(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111641498 A
(43)申请公布日 2020.09.08

(21)申请号 201910156817.0

(22)申请日 2019.03.01

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区科技南路55号

(72)发明人 游世林 谢振华 彭锦 余万涛 林兆骥 刘建华 王继刚 闫新成 张博山

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 江舟

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/06(2006.01)
H04L 29/06(2006.01)

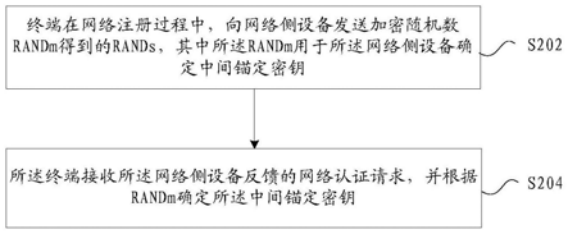
权利要求书3页 说明书11页 附图4页

(54)发明名称

密钥的确定方法及装置

(57)摘要

本发明提供了一种密钥的确定方法及装置。具体而言,该方法包括:终端在网络注册过程中,向网络侧设备发送加密随机数RANDm得到的RANDs,其中所述RANDm用于所述网络侧设备确定中间锚定密钥;所述终端接收所述网络侧设备反馈的网络认证请求,并根据RANDm确定所述中间锚定密钥。通过本发明,解决了基于SUCI加密技术只能基于终端的设备本体来实现共享密钥的问题,从而不仅保障了保证生成会话密钥的安全性,同时适用性广,对于会话的安全保护的运行效率高。



CN 111641498 A

1.一种密钥的确定方法,其特征在于,包括:

终端在网络注册过程中,向网络侧设备发送加密随机数RANDm得到的RANDs,其中所述RANDm用于所述网络侧设备确定中间锚定密钥;

所述终端接收所述网络侧设备反馈的网络认证请求,并根据RANDm确定所述中间锚定密钥。

2.根据权利要求1所述的方法,其特征在于,在向网络侧设备发送加密有随机数RANDm的RANDs之前,所述方法还包括:

所述终端将生成的所述RANDm加密为所述RANDs。

3.根据权利要求2所述的方法,其特征在于,所述终端通过如下至少之一的方式将生成的所述RANDm加密为所述RANDs:

所述终端的设备本体生成所述RANDm,并加密为所述RANDs;

所述终端通过用户签约卡生成所述RANDm,并加密为所述RANDs;

所述终端的设备本体生成所述RANDm,并通过用户签约卡加密为所述RANDs。

4.根据权利要求3所述的方法,其特征在于,将生成的所述RANDm加密为RANDs,还包括:

所述终端通过非对称密钥加密算法或对称密钥加密算法将所述RANDm加密为RANDs。

5.根据权利要求2-4任一项所述的方法,其特征在于,所述方法还包括:

所述终端使用与加密所述RANDm为所述RANDs时相同的算法在加密用户订阅标识SUCI中加密用户永久标识SUPI和所述RANDm,以得到更新后的加密用户订阅标识SUCI。

6.根据权利要求1所述的方法,其特征在于,在根据RANDm确定所述中间锚定密钥之后,所述方法还包括:

所述终端对所述RANDm进行更新。

7.根据权利要求6所述的方法,其特征在于,所述终端对所述RANDm进行更新,包括:

所述终端根据所述中间锚定密钥确定序列号SQN;所述终端通过对所述RANDm和所述SQN进行哈希计算,获取更新后的所述RANDm,或,

所述终端根据所述中间锚定密钥确定SQN⊕匿名密钥AK;所述终端通过对所述RANDm和所述SQN⊕AK进行哈希计算,获取更新后的所述RANDm。

8.根据权利要求6所述的方法,其特征在于,所述终端对所述RANDm进行更新,包括:

所述终端接收所述网络认证请求中携带的哈希计数器的计数结果,并根据所述RANDm和所述计数结果,获取更新后的所述RANDm。

9.根据权利要求1所述的方法,其特征在于,所述中间锚定密钥至少包括以下其中之一:K_{AUSF},K_{SEAF}。

10.根据权利要求9所述的方法,其特征在于,所述K_{AUSF}通过如下方式确定:

K_{AUSF}=哈希消息认证码HMAC-安全散列算法值SHA-256位RSA算法值RSA256(FC||服务网络名SN||SN长度||(SQN⊕AK)||(SQN⊕AK)长度,服务网络名CK||完整性保护密钥IK);其中,FC为正整数的计数值。

11.根据权利要求9所述的方法,其特征在于,所述K_{SEAF}通过如下方式确定:

K_{SEAF}=HMAC-SHA-RSA256(FC||SN||SN长度||RANDm||RANDm长度,K_{AUSF})。

12.一种密钥的确定方法,其特征在于,包括:

网络侧设备接收终端在网络注册过程中发送的RANDs,并对所述RANDs进行解密以获取

随机数RANDm；

所述网络侧设备根据所述RANDm确定中间锚定密钥；

所述网络侧设备向所述终端反馈网络认证请求，以使所述终端根据所述RANDm确定中间锚定密钥。

13.根据权利要求12所述的方法，其特征在于，所述方法还包括：

所述网络侧设备对所述终端更新后的加密用户订阅标识SUCI解密，以获取用户永久标识SUPI和所述RANDm。

14.根据权利要求12所述的方法，其特征在于，在所述网络侧设备根据所述RANDm确定中间锚定密钥之后，所述方法还包括：

所述网络侧设备对所述RANDm进行更新。

15.根据权利要求14所述的方法，其特征在于，所述网络侧设备包括以下其中之一：认证服务功能AUSF，签约数据管理功能UDM/ARPF。

16.根据权利要求15所述的方法，其特征在于，所述网络侧设备对所述RANDm进行更新，包括：

所述AUSF根据所述中间锚定密钥确定序列号SQN；所述AUSF通过对所述RANDm和所述SQN进行哈希计算，获取更新后的所述RANDm，或，

所述UDM/ARPF根据所述中间锚定密钥确定SQN ⊕ 匿名密钥AK；所述UDM/ARPF通过对所述RANDm和所述SQN ⊕ AK进行哈希计算，获取更新后的所述RANDm。

17.根据权利要求15所述的方法，其特征在于，所述网络侧设备对所述RANDm进行更新，包括：

所述网络侧设备通过哈希计数器获取计数结果；

根据所述RANDm以及所述计数结果进行哈希计算，获取更新后的所述RANDm。

18.根据权利要求12所述的方法，其特征在于，所述中间锚定密钥至少包括以下其中之一：K_{AUSF}，K_{SEAF}。

19.一种密钥的确定装置，其特征在于，位于终端，包括：

发送模块，用于在网络注册过程中，向网络侧设备发送加密随机数RANDm得到的RANDs，其中所述RANDm用于所述网络侧设备确定中间锚定密钥；

第一确定模块，用于接收所述网络侧设备反馈的网络认证请求，并根据RANDm确定所述中间锚定密钥。

20.根据权利要求19所述的装置，其特征在于，所述装置还包括：

加密模块，用于将生成的所述RANDm加密为所述RANDs。

21.一种密钥的确定装置，其特征在于，位于网络侧设备，包括：

接收模块，用于接收终端在网络注册过程中发送的RANDs，并对所述RANDs进行解密以获取随机数RANDm；

第二确定模块，用于根据所述RANDm确定中间锚定密钥；

反馈模块，用于向所述终端反馈网络认证请求，以使所述终端根据所述RANDm确定中间锚定密钥。

22.一种存储介质，其特征在于，所述存储介质中存储有计算机程序，其中，所述计算机程序被设置为运行时执行所述权利要求1-11，12-18任一项中所述的方法。

23.一种电子装置,包括存储器和处理器,其特征在于,所述存储器中存储有计算机程序,所述处理器被设置为运行所述计算机程序以执行所述权利要求1-11,12-18任一项中所述的方法。

