发明用于鉴权装置（用户终端）的结构示意图。该用户终端主要包括有依次连接的用户识别卡接口模块 121、AKA 算法参数生成模块 122、AKA 算法执行模块 123 及 P-CSCF 接口模块 124。其中，用户识别卡接口模块 121 用于与用户识别卡进行信息交互；AKA 算法参数生成模块 122 用于生成 AKA 算法所需的参数（如，随机数和密钥等）；AKA 算法执行模块 123 用于执行 AKA 算法；P-CSCF 接口模块 124 用于

与 P-CSCF 进行信息交互。

首先，用户识别卡接口模块 121 与用户识别卡进行信息交互，获得 CAVE 算法第一随机数及第一鉴权数据；AKA 算法参数生成模块 122 将该第一随机数和第一鉴权数据，进行组合或/及运算，得到 AKA 算法所需的第二随机数和一密钥，交由 AKA 算法执行模块 123 进行计算，AKA 算法执行模块 123 将该第二随机数及密钥利用 AKA 算法进行计算获得第二鉴权数据；该第二鉴权数据经 P-CSCF 接口模块 124 传送给 P-CSCF。

本发明在对 IMS 注册过程中，在终端侧和网络侧，同时采用 CAVE 算法，生成鉴权数据；并以该鉴权数据为密钥采用 AKA 算法，生成五元组的认证向量，或者直接以多个鉴权数据组成一个五元组的认证向量，从而实现终端与网络的相互鉴权过程。这种鉴权的方式无需对现有网络进行大的修改，且能够在接入网与 IMS 网之间建立很好的 IPSEC，可以解决现有技术中的安全性漏洞；可以防御更多来自外界的攻击。

以上所揭露的仅为本发明一种用于鉴权的装置、系统及方法的较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明申请专利范围所作的等同变化，仍属本发明所涵盖的范围。

权 利 要 求

1、一种用于鉴权的方法，其特征在于，包括:

第三实体生成第二鉴权数据及第二随机数，并将所述第二随机数发送给第二实体;

所述第二实体将根据所述第二随机数得到的第一随机数发送给第一实体;

所述第一实体根据所述第一随机数生成第一鉴权数据，并将所述第一鉴权数据发送给所述第二实体;

所述第二实体根据所述第一鉴权数据及所述第二随机数生成第三鉴权数据，并把所述第三鉴权数据发送给所述第三实体;

所述第三实体通过对比所述第二鉴权数据和所述第三鉴权数据的一致性来判断鉴权是否成功。

2、如权利要求 1 所述的方法，其特征在于， 所述第三实体生成第二鉴权数据及第二随机数的步骤包括:

所述第三实体生成第一随机数并将所述第一随机数利用第一算法生成第一鉴权数据;

所述第三实体以所述第一鉴权数据生成密钥，以所述第一随机数生成第二随机数，并以所述密钥和所述第二随机数利用第二算法生成第二鉴权数据。

3、如权利要求 1 所述的方法，其特征在于，所述第一实体根据所述第一随机数生成第一鉴权数据的步骤包括:

所述第一实体根据所述第一随机数利用第一算法生成第一鉴权数据;

所述第二实体根据所述第一鉴权数据及所述第二随机数生成第三鉴权数据的步骤包括:

所述第二实体以所述第一鉴权数据生成密钥，并以所述第二随机数和所述密钥利用第二算法生成第三鉴权数据。

4、如权利要求 1 所述的方法，其特征在于，所述第三实体生成第二鉴权数据及第二随机数的步骤包括:

所述第三实体生成第三随机数并将所述第三随机数据利用第一算法

生成第四鉴权数据，以所述第三随机数生成第一随机数，所述第三实体根据所述第一随机数利用所述第一算法计算出第一鉴权数据，并判断第四鉴权数据的正确性，如果所述第四鉴权数据正确，则所述第三实体采用所述第一随机数和所述第一鉴权数据生成第一密钥；

所述第三实体以所述第一密钥和/或所述第四鉴权数据生成第二密钥，以所述第一随机数生成第二随机数；

所述第三实体以所述第二密钥和所述第二随机数利用第二算法生成第二鉴权数据。

5、如权得要求 4 所述的方法，其特征在于，所述判断第四鉴权数据的正确性的步骤包括：

将第四鉴权数据与所述第一鉴权数据进行比较，如果一致，则所述第四鉴权数据正确，否则，所述第四鉴权数据不正确。

6、如权利要求 1 所述的方法，其特征在于，所述第一实体根据所述第一随机数生成第一鉴权数据，并将所述第一鉴权数据发送给所述第二实体的步骤还包括：

所述第一实体根据所述第一随机数利用第一算法生成第一鉴权数据及第一密钥，并将所述第一鉴权数据及第一密钥发送给所述第二实体；

所述第二实体根据所述第一鉴权数据及所述第二随机数生成第三鉴权数据的步骤包括：

所述第二实体以所述第一鉴权数据和/或所述第一密钥生成第二密钥，并以所述第二随机数和所述第二密钥利用第二算法生成第三鉴权数据。

7、如权利要求 1 所述的方法，其特征在于：

所述第一随机数包括多个随机数据，所述第一鉴权数据包括与所述多个随机数据相对应的多个鉴权数据。

8、如权利要求 1 至 7 任一项所述的方法，其特征在于，所述第一实体、第二实体分别为用户识别卡、用户终端，所述第三实体为包含有呼叫会话控制功能、归属用户服务器及归属位置寄存器功能的实体。

9、根据权利要求 2 至 6 任一项所述的方法，其特征在于，所述第一算法为 CAVE 算法，所述第二算法为 AKA 算法。

10、一种用于鉴权的方法，其特征在于，包括:

第三实体生成第二鉴权数据及第二随机数，并将所述第二随机数发送给第二实体;

所述第二实体根据所述第二随机数得到多个第一随机数，并将所述多个第一随机数发送给第一实体;

所述第一实体根据所述多个随机数生成相对应的多个第一鉴权数据，并将所述多个第一鉴权数据发送给所述第二实体;

所述第二实体将由所述多个第一鉴权数据组合成的第三鉴权数据发送给所述第三实体。

所述第三实体通过对比所述第三鉴权数据和所述第二鉴权数据的一致性来判断鉴权是否成功。

11、如权利要求 10 所述的方法，其特征在于，

所述第三实体生成第二鉴权数据及第二随机数的步骤包括:

所述第三实体生成多个第一随机数，并将所述多个第一随机数利用第一算法生成多个第一鉴权数据，所述第三实体将所述多个第一随机数组合成第二随机数;

所述第三实体将所述多个第一鉴权数据组合成第二鉴权数据;

所述第一实体根据所述多个随机数生成相对应的多个第一鉴权数据的步骤包括:

