(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 108809635 A
(43)申请公布日 2018.11.13

(21)申请号 201710908017.0

(22)申请日 2017.09.29

(66)本国优先权数据
201710313519.9 2017.05.05 CN

(71)申请人 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 吴荣 张博 甘露

(51)Int.Cl.
H04L 9/08(2006.01)
H04W 12/04(2009.01)

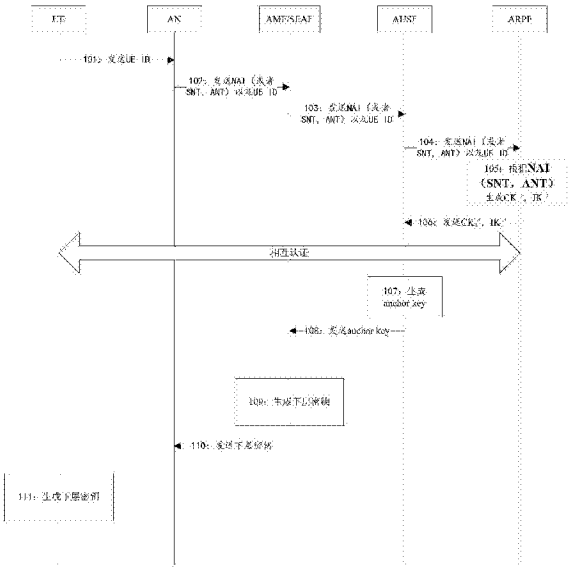
权利要求书4页 说明书31页 附图23页

(54)发明名称

锚密钥生成方法、设备以及系统

(57)摘要

本申请实施例提供了一种锚密钥生成方法，设备以及系统。其中，所述方法包括：第一通讯设备接收第二通讯设备发送指示标识，其中，指示标识用于指示终端的接入方式；第一通讯设备向第三通讯设备发送指示标识；第一通讯设备接收第三通讯设备返回的中间密钥，其中，中间密钥是根据指示标识生成的；第一通讯设备根据中间密钥生成锚密钥，其中，锚密钥对应终端的接入方式；第一通讯设备将锚密钥发送给第二通讯设备，以供第二通讯设备根据锚密钥为接入方式推衍下层密钥。上述方法能够为不同的接入方式生成统一的锚密钥，并且实现了将不同接入方式的锚密钥，以及基于锚密钥生成的下层密钥进行隔离。



CN 108809635 A

1.一种锚密钥生成方法,其特征在于,包括:

第一通讯设备接收第二通讯设备发送指示标识,其中,所述指示标识用于指示终端的接入方式;

所述第一通讯设备向第三通讯设备发送所述指示标识;

所述第一通讯设备接收所述第三通讯设备返回的中间密钥,其中,所述中间密钥是根据所述指示标识生成的;

所述第一通讯设备根据所述中间密钥生成锚密钥,其中,所述锚密钥对应所述终端的接入方式;

所述第一通讯设备将所述锚密钥发送给所述第二通讯设备,以供所述第二通讯设备根据所述锚密钥为所述接入方式推衍下层密钥。

2.根据权利要求1所述的方法,其特征在于,所述接入方式是根据接入类型以及运营商类型中的至少一个进行区分的。

3.根据权利要求2所述的方法,其特征在于,所述第一通讯设备根据所述中间密钥生成锚密钥具体为:

所述第一通讯设备根据以下公式生成锚密钥,

anchor key=KDF(IK$_1$'||CK$_1$')

其中,anchor key为所述锚密钥,(IK$_1$',CK$_1$')为所述中间钥匙,IK$_1$'为中间完整性密钥,CK$_1$'为中间保密性密钥,||的含义为级联,表示将符号两边的字符串连起来。

4.根据权利要求3所述的方法,其特征在于,所述指示标识包括接入类型标识以及运营商类型标识,所述接入类型标识用于指示所述接入类型,所述运营商类型标识用于指示所述运营商类型;

所述中间密钥是根据以下公式生成的:

$(CK_1', IK_1')=KDF(SQN\oplus AK, ANT, SNT, CK||IK)$;

其中,(CK$_1$',IK$_1$')为所述中间密钥,CK$_1$'为所述中间保密性密钥,IK$_1$'为所述中间完整性密钥,KDF为密钥生成算法,SQN为最新序列号,ANT为所述接入类型标识,SNT为所述运营商类型标识,CK为初始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK=f3(RAND),IK=f4(RAND),AK=f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

5.根据权利要求3所述的方法,其特征在于,所述中间密钥是根据以下公式生成的:

$(CK_1', IK_1')=KDF(SQN\oplus AK, NAI, CK||IK)$;

其中,(CK$_1$',IK$_1$')为所述中间密钥,CK$_1$'为所述中间保密性密钥,IK$_1$'为所述中间完整性密钥,KDF为密钥生成算法,SQN为最新序列号,NAI为所述指示标识,CK为初始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK=f3(RAND),IK=f4(RAND),AK=f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

6.根据权利要求2所述的方法,其特征在于,所述第一通讯设备根据所述中间密钥生成锚密钥具体为:

所述第一通讯设备根据以下公式生成EMSK',

EMSK'=PRF'(IK$_2$'||CK$_2$');

其中，EMSK'为扩展主会话密钥，(IK_2'，CK_2')为所述中间钥匙，IK_2'为中间完整性密钥，CK_2'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来；

所述第一通讯设备根据以下公式生成锚密钥，

anchor key＝KDF(EMSK'，SNT)；

其中，anchor key为所述锚密钥，SNT为所述运营商类型标识。

7.根据权利要求6所述的方法，其特征在于，所述中间密钥是根据以下公式生成的：

(CK_2'，IK_2')=KDF(SQN⊕AK，ANT，CK||IK)；

其中，(CK_2'，IK_2')为所述中间密钥，CK_2'为所述中间保密性密钥，IK_2'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

8.根据权利要求2所述的方法，其特征在于，所述第一通讯设备根据所述中间密钥生成锚密钥具体为：

所述第一通讯设备根据以下公式生成EMSK'，

EMSK'＝PRF'(IK_2'||CK_2')；

其中，EMSK'为扩展主会话密钥，(IK_2'，CK_2')为所述中间钥匙，IK2'为中间完整性密钥，CK2'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来；

所述第一通讯设备根据以下公式生成锚密钥，

anchor key＝KDF(EMSK'，ANT)；

其中，anchor key为所述锚密钥，ANT为所述接入类型标识。

9.根据权利要求8所述的方法，其特征在于，所述中间密钥是根据以下公式生成的：

(CK_2'，IK_2')=KDF(SQN⊕AK，SNT，CK||IK)；

其中，(CK_2'，IK_2')为所述中间密钥，CK_2'为所述中间保密性密钥，IK_2'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，SNT为所述运营商类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

10.一种通讯设备，其特征在于，包括：接收模块、发送模块以及生成模块，

所述接收模块用于接收第二通讯设备发送指示标识，其中，所述指示标识用于指示终端的接入方式；

所述发送模块用于向第三通讯设备发送所述指示标识；

所述接收模块用于接收所述第三通讯设备返回的中间密钥，其中，所述中间密钥是根据所述指示标识生成的；

所述生成模块用于根据所述中间密钥生成锚密钥，其中，所述锚密钥对应所述终端的接入方式；

所述发送模块用于将所述锚密钥发送给所述第二通讯设备，以供所述第二通讯设备根据所述锚密钥为所述接入方式推衍下层密钥。

11.根据权利要求10所述的设备，其特征在于，所述接入方式是根据接入类型以及运营商类型中的至少一个进行区分的。

12.根据权利要求11所述的设备，其特征在于，所述生成模块用于根据以下公式生成锚

密钥，

anchor key＝KDF(IK$_1$'||CK$_1$')

其中，anchor key为所述锚密钥，(IK$_1$'，CK$_1$')为所述中间钥匙，IK$_1$'为中间完整性密钥，CK$_1$'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来。

13.根据权利要求12所述的设备，其特征在于，所述指示标识包括接入类型标识以及运营商类型标识，所述接入类型标识用于指示所述接入类型，所述运营商类型标识用于指示所述运营商类型；

所述生成模块用于根据以下公式生成的：

(CK$_1$'，IK$_1$')=KDF(SQN⊕AK，ANT，SNT，CK||IK)；

其中，(CK$_1$'，IK$_1$')为所述中间密钥，CK$_1$'为所述中间保密性密钥，IK$_1$'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，SNT为所述运营商类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

14.根据权利要求12所述的设备，其特征在于，所述生成模块用于根据以下公式生成的：

(CK$_1$'，IK$_1$')=KDF(SQN⊕AK，NAI，CK||IK)；

其中，(CK$_1$'，IK$_1$')为所述中间密钥，CK$_1$'为所述中间保密性密钥，IK$_1$'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，NAI为所述指示标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

15.根据权利要求11所述的设备，其特征在于，所述生成模块用于根据以下公式生成EMSK'，

EMSK'＝PRF'(IK$_2$'||CK$_2$')；

其中，EMSK'为扩展主会话密钥，(IK$_2$'，CK$_2$')为所述中间钥匙，IK$_2$'为中间完整性密钥，CK$_2$'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来；

所述生成模块用于根据以下公式生成锚密钥，

anchor key＝KDF(EMSK'，SNT)；

其中，anchor key为所述锚密钥，SNT为所述运营商类型标识。

16.根据权利要求15所述的设备，其特征在于，所述生成模块用于根据以下公式生成的：

(CK$_2$'，IK$_2$')=KDF(SQN⊕AK，ANT，CK||IK)；

其中，(CK$_2$'，IK$_2$')为所述中间密钥，CK$_2$'为所述中间保密性密钥，IK$_2$'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

17.根据权利要求11所述的设备，其特征在于，所述生成模块用于根据以下公式生成EMSK'，

EMSK'＝PRF'(IK$_2$'||CK$_2$')；

其中，EMSK'为扩展主会话密钥，(IK_2'，CK_2')为所述中间钥匙，IK2'为中间完整性密钥，CK2'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来；

所述生成模块用于根据以下公式生成锚密钥，

anchor key＝KDF(EMSK'，ANT)；

其中，anchor key为所述锚密钥，ANT为所述接入类型标识。

18.根据权利要求17所述的设备，其特征在于，所述生成模块用于根据以下公式生成的：

(CK_2'，IK_2')=KDF(SQN⊕AK，SNT，CK||IK)；

其中，(CK_2'，IK_2')为所述中间密钥，CK_2'为所述中间保密性密钥，IK_2'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，SNT为所述运营商类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

19.一种通信系统，其特征在于，包括相互连接的接入和移动性控制功能网元、会话管理网元、认证服务器以及统一数据管理网元，其中，所述认证服务器为如权利要求10-18任一权利要求所述的认证服务器。

锚密钥生成方法、设备以及系统

技术领域

[0001] 本发明涉及通信领域，尤其涉及一种锚密钥生成方法、设备以及系统。

背景技术

[0002] 密钥是加密运算和解密运算的关键，也是密码系统的关键，所以，在信息安全系统中，密钥协商是认证流程中的重要一环。在现有的4G系统中，密钥协商过程如图1所示，该流程 的执行需要的网元包括用户设备(User Equipment，UE)、基站(eNodeB)、移动性管理实体 (MobilityManagement Entity，MME)、归属签约用户服务器(Home Subscriber Server，HSS) 以及鉴权中心(AUthentication Center，AuC)等，执行流程大致如下：

[0003] 步骤1：AuC根据根密钥K生成完整性密钥IK以及保密性密钥CK，并将完整性密钥IK以及 保密性密钥CK发送给HSS。相应地，HSS接收AuC发送的完整性密钥IK以及保密性密钥CK。

[0004] 步骤2：HSS根据完整性密钥IK以及保密性密钥CK生成中间密钥K_{ASME}，并将中间密钥 K_{ASME}发送给MME。相应地，MME接收HSS发送的中间密钥K_{ASME}。

[0005] 步骤3：MME根据中间密钥K_{ASME}生成用于对非接入层(Non Access Stratum，NAS)消息 进行保密性保护的NAS完整性密钥K_{NASenc}，以及，进行完整性保护的NAS完整性保护密钥K_{NASint}。

[0006] 步骤4：MME根据中间密钥K_{ASME}生成基站密钥K_{eNB}，并将基站密钥K_{eNB}发送给eNodeB。相应地，eNodeB接收MME发送的基站密钥K_{eNB}。

[0007] 步骤5：eNodeB根据基站密钥K_{eNB}分别生成用于对用户面数据的保密性进行保护的用户 面保密性密钥K_{UPenc}，用于对用户面数据的完整性进行保护的用户面完整性密钥K_{UPint}，用于 对控制面数据的保密性进行保护的控制面保密性密钥K_{RRCenc}，用于对控制面数据的完整性进 行保护的控制面完整性密钥K_{RRCint}。

[0008] 步骤6：UE根据根密钥K自行生成完整性密钥IK、保密性密钥CK、中间密钥K_{ASME}、用户 面保密性密钥K_{UPenc}、用户面完整性密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密 钥K_{RRCint}。

[0009] 经过图1所述的密钥协商流程之后，4G系统中将生成如图2所示的密钥架构。

[0010] 可以理解，图1是4G应用场景中，终端通过第三代合作伙伴计划(3rd Generation Partnership Project，3GPP)的接入方式接入到核心网的流程中的密钥协商流程。为了适应各种应用场景的 要求，终端可以通过各种不同的接入方式接入到核心网，例如，3GPP接入方式、可靠的非3GPP 接入方式，非可靠的3GPP接入方式等等，在不同的接入方式中，密钥协商流程也各不相同。为了能够兼容各种接入方式，在5G标准中，明确规定了需要在不同的接入方式的密钥协商流 程中生成一个统一的锚密钥(anchor key)。但是，如何生成一个统一的锚密钥是本领域的技 术人员需要解决的问题。

发明内容

[0011] 本申请实施例提供了一种锚密钥生成方法、设备以及系统，能够为不同的接入方式生成 统一的锚密钥，并且实现了将不同接入方式的锚密钥，以及基于锚密钥生成的下层密钥进行 隔离。

[0012] 第一方面，提供了一种锚密钥生成方法，包括：第一通讯设备接收第二通讯设备发送指 示标识，其中，所述指示标识用于指示终端的接入方式；所述第一通讯设备向第三通讯设备 发送所述指示标识；所述第一通讯设备接收所述第三通讯设备返回的中间密钥，其中，所述 中间密钥是根据所述指示标识生成的；所述第一通讯设备根据所述中间密钥生成锚密钥，其 中，所述锚密钥对应所述终端的接入方式；所述第一通讯设备将所述锚密钥发送给所述第二 通讯设备，以供所述第二通讯设备根据所述锚密钥为所述接入方式推衍下层密钥。

[0013] 在一些可能的实施方式中，所述接入方式是根据接入类型以及运营商类型中的至少一个 进行区分的。

[0014] 在一些可能的实施方式中，所述第一通讯设备根据所述中间密钥生成锚密钥具体为：

[0015] 所述第一通讯设备根据以下公式生成锚密钥，

[0016] anchor key＝KDF(IK$_1$'||CK$_1$')

[0017] 其中，anchor key为所述锚密钥，(IK$_1$'，CK$_1$')为所述中间钥匙，IK$_1$'为中间完整性密 钥，CK$_1$'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来。

[0018] 所述第一通讯设备至少可以根据以下两种方式生成中间密钥：

[0019] 当所述指示标识包括接入类型标识以及运营商类型标识时，所述中间密钥是根据以下公 式生成的：

[0020] $(CK_1', IK_1') = KDF(SQN \oplus AK, ANT, SNT, CK||IK)$;

[0021] 其中，所述接入类型标识用于指示所述接入类型，所述运营商类型标识用于指示所述运 营商类型；(CK$_1$'，IK$_1$')为所述中间密钥，CK$_1$'为所述中间保密性密钥，IK$_1$'为所述中间完 整性密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，SNT为所述运营商类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算 法，⊕的含义为异或运算。

[0022] 当所述指示标识是NAI时，所述中间密钥是根据以下公式生成的：

[0023] $(CK_1', IK_1') = KDF(SQN \oplus AK, NAI, CK||IK)$;

[0024] 其中，(CK$_1$'，IK$_1$')为所述中间密钥，CK$_1$'为所述中间保密性密钥，IK$_1$'为所述中间完 整性密钥，KDF为密钥生成算法，SQN为最新序列号，NAI为所述指示标识，CK为初始保 密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

[0025] 在一些可能的实施方式中，所述第一通讯设备根据以下公式生成所述中间密钥：

[0026] $(CK_2', IK_2') = KDF(SQN \oplus AK, ANT, CK||IK)$;

[0027] 其中，(CK$_2$'，IK$_2$')为所述中间密钥，CK$_2$'为所述中间保密性密钥，IK$_2$'为所述中间完 整性密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，CK为初 始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)， AK＝f5

(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0028] 所述第一通讯设备根据以下公式生成EMSK',

[0029] EMSK'=PRF'(IK$_2$'||CK$_2$');

[0030] 其中,EMSK'为扩展主会话密钥,(IK$_2$',CK$_2$')为所述中间钥匙,IK$_2$'为中间完整性密 钥,CK$_2$'为中间保密性密钥,||的含义为级联,表示将符号两边的字符串连起来;

[0031] 所述第一通讯设备根据以下公式生成锚密钥,

[0032] anchor key=KDF(EMSK',SNT);

[0033] 其中,anchor key为所述锚密钥,SNT为所述运营商类型标识。

[0034] 在一些可能的实施方式中,所述第一通讯设备根据以下公式生成所述中间密钥:

[0035] (CK$_2$', IK$_2$')=KDF(SQN⊕AK, SNT, CK||IK);

[0036] 其中,(CK$_2$',IK$_2$')为所述中间密钥,CK$_2$'为所述中间保密性密钥,IK$_2$'为所述中间完 整性密钥,KDF为密钥生成算法,SQN为最新序列号,SNT为所述运营商类型标识,CK为 初始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK=f3(RAND),IK=f4(RAND), AK=f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0037] 所述第一通讯设备根据以下公式生成EMSK',

[0038] EMSK'=PRF'(IK$_2$'||CK$_2$');

[0039] 其中,EMSK'为扩展主会话密钥,(IK$_2$',CK$_2$')为所述中间钥匙,IK2'为中间完整性密 钥,CK2'为中间保密性密钥,||的含义为级联,表示将符号两边的字符串连起来;

[0040] 所述第一通讯设备根据以下公式生成锚密钥,

[0041] anchor key=KDF(EMSK',ANT);

[0042] 其中,anchor key为所述锚密钥,ANT为所述接入类型标识。

[0043] 第二方面,提供了一种通讯设备,包括:接收模块、发送模块以及生成模块,所述接收 模块用于接收第二通讯设备发送指示标识,其中,所述指示标识用于指示终端的接入方式;所述发送模块用于向第三通讯设备发送所述指示标识;所述接收模块用于接收所述第三通讯 设备返回的中间密钥,其中,所述中间密钥是根据所述指示标识生成的;所述生成模块用于 根据所述中间密钥生成锚密钥,其中,所述锚密钥对应所述终端的接入方式;所述发送模块 用于将所述锚密钥发送给所述第二通讯设备,以供所述第二通讯设备根据所述锚密钥为所述 接入方式推衍下层密钥。

[0044] 在一些可能的实施方式中,所述接入方式是根据接入类型以及运营商类型中的至少一个 进行区分的。

[0045] 在一些可能的实施方式中,所述生成模块用于根据以下公式生成锚密钥,

[0046] anchor key=KDF(IK$_1$'||CK$_1$')

[0047] 其中,anchor key为所述锚密钥,(IK$_1$',CK$_1$')为所述中间钥匙,IK$_1$'为中间完整性密 钥,CK$_1$'为中间保密性密钥,||的含义为级联,表示将符号两边的字符串连起来。

[0048] 所述第一通讯设备至少可以根据以下两种方式生成中间密钥:

[0049] 当所述指示标识包括接入类型标识以及运营商类型标识时,所述生成模块用于根据以下 公式生成的:

[0050] (CK$_1$', IK$_1$')=KDF(SQN⊕AK, ANT, SNT, CK||IK);

[0051] 其中,所述接入类型标识用于指示所述接入类型,所述运营商类型标识用于指示

所述运 营商类型，(CK_1'，IK_1')为所述中间密钥，CK_1'为所述中间保密性密钥，IK_1'为所述中间完 整性密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，SNT为所述运营商类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算 法，⊕的含义为异或运算。

[0052] 当所述指示标识是NAI时，所述生成模块用于根据以下公式生成的：

[0053] $(CK_1', IK_1') = KDF(SQN \oplus AK, NAI, CK||IK)$;

[0054] 其中，(CK_1'，IK_1')为所述中间密钥，CK_1'为所述中间保密性密钥，IK_1'为所述中间完 整性密钥，KDF为密钥生成算法，SQN为最新序列号，NAI为所述指示标识，CK为初始保 密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

[0055] 在一些可能的实施方式中，生成模块用于根据以下公式生成的：

[0056] $(CK_2', IK_2') = KDF(SQN \oplus AK, ANT, CK||IK)$;

[0057] 其中，(CK_2'，IK_2')为所述中间密钥，CK_2'为所述中间保密性密钥，IK_2'为所述中间完 整性密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，CK为初 始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)， AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

[0058] 所述生成模块用于根据以下公式生成EMSK'，

[0059] EMSK'＝PRF'(IK_2'||CK_2')；

[0060] 其中，EMSK'为扩展主会话密钥，(IK_2'，CK_2')为所述中间钥匙，IK_2'为中间完整性密 钥，CK_2'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来；

[0061] 所述生成模块用于根据以下公式生成锚密钥，

[0062] anchor key＝KDF(EMSK'，SNT)；

[0063] 其中，anchor key为所述锚密钥，SNT为所述运营商类型标识。

[0064] 在一些可能的实施方式中，所述生成模块用于根据以下公式生成的：

[0065] $(CK_2', IK_2') = KDF(SQN \oplus AK, SNT, CK||IK)$；

[0066] 其中，(CK_2'，IK_2')为所述中间密钥，CK_2'为所述中间保密性密钥，IK_2'为所述中间完 整性密钥，KDF为密钥生成算法，SQN为最新序列号，SNT为所述运营商类型标识，CK为 初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)， AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

[0067] 所述生成模块用于根据以下公式生成EMSK'，

[0068] EMSK'＝PRF'(IK_2'||CK_2')；

[0069] 其中，EMSK'为扩展主会话密钥，(IK_2'，CK_2')为所述中间钥匙，IK2'为中间完整性密 钥，CK2'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来；