密钥的确定方法及装置

技术领域

[0001] 本发明涉及通信领域,具体而言,涉及一种密钥的确定方法及装置。

背景技术

[0002] 第三代合作伙伴计划(3rd Generation Partnership Project,3GPP)制定了各种移动网络的规范,包括认证与密钥协商过程(Authentication and Key Agreement,简称AKA过程),该过程用于UE与网络的互相认证并建立共同的密钥。

[0003] 图1是相关技术中移动系统的结构示意图,如图1所示,包括终端、基站、认证功能、认证服务功能和签约数据管理功能。其中基站为终端提供通讯等各项移动网络提供的服务,比如eNB或gNB;认证功能为移动网络的核心网的软件功能或硬件设备,用于通过信令与基站交互,使得移动网络终端可以实现相互认证,比如移动管理性功能MME(Mobility Management Entity),或安全锚定功能SEAF(Security Anchor Function),或接入和移动管理性功能AMF(Access and Mobility Management Function);认证服务功能用于与签约数据管理功能通过信令接口,获取与用户相关的密钥信息,并将该信息通过信令接口提供给认证功能,该功能可以是AUSF,该功能也可以与签约数据管理功能合设;签约数据管理功能存储并处理用户相关的数据,基于用户相关数据生成用于认证用户的信息和用户相关的密钥信息,并通过信令接口提供给认证服务功能,该功能可以是签约数据管理功能UDM(User Date Management)/ARPF(Authentication credential Repository and Processing Function)或家乡用户服务器HSS(Home Subscriber Server)。

[0004] 然而,当根密钥K发生泄露,终端业务就不受保护,很容易被攻击者破坏,如果采用了相关技术中的椭圆曲线加密技术加密SUPI为SUCI,虽然可以通过生成终端和网络的共享密钥来加扰K_{AUSF}或者K_{SEAF},以达到保护终端的中间锚定密钥,使用户的正常业务得到保护。但是基于SUCI加密技术来保护的,只能基于终端设备本体来实现,而例如终端设备中插入的用户签约卡,以及其他外界设备,上述方法是难以实现的。因此,相关技术中使用共享密钥存在适用对象窄,保护效率低的问题。

发明内容

[0005] 本发明实施例提供了一种密钥的确定方法及装置,以至少解决相关技术中基于SUCI加密技术只能基于终端的设备本体来实现共享密钥的问题。

[0006] 根据本发明的一个实施例,提供了一种密钥的确定方法,包括:终端在网络注册过程中,向网络侧设备发送加密随机数RANDm得到的RANDs,其中所述RANDm用于所述网络侧设备确定中间锚定密钥;所述终端接收所述网络侧设备反馈的网络认证请求,并根据RANDm确定所述中间锚定密钥。

[0007] 可选地,在向网络侧设备发送加密有随机数RANDm的RANDs之前,所述方法还包括:所述终端将生成的所述RANDm加密为所述RANDs。

[0008] 可选地,所述终端通过如下至少之一的方式将生成的所述RANDm加密为所述

RANDs:所述终端的设备本体生成所述RANDm,并加密为所述RANDs;所述终端通过用户签约卡生成所述RANDm,并加密为所述RANDs;所述终端的设备本体生成所述RANDm,并通过用户签约卡加密为所述RANDs。

[0009] 可选地,将生成的所述RANDm加密为RANDs,还包括:所述终端通过非对称密钥加密算法或对称密钥加密算法将所述RANDm加密为RANDs。

[0010] 可选地,所述终端使用与加密所述RANDm为所述RANDs时相同的算法在加密用户订阅标识SUCI中加密用户永久标识SUPI和所述RANDm,以得到更新后的加密用户订阅标识SUCI。

[0011] 可选地,在根据RANDm确定所述中间锚定密钥之后,所述方法还包括:所述终端对所述RANDm进行更新。

[0012] 可选地,所述终端对所述RANDm进行更新,包括:所述终端根据所述中间锚定密钥确定序列号SQN;所述终端通过对所述RANDm和所述SQN进行哈希计算,获取更新后的所述RANDm,或,所述终端根据所述中间锚定密钥确定SQN⊕匿名密钥AK;所述终端通过对所述RANDm和所述SQN⊕AK进行哈希计算,获取更新后的所述RANDm。

[0013] 可选地,所述终端对所述RANDm进行更新,包括:所述终端接收所述网络认证请求中携带的哈希计数器的计数结果,并根据所述RANDm和所述计数结果,获取更新后的所述RANDm。

[0014] 可选地,所述中间锚定密钥至少包括以下其中之一:K_{AUSF},K_{SEAF}。

[0015] 可选地,K_{AUSF}=哈希消息认证码HMAC-安全散列算法值SHA-256位RSA算法值RSA256(FC||服务网络名SN||SN长度||(SQN⊕AK)||(SQN⊕AK)长度,服务网络名CK||完整性保护密钥IK);其中,FC为正整数的计数值。

[0016] 可选地,所述K_{SEAF}通过如下方式确定:K_{SEAF}=HMAC-SHA-RSA256(FC||SN||SN长度||RANDm||RANDm长度,K_{AUSF})。

[0017] 根据本发明的一个实施例,提供了另一种密钥的确定方法,包括:网络侧设备接收终端在网络注册过程中发送的RANDs,并对所述RANDs进行解密以获取随机数RANDm;所述网络侧设备根据所述RANDm确定中间锚定密钥;所述网络侧设备向所述终端反馈网络认证请求,以使所述终端根据所述RANDm确定中间锚定密钥。

[0018] 可选地,所述网络侧设备对所述终端更新后的加密用户订阅标识SUCI解密,以获取用户永久标识SUPI和所述RANDm。

[0019] 可选地,在所述网络侧设备根据所述RANDm确定中间锚定密钥之后,所述方法还包括:所述网络侧设备对所述RANDm进行更新。

[0020] 可选地,所述网络侧设备包括以下其中之一:认证服务功能AUSF,签约数据管理功能UDM/ARPF。

[0021] 可选地,所述网络侧设备对所述RANDm进行更新,包括:所述AUSF根据所述中间锚定密钥确定序列号SQN;所述AUSF通过对所述RANDm和所述SQN进行哈希计算,获取更新后的所述RANDm,或,所述UDM/ARPF根据所述中间锚定密钥确定SQN⊕匿名密钥AK;所述UDM/ARPF通过对所述RANDm和所述SQN⊕AK进行哈希计算,获取更新后的所述RANDm。

[0022] 可选地,所述网络侧设备对所述RANDm进行更新,包括:所述网络侧设备通过哈希计数器获取计数结果;根据所述RANDm以及所述计数结果进行哈希计算,获取更新后的所述