所述第一实体将所述多个第一随机数利用第一算法生成多个第一鉴权数据。

12、如权利要求 10 或 11 所述的方法，其特征在于：所述第一实体、第二实体分别为用户识别卡、用户终端，所述第三实体为包含有呼叫会话控制功能、归属用户服务器及归属位置寄存器功能的实体，所述第二鉴权数据及第三鉴权数据均为一鉴权五元组。

13、如权利要求 11 所述的方法，其特征在于：所述第一算法为 CAVE 算法。

14、一种用于鉴权的系统，其特征在于：包括第一实体、第二实体和第三实体，其中，所述第一实体与所述第二实体之间拥有信任机制，所述

第二实体与所述第三实体之间可交换与第一随机数相关联的随机数;

所述第三实体用于根据由所述随机数获得的第一随机数利用第一算法生成第一鉴权数据，并将所述第一鉴权数据发送给所述第二实体，且依据所述第一鉴权数据生成第二鉴权数据；并用于通过对比所述第二鉴权数据及第三鉴权数据进行鉴权;

所述第一实体用于根据所述第一随机数利用第一算法生成第一鉴权数据，并把所述第一鉴权数据发送给所述第二实体;

所述第二实体用于依据所述第一鉴权数据生成第三鉴权数据，并把所述第三鉴权数据发送给所述第三实体。

15、如权利要求 14 所述的系统，其特征在于，所述第三实体进一步包括第四实体和第五实体，所述第四实体和第五实体之间拥有信任机制，且

所述第五实体用于根据所述第一随机数利用第一算法生成第一鉴权数据;

所述第四实体用于根据所述第一鉴权数据生成第二鉴权数据和接收来自所述第二实体的所述第三鉴权数据；并通过对比所述第二鉴权数据及第三鉴权数据进行鉴权。

16、如权利要求 14 或 15 所述的系统，其特征在于，

所述第三鉴权数据为所述第二实体以所述第一鉴权数据为密钥利用第二算法所生成;

所述第二鉴权数据为第三实体以所述第一鉴权数据为密钥利用第二算法所生成。

17、如权利要求 14 或 15 所述的系统，其特征在于，所述第一随机数包括多个随机数据，所述第一鉴权数据包括多个鉴权数据，所述多个随机数据与所述多个鉴权数据相对应。

18、如权利要求 14 或 15 所述的用于鉴权的系统，其特征在于，所述第二鉴权数据和所述第三鉴权数据分别由所述多个鉴权数据组合成。

19、如权利要求 16 所述的系统，其特征在于，所述第一实体、第二实体分别为用户识别卡、用户终端，所述第三实体为包含有归属用户服务

器及归属位置寄存器功能的实体；所述第一算法为 CAVE 算法，所述第二算法为 AKA 算法。

20、如权利要求 16 所述的系统，其特征在于，所述第一实体、第二实体分别为用户识别卡、用户终端，所述第四实体、第五实体分别为归属用户服务器、归属位置寄存器；所述第一算法为 CAVE 算法，所述第二算法为 AKA 算法。

21、一种用于鉴权的装置，包括用于与 S-CSCF 进行信息交互的 S-CSCF 接口模块，和用于进行第二算法运算的第二算法执行模块；其特征在于，还包括:

HLR 接口模块，用于与 HLR 进行信息交互，获取第一鉴权数据及第一随机数;

第二算法参数生成模块，用于从 HLR 接口模块处接收所述第一随机数及第一鉴权数据;并将由所述第一随机数及第一鉴权数据运算/组合获得的第二随机数和第一密钥传送给所述第二算法执行模块。

22、如权利要求 21 所述的装置，其特征在于:

所述第二算法执行模块将所获得的第二随机数和第一密钥利用第二算法进行计算，并将计算结果传送给 S-CSCF 接口模块。

23、如权利要求 21 或 22 所述的装置，其特征在于:

所述第二算法为 AKA 算法；所述第二鉴权数据为一鉴权五元组。

24、一种用于鉴权的装置，包括用于与 P-CSCF 进行信息交互的 P-CSCF 接口模块，以及用于进行第二算法运算的第二算法执行模块；其特征在于，还包括:

用户识别卡接口模块，用于与用户识别卡进行信息交互，将从网络收到的第二随机数发送给用户识别卡，并且接收用户识别卡所反馈的第一随机数及第一鉴权数据;

第二算法参数生成模块，用于从用户卡接口模块处接收所述第一随机数及第一鉴权数据，并将由所述第一随机数及第一鉴权数据运算/组合所获得的第二随机数和第一密钥传送给第二算法执行模块。

25、如权利要求 24 所述的装置，其特征在于:

所述第二算法执行模块将所获得的第二随机数和第一密钥利用第二算法进行计算，并将计算结果传送给 P-CSCF 接口模块。

26、如权利要求 24 或 25 所述的装置，其特征在于：

所述第二算法为 AKA 算法；所述第二鉴权数据为一鉴权五元组。

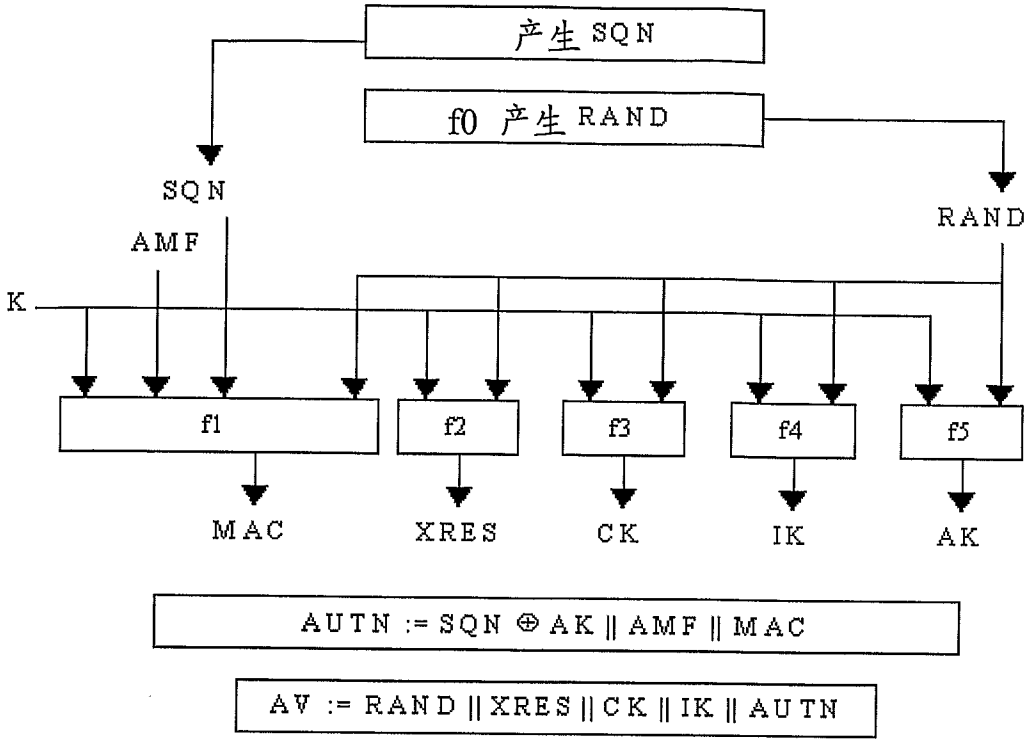

产生 SQN
f0 产生 RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

图 1

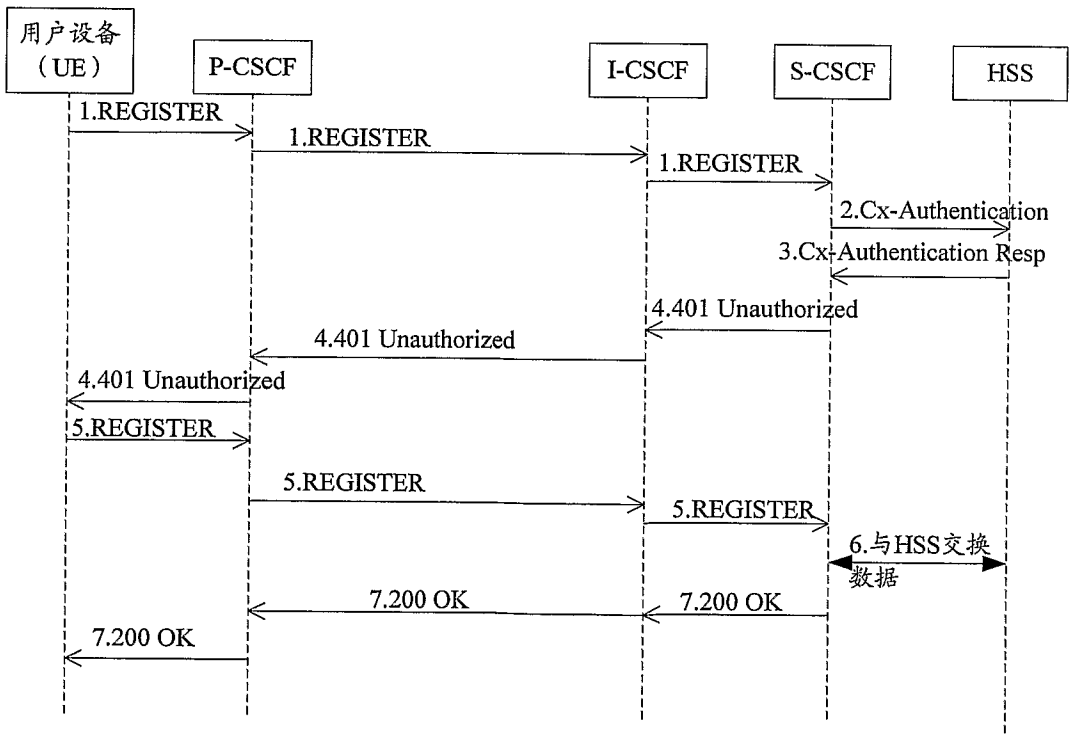

用户设备
(UE)
P-CSCF
I-CSCF
S-CSCF
HSS
1.REGISTER
1.REGISTER
1.REGISTER
2.Cx-Authentication
3.Cx-Authentication Resp
4.401 Unauthorized
4.401 Unauthorized
4.401 Unauthorized
5.REGISTER
5.REGISTER
5.REGISTER
6.与HSS交换
数据
7.200 OK
7.200 OK
7.200 OK

图 2

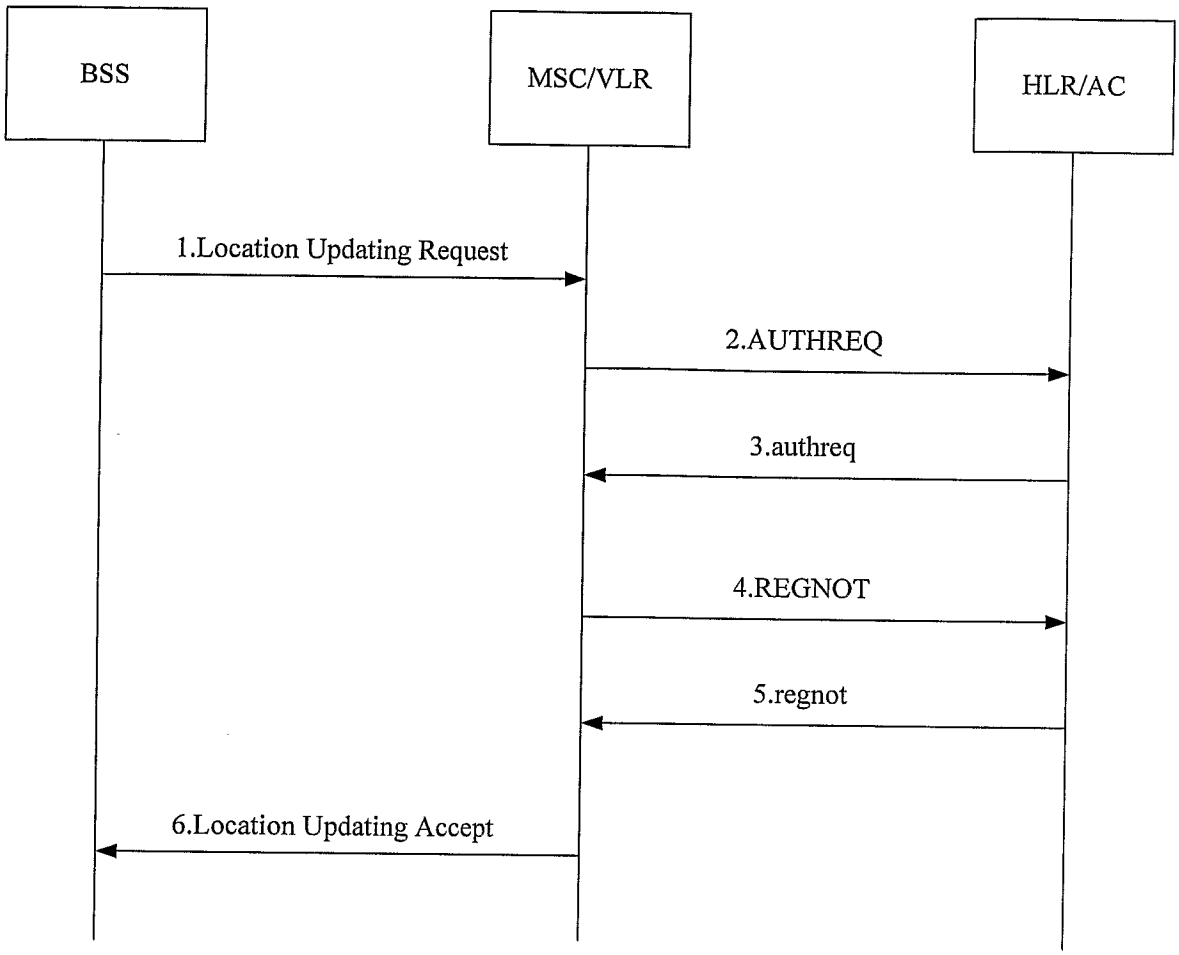

BSS
MSC/VLR
HLR/AC
1.Location Updating Request
2.AUTHREQ
3.authreq
4.REGNOT
5.regnot
6.Location Updating Accept