[0070] 所述生成模块用于根据以下公式生成锚密钥，

[0071] anchor key＝KDF(EMSK'，ANT)；

[0072] 其中，anchor key为所述锚密钥，ANT为所述接入类型标识。

[0073] 第三方面，提供了一种通讯设备，包括：存储器以及与所述存储器耦合的处理器、通信 模块，其中：所述通信模块用于发送或者接收外部发送的数据，所述存储器用于存储

第一方 面描述的方法的实现代码，所述处理器用于执行所述存储器中存储的程序代码，即执行第一 方面描述的方法。

[0074] 第四方面，提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行上述第一方面所述的方法。

[0075] 第五方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算 机执行上述第一方面所述的方法。

[0076] 第六方面，提供了一种通信系统，包括相互连接的接入和移动性控制功能网元、会话管 理网元、认证服务器以及统一数据管理网元，其中，所述认证服务器为如权利要求第二方面 或者第三方面任一项所述的认证服务器。

附图说明

[0077] 为了更清楚地说明本发明实施例或背景技术中的技术方案，下面将对本发明实施例或背 景技术中所需要使用的附图进行说明。

[0078] 图1是现有技术提供的一种4G应用场景中通过3GPP接入方式中密钥协商的流程示意 图；

[0079] 图2是图1所示的密钥协商的流程的密钥架构图；

[0080] 图3是本申请实施例涉及的通过3GPP接入方式接入5G核心网的网络架构图；

[0081] 图4是本申请实施例涉及的通过非3GPP接入方式接入5G核心网的网络架构图；

[0082] 图5是本申请实施例提供的第一种锚密钥生成方法的交互图；

[0083] 图6A至6B分别是图5所示的锚密钥生成方法中采用3GPP方式接入以及非3GPP方式接入时的具体交互图；

[0084] 图7是使用图5所示的锚密钥生成方法得到的密钥架构图；

[0085] 图8是本申请实施例提供的第二种锚密钥生成方法的交互图；

[0086] 图9是本申请实施例提供的第三种锚密钥生成方法的交互图；

[0087] 图10是使用图9所示的锚密钥生成方法得到的密钥架构图；

[0088] 图11是本申请实施例提供的第四种锚密钥生成方法的交互图；

[0089] 图12是使用图11所示的锚密钥生成方法得到的密钥架构图；

[0090] 图13是是本申请实施例提供的第五种锚密钥生成方法的交互图；

[0091] 图14A至14B分别是图13所示的锚密钥生成方法中采用3GPP方式接入以及非3GPP方式接入时的具体交互图；

[0092] 图15是使用图13所示的锚密钥生成方法得到的密钥架构图；

[0093] 图16是本申请实施例提供的第六种锚密钥生成方法的交互图；

[0094] 图17A至17B分别是图16所示的锚密钥生成方法中采用3GPP方式接入以及非3GPP方式接入时的具体交互图；

[0095] 图18是使用图16所示的锚密钥生成方法得到的密钥架构图；

[0096] 图19是本申请实施例提供的第七种锚密钥生成方法的交互图；

[0097] 图20是使用图19所示的锚密钥生成方法得到的密钥架构图；

[0098] 图21是本申请实施例提供的一种通讯设备的结构示意图；

[0099] 图22是本申请实施例提供的另一种通讯设备的结构示意图。

具体实施方式

[0100] 下面结合附图以及具体的实施例对本申请的多个实施例分别进行介绍。

[0101] 图3是本申请实施例涉及的一种网络架构图，其中，这种网络架构主要适用于通过3GPP 方式接入5G核心网的场景。图4是本申请实施例涉及的另一种网络架构图，其中，这种网 络架构主要适用于通过非3GPP方式接入5G核心网的场景。图3和图4所示的网络架构均包 括与密钥协商相关的网元：终端(Terminal)、接入节点(Access node,AN)(即图2中的N3IWF)、接入和移动性控制功能网元(Access and Mobility Function,AMF)、会话管理网元(Session Management Function,SMF)、认证服务器(Authentication Server Function,AUSF)以及统 一数据管理网元(Unified Data Management,UDM)。

[0102] 需要说明的是，AMF中可以部署安全锚点(Security Anchor Function,SEAF)，UDM中 可以部署认证信任状存储和操作功能网元(Authentication Credential Repository and Processing Function,ARPF)。当然，SEAF也可以不部署在AMF中，而是SEAF与AMF两 者单独部署。类似地，ARPF也可以不部署在UDM中，而是ARPF与UDM两者单独部署。

[0103] 下面分别对密钥协商相关的网元(终端、AN、AMF、SMF、AUSF以及UDM)分别进行 简单的介绍。

[0104] 终端，具体可以是UE(User Equipment)，通信设备(Communication Device)物联网(Internet of Things,IoT)设备中的任意一种。其中，用户设备可以是智能手机(smart phone)、智能 手表(smart watch)，智能平板等等。通信设备可以是服务器、网关(Gateway，GW)、基站 以及控制器等等。物联网设备可以是传感器，电表以及水表等等。

[0105] AN，可以是无线接入点，例如：基站、Wi-Fi接入点(Wireless Fidelity，无线保真)以 及蓝牙接入点等等，也可以是有线接入点，例如：网关，调制解调器，光纤接入，IP接入等等。

[0106] AMF，负责接入控制和移动性管理，也是非接入层(Non-access stratum,NAS)信令的 转发和处理节点。

[0107] SMF，用于执行会话、切片、流flow或者承载bearer的建立和管理，后续可以称执行该 会话管理网元的功能的物理实体为会话管理设备或者SM。其中切片、流flow或者承载bearer 的建立和管理由移动性管理网元负责。

[0108] AUSF，负责密钥的生成、管理和协商。AUSF可以作为一个独立的逻辑功能实体单独部 署，也可以集合在移动性管理(Mobility Management)网元，也就是AMF、会话管理网元SMF等设备中，可能是EPS AKA也可能是EAP AKA'的认证节点，或者其他认证协议的节点。

[0109] UDM，统一的数据管理，主要包括两部分，一部分为业务或者应用的前端，一部分为用 户数据库。具体来说，包括信任状的处理、位置管理、签约数据管理、策略控制等，同时也包括这些相关处理的信息存储。

[0110] SEAF，作为安全认证功能的节点，可能是EPS AKA也可能是EAP AKA'的认证节点，或者其他认证协议的节点；例如认证过程是EPS AKA的情况下，SEAF将接收中间密钥Kasme。

[0111] ARPF，存储安全信任状并使用安全信任状执行安全相关的操作，比如生成密钥，存储安 全的文件。ARPF应该部署在一个物理安全的位置，同时可以与AUSF交互。在实际部署中， ARPF可能是UDM的一个模块或者作为一个单独的网络实体并与UDM部署在一起。

[0112] 需要说明的是，图3以及图4中体现的是各个网元之间的逻辑关系，在实际中，有些网 元可以单独部署，也可以两两或多个网元集成部署在一个实体中。

[0113] 为了能够为不同的接入方式生成统一的锚密钥，本申请实施例提供了一种锚密钥生成方 法。上述方法除了能够生成统一的锚密钥之外，还能够将不同接入方式的锚密钥以及基于锚 密钥生成的下层密钥进行隔离。

[0114] 如图5所示，本申请实施例提供了第一种锚密钥生成方法。在本实施例中，AUSF即为 权利要求中的第一通讯设备，AMF或者SEAF即为权利要求中的第二通讯设备，ARPF即为权利要求中的第三通讯设备。该方法可以基于图3以及图4所示的网络架构来实现，该方法包括但不限于如下步骤。

[0115] 101:UE向AN发送终端标识。相应地，AN接收UE发送的终端标识。

[0116] 在本申请实施例中，终端标识可以是固定不变的标识，例如，媒体访问控制(Media Access Control，MAC)地址、网络协议(Internet Protocol，IP)地址、手机号码、国际移动设备标 识(International Mobile Equipment Identity，IMEI)、国际移动用户识别码(International Mobile Subscriber Identity，IMSI)、IP多媒体私有标识(IP Multimedia Private Identity，IMPI)、IP多 媒体公共标识(IP Multimedia Public Identity，IMPU)等等，也可以是临时分配的标识，例如， 临时移动用户标识符(TemporaryMobileSubscriberIdentity，TMSI)、全球唯一临时UE标识 (Globally Unique Temporary UE Identity，GUTI)等等。

[0117] 可以理解，除了终端标识之外，UE还可以将接入网参数、注册类型、安全参数、UE的5G网络能力，PDU session的状态等至少一种发送给AN。其中，接入网参数为可能为接入网的频点，临时用户标识，NSSAI等与服务网络相关的参数。注册类型为可以表明用户是初次注册、由于移动引起的注册、周期性注册更新等区分用户注册的行为。安全参数为认证和完整性保护相关的参数。NSSAI为网络切片选择辅助信息。UE的5G网络能力可能包括支持接入该网络的配置能力。PDU session为UE和数据网络之间的PDU的业务连接，类型可能为IP、以太网的业务连接。

[0118] 102:AN向AMF(或者SEAF)发送终端标识以及指示标识。相应地，AMF(或者SEAF) 接收AN发送的终端标识以及指示标识。

[0119] 在本申请实施例中，指示标识用于指示终端的接入方式。在5G标准中，可以按照不同 的划分依据对终端的接入方式进行划分。例如，接入方式的划分依据可以包括接入类型以及 运营商类型。其中，接入类型具体可以分为3GPP接入类型、可信的非3GPP接入类型以及 非可信的非3GPP接入类型。运营商类型具体可以分为A运营商类型或者B运营商类型。可以理解，运营商类型还可以有更多的类型，此处仅作为示例，不作具体限定。

[0120] 以划分依据包括接入类型以及运营商类型为例，所述接入方式的划分可以如表1所示：

[0121] 表1接入方式表

[0122]

接入类型 / 运营商类型	3GPP接入类型	可信的非3GPP接入类型	非可信的非3GPP接入类型
A运营商类型	接入方式1	接入方式2	接入方式3
B运营商类型	接入方式4	接入方式5	接入方式6

[0123] 需要说明的，不限于上述两种划分依据，接入方式的划分依据还可以是其他种类的划分 依据，例如，介质类型(有线接入或者无线接入)等等，此处不作具体限定。并且，不限于 接入类型以及运营商类型两种划分依据，接入方式的划分依据还可以是一种、三种、四种或 者更多，即，可以从更多维度或者更少维度对接入方式进行划分。例如，只从3GPP接入类型 和非3GPP接入类型这个维度进行区分。

[0124] 所述指示标识可以是携带在上述接入网参数中。所述指示标识可以是下述的任意一种方 式：所述指示标识可以是网络接入标识(Network Access Identifier，NAI)，用于同时指示接 入类型以及运营商类型。或者，所述指示标识可以包括接入类型标识以及运营商类型标识， 其中，所述接入类型标识用于指示所述接入类型，所述运营商类型标识用于指示所述运营商 类型。可以理解，上述例子仅作为举例，不构成具体限定。

[0125] 在一些可能的实现方式中，网络接入标识可以为SN Identity|Access Network Identity，即 可以特定表示某运营商下的某种接入，如中国联通的WLAN接入等等，此处的SN Identity 为4G网络中的定义，Access Network Identity为4G时非3GPP网络中的定义。也可能将SN Identity或者Access Network Identity的方式进行升级，使其能够表示某运营商的某种接入类 型。

[0126] 在一些可能的实现方式中，接入类型标识具体指示所述接入类型为3GPP接入类型、可 信的非3GPP接入类型以及非可信的非3GPP接入类型。例如，接入类型标识Access Network Type(ANT)可以直接为“3GPP network”，“Trusted Non-3GPP network”，“Untrusted Non-3GPP network”字符串，或者仅为“3GPP network”和“Non-3GPP network”字符串等等。

[0127] 在一些可能的实现方式中，所述运营商类型标识可以包括两部分，一部分用于指示运营 商，另一部分用于指示具体接入类型。例如，运营商类型标识可以指示为中国移动的LTE接 入或者中国联通的WLAN接入。在具体应用中，可以将SN Identity和Access Network Identity 的结合以作为运营商类型标识。也有可能只包括运营商的区分，比如中国移动、中国联通、中国电信等等。

[0128] 在一些可能的实现方式中，有可能指示标识只是运营商类型标识。

[0129] 在一些可能的实现方式中，有可能指示标识只是接入类型标识。

[0130] 103：AMF(或者SEAF)向AUSF发送终端标识以及指示标识。相应地，AUSF接收 AMF(或者SEAF)发送的终端标识以及指示标识。

[0131] 104：AUSF向ARPF发送终端标识以及指示标识。相应地，ARPF接收AUSF发送的终 端标识以及指示标识。

[0132] 105：ARPF根据保密性密钥CK以及完整性密钥IK以及指示标识生成中间密钥。

[0133] 在本申请实施例中，ARPF根据密钥生成算法生成中间密钥的方式可以包括以下几种：

[0134] 在第一种方式中，当指示标识为NAI时，ARPF根据下述密钥生成算法生成中间密钥：

[0135] $(CK_1', IK_1') = KDF(SQN \oplus AK, NAI, CK||IK)$；

[0136] 其中，(CK_1', IK_1')为所述中间密钥，CK_1'为所述中间保密性密钥，IK_1'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，NAI为所述指示标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

[0137] 在第二种方式中，当指示标识包括接入类型标识以及运营商类型标识时，ARPF根据下述密钥生成算法生成中间密钥：

[0138] $(CK_1', IK_1') = KDF(SQN \oplus AK, ANT, SNT, CK||IK)$；

[0139] 其中，(CK_1', IK_1')为所述中间密钥，CK_1'为所述中间保密性密钥，IK_1'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，SNT为所述运营商类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

[0140] 在一些可能的实施方式中，SQN可以是AuC生成的最新序列号，AuC在生成SQN之后，将SQN发送给所述ARPF。类似地，RAND可以是AuC生成的随机数，AuC在生成RAND之后，将RAND发送给所述ARPF。除了上述的方式之外，SQN以及RAND也可以是网络架构中的其它通讯设备生成并发送给的ARPF，甚至，SQN以及RAND可以是所述ARPF自己生成的，此处不作具体限定。

[0141] 在一些可能的实施方式中，CK可以是AuC根据公式CK＝f3(RAND)生成的，IK可以是AuC根据公式IK＝f4(RAND)生成的，AK可以是AuC根据公式AK＝f5(RAND)生成的。除了上述的方式之外，CK、IK以及AK也可以是网络架构中的其它通讯设备生成并发送给的ARPF，甚至，CK、IK以及AK可以是所述ARPF自己生成的，此处不作具体限定。

[0142] 106:ARPF向AUSF发送中间密钥。相应地，AUSF接收ARPF发送的中间密钥。

[0143] 107:AUSF根据中间密钥生成锚密钥。

[0144] 在本申请实施例中，AUSF根据以下公式生成锚密钥，

[0145] anchor key＝KDF($IK_1'||CK_1'$)

[0146] 其中，anchor key为所述锚密钥，(IK_1', CK_1')为所述中间密钥，IK_1'为中间完整性密钥，CK_1'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来。AUSF还可能根据以下公式生成锚密钥:anchor key＝KDF(IK_1', CK_1')

[0147] 108:AUSF将锚密钥发送给AMF(或者SEAF)。相应地，AMF(或者SEAF)接收AUSF发送的锚密钥。

[0148] 109:AMF(或者SEAF)基于锚密钥生成下层密钥。其中，下层密钥为基于锚密钥进行一次或者多次推衍得到的密钥。

[0149] 在本申请实施例中，锚密钥是根据中间密钥生成的，而中间密钥是根据指示标识生成的，所以，锚密钥与指示标识的关系可以表示为anchor key＝f(ANT,SNT)或者anchor key＝f(NAI)。其中，f表示为指示标识与锚密钥之间的映射函数，NAI为所述网络接入标识，ANT为所述接入类型标识，SNT为所述运营商类型标识。根据锚密钥与指示标识的映射

关系可知，当指 示标识不同时，锚密钥的值也自然不同。也就是说，当接入方式不同时，锚密钥的值也不同，即对不同接入方式的锚密钥进行了隔离。此外，AMF(或者SEAF)基于不同接入方式的锚 密钥分别推延不同接入方式的下层密钥，从而实现了对下层密钥的隔离。即，假设接入方式 为A接入方式，计算得到的锚密钥为a锚密钥，接入方式为B接入方式时，计算得到的锚密 钥为b锚密钥，则可以根据a锚密钥推衍A接入方式的下层密钥，根据b锚密钥推衍B接入 方式的下层密钥。

[0150] 110:AMF(或者SEAF)向AN发送下层密钥。

[0151] 111:UE根据根密钥生成锚密钥，然后再根据锚密钥推衍得到下层密钥。可以理解，UE 推衍下层密钥的过程与上述过程大体类似，此处将不再展开描述。

[0152] 可以理解，在步骤108中，AUSF还可以根据锚密钥生成K_{AMF}密钥或者K_{SEAF}密钥，然后发送给AMF或者SEAF，而不是将锚密钥发送给AMF或者SEAF，因此在步骤109中， AMF或者SEAF基于K_{AMF}密钥或者K_{SEAF}密钥生成下层密钥。

[0153] 需要说明的是，当接入方式不同时，步骤109至步骤111是不相同的，下面分别以接入 方式为3GPP接入方式以及非3GPP接入方式为例进行详细介绍。

[0154] 如图6A所示，假设接入方式为3GPP接入方式，锚密钥为anchor key 1，则步骤109至 步骤111可以用下述的步骤1111～1117步骤代替。

[0155] 1111:AMF(或者SEAF)根据以下公式生成下层密钥K_{amf1}密钥和/或K_{seaf1}密钥：

[0156] K_{amf1}＝KDF(anchor key1,AMF ID)；

[0157] K_{seaf1}＝KDF(anchor key1,SEAF ID)；

[0158] 其中，anchor key1为所述3GPP接入方式下的锚密钥，KDF为密钥生成算法，AMF ID为AMF的标识，SEAF ID为SEAF的标识。AMF的标识可以是AMF的MAC地址或者IP 地址等等，SEAF的标识可以是SEAF的MAC地址或者IP地址等等。

[0159] 1113:AMF(或者SEAF)再根据以下公式生成3GPP接入方式下的基站密钥K_{gNB}、3GPP-NAS保密性密钥$K\text{-}3GPP_{NASenc}$，以及，3GPP-NAS完整性保护密钥$K\text{-}3GPP_{NASint}$：

[0160] K_{gNB}＝KDF(K_{amf1}和/或Kseaf1,NAS Count1)；

[0161] $K\text{-}3GPP_{NASint}$＝KDF(K_{amf1}和/或Kseaf1,NAS-int-alg,alg-ID)；

[0162] $K\text{-}3GPP_{NASenc}$＝KDF(K_{amf1}和/或Kseaf1,NAS-enc-alg,alg-ID)；

[0163] 其中，NAS Count1为经由3GPP的接入点gNB的NAS消息的计数值，可能为上行计数值，也可以为下行计数值，NAS-int-alg为NAS消息对应的完整性算法，比如‘AES’,’SNOW 3G’,’ZUC’等，alg-ID为算法的标识，NAS-enc-alg为NAS消息对应的机密性算法，比如‘AES’,’SNOW 3G’,’ZUC’等。

[0164] 1115:AMF(或者SEAF)将基站密钥K_{gNB}发送给AN。此时，AN相应接收AMF(或 者SEAF)发送的基站密钥K_{gNB}。

[0165] 1117:AN根据基站密钥K_{gNB}生成用户面保密性密钥K_{UPenc}、用户面完整性密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密钥K_{RRCint}。

[0166] 在本申请实施例中，AN根据如下公式分别生成用户面保密性密钥K_{UPenc}、用户面完整性 密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密钥K_{RRCint}：

[0167] K_{UPenc}＝KDF(K_{gNB},UP-enc-alg,alg-ID)；

[0168] K_{UPin}＝KDF(K_{gNB},UP-int-alg,alg-ID)；

[0169] K_{RRCenc}＝KDFK_{gNB},RRC-enc-alg,alg-ID)；

[0170] K_{RRCint}＝KDF(K_{gNB},RRC-int-alg,alg-ID)；

[0171] 其中,KDF为密钥生成算法,K_{gNB}为基站密钥,alg-ID为算法标识,NAS-int-alg、NAS-enc-alg、UP-enc-alg、UP-int-alg、RRC-enc-alg以及RRC-int-alg的定义可以参考表2所 示的4G中的算法标识定义表格,具体如下：

[0172] 表2算法标识定义表格

[0173]

算法标识(Algorithm distinguisher)	值(Value)
NAS-enc-alg	0x01
NAS-int-alg	0x02
RRC-enc-alg	0x03
RRC-int-alg	0x04
UP-enc-alg	0x05
UP-int-alg	0x06

[0174] 1119:UE根据根密钥生成锚密钥,然后再根据锚密钥推衍用户面保密性密钥K_{UPenc}、用 户面完整性密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密钥K_{RRCint}。

[0175] 可以理解,AMF(或者SEAF)在接收到锚密钥之后,也可以不根据锚密钥推衍K_{amf1}密钥和/或K_{seaf1}密钥,再根据K_{amf1}密钥和/或K_{seaf1}密钥推衍基站密钥K_{gNB}、3GPP-NAS保密性 密钥K-3GPPNAS$_{enc}$,以及,3GPP-NAS完整性保护密钥K-3GPPNAS$_{int}$,而是,直接根据锚 密钥推衍基站密钥K_{gNB}、3GPP-NAS保密性密钥K-3GPPNAS$_{enc}$,以及,3GPP-NAS完整性保 护密钥K-3GPPNAS$_{int}$。

[0176] 如图6B所示,假设接入方式为非3GPP接入方式,锚密钥为anchor key 2,则步骤110 至步骤112可以用下述的步骤1112～1116步骤代替。

[0177] 1112:AMF(或者SEAF)根据以下公式生成K_{amf2}密钥和/或K_{seaf2}密钥：

[0178] K_{amf2}＝KDF(anchor key2,AMF ID)；

[0179] K_{seaf2}＝KDF(anchor key2,SEAF ID)；

[0180] 其中,anchor key2为所述非3GPP接入方式下的锚密钥,KDF为密钥生成算法,AMF ID 为AMF的标识,SEAF ID为SEAF的标识。