RANDm。

[0023] 可选地，所述中间锚定密钥至少包括以下其中之一：K_{AUSF}，K_{SEAF}。

[0024] 根据本发明的另一个实施例，提供了一种密钥的确定装置，位于终端，包括：发送模块，用于在网络注册过程中，向网络侧设备发送加密随机数RANDm得到的RANDs，其中所述RANDm用于所述网络侧设备确定中间锚定密钥；第一确定模块，用于接收所述网络侧设备反馈的网络认证请求，并根据RANDm确定所述中间锚定密钥。

[0025] 可选地，所述装置还包括：加密模块，用于将生成的所述RANDm加密为所述RANDs。

[0026] 根据本发明的另一个实施例，提供了另一种密钥的确定装置，包括：接收模块，用于接收终端在网络注册过程中发送的RANDs，并对所述RANDs进行解密以获取随机数RANDm；第二确定模块，用于根据所述RANDm确定中间锚定密钥；反馈模块，用于向所述终端反馈网络认证请求，以使所述终端根据所述RANDm确定中间锚定密钥。

[0027] 根据本发明的又一个实施例，还提供了一种存储介质，所述存储介质中存储有计算机程序，其中，所述计算机程序被设置为运行时执行上述任一项方法实施例中的步骤。

[0028] 根据本发明的又一个实施例，还提供了一种电子装置，包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器被设置为运行所述计算机程序以执行上述任一项方法实施例中的步骤。

[0029] 通过本发明，由于在终端和网络侧设备两侧利用终端产生的RANDm确定共享的中间锚定密钥，因此避免了基于SUCI加密技术只能基于终端的设备本体来实现共享密钥的问题，从而不仅保障了保证生成会话密钥的安全性，同时适用性广，对于会话的安全保护的运行效率高。

附图说明

[0030] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0031] 图1是相关技术中移动系统的结构示意图；

[0032] 图2是根据本发明实施例的一种密钥的确定方法的流程图；

[0033] 图3是根据本发明实施例的另一种密钥的确定方法的流程图；

[0034] 图4是根据本发明场景1的一种生成中间密钥K_{AUSF}的方法的流程图；

[0035] 图5是根据本发明场景2的一种生成中间密钥K_{SEAF}的方法的流程图；

[0036] 图6是根据本发明实施例的一种密钥的确定装置的结构框图；

[0037] 图7是根据本发明实施例的另一种密钥的确定装置的结构框图。

具体实施方式

[0038] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0039] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

[0040] 实施例1

[0041] 在本实施例中提供了一种密钥的确定方法，图2是根据本发明实施例的一种密钥

的确定方法的流程图，如图2所示，该流程包括如下步骤：

[0042] 步骤S202，终端在网络注册过程中，向网络侧设备发送加密随机数RANDm得到的RANDs，其中所述RANDm用于所述网络侧设备确定中间锚定密钥；

[0043] 步骤S204，所述终端接收所述网络侧设备反馈的网络认证请求，并根据RANDm确定所述中间锚定密钥。

[0044] 需要说明的是，上述提及的网络侧设备包括但不限于以下其中之一：AUSF，UDM/ARPF。

[0045] 具体而言，终端在在网络注册过程中首先将网络注册请求发送给基站，然后基站将该网络注册请求转发给第一认证功能实体。具体而言，在该网络注册请求可以携带：加密用户订阅标识(Subscription Concealed Identifier，简称SUCI)，RANDs，或5G用户临时标识(5G-Globally Unique Temporary UE Identity，简称5G-GUTI)，或新SUCI。需要说明的是，终端在网络注册过程当中，还需要携带例如小区标识，用户安全能力等协助终端进行注册的相关信息。而上述提到的SUCI可以是原有的SUCI，也可以是终端加密RANDm和SUPI得到的新SUCI。同时该第一认证功能实体包括但不限于：AMF。

[0046] 具体而言，在确定终端发送的网络注册请求中携带有5G用户临时标识的情况下，第一认证功能实体会根据该临时标识中的AMF标识，向第二认证功能实体发送携带有5G用户临时标识用户上下文请求消息。第二认证功能实体会向第一认证功能实体反馈上下文请求响应消息，在该上下文请求响应消息中，包括：用户上下文信息，其中，该用户上下文信息中至少包括：用户永久标识(Subscription Permanent Identifier，简称SUPI)和用户安全上下文信息。

[0047] 同时该第一认证功能实体包括但不限于：认证服务功能AUSF。

[0048] 具体而言，在确定终端发送的网络注册请求中携带有SUCI的情况，或者认证5G用户临时标识失败，或者第一认证功能实体需要发起AKA认证过程中，第一认证功能实体则会向网络侧设备发送认证请求消息，在该消息中携带：SUCI，RANDs或者SUPI，RANDs或者新SUCI。

[0049] 可选地，在向网络侧设备发送加密随机数RANDm得到的RANDs之前，所述方法还包括：所述终端将生成的所述RANDm加密为所述RANDs。

[0050] 可选地，所述终端通过如下至少之一的方式将生成的所述RANDm加密为所述RANDs：所述终端的设备本体生成所述RANDm，并加密为所述RANDs；所述终端通过用户签约卡生成所述RANDm，并加密为所述RANDs；所述终端的设备本体生成所述RANDm，并通过用户签约卡加密为所述RANDs。

[0051] 可选地，将生成的所述RANDm加密为RANDs，还包括：所述终端通过非对称密钥加密算法或对称密钥加密算法将所述RANDm加密为RANDs。

[0052] 可选地，所述终端使用与加密所述RANDm为所述RANDs时相同的算法在加密用户订阅标识SUCI中加密用户永久标识SUPI和所述RANDm，以得到更新后的加密用户订阅标识SUCI。

[0053] 可选地，在根据RANDm确定所述中间锚定密钥之后，所述方法还包括：所述终端对所述RANDm进行更新。

[0054] 可选地，所述终端对所述RANDm进行更新，包括：所述终端根据所述中间锚定密钥

确定序列号SQN;所述终端通过对所述RANDm和所述SQN进行哈希计算,获取更新后的所述RANDm,或,所述终端根据所述中间锚定密钥确定SQN⊕匿名密钥AK;所述终端通过对所述RANDm和所述SQN⊕AK进行哈希计算,获取更新后的所述RANDm。

[0055] 可选地,所述终端对所述RANDm进行更新,包括:所述终端接收所述网络认证请求中携带的哈希计数器的计数结果,并根据所述RANDm和所述计数结果,获取更新后的所述RANDm。

[0056] 可选地,所述中间锚定密钥至少包括以下其中之一:K_{AUSF},K_{SEAF}。

[0057] 可选地,KAUSF=哈希消息认证码(Hash Message Authentication Code,简称HMAC)-安全散列算法值(Secure Hash Algorithm,简称SHA)-256位RSA算法值(Ron Rivest、Adi Shamir和Leonard Adleman 256,简称RSA256(FC||服务网络名(Serving Network Identifier,简称SN)||SN长度||(SQN⊕AK)||(SQN⊕AK)长度,加密密钥(cipher Key,简称CK)||完整性保护密钥(Integrity Key,简称IK);其中,FC为正整数的计数值。