图 3

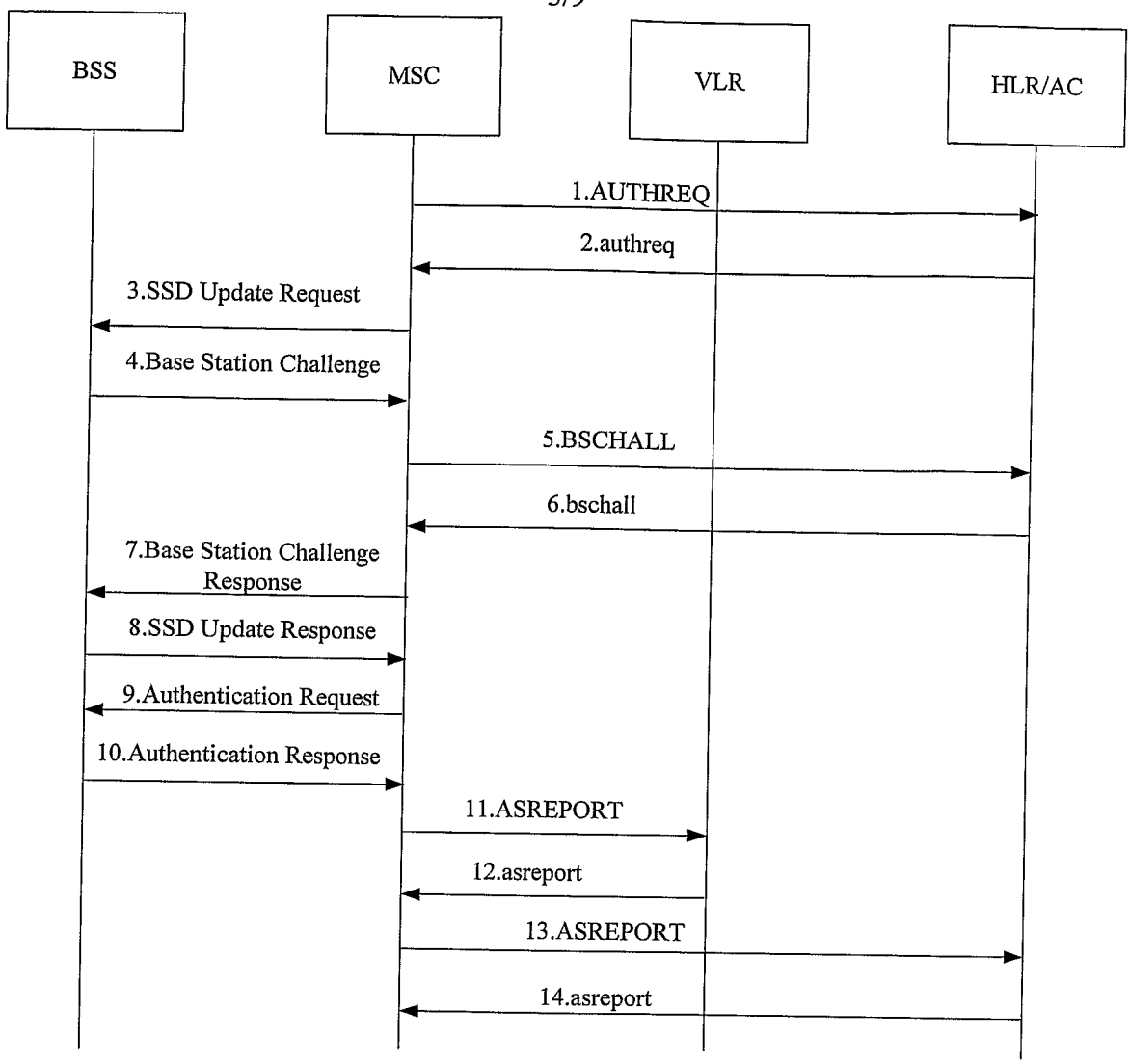

BSS
MSC
VLR
HLR/AC
1.AUTHREQ
2.authreq
3.SSD Update Request
4.Base Station Challenge
5.BSCHALL
6.bschall
7.Base Station Challenge Response
8.SSD Update Response
9.Authentication Request
10.Authentication Response
11.ASREPORT
12.asreport
13.ASREPORT
14.asreport