[0181] 1114:AMF(或者SEAF)再根据以下公式生成非3GPP接入方式下的接入点密钥K_{N3IWF}、非3GPP-NAS保密性密钥K-N3GPP$_{NASenc}$,以及,非3GPP-NAS完整性保护密钥K-N3GPP$_{NASint}$：

[0182] K_{N3IWF}＝KDF(K_{amf2}和/或K_{seaf2},NAS Count2)；

[0183] K-N3GPP$_{NASint}$＝KDF(K_{amf2}和/或K_{seaf2},NAS-int-alg,alg-ID)；

[0184] K-N3GPP$_{NASenc}$＝KDF(K_{amf2}和/或K_{seaf2},NAS-enc-alg,alg-ID)；

[0185] 其中,NAS Count2为经由非3GPP的接入点N3IWF的NAS消息的计数值,可能为上行计数值,也可以为下行计数值,NAS消息对应的完整性算法,比如‘AES’,’SNOW 3G’,’ZUC’等,alg-ID为算法的标识,NAS-enc-alg为NAS消息对应的机密性算法,比如‘AES’,’SNOW 3G’,’ZUC’等。

[0186] 1116:AMF(或者SEAF)将接入点密钥K_{N3IWF}发送给AN。此时,AN相应接收AMF (或者SEAF)发送的接入点密钥K_{N3IWF}。

[0187] 1118:UE根据根密钥生成锚密钥,然后再根据锚密钥推衍接入点密钥K_{N3IWF}。

[0188] 同样的,可以理解,在步骤1114中,AMF(或者SEAF)不是接收AUSF发送的锚密钥,而是AUSF根据锚密钥生成的K_{AMF}密钥或者K_{SEAF}密钥。

[0189] 可以理解,图5所示实施例中的密钥生成算法不限于KDF算法,在实际应用中,密钥生 成算法还可以是其它的算法,比如Trunc算法:取低位的截图算法;其他的HASH算法等,本申请不作具体限定。而且,密钥生成算法的自变量也可以包括其他的参数,例如,包括NSSAI (Network Slice Selection Association Information)、随机数(Random number)、随机数值 (Number used once,Nonce)、序列码(Sequence Number)、注册类型(registration type)、接 入层消息数量(NAS Count)、安全算法标识、安全标识、SQN⊕AK的长度以及生成密钥所 用的参数对应的长度等等,在实际应用中,可以根据需要从中选择中的一个或者多个参数作 为所述密钥生成算法的自变量。

[0190] 可以理解,AMF(或者SEAF)在接收到锚密钥之后,也可以不根据锚密钥推衍K_{amf1}密钥和/或K_{seaf1}密钥,再根据K_{amf1}密钥和/或K_{seaf1}密钥推衍接入点密钥K_{N3IWF}、非3GPP-NAS 保密性密钥$K\text{-}N3GPP_{NASenc}$,以及,非3GPP-NAS完整性保护密钥$K\text{-}N3GPP_{NASint}$,而是,直 接根据锚密钥推衍接入点密钥K_{N3IWF}、非3GPP-NAS保密性密钥$K\text{-}N3GPP_{NASenc}$,以及,非 3GPP-NAS完整性保护密钥$K\text{-}N3GPP_{NASint}$。

[0191] 执行图5所示的锚密钥生成方法之后,将生成如图7所示的密钥架构。其中,图7中隔 离线左边的为具体执行图6A所示的流程所生成的密钥架构,图7图中隔离线右边的为具体 执行图6B所示的流程所生成的密钥架构,两者之间能够很好地进行隔离。

[0192] 如图8所示,本申请实施例提供了第二种锚密钥生成方法。在本实施例中,AUSF即为 权利要求中的第一通讯设备为,AMF或者SEAF即为权利要求中的第二通讯设备,ARPF即为权利要求中的第三通讯设备。该方法可以基于图3以及图4所示的网络架构来实现,该方法包括但不限于如下步骤。

[0193] 201:UE向AN发送终端标识。相应地,AN接收UE发送的终端标识。

[0194] 202:AN向AMF(或者SEAF)发送终端标识以及指示标识。相应地,AMF(或者SEAF) 接收AN发送的终端标识以及指示标识。其中,指示标识包括ANT以及SNT。

[0195] 203:AMF(或者SEAF)向AUSF发送终端标识以及指示标识。相应地,AUSF接收 AMF(或者SEAF)发送的终端标识以及指示标识。

[0196] 204:AUSF向ARPF发送终端标识以及指示标识。相应地,ARPF接收AUSF发送的终 端标识以及指示标识。

[0197] 205:ARPF根据保密性密钥CK以及完整性密钥IK以及ANT生成中间密钥。

[0198] 在本申请实施例中,ARPF根据密钥生成算法生成中间密钥的方式可以包括以下几种:

[0199] 在第一种方式中,ARPF根据下述密钥生成算法生成中间密钥:

[0200] $(CK_1', IK_1') = KDF(SQN \oplus AK, ANT, CK||IK)$;

[0201] 其中,(CK_1', IK_1')为所述中间密钥,CK_1'为所述中间保密性密钥,IK_1'为所述中间完 整性密钥,KDF为密钥生成算法,SQN为最新序列号,ANT为所述接入类型标识,CK为初 始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK=f3(RAND),IK=f4(RAND), AK=f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0202] 在第二种方式中，ARPF根据下述密钥生成算法生成中间密钥：

[0203] $(CK_1', IK_1') = KDF(SQN \oplus AK, SNT, CK||IK)$；

[0204] 其中，(CK_1', IK_1')为所述中间密钥，CK_1'为所述中间保密性密钥，IK_1'为所述中间完整性密钥，KDF为密钥生成算法，SQN为最新序列号，SNT为所述运营商类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

[0205] 206：ARPF向AUSF发送中间密钥。相应地，AUSF接收ARPF发送的中间密钥。

[0206] 207：AUSF根据中间密钥生成锚密钥。

[0207] 针对步骤205中的第一种生成中间密钥的方式，AUSF根据中间密钥生成锚密钥的方式为：

[0208] 首先，AUSF根据中间密钥生成生成EMSK'，

[0209] $EMSK' = PRF'(IK_2'||CK_2')$；

[0210] 其中，EMSK'为扩展主会话密钥，(IK_2', CK_2')为所述中间钥匙，IK_2'为中间完整性密钥，CK_2'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来；

[0211] 然后，AUSF根据以下公式生成锚密钥，

[0212] anchor key＝KDF(EMSK'，SNT)；

[0213] 其中，anchor key为所述锚密钥，SNT为所述运营商类型标识。

[0214] 针对步骤205中的第二种生成中间密钥的方式，AUSF根据中间密钥生成锚密钥的方式为：

[0215] 首先，AUSF根据中间密钥生成生成EMSK'，

[0216] $EMSK' = PRF'(IK_2'||CK_2')$；

[0217] 其中，EMSK'为扩展主会话密钥，(IK_2', CK_2')为所述中间钥匙，IK_2'为中间完整性密钥，CK_2'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来；

[0218] 然后，AUSF根据以下公式生成锚密钥，

[0219] anchor key＝KDF(EMSK'，ANT)；

[0220] 其中，anchor key为所述锚密钥，ANT为所述接入类型标识。

[0221] 也可以EMSK'和其他的参数生成anchor key，不限定于指示标识。

[0222] 可以理解，该anchor key也可以由MSK'生成，此处仅以EMSK'生成anchor key为例。

[0223] 208：AUSF将锚密钥发送给AMF(或者SEAF)。相应地，AMF(或者SEAF)接收AUSF发送的锚密钥。

[0224] 209：AMF(或者SEAF)基于锚密钥生成下层密钥。其中，下层密钥为基于锚密钥进行一次或者多次推衍得到的密钥。

[0225] 210：AMF(或者SEAF)向AN发送下层密钥。

[0226] 211：UE根据根密钥生成锚密钥，然后再根据锚密钥推衍得到下层密钥。

[0227] 如图9所示，本申请实施例提供了第三种锚密钥生成方法。在本实施例中，AUSF即为权利要求中的第一通讯设备为，AMF或者SEAF即为权利要求中的第二通讯设备，ARPF即为权利要求中的第三通讯设备。该方法可以基于图3以及图4所示的网络架构来实现，该方法包括但不限于如下步骤。

[0228] 221:UE向AN发送终端标识。相应地,AN接收UE发送的终端标识。

[0229] 222:AN向AMF(或者SEAF)发送终端标识以及指示标识。相应地,AMF(或者SEAF) 接收AN发送的终端标识以及指示标识。其中,指示标识包括ANT以及SNT。

[0230] 223:AMF(或者SEAF)向AUSF发送终端标识以及指示标识。相应地,AUSF接收 AMF(或者SEAF)发送的终端标识以及指示标识。

[0231] 224:AUSF向ARPF发送终端标识以及指示标识。相应地,ARPF接收AUSF发送的终 端标识以及指示标识。

[0232] 225:ARPF根据保密性密钥CK以及完整性密钥IK以及ANT生成中间密钥。

[0233] 在本申请实施例中,ARPF根据密钥生成算法生成中间密钥的方式可以包括以下几种:

[0234] 在第一种方式中,ARPF根据下述密钥生成算法生成中间密钥:

[0235] $(CK_1', IK_1') = KDF(SQN \oplus AK, ANT, CK||IK)$;

[0236] 其中,(CK_1', IK_1')为所述中间密钥,CK_1'为所述中间保密性密钥,IK_1'为所述中间完 整性密钥,KDF为密钥生成算法,SQN为最新序列号,ANT为所述接入类型标识,CK为初 始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK=f3(RAND),IK=f4(RAND), AK=f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0237] 在第二种方式中,ARPF根据下述密钥生成算法生成中间密钥:

[0238] $(CK_1', IK_1') = KDF(SQN \oplus AK, SNT, CK||IK)$;

[0239] 其中,(CK_1', IK_1')为所述中间密钥,CK_1'为所述中间保密性密钥,IK_1'为所述中间完 整性密钥,KDF为密钥生成算法,SQN为最新序列号,SNT为所述运营商类型标识,CK 为初始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK=f3(RAND),IK=f4(RAND), AK=f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0240] 226:ARPF向AUSF发送中间密钥。相应地,AUSF接收ARPF发送的中间密钥。

[0241] 227:AUSF根据中间密钥生成锚密钥。

[0242] 针对步骤225中的第一种生成中间密钥的方式,AUSF根据中间密钥生成锚密钥的方式 为:

[0243] 首先,AUSF根据中间密钥生成生成EMSK',

[0244] $EMSK' = PRF'(IK_2'||CK_2')$;

[0245] 其中,EMSK'为扩展主会话密钥,(IK_2', CK_2')为所述中间钥匙,IK_2'为中间完整性密 钥,CK_2'为中间保密性密钥,||的含义为级联,表示将符号两边的字符串连起来;

[0246] 然后,AUSF根据以下公式生成锚密钥,

[0247] anchor key=KDF(EMSK',SNT);

[0248] 其中,anchor key为所述锚密钥,SNT为所述运营商类型标识。

[0249] 针对步骤225中的第二种生成中间密钥的方式,AUSF根据中间密钥生成锚密钥的方式 为:

[0250] 首先,AUSF根据中间密钥生成生成EMSK',

[0251] $EMSK' = PRF'(IK_2'||CK_2')$;

[0252] 其中,EMSK'为扩展主会话密钥,(IK_2', CK_2')为所述中间钥匙,IK_2'为中间完整性密 钥,CK_2'为中间保密性密钥,||的含义为级联,表示将符号两边的字符串连起来;

[0253] 然后，AUSF根据以下公式生成锚密钥，

[0254] anchor key＝KDF(EMSK'，ANT)；

[0255] 其中，anchor key为所述锚密钥，ANT为所述接入类型标识。

[0256] 可以理解，也可以EMSK'和其他的参数生成anchor key，不限定于指示标识。

[0257] 可以理解，该anchor key也可以由MSK'生成，此处仅以EMSK'生成anchor key为例。

[0258] 228：AUSF根据锚密钥生成K_{AMF}密钥和/或K_{SEAF}密钥。

[0259] 在本申请实施例中，AUSF根据下述密钥生成算法生成K_{AMF}密钥或者K_{SEAF}密钥，

[0260] K_{AMF}＝KDF(anchor key，AMF ID)；

[0261] K_{SEAF}＝KDF(anchor key，SEAF ID)；

[0262] 其中，anchor key为所述锚密钥，KDF为密钥生成算法，AMF ID为AMF的标识，SEAF ID为SEAF的标识。

[0263] 229：AUSF将K_{AMF}密钥和/或K_{SEAF}密钥发送给AMF(或者SEAF)。相应地，AMF(或者SEAF)接收AUSF发送的K_{AMF}密钥和/或K_{SEAF}密钥。

[0264] 230：AMF(或者SEAF)基于K_{AMF}密钥或者K_{SEAF}密钥生成下层密钥。其中，下层密钥为基于K_{AMF}密钥或者K_{SEAF}密钥进行一次或者多次推衍得到的密钥。

[0265] 231：AMF(或者SEAF)向AN发送下层密钥。

[0266] 232：UE根据根密钥生成锚密钥，然后再根据锚密钥推衍得到下层密钥。

[0267] 可以理解，AUSF在生成锚密钥之后，也可以直接将锚密钥发送给AMF，然后，AMF再根据锚密钥生成下层密钥，并发送给AN。

[0268] 执行图9所示的锚密钥生成方法之后，将生成如图10所示的密钥架构。其中，图9中隔离线左边的为UE和3GPP网络所对应的密钥架构，图9图中隔离线右边的为UE和非3GPP网络所对应的密钥架构，两者之间能够很好地进行隔离。

[0269] 可以理解，对步骤227，AUSF还可以根据中间密钥生成了2个密钥，分别是MSK'和EMSK'。其中MSK'和EMSK'分别取PRF'($IK_2'||CK_2'$)的生成的密钥的不同部分，如MSK'取前512bits，EMSK'取后512bits。

[0270] 然后，基于MSK'生成anchor key，即anchor key＝KDF(MSK'，ANT)，此处同上面的描述。

[0271] 而EMSK'则被AUSF保留或推衍后被保留，用于后续扩展。

[0272] 如图11所示，本申请实施例提供了第四种锚密钥生成方法。在本实施例中，AUSF即为权利要求中的第一通讯设备为，SEAF即为权利要求2中的第二通讯设备，ARPF即为权利要求中的第三通讯设备。该方法可以基于图3以及图4所示的网络架构来实现，并且，在本实施例中，AMF的数量为m个，分别命名为AMF_1～AMF_m。该方法包括但不限于如下步骤。

[0273] 301：UE向AN发送终端标识。相应地，AN接收UE发送的终端标识。

[0274] 302：AN向AMF_1至AMF_m发送终端标识以及指示标识。相应地，AMF_1至AMF_m接收AN发送的终端标识以及指示标识。

[0275] 303：AMF_1至AMF_m向SEAF发送终端标识以及指示标识。相应地，SEAF接收AMF_m发送的终端标识以及指示标识。

[0276] 304：SEAF向AUSF发送终端标识以及指示标识。相应地，AUSF接收SEAF发送的终端

标识以及指示标识。

[0277] 305:AUSF向ARPF发送终端标识以及指示标识。相应地,ARPF接收AUSF发送的终 端标识以及指示标识。

[0278] 306:ARPF根据保密性密钥CK以及完整性密钥IK以及ANT生成中间密钥。

[0279] 307:ARPF向AUSF发送中间密钥。相应地,AUSF接收ARPF发送的中间密钥。

[0280] 308:AUSF根据中间密钥生成锚密钥。

[0281] 309:AUSF将锚密钥发送给SEAF。相应地,SEAF接收AUSF发送的锚密钥。

[0282] 310:SEAF根据锚密钥以及AMF_1至AMF_2的标识分别生成K_{AMF_1}至K_{AMF_m}。

[0283] 在本申请实施例中,SEAF根据以下公式分别生成K_{AMF_1}至K_{AMF_m},

[0284] K_{AMF_1}=KDF(anchor key,AMF_1 ID);

[0285] K_{AMF_2}=KDF(anchor key,AMF_2 ID);

[0286] ……

[0287] K_{AMF_m}=KDF(anchor key,AMF_m ID);

[0288] 其中,anchor key为所述锚密钥,AMF_1 ID至AMF_m ID分别为AMF_1至AMF_m的 标识。

[0289] 311:SEAF分别向AMF_1至AMF_m下发K_{AMF_1}至K_{AMF_m}。相应地,AMF_1至AMF_2 分别接收SEAF发送的K_{AMF_1}至K_{AMF_m}。

[0290] 312:AMF_1至AMF_m分别基于K_{AMF_1}至K_{AMF_m}生成下层密钥。

[0291] 在本申请实施例中,AMF_1基于K_{AMF_1}生成下层密钥1;AMF_2基于K_{AMF_2}生成下层 密钥2;……;AMF_m基于K_{AMF_m}生成下层密钥m。

[0292] 下面将以AMF_1基于K_{AMF_1}生成下层密钥1为例进行说明。

[0293] AMF_1根据以下公式生成3GPP接入方式下的基站密钥K_{gNB1}、3GPP-NAS保密性密钥$K\text{-}3GPP_{NASenc1}$,以及,3GPP-NAS完整性保护密钥$K\text{-}3GPP_{NASint1}$:

[0294] K_{gNB1}=KDF(K_{AMF_1},NAS Count1);

[0295] $K\text{-}3GPP_{NASint}$=KDF(K_{AMF_1},NAS-int-alg,alg-ID);

[0296] $K\text{-}3GPP_{NASenc}$=KDF(K_{AMF_1},NAS-enc-alg,alg-ID);

[0297] 其中,NAS Count1为经由3GPP的接入点gNB的NAS消息的计数值,可能为上行计数值,也可以为下行计数值,NAS-int-alg为NAS消息对应的完整性算法,比如‘AES’,’SNOW 3G’,’ZUC’等,alg-ID为算法的标识,NAS-enc-alg为NAS消息对应的机密性算法,比如‘AES’,’SNOW 3G’,’ZUC’等。

[0298] 313:AMF向AN发送下层密钥。

[0299] 314:UE根据根密钥生成锚密钥,然后再根据锚密钥推衍得到下层密钥。

[0300] 执行图11所示的锚密钥生成方法之后,将生成如图12所示的密钥架构。其中,图12中 隔离线左边的为UE和3GPP网络对应的密钥架构,图12图中隔离线右边的为UE和非3GPP网络对应的密钥架构,两者之间能够很好地进行隔离。

[0301] 可以理解,图8、图9以及图11所示的实施例是基于图5所示的实施例演变过来的,为 了简便起见,图8、图9以及图11所示的实施例中只描述了与图5所示的实施例不相同的部 分,而图8、图9以及图11所示的实施例中与图5所示的实施例相同的部分,可以参见图5以及相关内容,此处不再重复赘述。

[0302] 如图13所示，本申请实施例提供了第五种锚密钥生成方法。该方法可以基于图3以及图 4所示的网络架构来实现，该方法包括但不限于如下步骤。

[0303] 401：UE向AN发送终端标识。相应地，AN接收UE发送的终端标识。

[0304] 在本申请实施例中，终端标识可以是固定不变的标识，例如，媒体访问控制(Media Access Control，MAC)地址、网络协议(Internet Protocol，IP)地址、手机号码、国际移动设备标 识(International Mobile Equipment Identity，IMEI)、国际移动用户识别码(International Mobile Subscriber Identity，IMSI)、IP多媒体私有标识(IP Multimedia Private Identity，IMPI)、IP多 媒体公共标识(IP Multimedia Public Identity，IMPU)等等，也可以是临时分配的标识，例如， 临时移动用户标识符(TemporaryMobileSubscriberIdentity，TMSI)、全球唯一临时UE标识 (Globally Unique Temporary UE Identity，GUTI)等等。

[0305] 可以理解，除了终端标识之外，UE还可以将接入网参数、注册类型、安全参数、UE的5G网络能力，PDU session的状态等至少一种发送给AN。其中，接入网参数为可能为接入网的频点，临时用户标识，NSSAI等与服务网络相关的参数。注册类型为可以表明用户是初次注册、由于移动引起的注册、周期性注册更新等区分用户注册的行为。安全参数为认证和完整性保护相关的参数。。NSSAI为网络切片选择辅助信息。UE的5G网络能力可能包括支持 接入该网络的配置能力。PDU session为UE和数据网络之间的PDU的业务连接，类型可能 为IP、以太网的业务连接。

[0306] 402：AN向AMF(或者SEAF)发送终端标识以及指示标识。相应地，AMF(或者SEAF) 接收AN发送的终端标识以及指示标识。

[0307] 在本申请实施例中，指示标识用于指示终端的接入方式。在5G标准中，可以按照不同 的划分依据对终端的接入方式进行划分。例如，接入方式的划分依据可以包括接入类型以及 运营商类型。其中，接入类型具体可以分为3GPP接入类型、可信的非3GPP接入类型以及 非可信的非3GPP接入类型。运营商类型具体可以分为A运营商类型或者B运营商类型。可以理解，运营商类型还可以有更多的类型，此处仅作为示例，不作具体限定。

[0308] 以划分依据包括接入类型以及运营商类型为例，所述接入方式的划分可以如表1所示。需要说明的，不限于上述两种划分依据，接入方式的划分依据还可以是其他种类的划分依据， 例如，介质类型(有线接入或者无线接入)等等，此处不作具体限定。并且，不限于接入类 型以及运营商类型两种划分依据，接入方式的划分依据还可以是一种、三种、四种或者更多， 即，可以从更多维度或者更少维度对接入方式进行划分。

[0309] 所述指示标识可以是携带在上述接入网参数中。所述指示标识可以是下述的任意一种方 式：所述指示标识可以是网络接入标识(Network Access Identifier，NAI)，用于同时指示接 入类型以及运营商类型。或者，所述指示标识可以包括接入类型标识以及运营商类型标识， 其中，所述接入类型标识用于指示所述接入类型，所述运营商类型标识用于指示所述运营商 类型。可以理解，上述例子仅作为举例，不构成具体限定。

[0310] 在一些可能的实现方式中，网络接入标识可以为SN Identity|Access Network Identity，即 可以特定表示某运营商下的某种接入，如中国联通的WLAN接入等等，此处的SN Identity 为4G网络中的定义，Access Network Identity为4G时非3GPP网络中的定义。也可能将SN Identity或者Access Network Identity的方式进行升级，使其能够表示某运