[0058] 可选地,所述K_{SEAF}通过如下方式确定:K_{SEAF}=HMAC-SHA-RSA256(FC||SN||SN长度||RANDm||RANDm长度,K_{AUSF})。

[0059] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,或者网络设备等)执行本发明各个实施例所述的方法。

[0060] 实施例2

[0061] 在本实施例中提供了另一种密钥的确定方法,图3是根据本发明实施例的另一种密钥的确定方法的流程图,如图3所示,该流程包括如下步骤:

[0062] 步骤S302,网络侧设备接收终端在网络注册过程中发送的RANDs,并对所述RANDs进行解密以获取随机数RANDm;

[0063] 步骤S304,所述网络侧设备根据所述RANDm确定中间锚定密钥;

[0064] 步骤S306,所述网络侧设备向所述终端反馈网络认证请求,以使所述终端根据所述RANDm确定中间锚定密钥。可选地,所述网络侧设备对所述终端更新后的加密用户订阅标识SUCI解密,以获取用户永久标识SUPI和所述RANDm。

[0065] 可选地,在所述网络侧设备根据所述RANDm确定中间锚定密钥之后,所述方法还包括:所述网络侧设备对所述RANDm进行更新。

[0066] 可选地,所述网络侧设备包括以下其中之一:认证服务功能AUSF,签约数据管理功能UDM/ARPF。

[0067] 可选地,所述网络侧设备对所述RANDm进行更新,包括:所述AUSF根据所述中间锚定密钥确定序列号SQN;所述AUSF通过对所述RANDm和所述SQN进行哈希计算,获取更新后的所述RANDm,或,所述UDM/ARPF根据所述中间锚定密钥确定SQN⊕匿名密钥AK;所述UDM/ARPF通过对所述RANDm和所述SQN⊕AK进行哈希计算,获取更新后的所述RANDm。

[0068] 可选地,所述网络侧设备对所述RANDm进行更新,包括:所述网络侧设备通过哈希计数器获取计数结果;根据所述RANDm以及所述计数结果进行哈希计算,获取更新后的所述

RANDm。

[0069] 可选地,所述中间锚定密钥至少包括以下其中之一:K_{AUSF},K_{SEAF}。

[0070] 为了更好的理解上述实施例中记载的技术方案,还提供了如下的两个场景以便理解。

[0071] 场景1:

[0072] 图4是根据本发明场景1的生成中间密钥K_{AUSF}的流程图。如图4所示:包括:

[0073] 步骤400,终端产生随机数RANDm,加密得到RANDs:

[0074] 终端设备产生随机数RANDm,使用用户签约卡保存的非对称密钥加密算法的公钥或者对称密钥加密算法的共享密钥加密得到RANDs,所述非对称密钥加密算法的公钥和对称密钥加密算法的共享密钥均为归属网络向用户下发网络密钥,包括对应的密钥索引号,分别保存在用户签约卡和签约数据管理功能(UDM/ARPF)中;

[0075] 或者用户签约卡产生随机数RANDm,使用非对称密钥加密算法的公钥或者对称密钥加密算法的共享密钥加密得到RANDs,所述非对称密钥加密算法的公钥和对称密钥加密算法的共享密钥均为归属网络向用户下发网络密钥,包括对应的密钥索引号,分别保存在用户签约卡和签约数据管理功能(UDM/ARPF)中;

[0076] 或者终端设备产生随机数RANDm,将RANDm送到用户设备卡中,使用非对称密钥加密算法的公钥或者对称密钥加密算法的共享密钥加密得到RANDs,所述非对称密钥加密算法的公钥和对称密钥加密算法的共享密钥均为归属网络向用户下发网络密钥,包括对应的密钥索引号,分别保存在用户签约卡和签约数据管理功能(UDM/ARPF)中;

[0077] 所述加密也可以在SUPI加密为SUCI,加RANDm添加到SUPI中的用户号码(MSIN)前或者后,采用一次加密得到新SUCI,也可以分别加密。具体的,新SUCI=MCC(移动国家码)||MNC(移动网络号)||RouteID(路由号)||密钥索引号||加密(MSIN||RANDm)或者新SUCI=MCC(移动国家码)||MNC(移动网络号)||RouteID(路由号)||密钥索引号||加密(RANDm||MSIN);

[0078] 步骤401,终端向基站发起注册请求消息,所述消息携带小区标识,用户安全能力.所述消息还携带SUCI,RANDs;或者所述消息还携带新SUCI;或者所述消息携带5G-GUTI。步骤402,基站向第一认证功能实体转发注册请求消息。

[0079] 步骤403,如果用户标识是5G用户临时标识,第一认证功能实体根据5G用户临时标识中的AMF标识,向第二认证功能实体发起用户上下文请求消息,所述消息携带5G用户临时标识,第二认证功能实体向第一认证功能实体会送用户上下文请求响应消息,所述消息携带用户上下文,其中所述用户上下文至少包括用户永久标识SUPI和用户安全上下文;

[0080] 步骤404,如果用户标识为SUCI或者新SUCI,或者步骤403失败,或者认证功能需要发起AKA认证过程,第一认证功能实体向认证服务功能/签约数据管理功能发起认证请求消息,消息携带SUCI或者新SUCI或者SUPI,或者消息还携带RANDs;

[0081] 步骤405,签约数据管理功能UDM/ARPF解密SUCI得到SUPI,同时解密RANDs得到RANDm,或者解密新SUCI得到SUPI和RANDm,或者根据SUPI查询到用户签约参数,根据根密钥K生成归属鉴权向量(RAND,认证令牌(AUthentication TokeN,简称AUTN),期望响应(eXpected RESponse*,简称XRES*,和K_{AUSF}),其中AUTN=(SQN⊕AK)||AMF||MAC,MAC=F1K(SQN||RAND||AMF),XRES*=F2K(RAND),AK=F5K(RAND),加密密钥CK=F3K(RAND),完整性

保护密钥CK＝F4K(RAND)，K_{AUSF}＝HMAC-SHA-RSA256(FC||SN||SN长度||(SQN⊕AK)||(SQN⊕AK)长度||RANDm||RANDm长度,CK||IK)其中FC＝0x6A,SN为服务网络名称,F1K,F2K,F3K,F4K,F5K为K为密钥的密钥生成函数,AMF为认证管理域参数(AMF,Authentication Management Field)。签约数据管理功能UDM/ARPF哈希RANDm和SQN得到新RANDm,或者签约数据管理功能UDM/ARPF开始计数一个计数器Count,哈希计数器计数Count和RANDm得到新RANDm,签约数据管理功能UDM/ARPF保存新RANDm。向认证功能服务功能发下发归属鉴权向量(RAND,AUTN,XRES*,和KAUSF)和SUPI,认证服务功能保存归属鉴权向量和SUPI,并由XRES*哈希散列得到HXRES*,KAUSF生成得到KSEAF,这样的得到鉴权向量(RAND,AUTN,HXRES*,和K_{SEAF})。

[0082] 步骤406,向第一认证功能实体发送认证请求响应消息,所述消息携带AUTN,RAND和HXRES*,或者计数器Count;

[0083] 步骤407,第一认证功能实体向终端发送用户认证请求消息,所述消息携带AUTN和RAND,或者计数器Count;