图 4

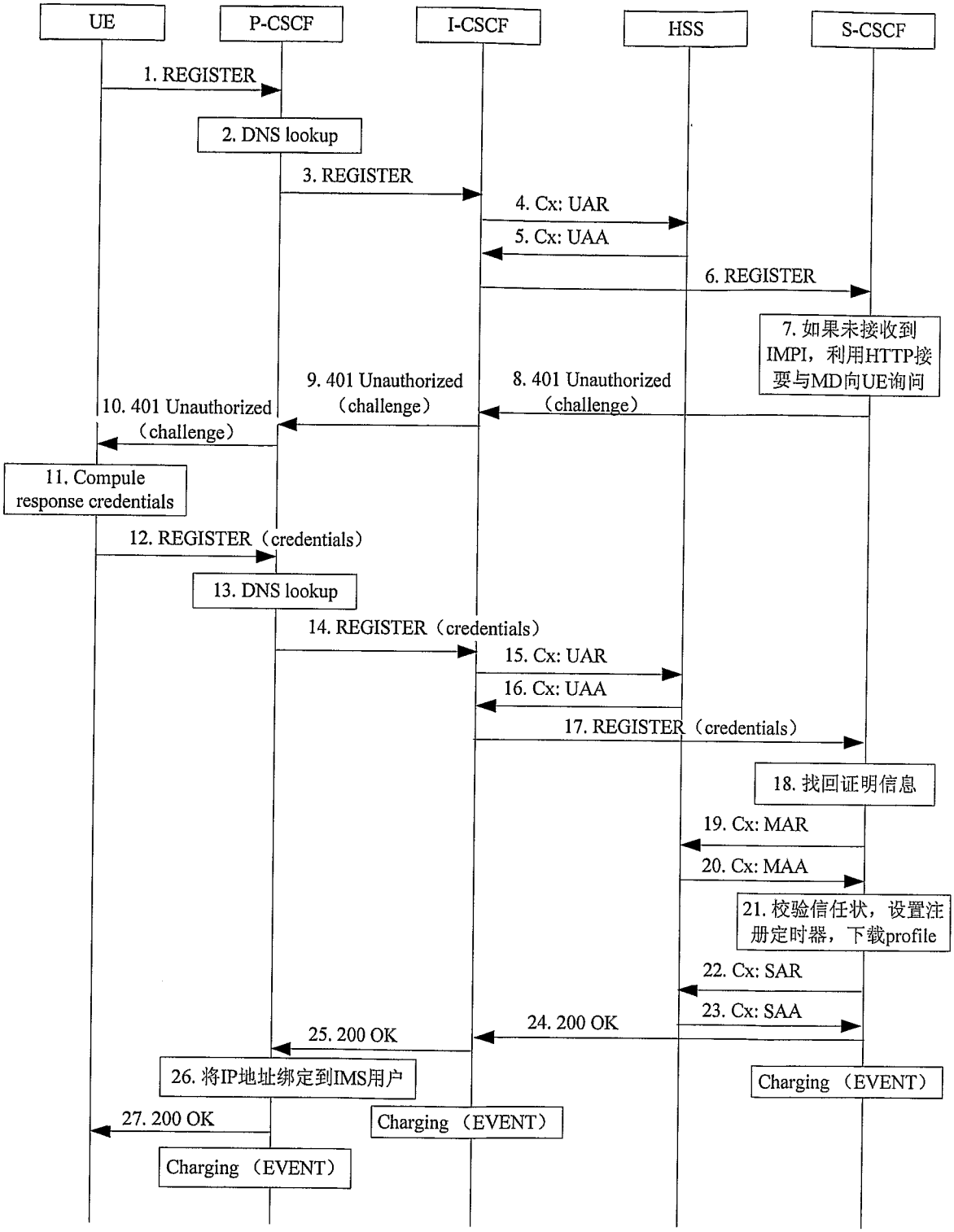

UE
P-CSCF
I-CSCF
HSS
S-CSCF
1. REGISTER
2. DNS lookup
3. REGISTER
4. Cx: UAR
5. Cx: UAA
6. REGISTER
7. 如果未接收到IMPI，利用HTTP接要与MD向UE询问
8. 401 Unauthorized (challenge)
9. 401 Unauthorized (challenge)
10. 401 Unauthorized (challenge)
11. Compule response credentials
12. REGISTER (credentials)
13. DNS lookup
14. REGISTER (credentials)
15. Cx: UAR
16. Cx: UAA
17. REGISTER (credentials)
18. 找回证明信息
19. Cx: MAR
20. Cx: MAA
21. 校验信任状，设置注册定时器，下载profile
22. Cx: SAR
23. Cx: SAA
24. 200 OK
25. 200 OK
26. 将IP地址绑定到IMS用户
27. 200 OK
Charging (EVENT)
Charging (EVENT)
Charging (EVENT)

图 5

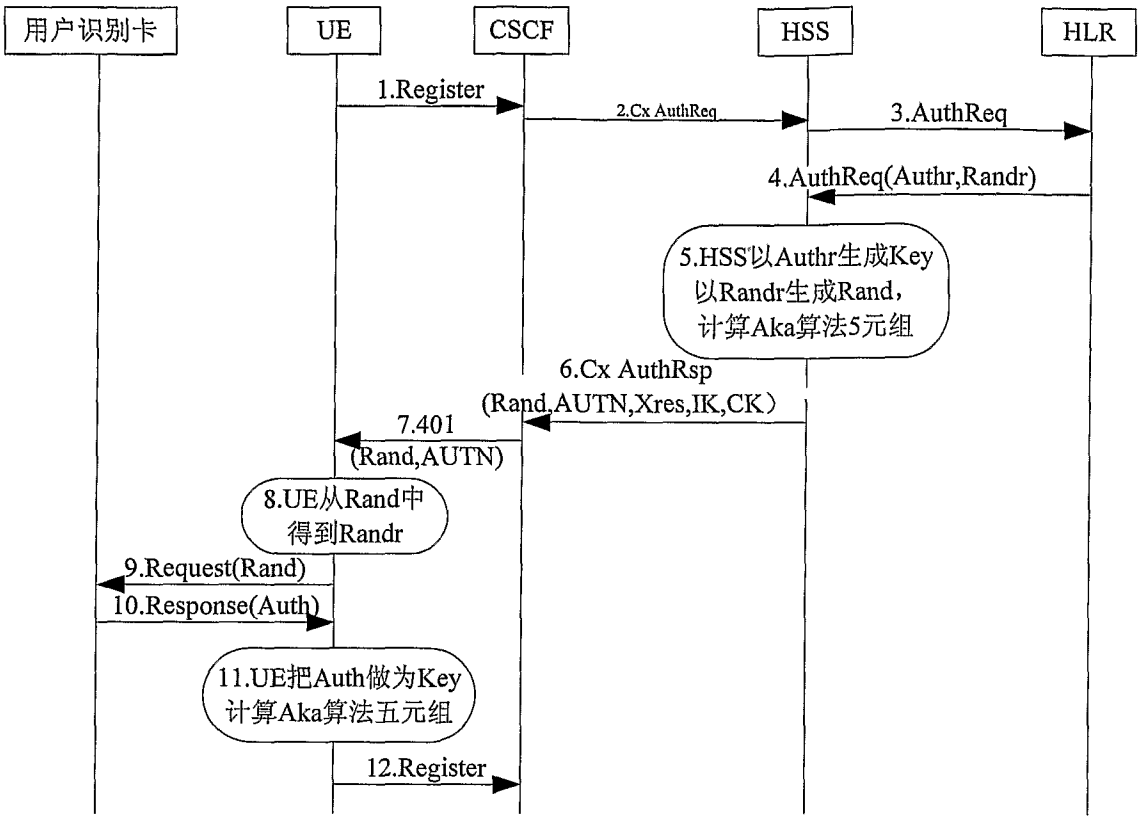

用户识别卡
UE
CSCF
HSS
HLR
1.Register
2.Cx AuthReq
3.AuthReq
4.AuthReq(Authr,Randr)
5.HSS以Authr生成Key
以Randr生成Rand，
计算Aka算法5元组
6.Cx AuthRsp
(Rand,AUTN,Xres,IK,CK)
7.401
(Rand,AUTN)
8.UE从Rand中
得到Randr
9.Request(Rand)
10.Response(Auth)
11.UE把Auth做为Key
计算Aka算法五元组
12.Register