营商的某种接入类 型。

[0311] 在一些可能的实现方式中，接入类型标识具体指示所述接入类型为3GPP接入类型、可 信的非3GPP接入类型以及非可信的非3GPP接入类型。例如，接入类型标识Access Network Type(ANT)可以直接为“3GPP network”，“Trusted Non-3GPP network”，“Untrusted Non-3GPP network”字符串，或者仅为“3GPP network”和“Non-3GPP network”字符串等等。

[0312] 在一些可能的实现方式中，所述运营商类型标识可以包括两部分，一部分用于指示运营 商，另一部分用于指示具体接入类型。例如，运营商类型标识可以指示为中国移动的LTE接 入或者中国联通的WLAN接入。在具体应用中，可以将SN Identity和Access Network Identity 的结合以作为运营商类型标识；也有可能只包括运营商的区分，比如中国移动、中国联通、中国电信等等。

[0313] 在一些可能的实现方式中，有可能指示标识只是运营商类型标识。

[0314] 在一些可能的实现方式中，有可能指示标识只是接入类型标识。

[0315] 403：AMF(或者SEAF)向AUSF发送终端标识以及指示标识。相应地，AUSF接收 AMF(或者SEAF)发送的终端标识以及指示标识。

[0316] 404：AUSF向ARPF发送终端标识以及指示标识。相应地，ARPF接收AUSF发送的终 端标识以及指示标识。

[0317] 405：ARPF根据保密性密钥CK、完整性密钥IK以及指示标识生成锚密钥。

[0318] 在本申请实施例中，ARPF根据生成锚密钥的方式可以包括以下几种：

[0319] 在第一种方式中，ARPF根据下述公式生成锚密钥：

[0320] $anchor\ key = KDF(SQN \oplus AK, NAI, CK||IK)$；

[0321] 其中，anchor key为所述锚密钥，KDF为密钥生成算法，SQN为最新序列号，NAI为所述指示标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机数，f3，f4以及f5均为生成算法，⊕的含 义为异或运算。

[0322] 在第二种方式中，ARPF根据下述公式生成锚密钥：

[0323] $anchor\ key = KDF(SQN \oplus AK, ANT, SNT, CK||IK)$；

[0324] 其中，anchor key为所述锚密钥，KDF为密钥生成算法，SQN为最新序列号，ANT为所述接入类型标识，SNT为所述运营商类型标识，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，CK＝f3(RAND)，IK＝f4(RAND)，AK＝f5(RAND)，RAND为随机 数，f3，f4以及f5均为生成算法，⊕的含义为异或运算。

[0325] 在一些可能的实施方式中，SQN可以是AuC生成的最新序列号，AuC在生成SQN之后，将SQN发送给所述ARPF。类似地，RAND可以是AuC生成的随机数，AuC在生成RAND 之后，将RAND发送给所述ARPF。除了上述的方式之外，SQN以及RAND也可以是网络 架构中的其它通讯设备生成并发送给的ARPF，甚至，SQN以及RAND可以是所述ARPF自 己生成的，此处不作具体限定。

[0326] 在一些可能的实施方式中，CK可以是AuC根据公式CK＝f3(RAND)生成的，IK可以是AuC根据公式IK＝f4(RAND)生成的，AK可以是AuC根据公式AK＝f5(RAND)生成 的。除了上述的方式之外，CK、IK以及AK也可以是网络架构中的其它通讯设备生成并发送 给的ARPF，

甚至，CK、IK以及AK可以是所述ARPF自己生成的，此处不作具体限定。

[0327] 406：ARPF向AUSF发送锚密钥。相应地，AUSF接收ARPF发送的锚密钥。

[0328] 407：AUSF根据锚密钥生成K_{amf}/K_{seaf}。

[0329] 在本申请实施例中，AUSF根据以下公式生成K_{amf}/K_{seaf}：

[0330] K_{amf}＝KDF(anchor key，AMF ID)；

[0331] K_{seaf}＝KDF(anchor key，SEAF ID)；

[0332] 其中，anchor key为所述锚密钥，KDF为密钥生成算法，AMF ID为AMF的标识，SEAF ID为SEAF的标识。AMF的标识可以是AMF的MAC地址或者IP地址等等，SEAF的标识 可以是SEAF的MAC地址或者IP地址等等。

[0333] 408：AUSF将K_{amf}/K_{seaf}发送给AMF(或者SEAF)。相应地，AMF(或者SEAF)接收 AUSF发送的K_{amf}/K_{seaf}。

[0334] 409：AMF(或者SEAF)基于K_{amf}/K_{seaf}生成下层密钥。其中，下层密钥为基于锚密钥进行一次或者多次推衍得到的密钥。

[0335] 410：AMF(或者SEAF)向AN发送下层密钥。

[0336] 411：UE根据CK、IK以及指示标识自行推衍生成下层密钥。可以理解，UE推衍下层密钥的过程与上述过程大体类似，此处将不再展开描述。

[0337] 可以理解，AUSF在生成锚密钥之后，也可以直接将锚密钥发送给AMF，然后，AMF 再将根据锚密钥生成下层密钥，并发送给AN。

[0338] 需要说明的是，当接入方式不同时，步骤409至步骤411是不相同的，下面分别以接入 方式为3GPP接入方式以及非3GPP接入方式为例进行详细介绍。

[0339] 如图14A所示，假设接入方式为3GPP接入方式，锚密钥为anchor key 1，则步骤409至 步骤411可以用下述的步骤4111～4117步骤代替。

[0340] 4111：AMF(或者SEAF)根据K_{amf1}/K_{seaf1}生成基站密钥K_{gNB}，3GPP-NAS保密性密钥 K-$3GPP_{NASenc}$，3GPP-NAS完整性保护密钥K-$3GPP_{NASint}$。

[0341] 具体地，AMF(或者SEAF)根据以下公式生成3GPP接入方式下的基站密钥K_{gNB}、3GPP-NAS保密性密钥K-$3GPP_{NASenc}$，以及，3GPP-NAS完整性保护密钥K-$3GPP_{NASint}$：

[0342] K_{gNB}＝KDF(K_{amf1}和/或K_{seaf1}，NAS Count1)；

[0343] K-$3GPP_{NASint}$＝KDF(K_{amf1}和/或K_{seaf1}，NAS-int-alg，alg-ID)；

[0344] K-$3GPP_{NASenc}$＝KDF(K_{amf1}和/或K_{seaf1}，NAS-enc-alg，alg-ID)；

[0345] 其中，NAS Count1为经由3GPP的接入点gNB的NAS消息的计数值，可能为上行计数值，也可以为下行计数值，NAS-int-alg为NAS消息对应的完整性算法，比如‘AES’，’SNOW 3G’，’ZUC’等，alg-ID为算法的标识，NAS-enc-alg为NAS消息对应的机密性算法，比如‘AES’，’SNOW 3G’，’ZUC’等。

[0346] 4113：AMF(或者SEAF)将基站密钥K_{gNB}发送给AN。此时，AN相应接收AMF(或 者SEAF)发送的基站密钥K_{gNB}。

[0347] 4115：AN根据基站密钥K_{gNB}生成用户面保密性密钥K_{UPenc}、用户面完整性密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密钥K_{RRCint}。

[0348] 在本申请实施例中，AN根据如下公式分别生成用户面保密性密钥K_{UPenc}、用户面完整性 密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密钥K_{RRCint}：

[0349] K_{UPenc}＝KDF(K_{gNB},UP-enc-alg,alg-ID)；

[0350] K_{UPin}＝KDF(K_{gNB},UP-int-alg,alg-ID)；

[0351] K_{RRCenc}＝KDFK_{gNB},RRC-enc-alg,alg-ID)；

[0352] K_{RRCint}＝KDF(K_{gNB},RRC-int-alg,alg-ID)；

[0353] 其中,KDF为密钥生成算法,K_{gNB}为基站密钥,alg-ID为算法标识,UP-enc-alg、UP-int-alg、RRC-enc-alg以及RRC-int-alg的定义可以参考表2所示的4G中的算法标识定 义表格。

[0354] 4117:UE根据CK、IK以及指示标识自行推衍锚密钥,然后,根据锚密钥自行推衍用户 面保密性密钥K_{UPenc}、用户面完整性密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密 钥K_{RRCint}。

[0355] 如图14B所示,假设接入方式为非3GPP接入方式,锚密钥为anchor key 2,则步骤409 至步骤411可以用下述的步骤4112～4116步骤代替。

[0356] 4112:AMF(或者SEAF)根据锚密钥anchor key 2生成接入点密钥K_{N3IWF}、非3GPP-NAS保密性密钥K-N3GPP$_{NASenc}$,以及,非3GPP-NAS完整性保护密钥K-N3GPP$_{NASint}$。

[0357] 具体地,AMF(或者SEAF)再根据以下公式生成非3GPP接入方式下的接入点密钥K_{N3IWF}、 非3GPP-NAS保密性密钥K-N3GPP$_{NASenc}$,以及,非3GPP-NAS完整性保护密钥K-N3GPP$_{NASint}$:

[0358] K_{N3IWF}＝KDF(K_{amf2}和/或K_{seaf2},NAS Count2)；

[0359] K-N3GPP$_{NASint}$＝KDF(K_{amf2}和/或K_{seaf2},NAS-int-alg,alg-ID)；

[0360] K-N3GPP$_{NASenc}$＝KDF(K_{amf2}和/或K_{seaf2},NAS-enc-alg,alg-ID)；

[0361] 其中,NAS Count2为经由非3GPP的接入点N3IWF的NAS消息的计数值,可能为上行计数值,也可以为下行计数值,NAS-int-alg为NAS消息对应的完整性算法,比如‘AES’,’SNOW 3G’,’ZUC’等,alg-ID为算法的标识,NAS-enc-alg为NAS消息对应的机密性算法,比如‘AES’,’SNOW 3G’,’ZUC’等。

[0362] 4114:AMF(或者SEAF)将接入点密钥K_{N3IWF}发送给AN。此时,AN相应接收AMF (或者SEAF)发送的接入点密钥K_{N3IWF}。

[0363] 4116、UE根据CK、IK以及指示标识自行推衍锚密钥,然后,根据锚密钥自行推衍接入 点密钥K_{N3IWF}。

[0364] 可以理解,图13所示实施例中的密钥生成算法不限于KDF算法,在实际应用中,密钥 生成算法还可以是其它的算法,比如Trunc算法:取低位的截图算法;其他的HASH算法等, 本申请不作具体限定。而且,密钥生成算法的自变量也可以包括其他的参数,例如,包括NSSAI、 随机数、随机数值、序列码、注册类型、接入层消息数量、安全算法标识、安全标识以及SQN ⊕AK的长度以及生成密钥所用的参数对应的长度等等,在实际应用中,可以根据需要从中 选择中的一个或者多个参数作为所述密钥生成算法的自变量。

[0365] 执行图13所示的锚密钥生成方法之后,将生成如图15所示的密钥架构。其中,图15中 隔离线左边的为具体执行图14A所示的流程所生成的密钥架构,图15图中隔离线右边的为 具体执行图14B所示的流程所生成的密钥架构,两者之间能够很好地进行隔离。

[0366] 如图16所示,本申请实施例提供了第六种锚密钥生成方法。该方法可以基于图3以及图 4所示的网络架构来实现,该方法包括但不限于如下步骤。

[0367] 501:UE向AN发送终端标识。相应地,AN接收UE发送的终端标识。

[0368] 在本申请实施例中,终端标识可以是固定不变的标识,例如,媒体访问控制(Media Access Control,MAC)地址、网络协议(Internet Protocol,IP)地址、手机号码、国际移动设备标 识(International Mobile Equipment Identity,IMEI)、国际移动用户识别码(International Mobile Subscriber Identity,IMSI)、IP多媒体私有标识(IP Multimedia Private Identity,IMPI)、IP多 媒体公共标识(IP Multimedia Public Identity,IMPU)等等,也可以是临时分配的标识,例如, 临时移动用户标识符(TemporaryMobileSubscriberIdentity,TMSI)、全球唯一临时UE标识 (Globally Unique Temporary UE Identity,GUTI)等等。

[0369] 可以理解,除了终端标识之外,UE还可以将接入网参数、注册类型、安全参数、UE的5G网络能力,PDU session的状态等至少一种发送给AN。其中,接入网参数为可能为接入网的频点,临时用户标识,NSSAI等与服务网络相关的参数。注册类型为可以表明用户是初次注册、由于移动引起的注册、周期性注册更新等区分用户注册的行为。安全参数为认证和完整性保护相关的参数。NSSAI为网络切片选择辅助信息。UE的5G网络能力可能包括支持接入该网络的配置能力。PDU session为UE和数据网络之间的PDU的业务连接,类型可能为IP、以太网的业务连接。

[0370] 502:AN向AMF(或者SEAF)发送终端标识以及指示标识。相应地,AMF(或者SEAF) 接收AN发送的终端标识以及指示标识。

[0371] 在本申请实施例中,指示标识用于指示终端的接入方式。在5G标准中,可以按照不同 的划分依据对终端的接入方式进行划分。例如,接入方式的划分依据可以包括接入类型以及 运营商类型。其中,接入类型具体可以分为3GPP接入类型、可信的非3GPP接入类型以及 非可信的非3GPP接入类型。运营商类型具体可以分为A运营商类型或者B运营商类型。可以理解,运营商类型还可以有更多的类型,此处仅作为示例,不作具体限定。

[0372] 以划分依据包括接入类型以及运营商类型为例,所述接入方式的划分可以如表1所示。需要说明的,不限于上述两种划分依据,接入方式的划分依据还可以是其他种类的划分依据, 例如,介质类型(有线接入或者无线接入)等等,此处不作具体限定。并且,不限于接入类 型以及运营商类型两种划分依据,接入方式的划分依据还可以是一种、三种、四种或者更多, 即,可以从更多维度或者更少维度对接入方式进行划分。

[0373] 所述指示标识可以是携带在上述接入网参数中。所述指示标识可以包括接入类型标识以 及运营商类型标识,其中,所述接入类型标识用于指示所述接入类型,所述运营商类型标识 用于指示所述运营商类型。可以理解,上述例子仅作为举例,不构成具体限定。

[0374] 在一些可能的实现方式中,接入类型标识具体指示所述接入类型为3GPP接入类型、可 信的非3GPP接入类型以及非可信的非3GPP接入类型。例如,接入类型标识Access Network Type(ANT)可以直接为“3GPP network”,“Trusted Non-3GPP network”,“Untrusted Non-3GPP network”字符串,或者仅为“3GPP network”和“Non-3GPP network”字符串等等。

[0375] 在一些可能的实现方式中,所述运营商类型标识可以包括两部分,一部分用于指示运营 商,另一部分用于指示具体接入类型。例如,运营商类型标识可以指示为中国移动的LTE接 入或者中国联通的WLAN接入。在具体应用中,可以将SN Identity和Access

Network Identity 的结合以作为运营商类型标识;也有可能只包括运营商的区分,比如中国移动、中国联通、中国电信等等。

[0376] 在一些可能的实现方式中,有可能指示标识只是运营商类型标识。

[0377] 在一些可能的实现方式中,有可能指示标识只是接入类型标识。

[0378] 503:AMF(或者SEAF)向AUSF发送终端标识以及指示标识。相应地,AUSF接收 AMF(或者SEAF)发送的终端标识以及指示标识。

[0379] 504:AUSF向ARPF发送终端标识以及指示标识。相应地,ARPF接收AUSF发送的终 端标识以及指示标识。

[0380] 505:ARPF根据保密性密钥CK以及完整性密钥IK以及指示标识生成共享密钥。

[0381] 在本申请实施例中,ARPF生成共享密钥的方式可以包括以下几种:

[0382] 在第一种方式中,ARPF根据以下公式生成共享密钥shared key:

[0383] shared key=KDF(SQN⊕AK, ANT, CK||IK);

[0384] 其中,KDF为密钥生成算法,SQN为最新序列号,ANT为所述接入类型标识,CK为初始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK=f3(RAND),IK=f4(RAND), AK=f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0385] 在第二种方式中,ARPF根据以下公式生成共享密钥shared key:

[0386] shared key=KDF(SQN⊕AK, SNT, CK||IK);

[0387] 其中,KDF为密钥生成算法,SQN为最新序列号,SNT为所述运营商类型标识,CK为初始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK=f3(RAND),IK=f4(RAND), AK=f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0388] 在一些可能的实施方式中,SQN可以是AuC生成的最新序列号,AuC在生成SQN之后,将SQN发送给所述ARPF。类似地,RAND可以是AuC生成的随机数,AuC在生成RAND 之后,将RAND发送给所述ARPF。除了上述的方式之外,SQN以及RAND也可以是网络 架构中的其它通讯设备生成并发送给的ARPF,甚至,SQN以及RAND可以是所述ARPF自 己生成的,此处不作具体限定。

[0389] 在一些可能的实施方式中,CK可以是AuC根据公式CK=f3(RAND)生成的,IK可以是AuC根据公式IK=f4(RAND)生成的,AK可以是AuC根据公式AK=f5(RAND)生成 的。除了上述的方式之外,CK、IK以及AK也可以是网络架构中的其它通讯设备生成并发送 给的ARPF,甚至,CK、IK以及AK可以是所述ARPF自己生成的,此处不作具体限定。

[0390] 506:ARPF向AUSF发送共享密钥。相应地,AUSF接收ARPF发送的共享密钥。

[0391] 507:AUSF向发送共享密钥。相应地,AMF(或者SEAF)接收AUSF发送的共享密钥。

[0392] 508:AMF(或者SEAF)根据共享密钥生成锚密钥。

[0393] 针对步骤505中的第一种生成共享密钥的方式,AMF根据共享密钥生成锚密钥的方式为:

[0394] anchor key=KDF(shared key,SNT);

[0395] 其中,anchor key为所述锚密钥,KDF为密钥生成算法,SNT为所述运营商类型标识。

[0396] 针对步骤505中的第二种生成共享密钥的方式,AMF根据共享密钥生成锚密钥的方式为:

[0397] anchor key＝KDF(shared key,ANT)；

[0398] 其中,anchor key为所述锚密钥,KDF为密钥生成算法,ANT为所述接入类型标识。

[0399] 509:AMF(或者SEAF)根据锚密钥生成下层密钥。其中,下层密钥为基于锚密钥进行一次或者多次推衍得到的密钥。

[0400] 可以理解,AMF(或者SEAF)根据K_{amf}密钥/K_{seaf}密钥生成下层密钥的过程与图6A以及图6B所示的过程基本相同,具体请参见图6A以及图6B以及相关内容,此处不再重复赘述。

[0401] 510:AMF(或者SEAF)向AN发送下层密钥。

[0402] 511:UE根据AK,IK,SNT以及ANT生成下层密钥。可以理解,UE推衍下层密钥的 过程与上述过程大体类似,此处将不再展开描述。

[0403] 需要说明的是,当接入方式不同时,步骤509至步骤511是不相同的,下面分别以接入 方式为3GPP接入方式以及非3GPP接入方式为例进行详细介绍。

[0404] 如图17A所示,假设接入方式为3GPP接入方式,锚密钥为anchor key 1,则步骤509至 步骤511可以用下述的步骤5111～5117步骤代替。

[0405] 5111:AMF(或者SEAF)根据anchor key1生成基站密钥K_{gNB},3GPP-NAS保密性密钥$K\text{-}3GPP_{NASenc}$,3GPP-NAS完整性保护密钥$K\text{-}3GPP_{NASint}$。

[0406] 具体地,AMF(或者SEAF)根据以下公式生成3GPP接入方式下的基站密钥K_{gNB}、3GPP-NAS保密性密钥$K\text{-}3GPP_{NASenc}$,以及,3GPP-NAS完整性保护密钥$K\text{-}3GPP_{NASint}$:

[0407] K_{gNB}＝KDF(anchor key 1,NAS Count1)；

[0408] $K\text{-}3GPP_{NASint}$＝KDF(anchor key 1,NAS-int-alg,alg-ID)；

[0409] $K\text{-}3GPP_{NASenc}$＝KDF(anchor key 1,NAS-enc-alg,alg-ID)；

[0410] 其中,NAS Count1为经由3GPP的接入点gNB的NAS消息的计数值,可能为上行计数值,也可以为下行计数值,NAS-int-alg为NAS消息对应的完整性算法,比如'AES','SNOW 3G','ZUC'等,alg-ID为算法的标识,NAS-enc-alg为NAS消息对应的机密性算法,比如'AES','SNOW 3G','ZUC'等。

[0411] 5113:AMF(或者SEAF)将基站密钥K_{gNB}发送给AN。此时,AN相应接收AMF(或 者SEAF)发送的基站密钥K_{gNB}。

[0412] 5115:AN根据基站密钥K_{gNB}生成用户面保密性密钥K_{UPenc}、用户面完整性密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密钥K_{RRCint}。

[0413] 在本申请实施例中,AN根据如下公式分别生成用户面保密性密钥K_{UPenc}、用户面完整性 密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面完整性密钥K_{RRCint}:

[0414] K_{UPenc}＝KDF(K_{gNB},UP-enc-alg,alg-ID)；

[0415] K_{UPin}＝KDF(K_{gNB},UP-int-alg,alg-ID)；

[0416] K_{RRCenc}＝KDFK_{gNB},RRC-enc-alg,alg-ID)；

[0417] K_{RRCint}＝KDF(K_{gNB},RRC-int-alg,alg-ID)；

[0418] 其中,KDF为密钥生成算法,K_{gNB}为基站密钥,alg-ID为算法标识,UP-enc-alg、UP-int-alg、RRC-enc-alg以及RRC-int-alg的定义可以参考表2所示的4G中的算法标识定 义表格。

[0419] 5117:UE根据自行根据AK,IK,SNT以及ANT生成锚密钥,然后,根据锚密钥自行 推

衍用户面保密性密钥K_{UPenc}、用户面完整性密钥K_{UPint}、控制面保密性密钥K_{RRCenc}、控制面 完整性密钥K_{RRCint}。

[0420] 如图17B所示，假设接入方式为非3GPP接入方式，锚密钥为anchor key 2，则步骤509 至步骤511可以用下述的步骤5112～5116步骤代替。

[0421] 5112:AMF(或者SEAF)根据锚密钥anchor key 2生成接入点密钥K_{N3IWF}、非3GPP-NAS保密性密钥$K\text{-}N3GPP_{NASenc}$，以及，非3GPP-NAS完整性保护密钥$K\text{-}N3GPP_{NASint}$。