[0084] 步骤408,终端收到RAND和AUTN后,按照步骤405相似计算方法算出SQN和XMAC,验证AUTN中的SQN是否大于终端SQN、验证“MAC＝XMAC”,这些验证通过后,同时计算出RES*,生成K_{AUSF}＝HMAC-SHA-RSA256(FC||SN||SN长度||(SQN⊕AK)||(SQN⊕AK)长度||RANDm||RANDm长度,CK||IK)其中FC＝0x6A,SN为服务网络名称。终端哈希RANDm和SQN得到新RANDm,或者终端哈希计数器计数Count和RANDm得到新RANDm,保存新RANDm;需要说明的是,网络侧设备在408步骤与终端在405步骤计算出的新的RANDm是相同的。

[0085] 步骤409,终端向第一认证功能实体发送用户认证请求响应消息,所述消息携带RES*;

[0086] 步骤410,第一认证功能实体由RES*推导出HRES*,然后将HRES*和HXRES*进行比较,如果比较通过,拜访网络鉴权成功,向认证服务功能/签约数据管理功能发送认证执行消息,所述消息携带RES*;

[0087] 步骤411,认证服务功能/签约数据管理功能比较RES*和XRES*,如果相等,在归属网络鉴权成功,生成出K_{SEAF}＝HMAC-SHA-RSA256(FC||SN||SN长度,K_{AUSF})其中FC＝0x6C,SN为服务网络名称,如果步骤305未哈希得到新RANDm,则按照步骤405中描述获得新RANDm,签约数据管理功能保存新RANDm;

[0088] 步骤412,向第一认证功能实体回送认证确认消息,所述消息携带SUPI和中间密钥K_{SEAF};

[0089] 步骤413,第一认证功能实体由中间密钥K_{SEAF}生成出K_{AMF},其中所述K_{AMF}＝HMAC-SHA-RSA256(FC||SUPI||SUPI长度||ABBA||ABBA长度,K_{SEAF})其中FC＝0x6D,ABBA为防止降维攻击参数,再由K_{AMF}生成出接入层加密密钥和完整性保护密钥,非接入层加密密钥$K_{NAS-enc}$和完整性保护密钥,向终端回送注册请求响应消息,所述消息携带5G-GUTI。

[0090] 步骤414,终端安全网络密钥生成方法生成K_{SEAF}和K_{AMF},再由K_{AMF}生成出接入层加密密钥和完整性保护密钥,非接入层加密密钥$K_{NAS-enc}$和完整性保护密钥,如果步骤408未哈希得到新RANDm,则按照步骤408哈希得到保存新RANDm。

[0091] 终端发生移动,移动到新的小区驻留,发起新的注册请求消息,则会使用5G-GUTI进行注册,如果再发起一次AKA成功过程,网络将会使用新RANDm来生成K_{AUSF},如果注册过程

中需要获取SUCI,终端可按照上述发明流程产生新的RANDm来生成K_{AUSF},这样终端和网络都可获得受保护接入层和非接入层会话密钥,保护终端和网络的正常业务。

[0092] 场景2:

[0093] 图5是根据本发明场景2的一种生成中间密钥K_{seaf}的流程图。如图5所示:包括:

[0094] 步骤500,终端产生随机数RANDm,加密得到RANDs:

[0095] 终端设备产生随机数RANDm,使用用户签约卡保存的非对称密钥加密算法的公钥或者对称密钥加密算法的共享密钥加密得到RANDs,所述非对称密钥加密算法的公钥和对称密钥加密算法的共享密钥均为归属网络向用户下发网络密钥,包括对应的密钥索引号,分别保存在用户签约卡和签约数据管理功能(UDM/ARPF)中;

[0096] 或者用户签约卡产生随机数RANDm,使用非对称密钥加密算法的公钥或者对称密钥加密算法的共享密钥加密得到RANDs,所述非对称密钥加密算法的公钥和对称密钥加密算法的共享密钥均为归属网络向用户下发网络密钥,包括对应的密钥索引号,分别保存在用户签约卡和签约数据管理功能(UDM/ARPF)中;

[0097] 或者终端设备产生随机数RANDm,将RANDm送到用户设备卡中,使用非对称密钥加密算法的公钥或者对称密钥加密算法的共享密钥加密得到RANDs,所述非对称密钥加密算法的公钥和对称密钥加密算法的共享密钥均为归属网络向用户下发网络密钥,包括对应的密钥索引号,分别保存在用户签约卡和签约数据管理功能(UDM/ARPF)中;

[0098] 所述加密也可以在SUPI加密为SUCI,加RANDm添加到SUPI中的用户号码(MSIN)前或者后,采用一次加密得到新SUCI,也可以分别加密。具体的,新SUCI=MCC(移动国家码)||MNC(移动网络号)||RouteID(路由号)||密钥索引号||加密(MSIN||RANDm)或者新SUCI=MCC(移动国家码)||MNC(移动网络号)||RouteID(路由号)||密钥索引号||加密(RANDm||MSIN);

[0099] 步骤501,终端向基站发起注册请求消息,所述消息携带小区标识,用户安全能力,所述消息还携带SUCI,RANDs;或者所述消息还携带新SUCI;或者所述消息携带5G-GUTI;

[0100] 步骤502,基站向第一认证功能实体转发注册请求消息。

[0101] 步骤503,如果用户标识是5G用户临时标识,第一认证功能实体根据5G用户临时标识中的AMF标识,向第二认证功能实体发起用户上下文请求消息,所述消息携带5G用户临时标识,第二认证功能实体向第一认证功能实体会送用户上下文请求响应消息,所述消息携带用户上下文,其中所述用户上下文至少包括用户永久标识SUPI和用户安全上下文;

[0102] 步骤504,如果用户标识为SUCI或者新SUCI,或者步骤503失败,或者认证功能需要发起AKA认证过程,第一认证功能实体向认证服务功能/签约数据管理功能发起认证请求消息,消息携带SUCI或者新SUCI或者SUPI,或者消息还携带RANDs;

[0103] 步骤505,签约数据管理功能UDM/ARPF解密SUCI得到SUPI,同时解密RANDs得到RANDm,或者解密新SUCI得到SUPI和RANDm,或者根据SUPI查询到用户签约参数,根据根密钥K生成归属鉴权向量(RAND,AUTN,XRES*,和K_{AUSF}),其中AUTN=(SQN⊕AK)||AMF||MAC,MAC=F1K(SQN||RAND||AMF),XRES*=F2K(RAND),AK=F5K(RAND),加密密钥CK=F3K(RAND),完整性保护密钥CK=F4K(RAND),K_{AUSF}=HMAC-SHA-RSA256(FC||SN||SN长度||(SQN⊕AK)||(SQN⊕AK)长度||,CK||IK)其中FC=0x6A,SN为服务网络名称,F1K,F2K,F3K,F4K,F5K为K为密钥的密钥生成函数,AMF为认证管理域参数(AMF,Authentication Management Field)。向认

证功能服务功能发下发归属鉴权向量(RAND,AUTN,XRES*,和K_{AUSF}),SUPI,RANDm,或者计数器Count,认证服务功能保存归属鉴权向量,SUPI,RANDm,或者计数器Count,并由XRES*哈希散列得到HXRES*,K_{AUSF}生成得到K_{SEAF},这样的得到鉴权向量(RAND,AUTN,HXRES*,和K_{SEAF}),向第一认证功能实体发送认证请求响应消息,所述消息携带AUTN,RAND和HXRES*;