图 6

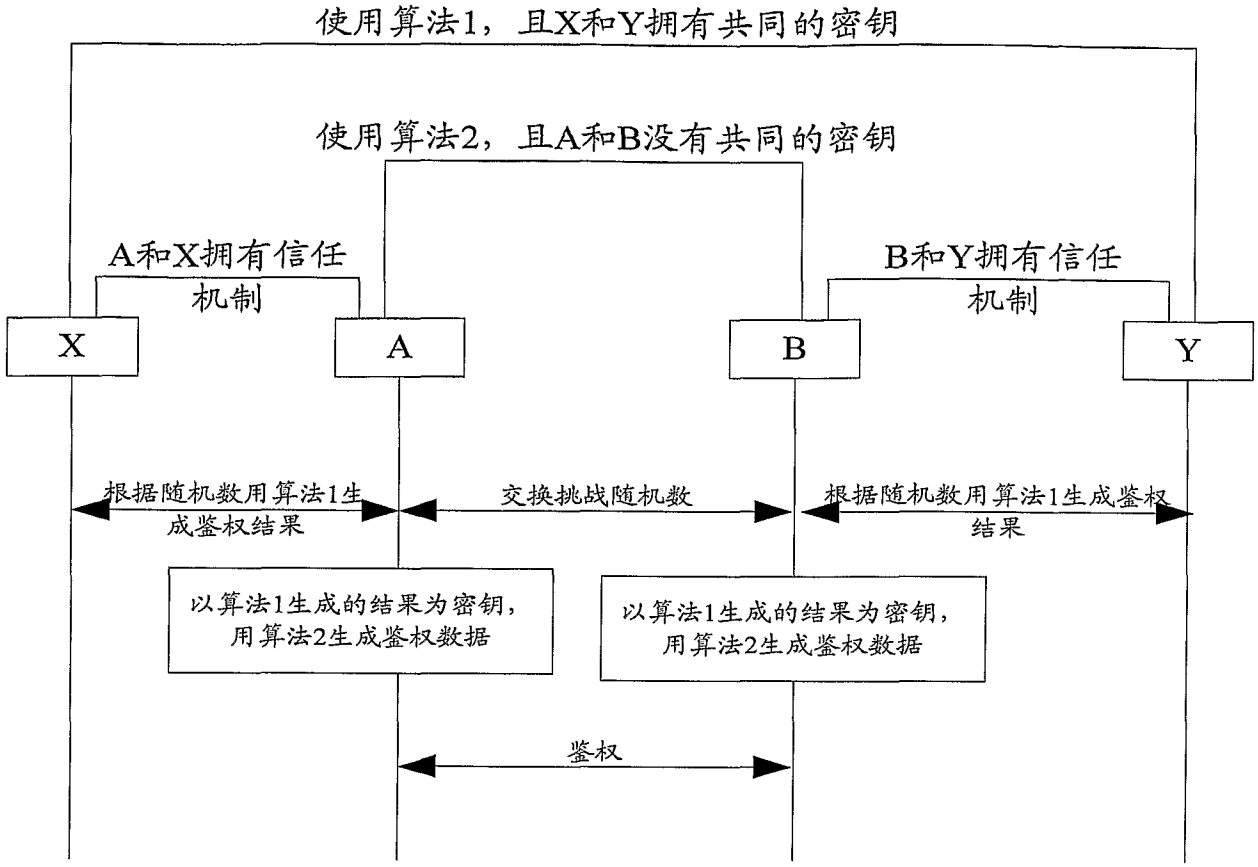

使用算法1，且X和Y拥有共同的密钥
使用算法2，且A和B没有共同的密钥
A和X拥有信任机制
B和Y拥有信任机制
X
A
B
Y
根据随机数用算法1生成鉴权结果
交换挑战随机数
根据随机数用算法1生成鉴权结果
以算法1生成的结果为密钥，用算法2生成鉴权数据
以算法1生成的结果为密钥，用算法2生成鉴权数据
鉴权