[0422] 具体地，AMF(或者SEAF)再根据以下公式生成非3GPP接入方式下的接入点密钥K_{N3IWF}、 非3GPP-NAS保密性密钥$K\text{-}N3GPP_{NASenc}$，以及，非3GPP-NAS完整性保护密钥$K\text{-}N3GPP_{NASint}$:

[0423] K_{N3IWF}=KDF(anchor key 2,NAS Count2)；

[0424] $K\text{-}N3GPP_{NASint}$=KDF(anchor key 2,NAS-int-alg,alg-ID)；

[0425] $K\text{-}N3GPP_{NASenc}$=KDF(anchor key 2,NAS-enc-alg,alg-ID)；

[0426] 其中，NAS Count2为经由非3GPP的接入点N3IWF的NAS消息的计数值，可能为上行计数值，也可以为下行计数值，NAS-int-alg为NAS消息对应的完整性算法，比如‘AES’,’SNOW 3G’,’ZUC’等，alg-ID为算法的标识，NAS-enc-alg为NAS消息对应的机密性算法，比如‘AES’,’SNOW 3G’,’ZUC’等。

[0427] 5114:AMF(或者SEAF)将接入点密钥K_{N3IWF}发送给AN。此时，AN相应接收AMF (或者SEAF)发送的接入点密钥K_{N3IWF}。

[0428] 5116:UE根据自行根据AK，IK，SNT以及ANT生成锚密钥，然后，根据锚密钥自行 推衍接入点密钥K_{N3IWF}。

[0429] 可以理解，图16所示实施例中的密钥生成算法不限于KDF算法，在实际应用中，密钥 生成算法还可以是其它的算法，比如Trunc算法：取低位的截图算法；其他的HASH算法等， 本申请不作具体限定。而且，密钥生成算法的自变量也可以包括其他的参数，例如，包括NSSAI、 随机数、随机数值、序列码、注册类型、接入层消息数量、安全算法标识、安全标识、SQN⊕ AK的长度以及生成密钥所用的参数对应的长度等等，在实际应用中，可以根据需要从中选 择中的一个或者多个参数作为所述密钥生成算法的自变量。

[0430] 执行图16所示的锚密钥生成方法之后，将生成如图18所示的密钥架构。其中，图18中 隔离线左边的为具体执行图17A所示的流程所生成的密钥架构，图18图中隔离线右边的为 具体执行图17B所示的流程所生成的密钥架构，两者之间能够很好地进行隔离。

[0431] 如图19所示，本申请实施例提供了第七种锚密钥生成方法。该方法可以基于图3以及图 4所示的网络架构来实现，该方法包括但不限于如下步骤。

[0432] 601:UE向AN发送终端标识。相应地，AN接收UE发送的终端标识。

[0433] 在本申请实施例中，终端标识可以是固定不变的标识，例如，媒体访问控制(Media Access Control,MAC)地址、网络协议(Internet Protocol,IP)地址、手机号码、国际移动设备标 识(International Mobile Equipment Identity,IMEI)、国际移动用户识别码(International Mobile Subscriber Identity,IMSI)、IP多媒体私有标识(IP Multimedia Private Identity,IMPI)、IP多 媒体公共标识(IP Multimedia Public Identity,IMPU)等等，也可以是临时分配的标识，例如， 临时移动用户标识符(TemporaryMobileSubscriberIdentity,TMSI)、全球唯一临时UE标识 (Globally Unique

Temporary UE Identity,GUTI)等等。

[0434] 可以理解,除了终端标识之外,UE还可以将接入网参数、注册类型、安全参数、UE的5G网络能力,PDU session的状态等至少一种发送给AN。其中,接入网参数为可能为接入网的频点,临时用户标识,NSSAI等与服务网络相关的参数。注册类型为可以表明用户是初次注册、由于移动引起的注册、周期性注册更新等区分用户注册的行为。安全参数为认证和完整性保护相关的参数。NSSAI为网络切片选择辅助信息。UE的5G网络能力可能包括支持接入该网络的配置能力。PDU session为UE和数据网络之间的PDU的业务连接,类型可能为IP、以太网的业务连接。

[0435] 602:AN向AMF(或者SEAF)发送终端标识以及指示标识。相应地,AMF(或者SEAF) 接收AN发送的终端标识以及指示标识。

[0436] 在本申请实施例中,指示标识用于指示终端的接入方式。在5G标准中,可以按照不同 的划分依据对终端的接入方式进行划分。例如,接入方式的划分依据可以包括接入类型以及 运营商类型。其中,接入类型具体可以分为3GPP接入类型、可信的非3GPP接入类型以及 非可信的非3GPP接入类型。运营商类型具体可以分为A运营商类型或者B运营商类型。可以理解,运营商类型还可以有更多的类型,此处仅作为示例,不作具体限定。

[0437] 以划分依据包括接入类型以及运营商类型为例,所述接入方式的划分可以如表1所示。需要说明的,不限于上述两种划分依据,接入方式的划分依据还可以是其他种类的划分依据, 例如,介质类型(有线接入或者无线接入)等等,此处不作具体限定。并且,不限于接入类 型以及运营商类型两种划分依据,接入方式的划分依据还可以是一种、三种、四种或者更多, 即,可以从更多维度或者更少维度对接入方式进行划分。

[0438] 所述指示标识可以是携带在上述接入网参数中。所述指示标识可以包括接入类型标识以 及运营商类型标识,其中,所述接入类型标识用于指示所述接入类型,所述运营商类型标识 用于指示所述运营商类型。可以理解,上述例子仅作为举例,不构成具体限定。

[0439] 在一些可能的实现方式中,接入类型标识具体指示所述接入类型为3GPP接入类型、可 信的非3GPP接入类型以及非可信的非3GPP接入类型。例如,接入类型标识Access Network Type(ANT)可以直接为“3GPP network”,“Trusted Non-3GPP network”,“Untrusted Non-3GPP network”字符串,或者仅为“3GPP network”和“Non-3GPP network”字符串等等。

[0440] 在一些可能的实现方式中,所述运营商类型标识可以包括两部分,一部分用于指示运营 商,另一部分用于指示具体接入类型。例如,运营商类型标识可以指示为中国移动的LTE接 入或者中国联通的WLAN接入。在具体应用中,可以将SN Identity和Access Network Identity 的结合以作为运营商类型标识;也有可能只包括运营商的区分,比如中国移动、中国联通、中国电信等等。

[0441] 在一些可能的实现方式中,有可能指示标识只是运营商类型标识。

[0442] 在一些可能的实现方式中,有可能指示标识只是接入类型标识。

[0443] 603:AMF(或者SEAF)向AUSF发送终端标识以及指示标识。相应地,AUSF接收 AMF(或者SEAF)发送的终端标识以及指示标识。

[0444] 604:AUSF向ARPF发送终端标识以及指示标识。相应地,ARPF接收AUSF发送的终 端标识以及指示标识。

[0445] 605:ARPF根据根密钥K以及指示标识生成锚密钥。

[0446] 在本申请实施例中,ARPF根据密钥生成算法生成锚密钥的方式可以包括以下几种:

[0447] 在第一种方式中,当指示标识为NAI时,ARPF根据下述密钥生成算法生成锚密钥anchor key:

[0448] anchor key =KDF(SQN⊕AK, NAI, K);

[0449] 其中,KDF为密钥生成算法,SQN为最新序列号,NAI为所述指示标识,K为根密钥,AK为匿名密钥AK=f5(RAND),RAND为随机数,f3为生成算法,⊕的含义为异或运算。

[0450] 在第二种方式中,当指示标识包括接入类型标识以及运营商类型标识时,ARPF根据下 述密钥生成算法生成锚密钥anchor key:

[0451] anchor key =KDF(SQN⊕AK, ANT, SNT, K);

[0452] 其中,KDF为密钥生成算法,SQN为最新序列号,ANT为所述接入类型标识,SNT为 所述运营商类型标识,AK为匿名密钥,AK=f5(RAND),RAND为随机数,f5为生成算法, ⊕的含义为异或运算。

[0453] 在一些可能的实施方式中,SQN可以是AuC生成的最新序列号,AuC在生成SQN之后,将SQN发送给所述ARPF。类似地,RAND可以是AuC生成的随机数,AuC在生成RAND 之后,将RAND发送给所述ARPF。除了上述的方式之外,SQN以及RAND也可以是网络 架构中的其它通讯设备生成并发送给的ARPF,甚至,SQN以及RAND可以是所述ARPF自 己生成的,此处不作具体限定。

[0454] 在一些可能的实施方式中,AK可以是AuC根据公式AK=f5(RAND)生成的。除了上述的方式之外,AK也可以是网络架构中的其它通讯设备生成并发送给的ARPF,甚至,AK 可以是所述ARPF自己生成的,此处不作具体限定。

[0455] 606:ARPF向AUSF发送锚密钥。相应地,AUSF接收ARPF发送的锚密钥。

[0456] 607:AUSF根据锚密钥生成K_{amf}密钥和/或K_{seaf}密钥。

[0457] 在本申请实施例中,AUSF根据以下公式生成K_{amf}密钥和/或K_{seaf}密钥:

[0458] K_{amf}=KDF(anchor key,AMF ID);

[0459] K_{seaf}=KDF(anchor key,SEAF ID);

[0460] 其中,anchor key为所述锚密钥,KDF为密钥生成算法,AMF ID为AMF的标识,SEAF ID为SEAF的标识。

[0461] 608:AUSF将K_{amf}密钥/K_{seaf}密钥发送给AMF/SEAF。相应地,AMF/SEAF接收AUSF 发送的K_{amf}密钥/K_{seaf}密钥。

[0462] 609:AMF(或者SEAF)根据K_{amf}密钥/K_{seaf}密钥生成下层密钥。其中,下层密钥为基于锚密钥进行一次或者多次推衍得到的密钥。

[0463] 可以理解,AMF(或者SEAF)根据K_{amf}密钥/K_{seaf}密钥生成下层密钥的过程与图14A以及图14B所示的过程基本相同,具体请参见图14A以及图14B以及相关内容,此处不再重复赘述。

[0464] 610:AMF(或者SEAF)向AN发送下层密钥。

[0465] 611:UE根据K,SNT以及ANT生成下层密钥。可以理解,UE推衍下层密钥的过程与 上述过程大体类似,此处将不再展开描述。

[0466] 可以理解，AUSF在生成锚密钥之后，也可以直接将锚密钥发送给AMF，然后，AMF 再根据锚密钥生成下层密钥，并发送给AN。

[0467] 可以理解，图19所示实施例中的密钥生成算法不限于KDF算法，在实际应用中，密钥 生成算法还可以是其它的算法，比如Trunc算法：取低位的截图算法；其他的HASH算法等，本申请不作具体限定。而且，密钥生成算法的自变量也可以包括其他的参数，例如，包括NSSAI、随机数、随机数值、序列码、注册类型、接入层消息数量、安全算法标识、安全标识、SQN⊕AK的长度以及生成密钥所用的参数对应的长度等等，在实际应用中，可以根据需要从中选 择中的一个或者多个参数作为所述密钥生成算法的自变量。

[0468] 执行图19所示的锚密钥生成方法之后，将生成如图20所示的密钥架构。其中，图20中 隔离线左边的为具体执行3GPP接入方式的流程所生成的密钥架构，图20图中隔离线右边的 为具体执行非3GPP接入方式的流程所生成的密钥架构，两者之间能够很好地进行隔离。

[0469] 在本发明的另一个实施例中，公开了一种在AUSF中保留一个密钥的实现方式。该保留的 密钥可简写为K_{left}。

[0470] 具体的，需要指出的是，由于AUSF会向第二通讯设备SEAF发送锚密钥，而在可能的场 景部署中，SEAF属于服务网络的安全网元，AUSF属于归属网络的安全网元，特别在漫游的场 景下，如果认证发生在UE和归属网络的安全网元之间，则UE和AUSF可以基于该认证过后的 保留密钥生成最终的保护密钥，从而实现UE和归属网络之间端到端的安全保护或者更高的安 全保护。

[0471] 需要指出的是，该保留的密钥可由ARPF生成，然后发送给AUSF，或者该保留的密钥可直 接由AUSF生成。

[0472] 方法一，ARPF可根据IK，CK，SQN，AK，服务网络标识，密钥特征标识，RAND或nonce等参数生成保留密钥K_{left}。

[0473] 其中，SQN为最新序列号，CK为初始保密性密钥，IK为初始完整性密钥，AK为匿名密钥，RAND和Nonce均可以认为是随机数；其中密钥特征标识可以为：KEYLEFT，AUSFKEY，KEYAUSF，KEYSEAF，SEAFKEY等类似字符串。

[0474] 后续所涉及的生成函数KDF也可以为伪随机函数(pesudo random function，PRF)等。具体可参见为RFC5448 3.4.1章节中的定义。

[0475] 举例来说，K_{left}= KDF(IK，CK， SQN⊕AK，可选参数)；KDF为密钥生成算法。

[0476] 其中，可选参数为authent ication method name、服务网络标识，密钥特征标识，RAND，nonce中的一个或多个。

[0477] 其中，authent ication method name：可以为'EAP-AKA'‘，'5G-EAP‘，'EPS-AKA*‘等标识认证方法的标识；

[0478] 对于EPS-AKA*，ARPF可根据K_{asme*}、authentication method name、服务网络标识，网 络类型标识，密钥特征标识，RAND，nonce等参数生成K_{left}。

[0479] 其中，K_{asme*}为类似于4G LTE中K_{asme}的密钥。

[0480] 比如，K_{left}＝KDF(K_{asme*}，第一参数组)；

[0481] 其中，所述第一参数组为authentication method name、服务网络标识，网络类型标 识，密钥特征标识，RAND，nonce中的一个或多个。

[0482] 需要指出的是，方法一描述的生成保留密钥的过程可分别与图5、图8、图9、图11、图13以及图16描述的方法相结合。

[0483] 方法二，对于EAP-AKA'，ARPF可根据IK'，CK'，authentication method name，服务网络标识，密钥特征标识，AUSF ID，RAND，nonce等中的一个或多个参数生成K_{left}。

[0484] 比如，K_{left}＝KDF(IK'，CK'，服务网络标识，密钥特征标识，第二参数组)。

[0485] 其中，第二参数组为authentication method name，AUSF ID，RAND，nonce等中的一 个或多个。

[0486] 需要说明的是，此处也可由ARPF将IK' CK'发送给AUSF后，由AUSF执行K_{left}的生成。

[0487] 需要指出的是，方法二描述的生成保留密钥的过程可分别与图5、图8、图9以及图11描述的方法相结合。

[0488] 方法三，AUSF可根据EMSK、MSK等参数生成K_{left}。EMSK：为扩展性主会话密钥。参见RFC5448。MSK：主会话密钥。参见RFC5448。

[0489] 举例来说，K_{left}＝trunc(EMSK or MSK)，该公式的含义为直接通过截取EMSK或MSK的 某些bit位作为K_{left}，其中trunc为用于对值进行截断。比如，trunc(number)表示截断数字； trunc(date)表示截断日期。格式：TRUNC(n1，n2)，n1表示被截断的数字，n2表示要截断到 那一位。n2可以是负数，表示截断小数点前。注意，TRUNC截断不是四舍五入。

[0490] 举例来说，K_{left}＝KDF(EMSK or MSK，密钥特征标识，第三参数组)

[0491] 其中，第三参数组为服务网络标识，authentication method name，随机数等中的一 个或多个。

[0492] 举例来说，K_{left}也可以理解为就是EMSK。

[0493] 需要指出的是，方法三描述的生成保留密钥的过程可分别与图8、图9以及图11描述 的方法相结合。

[0494] 可以理解的是，当存在K_{left}时，anchor key则可以为基于K_{left}生成的密钥。

[0495] 具体来说，anchor key可为根据K_{left}，服务网络标识，密钥特征标识，RAND或nonce等 参数生成。

[0496] 另外，在本发明的另一实施例中，图6B的步骤1114、图14B的步骤4112、图17B步骤5112的细化可替换为：

[0497] AMF(或者SEAF)根据K_{amf2}，K_{seaf2}，NAS Count2，NAS连接区分标识，N3IWF标识等参数生成非3GPP接入方式下的接入点密钥K_{N3IWF}。

[0498] 举例来说，

[0499] K_{N3IWF}＝KDF(K_{amf2}和/或K_{seaf2}，NAS Count2)；

[0500] 其中，NAS Count2为经由非3GPP的接入点N3IWF的NAS消息的计数值，可能为上行计 数值，也可以为下行计数值。其中，A和/或B表示三种可能：A、B或(A和B)。

[0501] 该公式：K_{N3IWF}＝KDF(K_{amf2}和/或K_{seaf2}，NAS Count2)包含三种可能：

[0502] 第一种：K_{N3IWF}＝KDF(K_{amf2}，NAS Count2)；

[0503] 第二种：K_{N3IWF}＝KDF(K_{seaf2}，NAS Count2)；

[0504] 第三种：K_{N3IWF}＝KDF(K_{amf2}，K_{seaf2}，NAS Count2)。

[0505] 图21示出了一种通讯设备的结构示意图，在本实施方式中，通讯设备包括：接收模

块 710、发送模块720以及生成模块730。下面展开描述。

[0506] 所述接收模块710用于接收第二通讯设备发送指示标识，其中，所述指示标识用于指示 终端的接入方式。

[0507] 所述发送模块720用于向第三通讯设备发送所述指示标识；

[0508] 所述接收模块710用于接收所述第三通讯设备返回的中间密钥，其中，所述中间密钥是 根据所述指示标识生成的；

[0509] 所述生成模块730用于根据所述中间密钥生成锚密钥，其中，所述锚密钥对应所述终端 的接入方式；

[0510] 所述发送模块720用于将所述锚密钥发送给所述第二通讯设备，以供所述第二通讯设备 根据所述锚密钥为所述接入方式推衍下层密钥。

[0511] 需要说明，图21实施例中未提及的内容以及各个功能单元的具体实现，请参考图5至图 10以及相关内容，这里不再赘述。

[0512] 基于同一发明构思，本发明实施例还提供一种装置(如图22所示)，该装置用于实现前 述图5至图12实施例所描述的方法。如图22所示，装置800包括：发射器803、接收器804、存储器802和与存储器802耦合的处理器801(处理器801的数量可以是一个或多个，图20中以一个处理器为例)。发射器803、接收器804、存储器802和处理器801可通过总线 或者其它方式连接(图20中以通过总线805连接为例)。其中，发射器803用于向外部发送 数据，接收器804用于从外部接收数据。存储器802用于存储程序代码，处理器801用于 调用并运行存储于存储器802中的程序代码。

[0513] 通过接收器804接收第二通讯设备发送指示标识，其中，所述指示标识用于指示终端的 接入方式；

[0514] 通过发射器803向第三通讯设备发送所述指示标识；所述第一通讯设备接收所述第三通 讯设备返回的中间密钥，其中，所述中间密钥是根据所述指示标识生成的；

[0515] 处理器801根据所述中间密钥生成锚密钥，其中，所述锚密钥对应所述终端的接入方式；

[0516] 通过发射器803将所述锚密钥发送给所述第二通讯设备，以供所述第二通讯设备根据所 述锚密钥为所述接入方式推衍下层密钥。

[0517] 在一些可能的实施方式中，所述接入方式是根据接入类型以及运营商类型中的至少一个 进行区分的。

[0518] 在一些可能的实施方式中，处理器801根据以下公式生成锚密钥，

[0519] anchor key＝KDF(IK$_1$'||CK$_1$')

[0520] 其中，anchor key为所述锚密钥，(IK$_1$'，CK$_1$')为所述中间钥匙，IK$_1$'为中间完整性密 钥，CK$_1$'为中间保密性密钥，||的含义为级联，表示将符号两边的字符串连起来。

[0521] 处理器801至少可以根据以下两种方式生成中间密钥：

[0522] 当所述指示标识包括接入类型标识以及运营商类型标识时，所述中间密钥是处理器801 根据以下公式生成的：

[0523] $(CK_1', IK_1') = KDF(SQN \oplus AK, ANT, SNT, CK \| IK)$；

[0524] 其中，所述接入类型标识用于指示所述接入类型，所述运营商类型标识用于指示所述运 营商类型；(CK$_1$'，IK$_1$')为所述中间密钥，CK$_1$'为所述中间保密性密钥，IK$_1$'为所述

中间完 整性密钥,KDF为密钥生成算法,SQN为最新序列号,ANT为所述接入类型标识,SNT为所述运营商类型标识,CK为初始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK＝f3(RAND),IK＝f4(RAND),AK＝f5(RAND),RAND为随机数,f3,f4以及f5均为生成算 法,⊕的含义为异或运算。

[0525] 当所述指示标识是NAI时,所述中间密钥是处理器801根据以下公式生成的:

[0526] $(CK_1', IK_1') = KDF(SQN \oplus AK, NAI, CK||IK)$;

[0527] 其中,(CK_1', IK_1')为所述中间密钥,CK_1'为所述中间保密性密钥,IK_1'为所述中间完 整性密钥,KDF为密钥生成算法,SQN为最新序列号,NAI为所述指示标识,CK为初始保 密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK＝f3(RAND),IK＝f4(RAND),AK＝f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0528] 在一些可能的实施方式中,处理器801根据以下公式生成所述中间密钥:

[0529] $(CK_2', IK_2') = KDF(SQN \oplus AK, ANT, CK||IK)$;

[0530] 其中,(CK_2', IK_2')为所述中间密钥,CK_2'为所述中间保密性密钥,IK_2'为所述中间完 整性密钥,KDF为密钥生成算法,SQN为最新序列号,ANT为所述接入类型标识,CK为初 始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK＝f3(RAND),IK＝f4(RAND), AK＝f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0531] 处理器801根据以下公式生成EMSK',

[0532] $EMSK' = PRF'(IK_2'||CK_2')$;

[0533] 其中,EMSK'为扩展主会话密钥,(IK_2', CK_2')为所述中间钥匙,IK_2'为中间完整性密 钥,CK_2'为中间保密性密钥,||的含义为级联,表示将符号两边的字符串连起来;

[0534] 处理器801根据以下公式生成锚密钥,

[0535] anchor key＝KDF(EMSK',SNT);

[0536] 其中,anchor key为所述锚密钥,SNT为所述运营商类型标识。

[0537] 在一些可能的实施方式中,处理器801根据以下公式生成所述中间密钥:

[0538] $(CK_2', IK_2') = KDF(SQN \oplus AK, SNT, CK||IK)$;