[0104] 步骤506,UDM/ARPF向第一认证功能实体发送用户认证请求消息,所述消息携带AUTN和RAND;

[0105] 步骤507,第一认证功能实体向终端发送用户认证请求消息,所述消息携带AUTN和RAND;

[0106] 步骤508,终端收到RAND和AUTN后,按照步骤505相似计算方法算出SQN和XMAC,验证AUTN中的SQN是否大于终端SQN、验证"MAC=XMAC",这些验证通过后,同时计算出RES*,生成K_{AUSF}=HMAC-SHA-RSA256(FC||SN||SN长度||(SQN⊕AK)||(SQN⊕AK)长度,CK||IK),其中FC=0x6A,SN为服务网络名称;

[0107] 步骤509,终端向第一认证功能实体发送用户认证请求响应消息,所述消息携带RES*;

[0108] 步骤510,第一认证功能实体由RES*推导出HRES*,然后将哈希相应(Hash RESponse,简称HRES*)和HXRES*进行比较,如果比较通过,拜访网络鉴权成功,向认证服务功能/签约数据管理功能发送认证执行消息,所述消息携带RES*;

[0109] 步骤511,认证服务功能/签约数据管理功能比较响应(RESponse,简称RES*)和XRES*,如果相等,在归属网络鉴权成功,生成出K_{SEAF}=HMAC-SHA-RSA256(FC||SN||SN长度||RANDm||RANDm长度,K_{AUSF})其中FC=0x6C,SN为服务网络名称。认证服务功能AUSF哈希RANDm和(SQN⊕AK)得到新RANDm,哈希计数器计数Count和RANDm得到新RANDm,认证服务功能AUSF将新RANDm和Count+1送签约数据管理功能UDM/ARPF保存;

[0110] 步骤512,向第一认证功能实体回送认证确认消息,所述消息携带SUPI,中间密钥K_{SEAF}和Count;

[0111] 步骤513,第一认证功能实体由中间密钥K_{SEAF}生成出K_{AMF},其中所述K_{AMF}=HMAC-SHA-RSA256(FC||SUPI||SUPI长度||ABBA||ABBA长度,K_{SEAF})其中FC=0x6D,ABBA为防止降维攻击参数,再由K_{AMF}生成出接入层加密密钥和完整性保护密钥,非接入层加密密钥$K_{NAS-enc}$和完整性保护密钥,向终端回送注册请求响应消息,所述消息携带5G-GUTI,Count。

[0112] 步骤514,终端安全网络密钥生成方法生成K_{SEAF}=HMAC-SHA-RSA256(FC||SN||SN长度||RANDm||RANDm长度,K_{AUSF})其中FC=0x6C,SN为服务网络名称,再由K_{SEAF}生成出K_{AMF},再由K_{AMF}生成出接入层加密密钥和完整性保护密钥,非接入层加密密钥$K_{NAS-enc}$和完整性保护密钥。终端哈希RANDm和SQN得到新RANDm,或者终端哈希计数器计数Count和RANDm得到新RANDm,保存对应的RANDm。

[0113] 终端发生移动,移动到新的小区驻留,发起新的注册请求消息,则会使用5G-GUTI进行注册,如果再发起一次AKA成功过程,网络将会使用新RANDm来生成K_{SEAF},如果注册过程中需要获取SUCI,终端可按照上述发明流程产生新的RANDm来生成网络和终端K_{SEAF},这样终端和网络都可获得受保护接入层和非接入层会话密钥,保护终端和网络的正常业务。

[0114] 实施例3

[0115] 在本实施例中还提供了一种密钥的确定装置,该装置用于实现上述实施例及优选

实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0116] 图6是根据本发明实施例的一种密钥的确定装置的结构框图，如图6所示，位于终端，该装置包括：

[0117] 发送模块62，用于在网络注册过程中，向网络侧设备发送加密随机数RANDm得到的RANDs，其中所述RANDm用于所述网络侧设备确定中间锚定密钥；

[0118] 第一确定模块64，用于接收所述网络侧设备反馈的网络认证请求，并根据RANDm确定所述中间锚定密钥。

[0119] 可选地，所述装置还包括：加密模块，用于将生成的所述RANDm加密为所述RANDs。

[0120] 需要说明的是，上述各个模块是可以通过软件或硬件来实现的，对于后者，可以通过以下方式实现，但不限于此：上述模块均位于同一处理器中；或者，上述各个模块以任意组合的形式分别位于不同的处理器中。

[0121] 实施例4

[0122] 在本实施例中还提供了一种密钥的确定装置，该装置用于实现上述实施例及优选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0123] 图7是根据本发明实施例的另一种密钥的确定装置的结构框图，如图7所示，位于网络侧设备，该装置包括：

[0124] 接收模块72，用于接收终端在网络注册过程中发送的RANDs，并对所述RANDs进行解密以获取随机数RANDm；

[0125] 第二确定模块74，用于根据所述RANDm确定中间锚定密钥；

[0126] 反馈模块76，用于向所述终端反馈网络认证请求，以使所述终端根据所述RANDm确定中间锚定密钥。

[0127] 实施例5

[0128] 本发明的实施例还提供了一种存储介质，该存储介质中存储有计算机程序，其中，该计算机程序被设置为运行时执行上述任一项方法实施例中的步骤。

[0129] 可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的计算机程序：

[0130] S1，终端在网络注册过程中，向网络侧设备发送加密有随机数RANDm的RANDs，其中所述RANDs用于所述网络侧设备确定中间锚定密钥；

[0131] S2，所述终端接收所述网络侧设备反馈的网络认证请求，并根据RANDm确定所述中间锚定密钥。

[0132] 或，

[0133] S1，网络侧设备接收终端在网络注册过程中发送的RANDs，并对所述RANDs进行解密以获取随机数RANDm；

[0134] S2，所述网络侧设备根据所述RANDm确定中间锚定密钥；

[0135] S3，所述网络侧设备向所述终端反馈网络认证请求，以使所述终端根据所述RANDm

确定中间锚定密钥。

[0136] 可选地，在本实施例中，上述存储介质可以包括但不限于：U盘、只读存储器(Read-Only Memory，简称为ROM)、随机存取存储器(Random Access Memory，简称为RAM)、移动硬盘、磁碟或者光盘等各种可以存储计算机程序的介质。

[0137] 本发明的实施例还提供了一种电子装置，包括存储器和处理器，该存储器中存储有计算机程序，该处理器被设置为运行计算机程序以执行上述任一项方法实施例中的步骤。

[0138] 可选地，上述电子装置还可以包括传输设备以及输入输出设备，其中，该传输设备和上述处理器连接，该输入输出设备和上述处理器连接。

[0139] 可选地，在本实施例中，上述处理器可以被设置为通过计算机程序执行以下步骤：

[0140] S1，终端在网络注册过程中，向网络侧设备发送加密随机数RANDm得到的RANDs，其中所述RANDm用于所述网络侧设备确定中间锚定密钥；

[0141] S2，所述终端接收所述网络侧设备反馈的网络认证请求，并根据RANDm确定所述中间锚定密钥。

[0142] 或，

[0143] S1，网络侧设备接收终端在网络注册过程中发送的RANDs，并对所述RANDs进行解密以获取随机数RANDm；

[0144] S2，所述网络侧设备根据所述RANDm确定中间锚定密钥；

[0145] S3，所述网络侧设备向所述终端反馈网络认证请求，以使所述终端根据所述RANDm确定中间锚定密钥。

[0146] 可选地，本实施例中的具体示例可以参考上述实施例及可选实施方式中所描述的示例，本实施例在此不再赘述。

[0147] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0148] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。