图 7

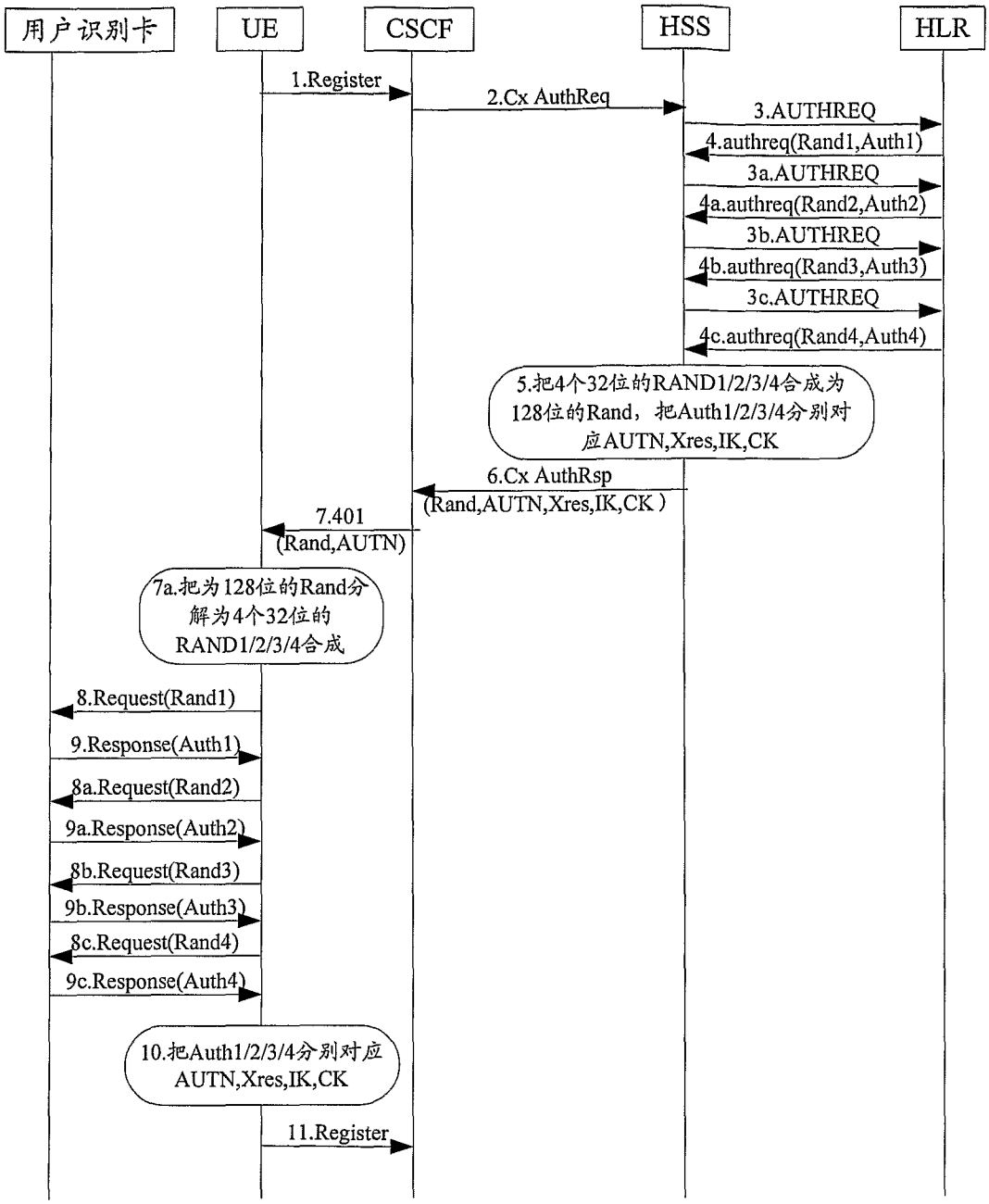

用户识别卡
UE
CSCF
HSS
HLR
1.Register
2.Cx AuthReq
3.AUTHREQ
4.authreq(Rand1,Auth1)
3a.AUTHREQ
4a.authreq(Rand2,Auth2)
3b.AUTHREQ
4b.authreq(Rand3,Auth3)
3c.AUTHREQ
4c.authreq(Rand4,Auth4)
5.把4个32位的RAND1/2/3/4合成为128位的Rand，把Auth1/2/3/4分别对应AUTN,Xres,IK,CK
6.Cx AuthRsp (Rand,AUTN,Xres,IK,CK)
7.401 (Rand,AUTN)
7a.把为128位的Rand分解为4个32位的RAND1/2/3/4合成
8.Request(Rand1)
9.Response(Auth1)
8a.Request(Rand2)
9a.Response(Auth2)
8b.Request(Rand3)
9b.Response(Auth3)
8c.Request(Rand4)
9c.Response(Auth4)
10.把Auth1/2/3/4分别对应AUTN,Xres,IK,CK
11.Register

图 8

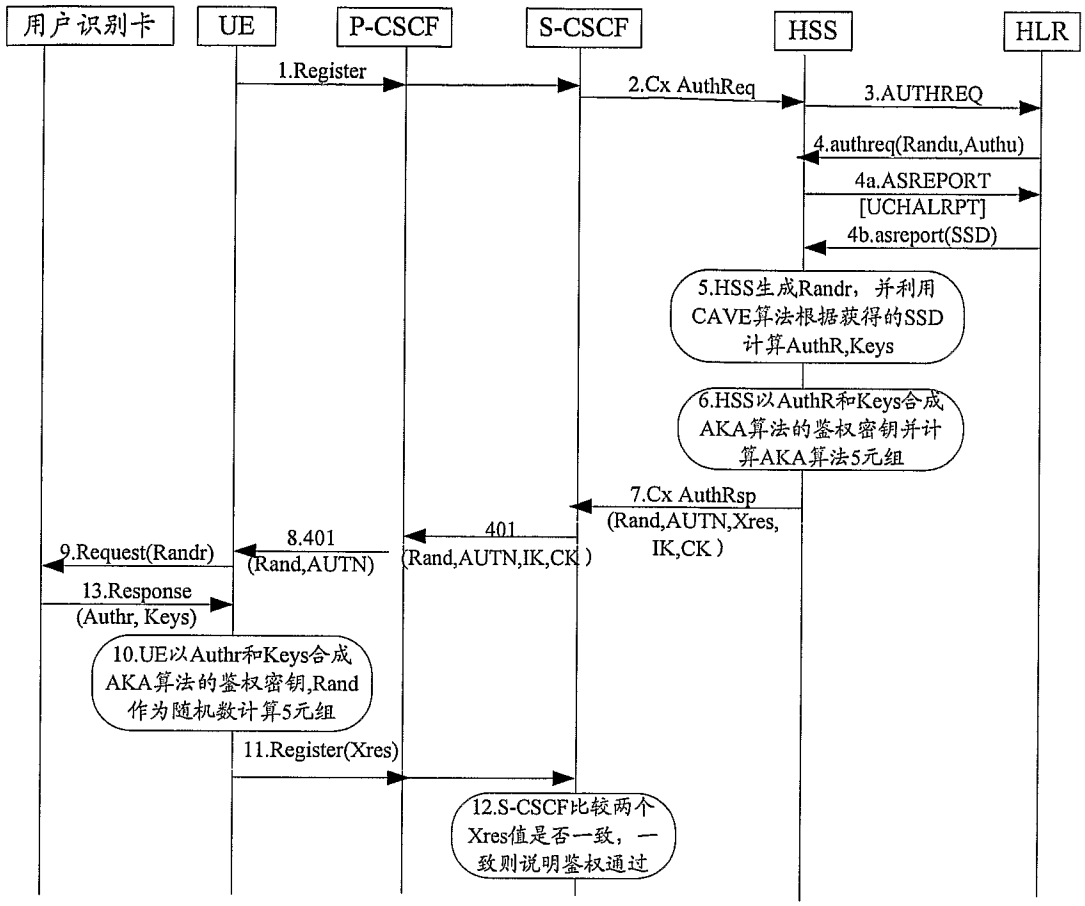

用户识别卡
UE
P-CSCF
S-CSCF
HSS
HLR
1.Register
2.Cx AuthReq
3.AUTHREQ
4.authreq(Randu,Authu)
4a.ASREPORT
[UCHALRPT]
4b.asreport(SSD)
5.HSS生成Randr，并利用CAVE算法根据获得的SSD计算AuthR,Keys
6.HSS以AuthR和Keys合成AKA算法的鉴权密钥并计算AKA算法5元组
7.Cx AuthRsp
(Rand,AUTN,Xres,IK,CK)
8.401
(Rand,AUTN)
401
(Rand,AUTN,IK,CK)
9.Request(Randr)
13.Response
(Authr, Keys)
10.UE以Authr和Keys合成AKA算法的鉴权密钥,Rand作为随机数计算5元组
11.Register(Xres)
12.S-CSCF比较两个Xres值是否一致，一致则说明鉴权通过