[0539] 其中,(CK_2', IK_2')为所述中间密钥,CK_2'为所述中间保密性密钥,IK_2'为所述中间完 整性密钥,KDF为密钥生成算法,SQN为最新序列号,SNT为所述运营商类型标识,CK为 初始保密性密钥,IK为初始完整性密钥,AK为匿名密钥,CK＝f3(RAND),IK＝f4(RAND),AK＝f5(RAND),RAND为随机数,f3,f4以及f5均为生成算法,⊕的含义为异或运算。

[0540] 处理器801根据以下公式生成EMSK',

[0541] $EMSK' = PRF'(IK_2'||CK_2')$;

[0542] 其中,EMSK'为扩展主会话密钥,(IK_2', CK_2')为所述中间钥匙,IK2'为中间完整性密 钥,CK2'为中间保密性密钥,||的含义为级联,表示将符号两边的字符串连起来;

[0543] 处理器801根据以下公式生成锚密钥,

[0544] anchor key＝KDF(EMSK',ANT);

[0545] 其中,anchor key为所述锚密钥,ANT为所述接入类型标识。

[0546] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的 形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机

可用存储 介质(包括但不限于磁盘存储器和光学存储器等)上实施的计算机程序产品的形式。

[0547] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/ 或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方 框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计 算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使 得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流 程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0548] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工 作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制 造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定 的功能。

[0549] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或 其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编 程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多 个方框中指定的功能的步骤。

[0550] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范 围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则 本发明也意图包含这些改动和变型在内。

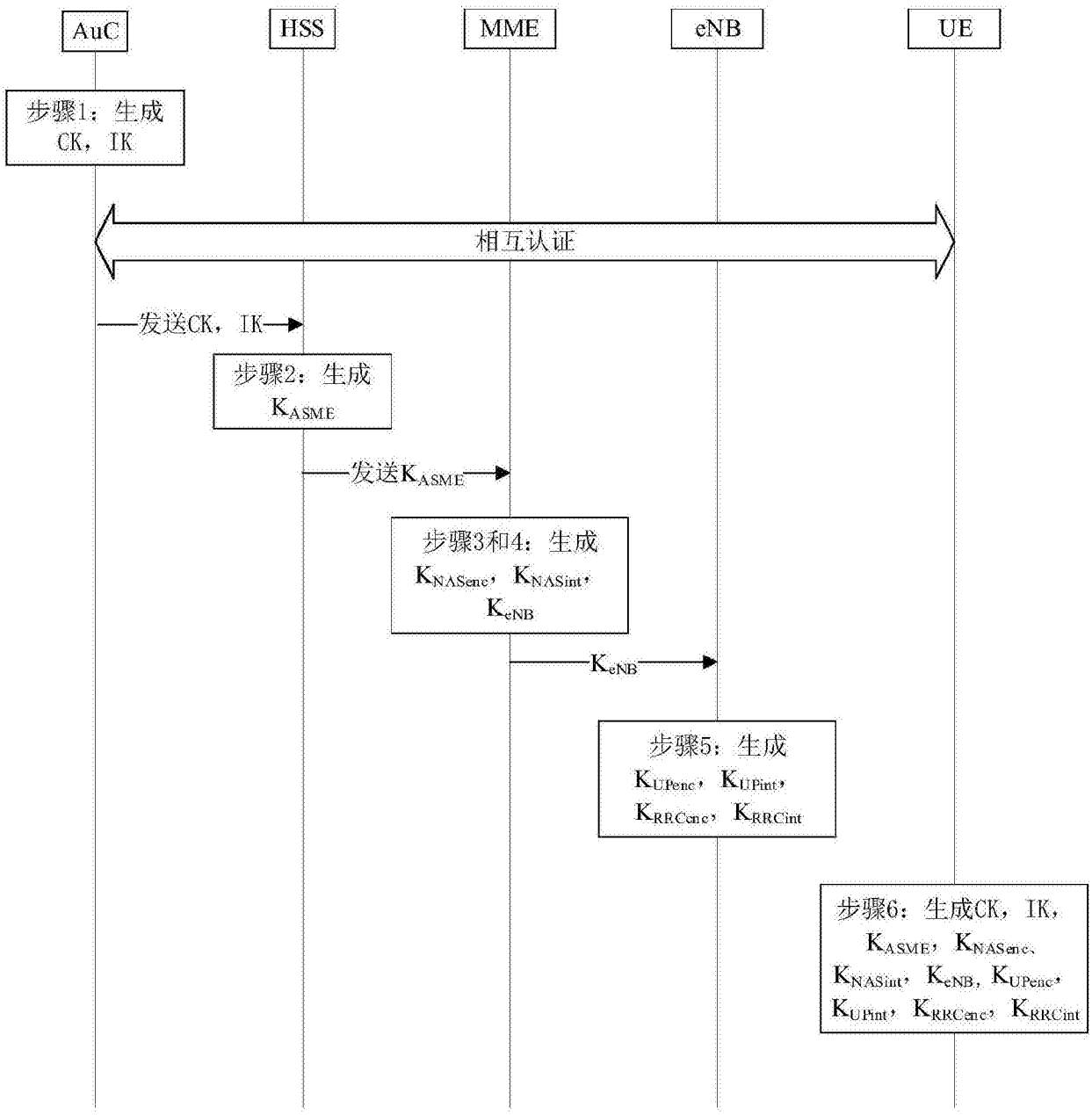

AuC
HSS
MME
eNB
UE
步骤1：生成 CK，IK
相互认证
发送CK，IK
步骤2：生成 K_{ASME}
发送K_{ASME}
步骤3和4：生成 K_{NASenc}，K_{NASint}，K_{eNB}
K_{eNB}
步骤5：生成 K_{UPenc}，K_{UPint}，K_{RRCenc}，K_{RRCint}
步骤6：生成CK，IK，K_{ASME}，K_{NASenc}、K_{NASint}，K_{eNB}，K_{UPenc}，K_{UPint}，K_{RRCenc}，K_{RRCint}

图1

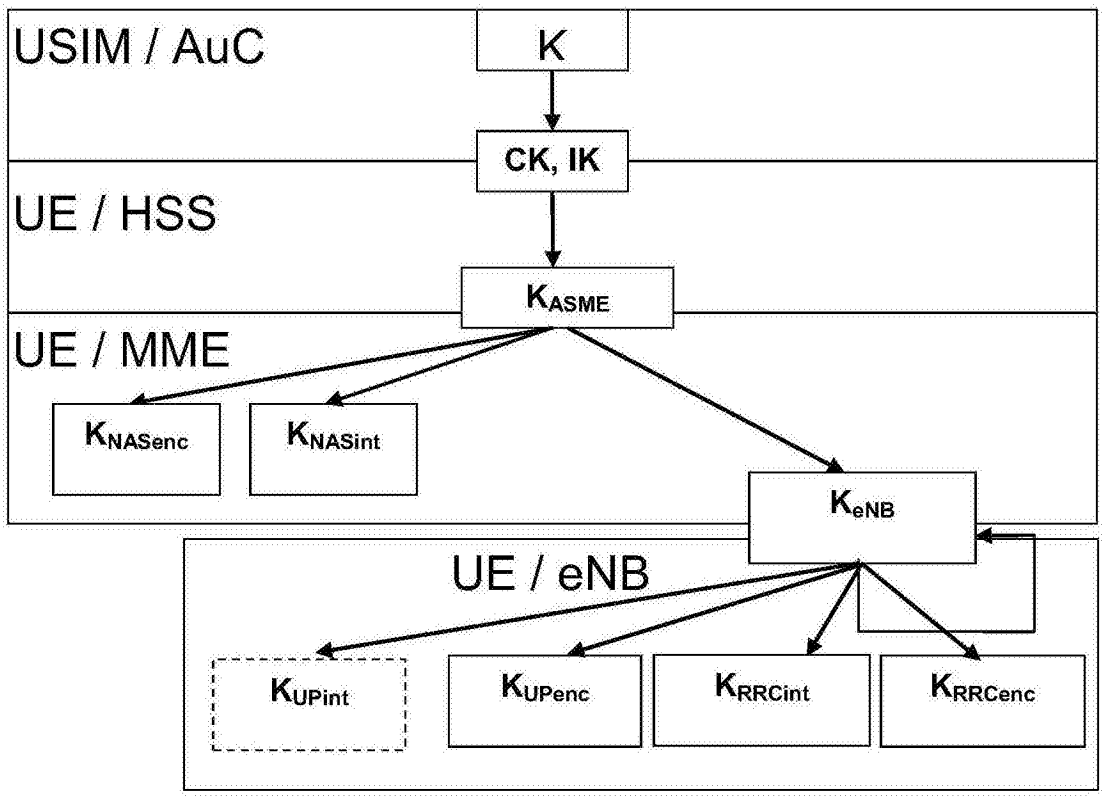

USIM / AuC
K
CK, IK
UE / HSS
KASME
UE / MME
KNASenc
KNASint
KeNB
UE / eNB
KUPint
KUPenc
KRRCint
KRRCenc

图2

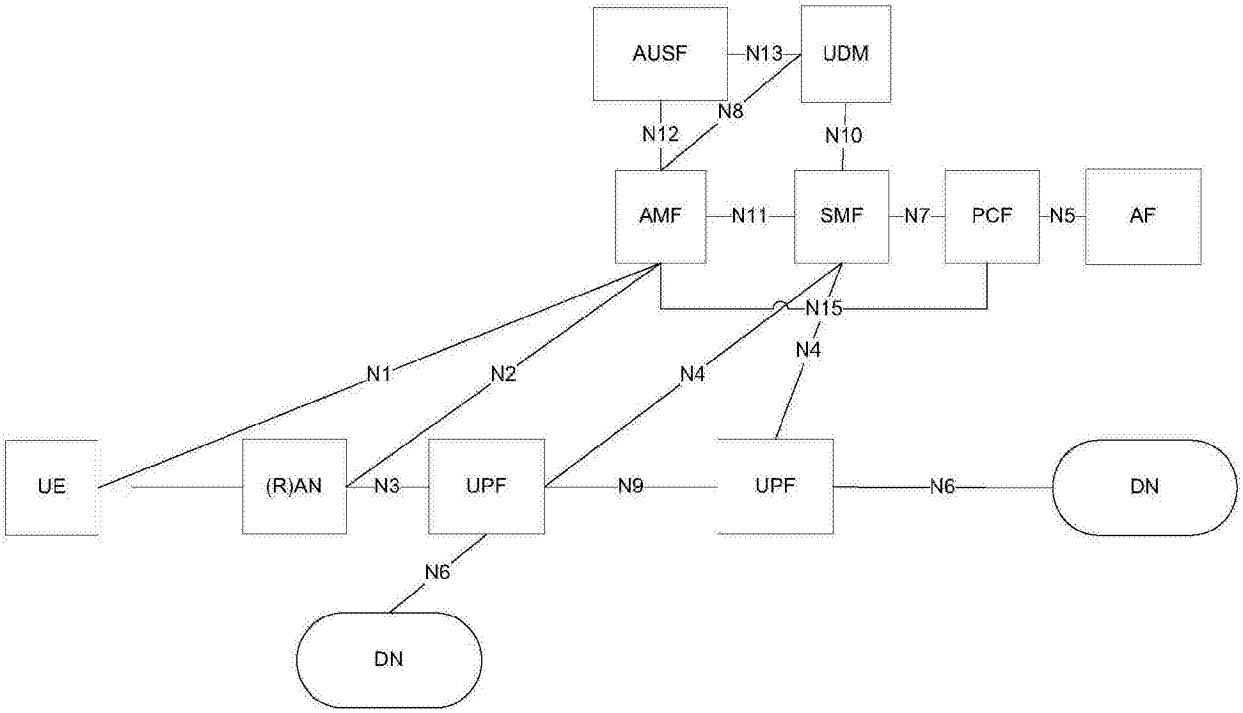

AUSF
N13
UDM
N8
N12
N10
AMF
N11
SMF
N7
PCF
N5
AF
N15
N4
N1
N2
N4
UE
(R)AN
N3
UPF
N9
UPF
N6
DN
N6
DN

图3

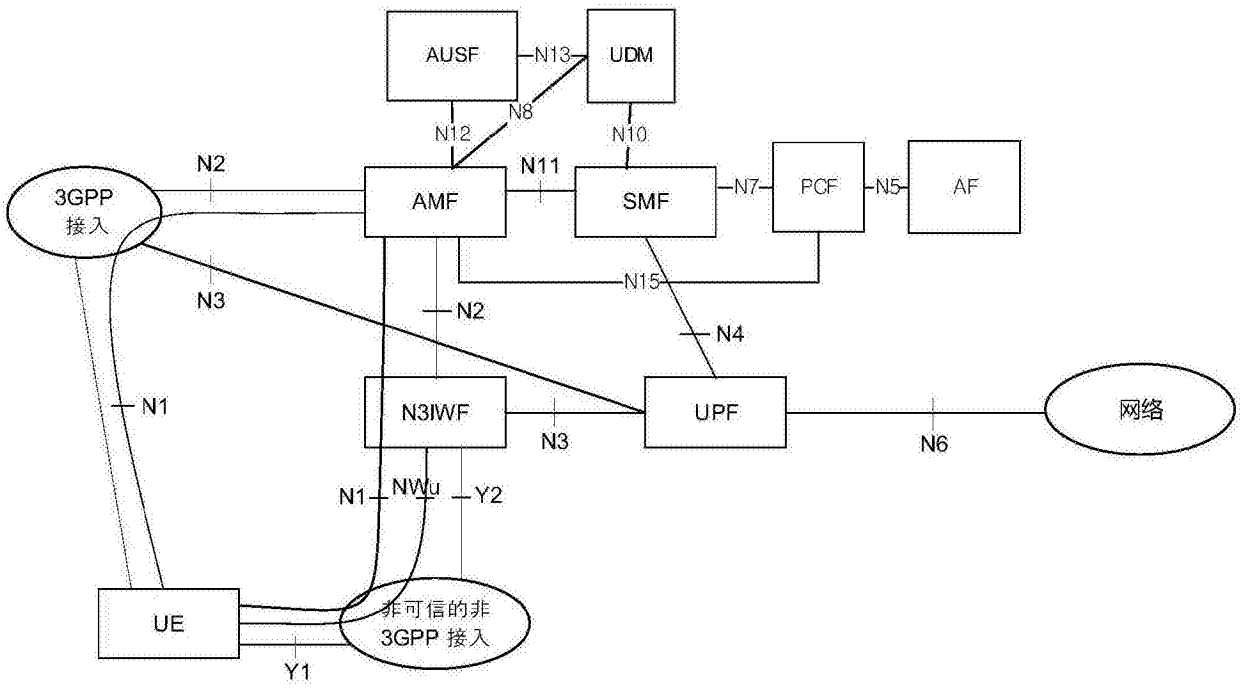

AUSF
N13
UDM
N8
N12
N10
N2
N11
3GPP
接入
AMF
SMF
N7
PCF
N5
AF
N3
N15
N2
N4
N1
N3IWF
UPF
网络
N3
N6
N1
NWu
Y2
UE
非可信的非
3GPP 接入
Y1

图4

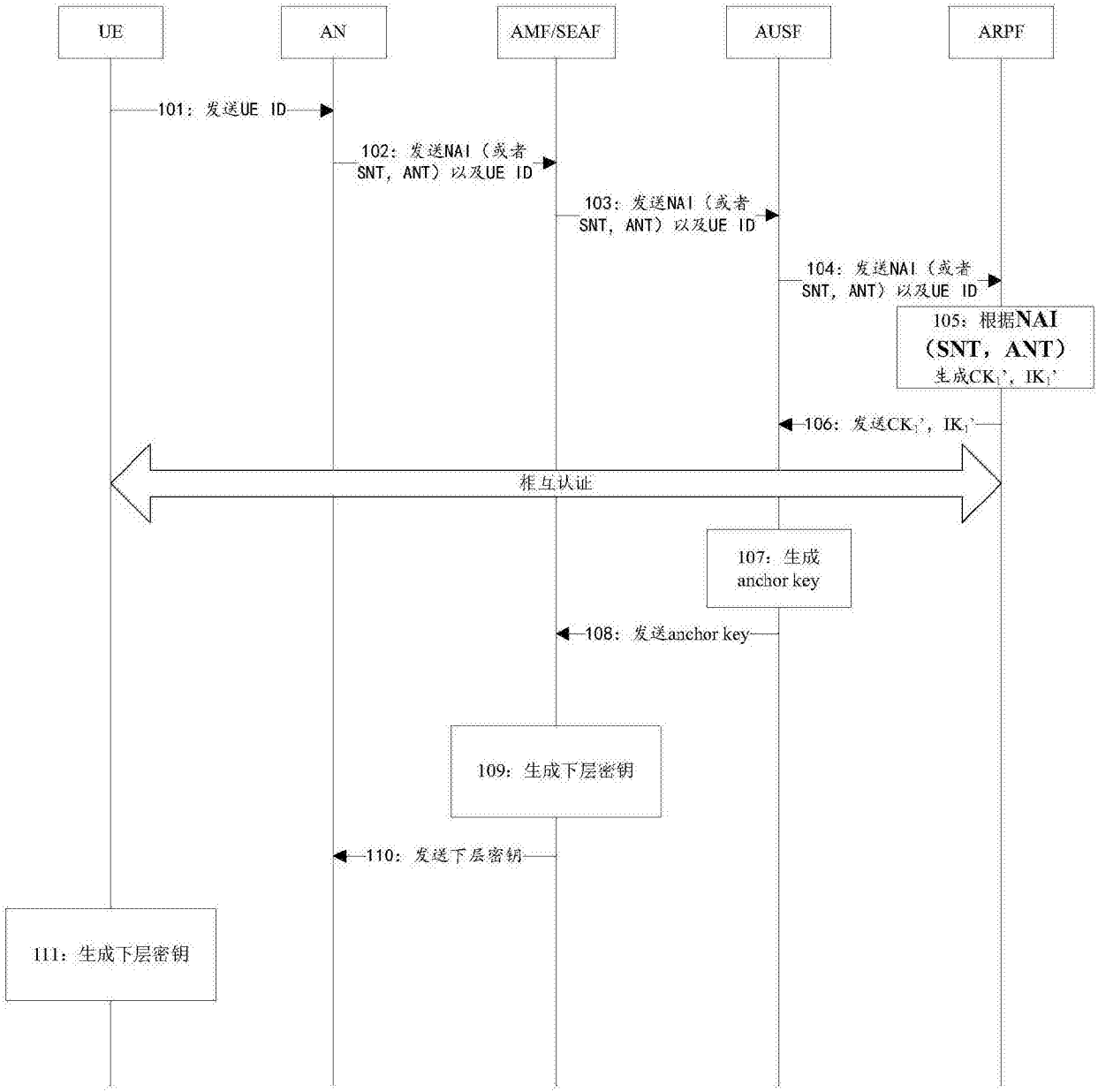

UE
AN
AMF/SEAF
AUSF
ARPF
101：发送UE ID
102：发送NAI（或者SNT，ANT）以及UE ID
103：发送NAI（或者SNT，ANT）以及UE ID
104：发送NAI（或者SNT，ANT）以及UE ID
105：根据NAI（SNT，ANT）生成CK1'，IK1'
106：发送CK1'，IK1'
相互认证
107：生成anchor key
108：发送anchor key
109：生成下层密钥
110：发送下层密钥
111：生成下层密钥

图5

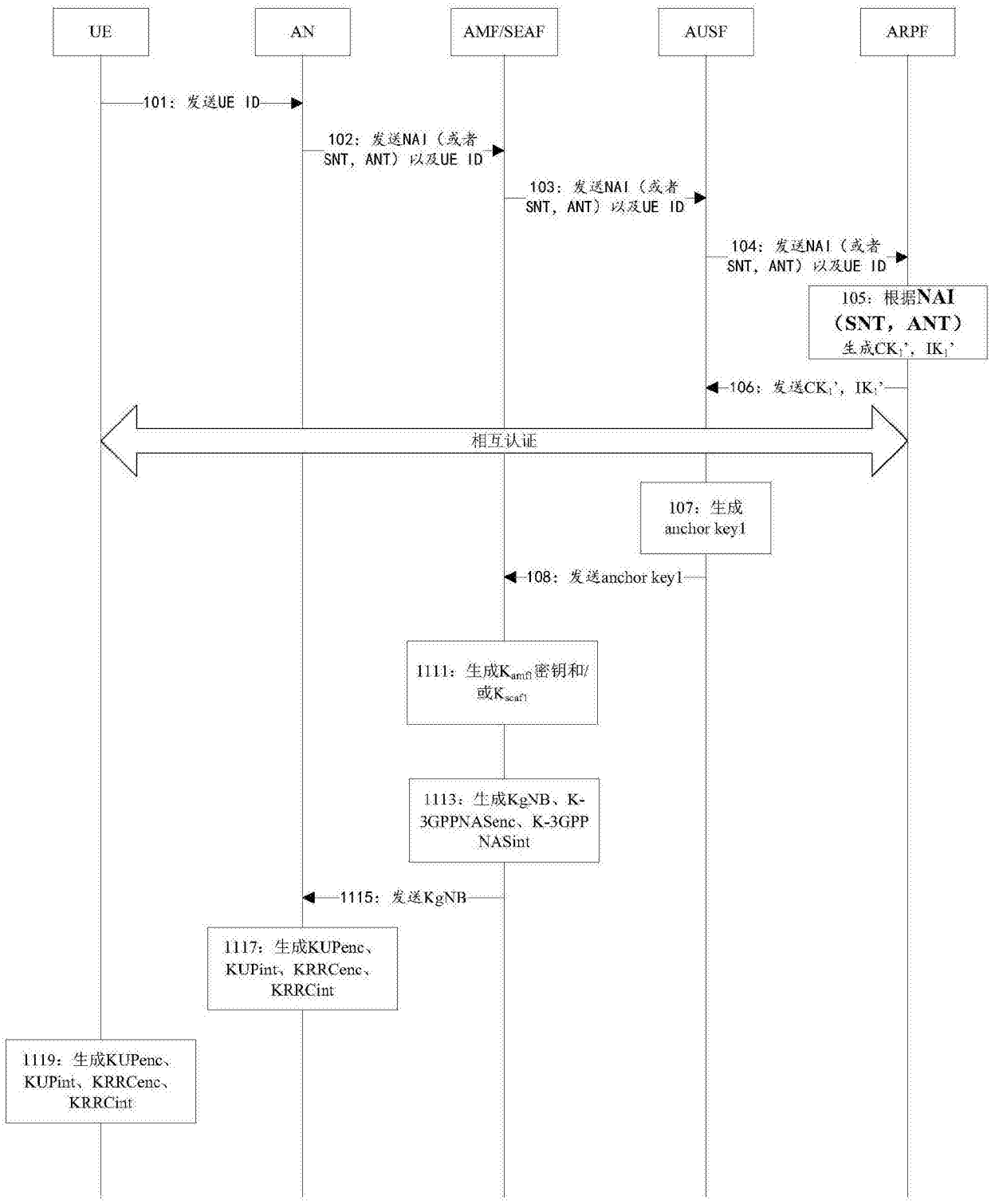

UE
AN
AMF/SEAF
AUSF
ARPF
101：发送UE ID
102：发送NAI（或者SNT，ANT）以及UE ID
103：发送NAI（或者SNT，ANT）以及UE ID
104：发送NAI（或者SNT，ANT）以及UE ID
105：根据NAI（SNT，ANT）生成CK1'，IK1'
106：发送CK1'，IK1'
相互认证
107：生成anchor key1
108：发送anchor key1
1111：生成Kamf密钥和/或Kseaf
1113：生成KgNB、K-3GPPNASenc、K-3GPP NASint
1115：发送KgNB
1117：生成KUPenc、KUPint、KRRCenc、KRRCint
1119：生成KUPenc、KUPint、KRRCenc、KRRCint