终端设备
基站
认证功能
认证服务功能
签约数据管理功能

图1

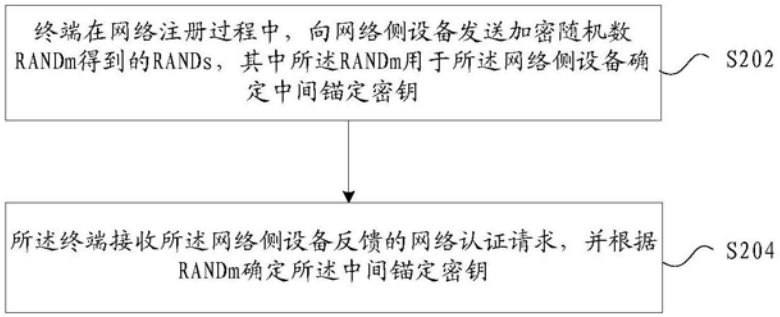

终端在网络注册过程中，向网络侧设备发送加密随机数RANDm得到的RANDs，其中所述RANDm用于所述网络侧设备确定中间锚定密钥
S202
所述终端接收所述网络侧设备反馈的网络认证请求，并根据RANDm确定所述中间锚定密钥
S204

图2

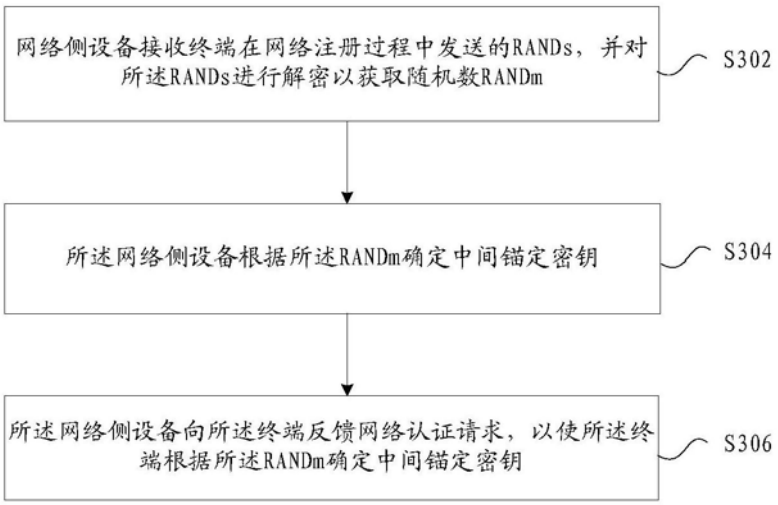

网络侧设备接收终端在网络注册过程中发送的RANDs，并对所述RANDs进行解密以获取随机数RANDm
S302
所述网络侧设备根据所述RANDm确定中间锚定密钥
S304
所述网络侧设备向所述终端反馈网络认证请求，以使所述终端根据所述RANDm确定中间锚定密钥
S306

图3

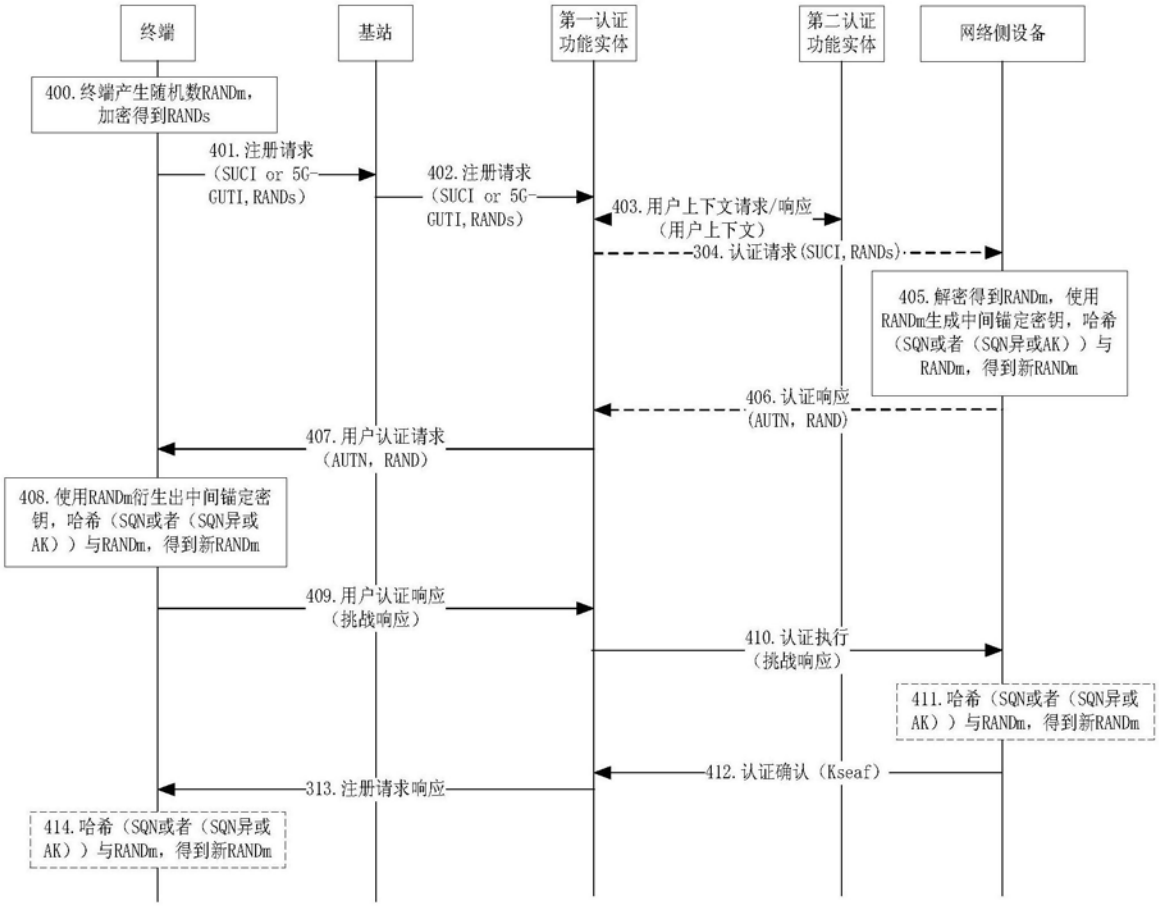

终端
基站
第一认证功能实体
第二认证功能实体
网络侧设备
400.终端产生随机数RANDm，加密得到RANDs
401.注册请求（SUCI or 5G-GUTI,RANDs）
402.注册请求（SUCI or 5G-GUTI,RANDs）
403.用户上下文请求/响应（用户上下文）
304.认证请求(SUCI,RANDs)
405.解密得到RANDm，使用RANDm生成中间锚定密钥，哈希（SQN或者（SQN异或AK））与RANDm，得到新RANDm
406.认证响应（AUTN，RAND）
407.用户认证请求（AUTN，RAND）
408.使用RANDm衍生出中间锚定密钥，哈希（SQN或者（SQN异或AK））与RANDm，得到新RANDm
409.用户认证响应（挑战响应）
410.认证执行（挑战响应）
411.哈希（SQN或者（SQN异或AK））与RANDm，得到新RANDm
412.认证确认（Kseaf）
313.注册请求响应
414.哈希（SQN或者（SQN异或AK））与RANDm，得到新RANDm