图 9

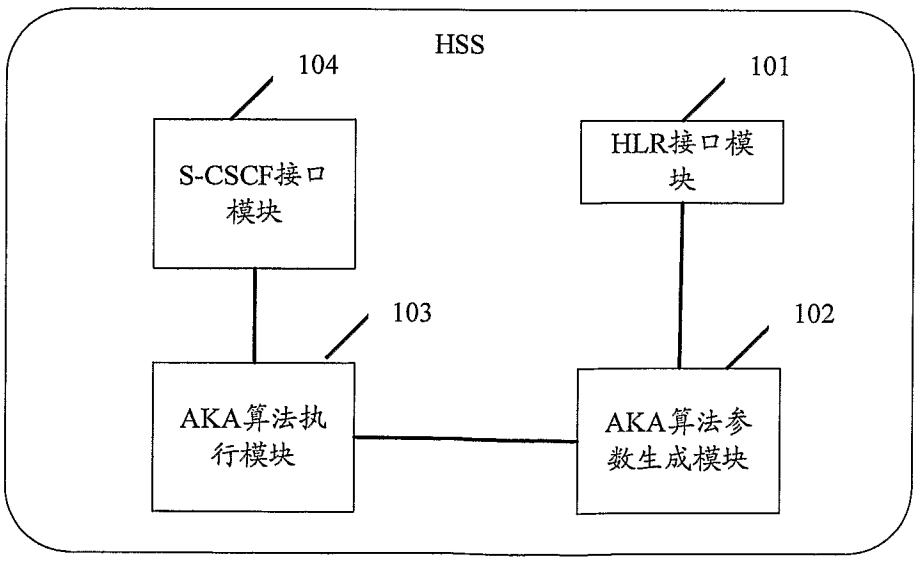

HSS
104
S-CSCF接口模块
101
HLR接口模块
103
AKA算法执行模块
102
AKA算法参数生成模块

图 10

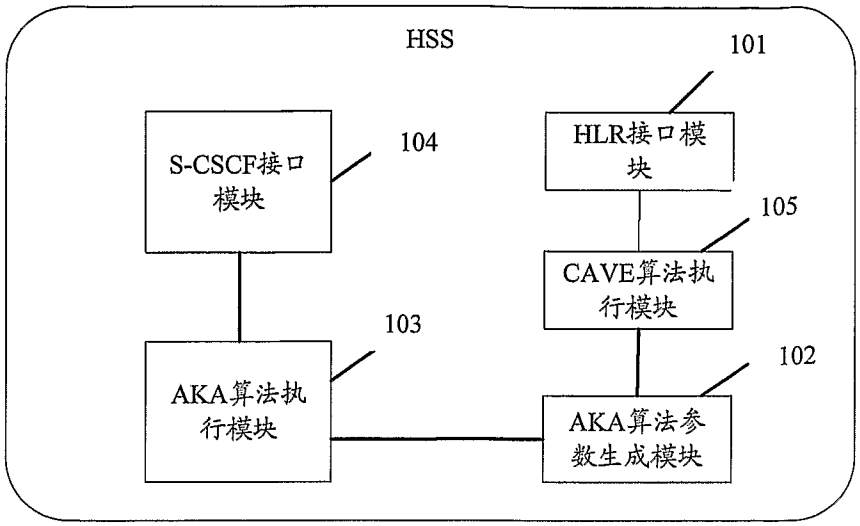

HSS
101
HLR接口模块
104
S-CSCF接口模块
105
CAVE算法执行模块
103
102
AKA算法执行模块
AKA算法参数生成模块

图 11

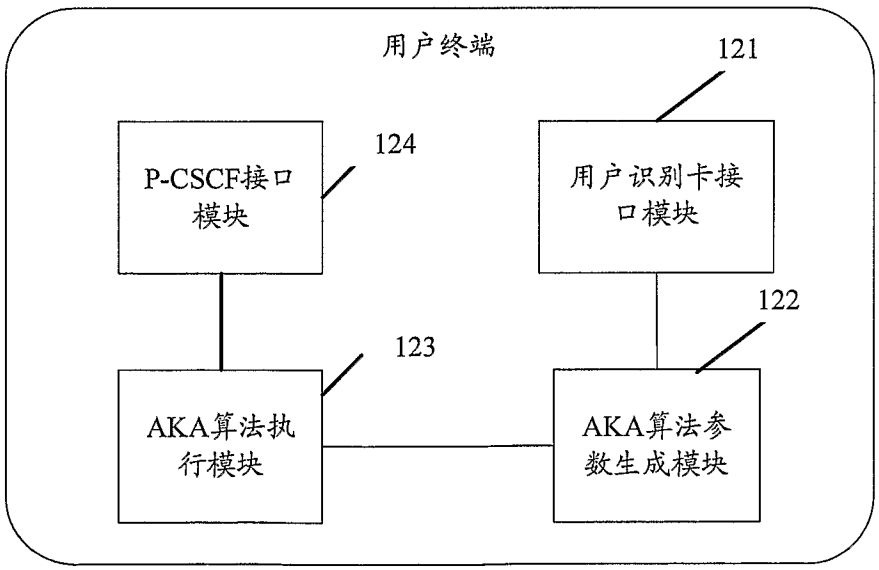

用户终端
121
P-CSCF接口模块
124
用户识别卡接口模块
122
123
AKA算法执行模块
AKA算法参数生成模块

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/000914

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:H04L 9

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT,CNKI,WPI,EPODOC,PAJ: authenticat+, random, arithmetic, calculat+, SIM

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US5661806A (FRANCE TELECOM) 26 Aug. 1997 (26.08.1997) ,see description column 4, line 50- column5,line 25, figure 2	1-3, 6-9, 14-26
A		4-5,10-13
A	WO2005120113 A1 (ERICSSON TELEFON AB L M et al) 15 Dec.2005(15.12.2005), see the whole document	1-26

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 Jun.2007(15.06.2007)	**05 Jul. 2007 (05.07.2007)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer CUI Xianli Telephone No. (86-10)62084555

Form PCT/ISA /210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/000914

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US5661806A	26.08.1997	EP0675615 A1	04.10.1995
		FR2718312 A1	06.10.1995
		JP8008899 A	12.01.1996
WO2005120113 A1	15.12.2005	EP1752007 A1	14.02.2007

国际检索报告

国际申请号
PCT/CN2007/000914

A. 主题的分类

H04L 9/00(2006.01)i

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:H04L 9

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,CNKI:鉴权，密钥，密码，随机，算法，SIM，计算

WPI，EPODOC，PAJ：authenticat+，random，arithmetic，calculat+，SIM

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	US5661806A (FRANCE TELECOM) 26. 8 月 1997（26.08.1997），参见说明书第 4 栏 50 行-第 5 栏 25 行，附图 2	1-3，6-9，14-26
A		4-5，10-13
A	WO2005120113 A1 (ERICSSON TELEFON AB L M 等) 15.12 月 2005 (15.12.2005), 参见全文	1-26

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
15.6 月 2007（15.06.2007）	**05.7 月 2007 (05.07.2007)**
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 崔宪丽 电话号码：(86-10) **62084555**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2007/000914

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US5661806A	26.08.1997	EP0675615 A1	04.10.1995
		FR2718312 A1	06.10.1995
		JP8008899 A	12.01.1996
WO2005120113 A1	15.12.2005	EP1752007 A1	14.02.2007