图6A

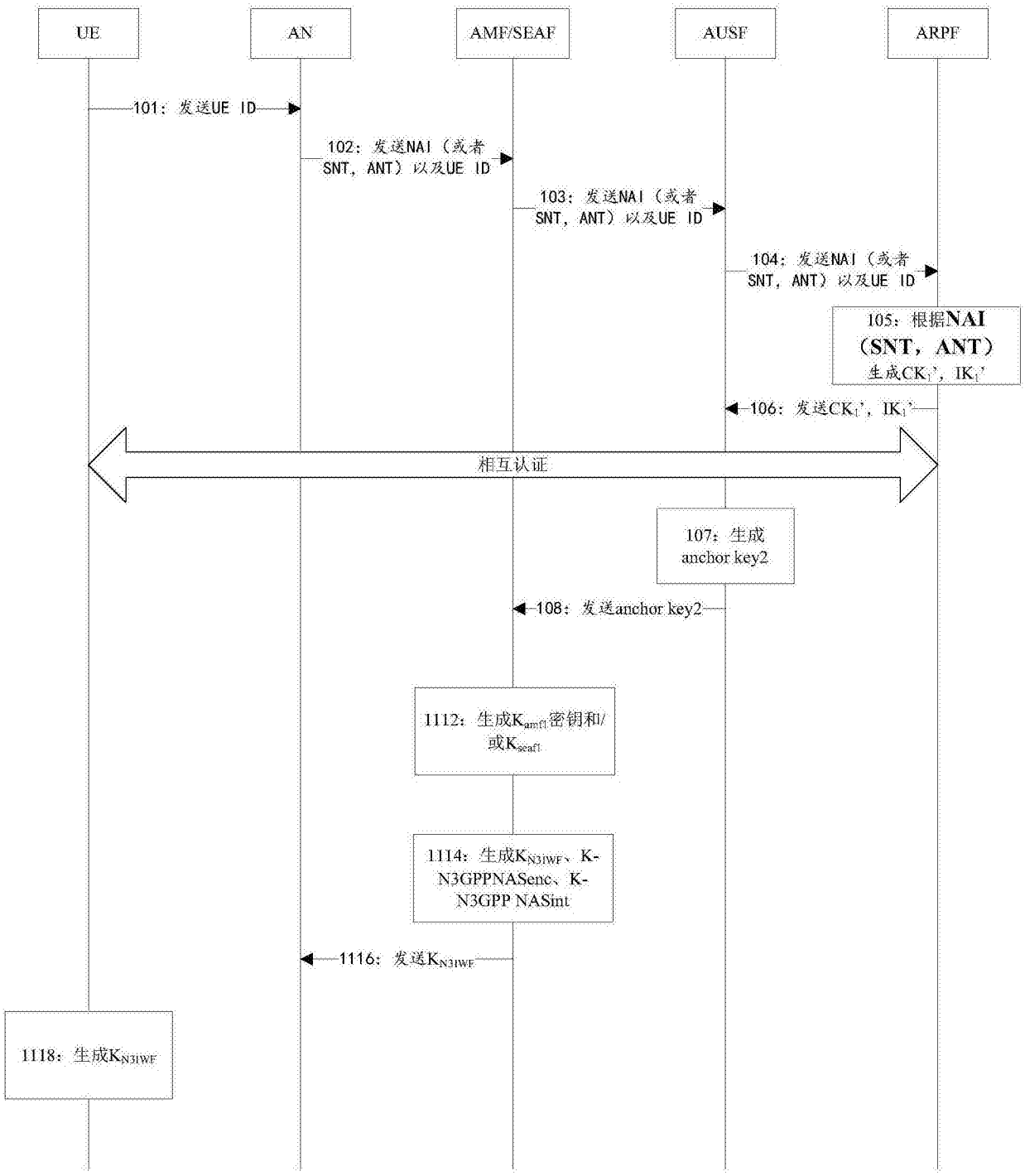

UE
AN
AMF/SEAF
AUSF
ARPF
101：发送UE ID
102：发送NAI（或者SNT，ANT）以及UE ID
103：发送NAI（或者SNT，ANT）以及UE ID
104：发送NAI（或者SNT，ANT）以及UE ID
105：根据NAI（SNT，ANT）生成CK1'，IK1'
106：发送CK1'，IK1'
相互认证
107：生成anchor key2
108：发送anchor key2
1112：生成Kamf1密钥和/或Kseaf1
1114：生成KN3IWF、K-N3GPPNASenc、K-N3GPP NASint
1116：发送KN3IWF
1118：生成KN3IWF

图6B

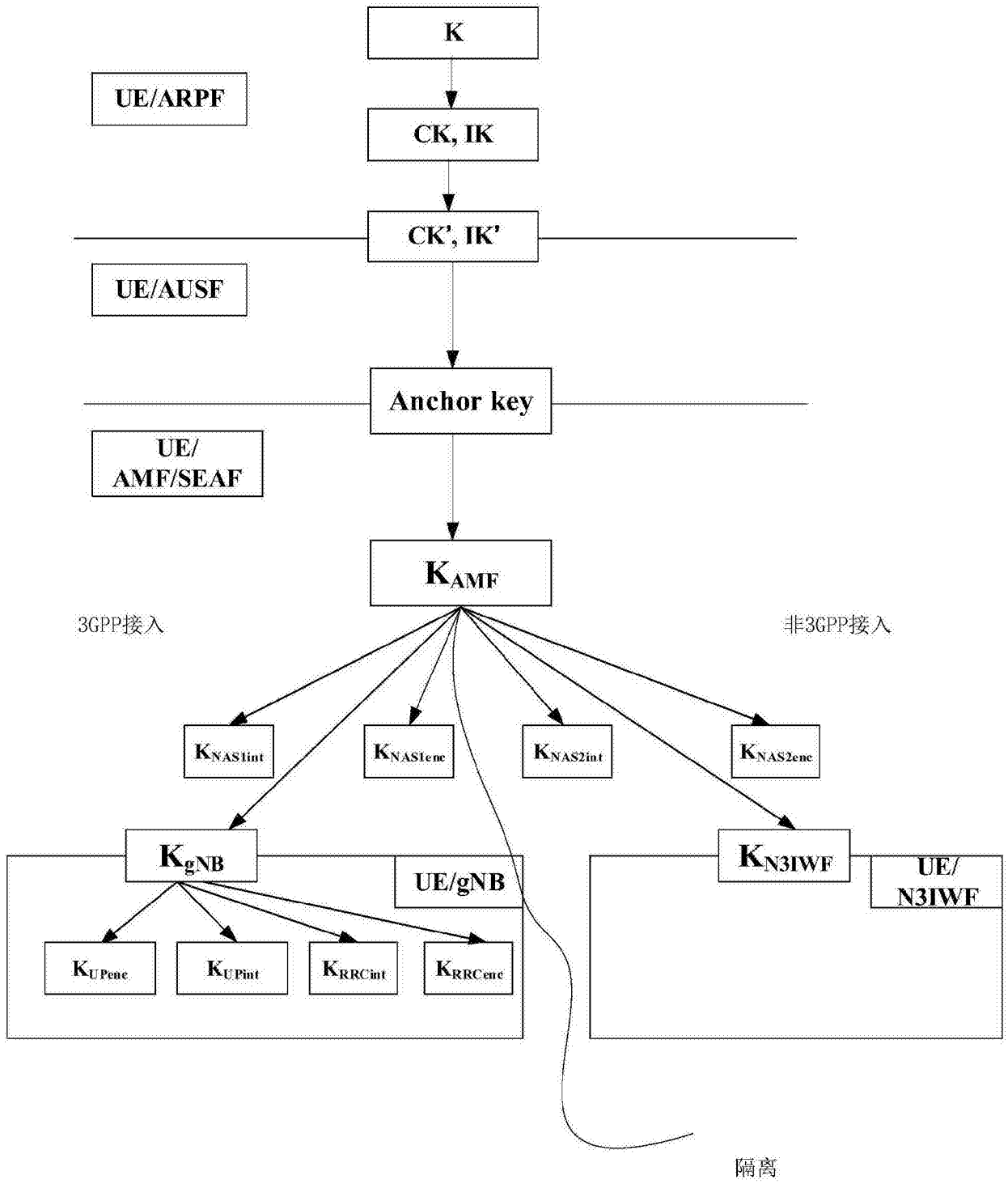

K
UE/ARPF
CK, IK
CK', IK'
UE/AUSF
Anchor key
UE/
AMF/SEAF
K_AMF
3GPP接入
非3GPP接入
K_NAS1int
K_NAS1enc
K_NAS2int
K_NAS2enc
K_gNB
UE/gNB
K_N3IWF
UE/
N3IWF
K_UPenc
K_UPint
K_RRCint
K_RRCenc
隔离

图7

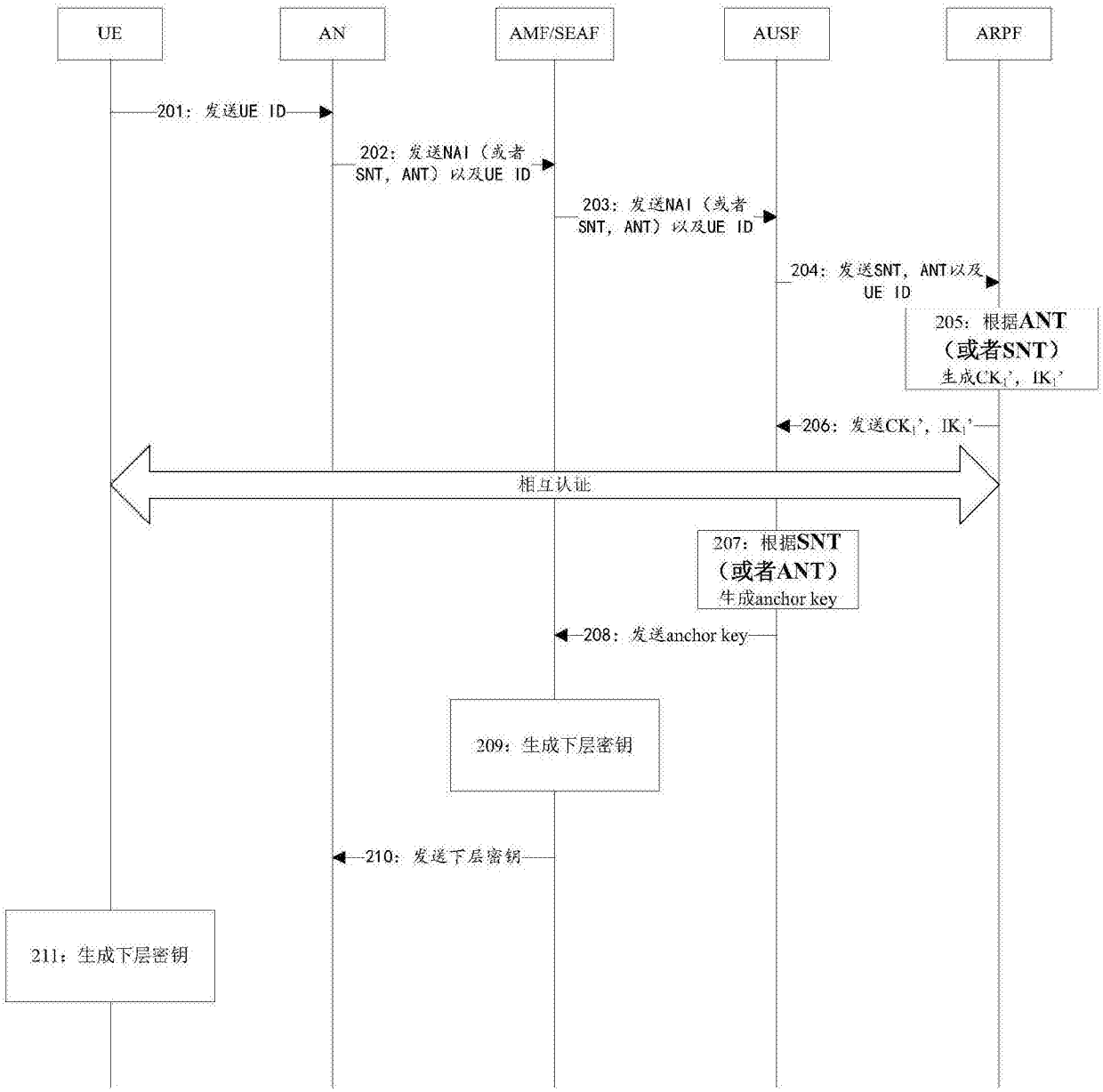

UE
AN
AMF/SEAF
AUSF
ARPF
201：发送UE ID
202：发送NAI（或者SNT，ANT）以及UE ID
203：发送NAI（或者SNT，ANT）以及UE ID
204：发送SNT，ANT以及UE ID
205：根据ANT（或者SNT）生成CK1'，IK1'
206：发送CK1'，IK1'
相互认证
207：根据SNT（或者ANT）生成anchor key
208：发送anchor key
209：生成下层密钥
210：发送下层密钥
211：生成下层密钥

图8

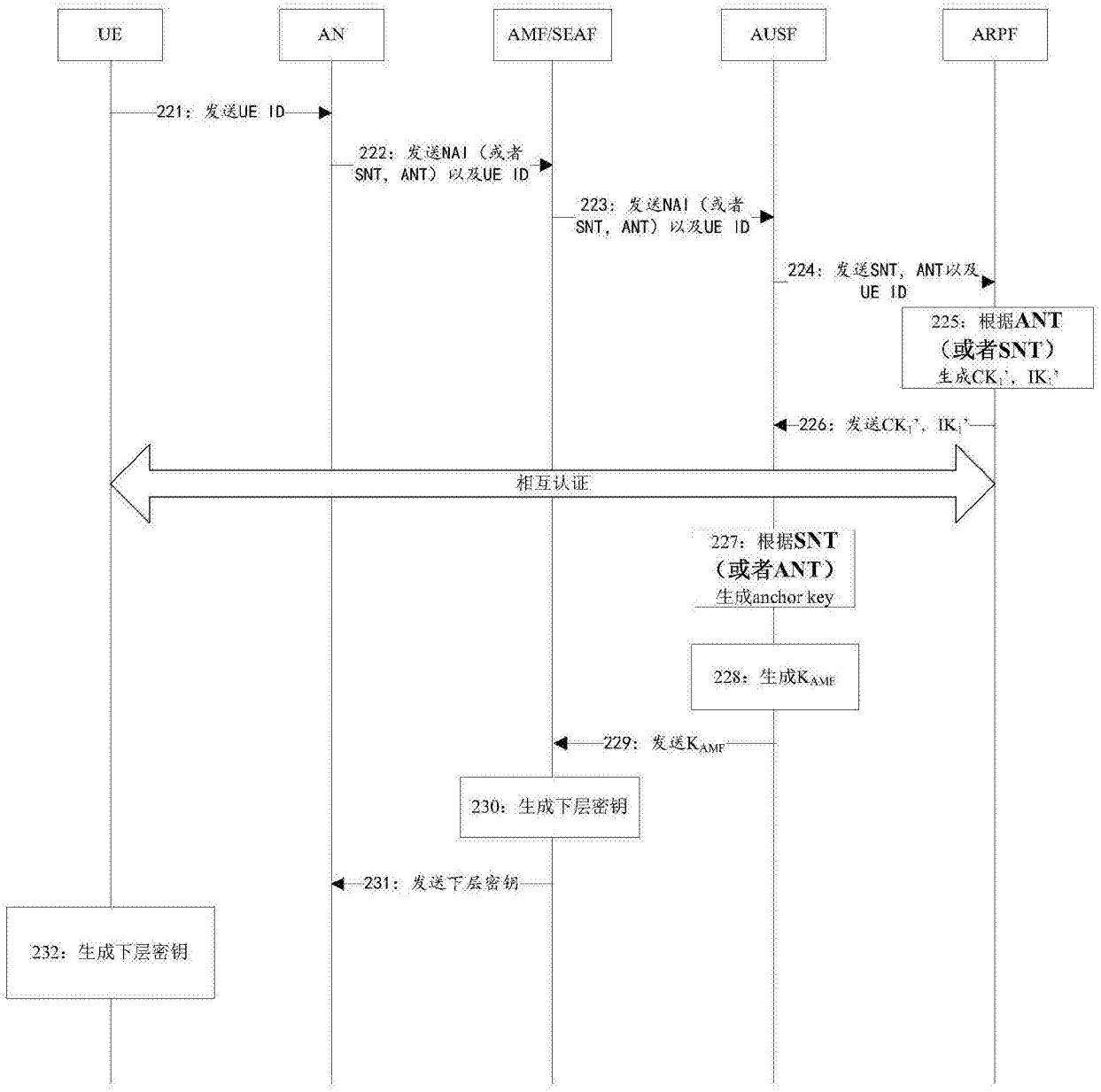

UE
AN
AMF/SEAF
AUSF
ARPF
221：发送UE ID
222：发送NAI（或者SNT，ANT）以及UE ID
223：发送NAI（或者SNT，ANT）以及UE ID
224：发送SNT，ANT以及UE ID
225：根据ANT（或者SNT）生成CK1'，IK1'
226：发送CK1'，IK1'
相互认证
227：根据SNT（或者ANT）生成anchor key
228：生成KAME
229：发送KAMF
230：生成下层密钥
231：发送下层密钥
232：生成下层密钥

图9

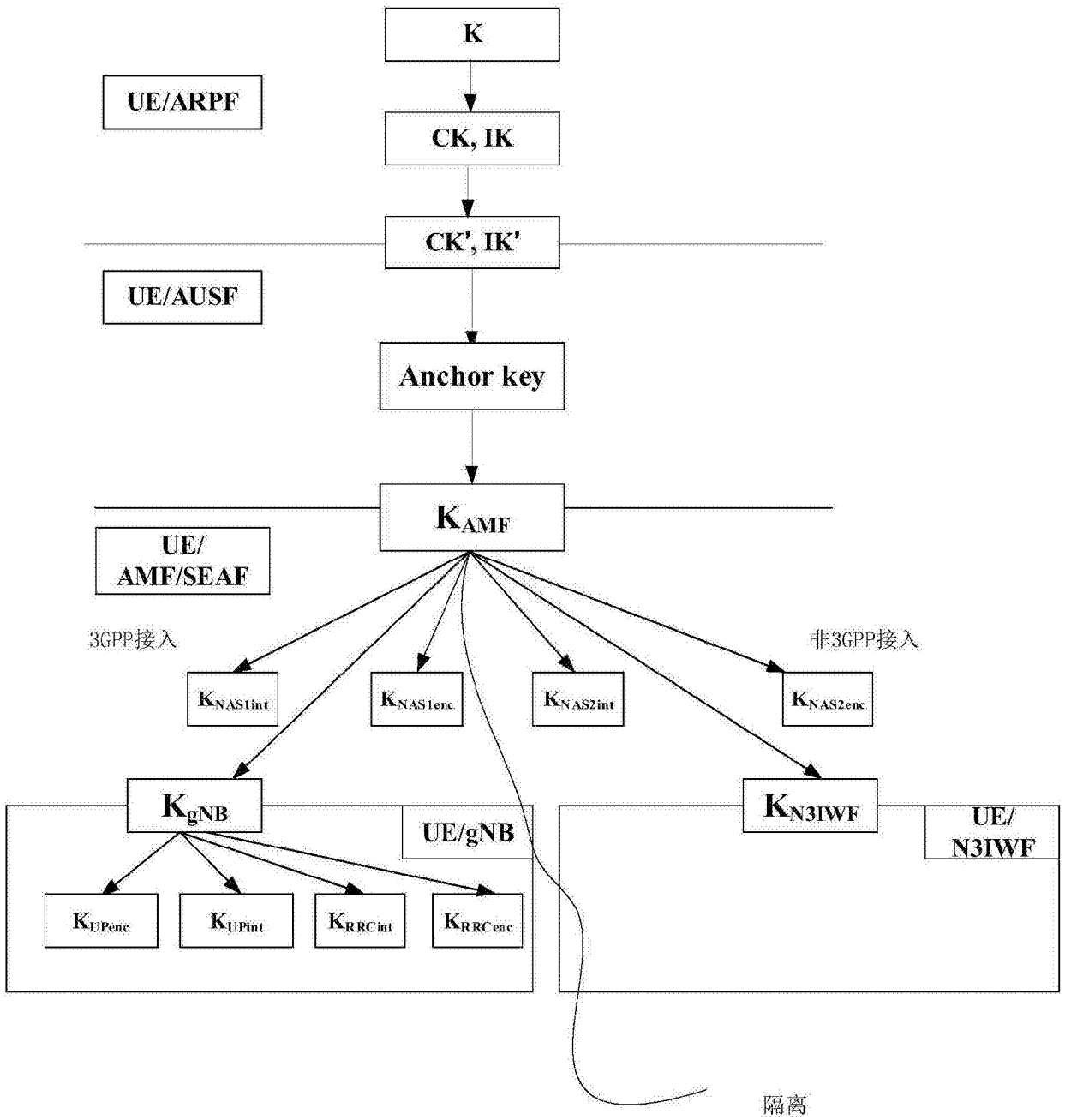

K
UE/ARPF
CK, IK
CK', IK'
UE/AUSF
Anchor key
K_{AMF}
UE/
AMF/SEAF
3GPP接入
非3GPP接入
$K_{NAS1int}$
$K_{NAS1enc}$
$K_{NAS2int}$
$K_{NAS2enc}$
K_{gNB}
UE/gNB
K_{N3IWF}
UE/
N3IWF
K_{UPenc}
K_{UPint}
K_{RRCint}
K_{RRCenc}
隔离