图4

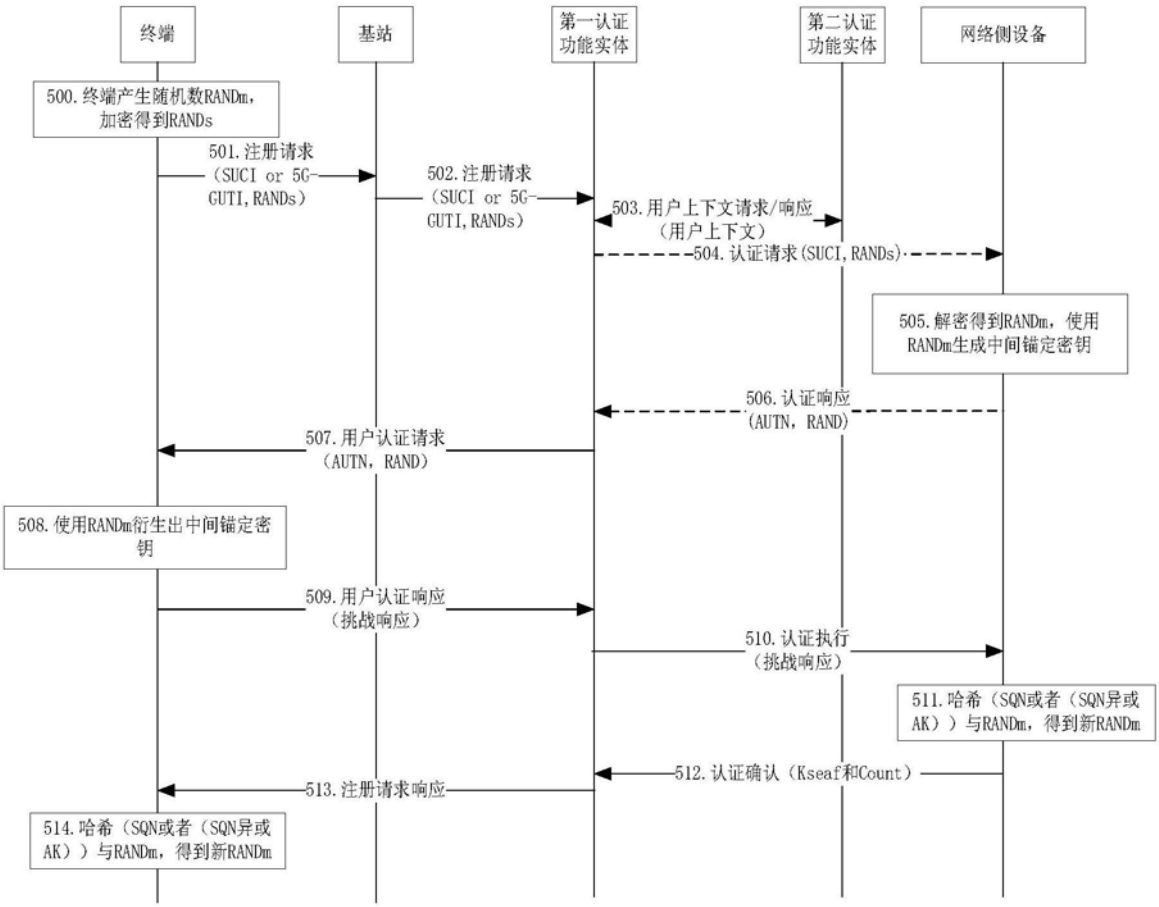

终端
基站
第一认证功能实体
第二认证功能实体
网络侧设备
500.终端产生随机数RANDm，加密得到RANDs
501.注册请求（SUCI or 5G-GUTI,RANDs）
502.注册请求（SUCI or 5G-GUTI,RANDs）
503.用户上下文请求/响应（用户上下文）
504.认证请求(SUCI,RANDs)
505.解密得到RANDm，使用RANDm生成中间锚定密钥
506.认证响应（AUTN，RAND）
507.用户认证请求（AUTN，RAND）
508.使用RANDm衍生出中间锚定密钥
509.用户认证响应（挑战响应）
510.认证执行（挑战响应）
511.哈希（SQN或者（SQN异或AK））与RANDm，得到新RANDm
512.认证确认（Kseaf和Count）
513.注册请求响应
514.哈希（SQN或者（SQN异或AK））与RANDm，得到新RANDm

图5

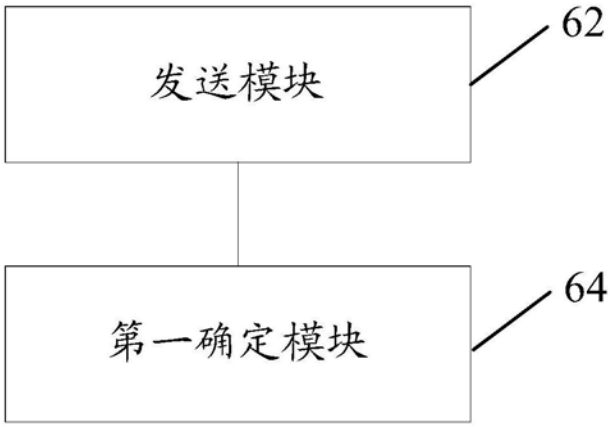

发送模块
62
第一确定模块
64

图6

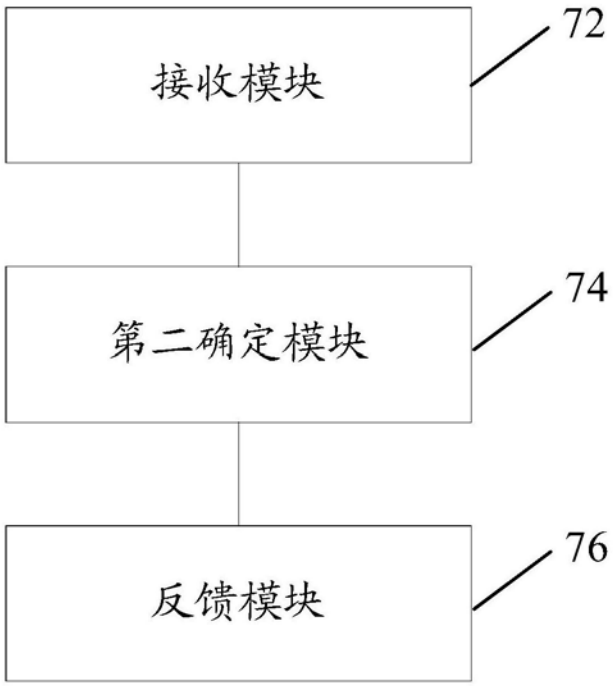


图7