图10

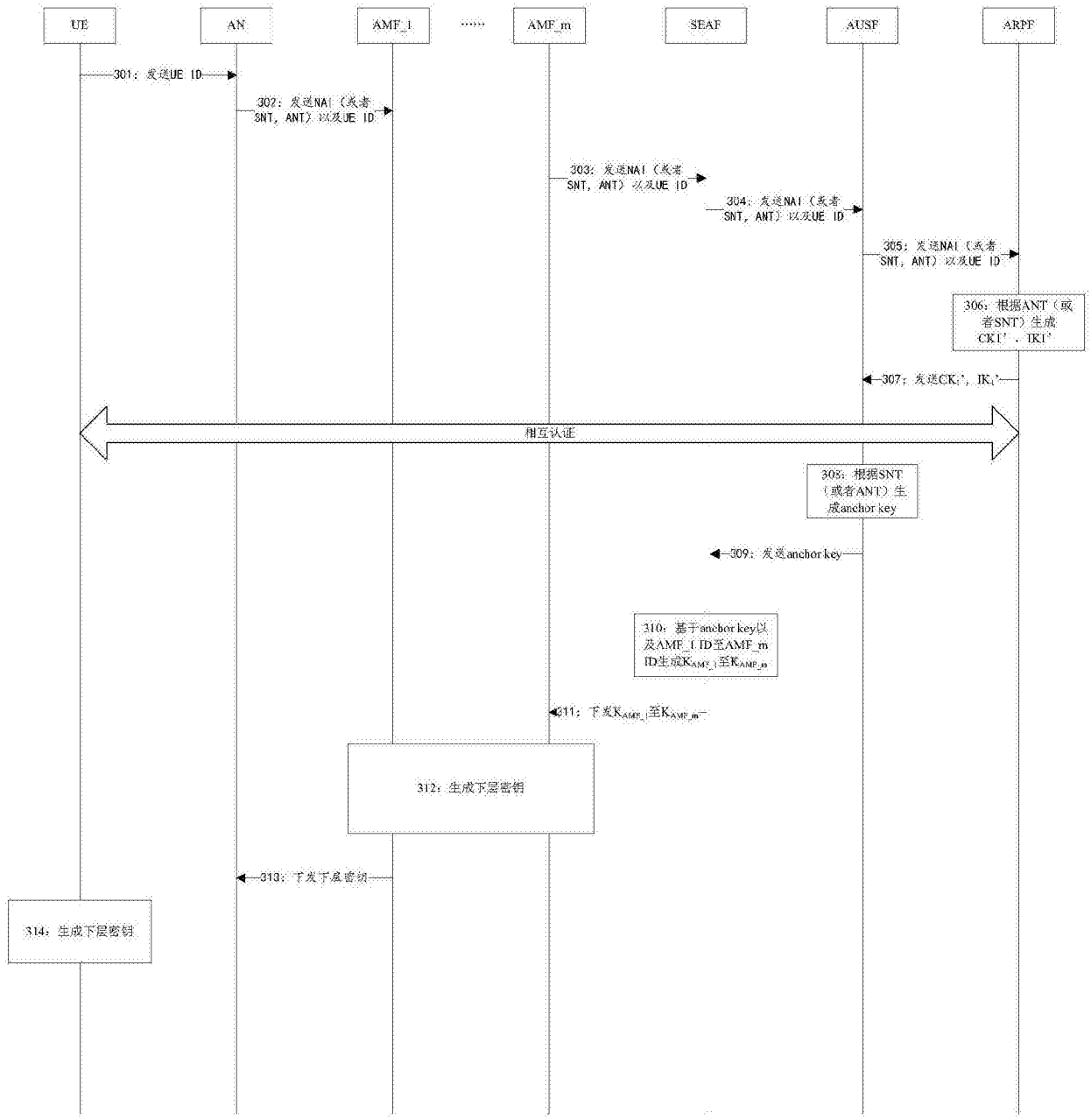

UE
AN
AMF_1
……
AMF_m
SEAF
AUSF
ARPF
301：发送UE ID
302：发送NAI（或者SNT，ANT）以及UE ID
303：发送NAI（或者SNT，ANT）以及UE ID
304：发送NAI（或者SNT，ANT）以及UE ID
305：发送NAI（或者SNT，ANT）以及UE ID
306：根据ANT（或者SNT）生成CK1'，IK1'
307：发送CK1'，IK1'
相互认证
308：根据SNT（或者ANT）生成anchor key
309：发送anchor key
310：基于anchor key以及AMF_1 ID至AMF_m ID生成K_AMF_1至K_AMF_m
311：下发K_AMF_1至K_AMF_m
312：生成下层密钥
313：下发下层密钥
314：生成下层密钥

图11

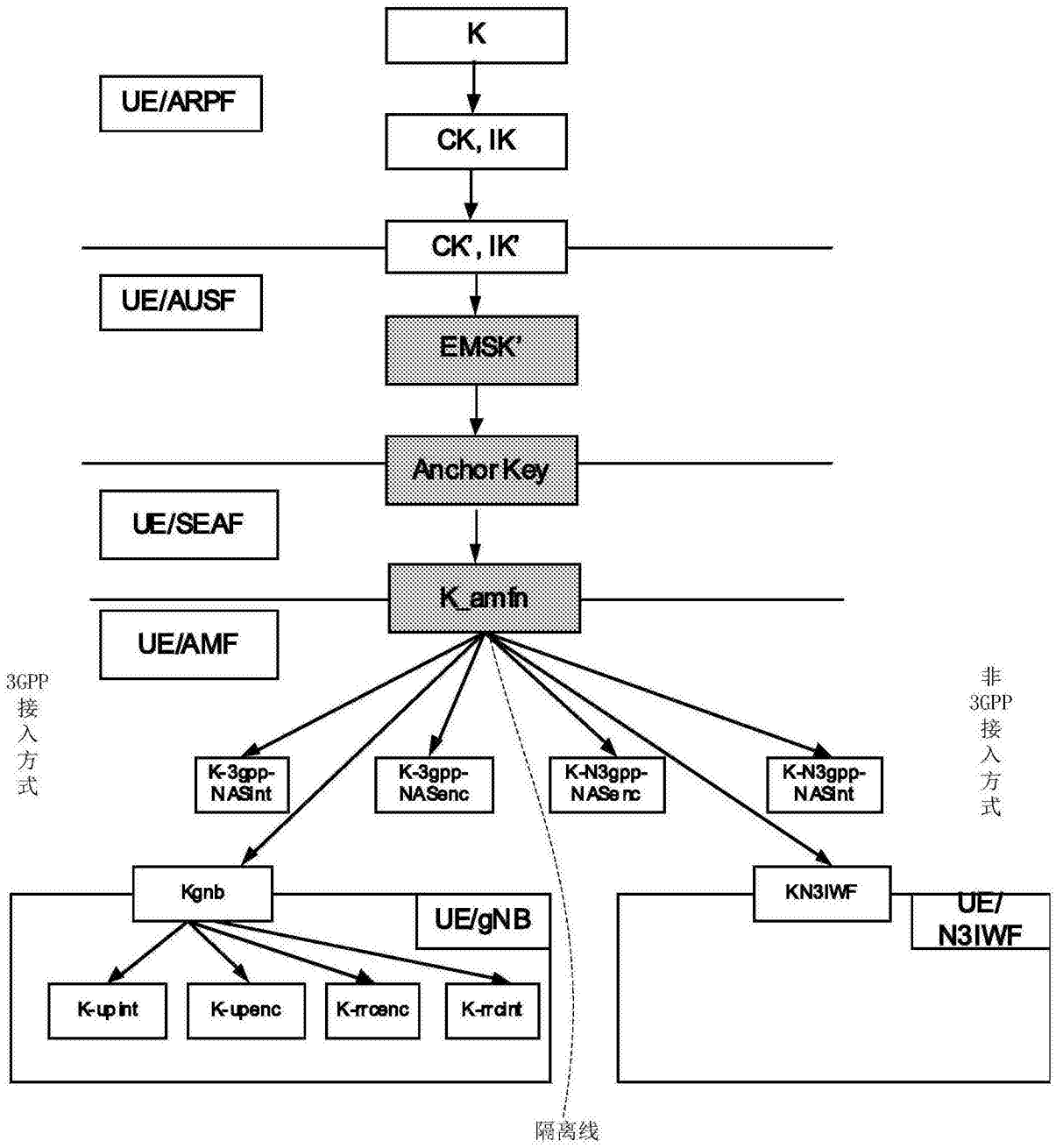

K
UE/ARPF
CK, IK
CK', IK'
UE/AUSF
EMSK'
Anchor Key
UE/SEAF
K_amfn
UE/AMF
3GPP 接入方式
非3GPP接入方式
K-3gpp-NASint
K-3gpp-NASenc
K-N3gpp-NASenc
K-N3gpp-NASint
Kgnb
UE/gNB
KN3IWF
UE/N3IWF
K-upint
K-upenc
K-rrcenc
K-rrcint
隔离线

图12

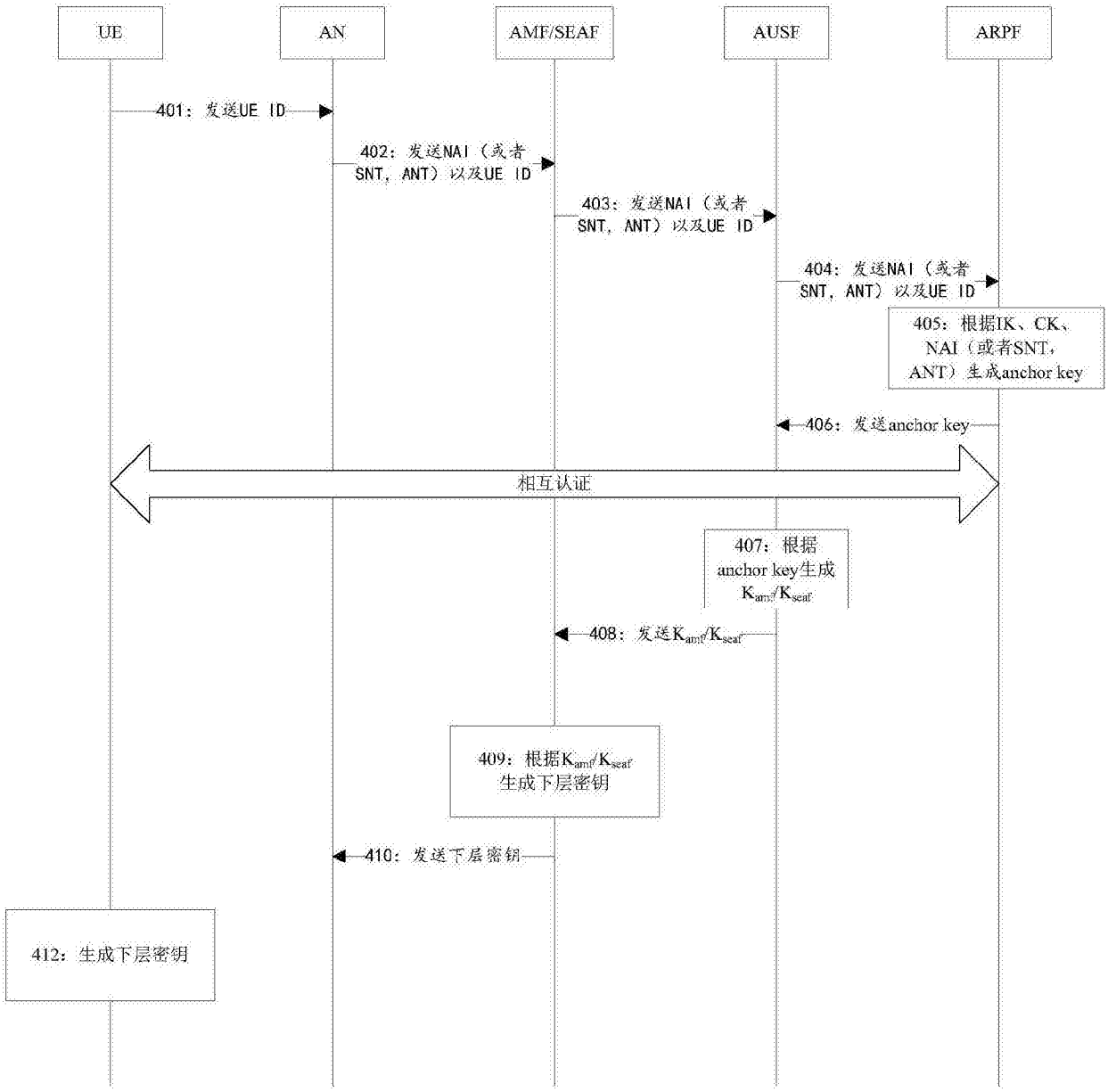

UE
AN
AMF/SEAF
AUSF
ARPF
401：发送UE ID
402：发送NAI（或者SNT，ANT）以及UE ID
403：发送NAI（或者SNT，ANT）以及UE ID
404：发送NAI（或者SNT，ANT）以及UE ID
405：根据IK、CK、NAI（或者SNT，ANT）生成anchor key
406：发送anchor key
相互认证
407：根据anchor key生成 K_{amf}/K_{seaf}
408：发送 K_{amf}/K_{seaf}
409：根据 K_{amf}/K_{seaf} 生成下层密钥
410：发送下层密钥
412：生成下层密钥

图13

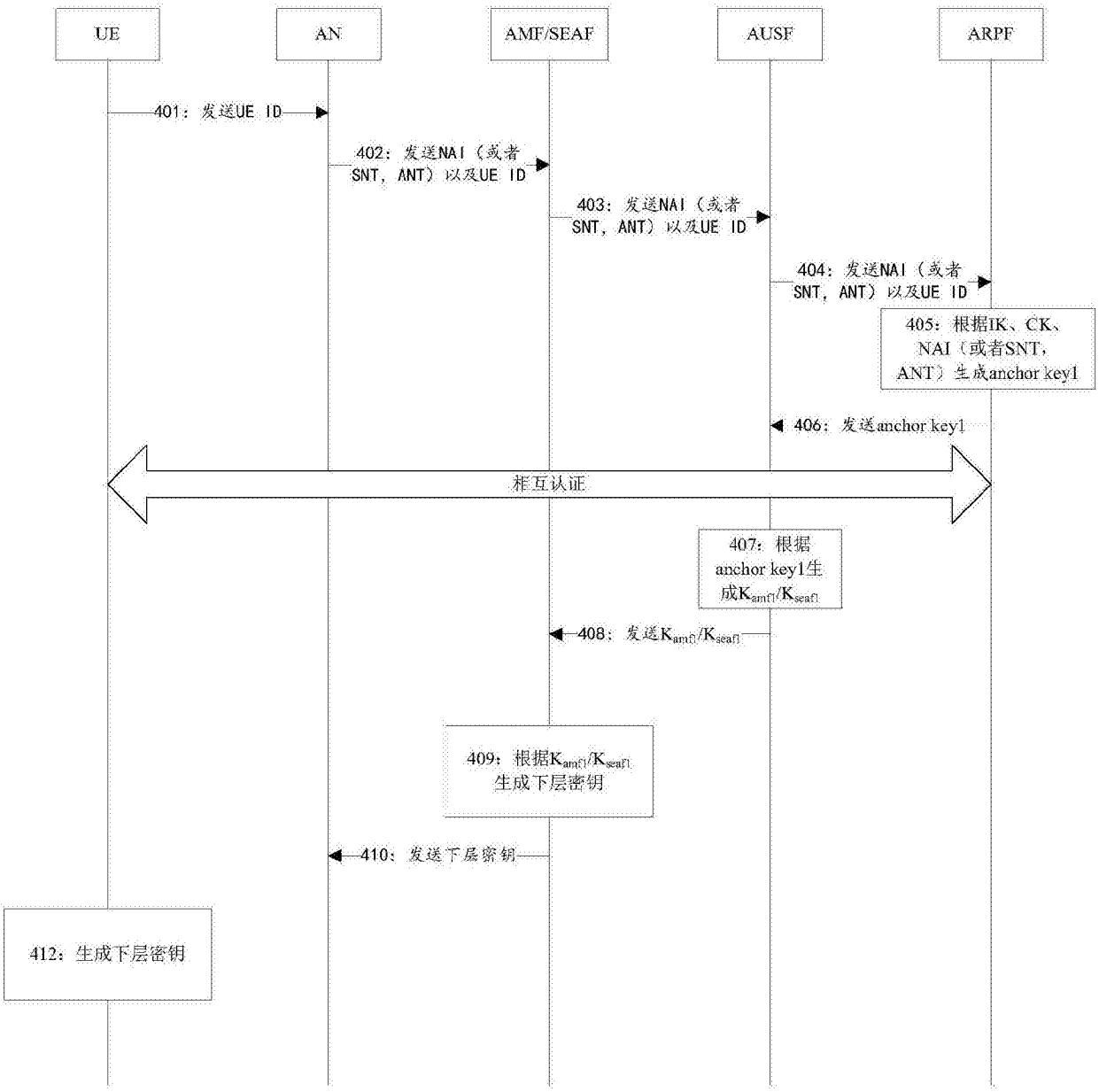

UE
AN
AMF/SEAF
AUSF
ARPF
401：发送UE ID
402：发送NAI（或者SNT，ANT）以及UE ID
403：发送NAI（或者SNT，ANT）以及UE ID
404：发送NAI（或者SNT，ANT）以及UE ID
405：根据IK、CK、NAI（或者SNT，ANT）生成anchor key1
406：发送anchor key1
相互认证
407：根据anchor key1生成Kamf()/Kseaf()
408：发送Kamf()/Kseaf()
409：根据Kamf()/Kseaf()生成下层密钥
410：发送下层密钥
412：生成下层密钥

图14A

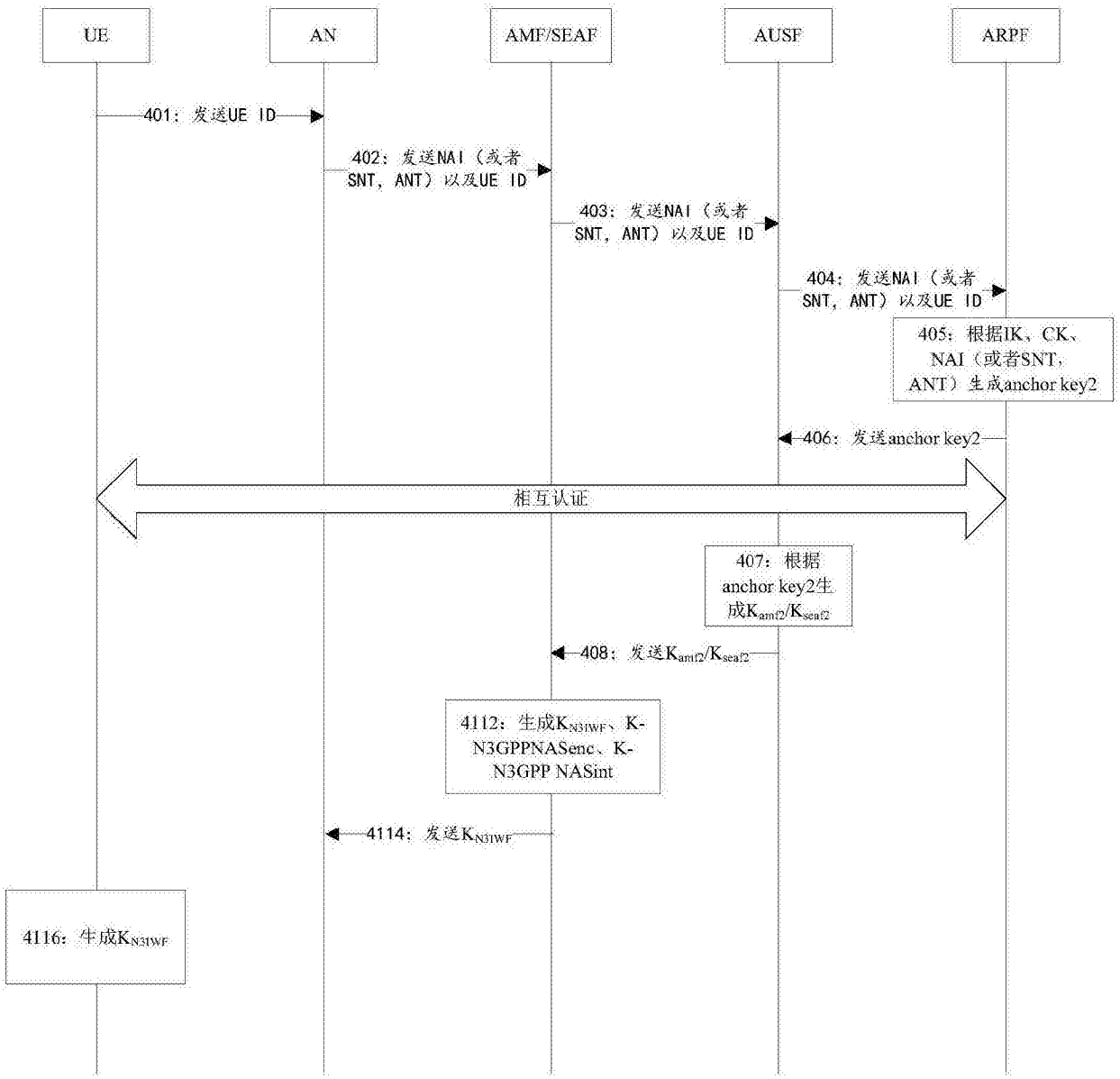

UE
AN
AMF/SEAF
AUSF
ARPF
401：发送UE ID
402：发送NAI（或者SNT，ANT）以及UE ID
403：发送NAI（或者SNT，ANT）以及UE ID
404：发送NAI（或者SNT，ANT）以及UE ID
405：根据IK、CK、NAI（或者SNT，ANT）生成anchor key2
406：发送anchor key2
相互认证
407：根据anchor key2生成K_{amf2}/K_{seaf2}
408：发送K_{amf2}/K_{seaf2}
4112：生成K_{N3IWF}、K-N3GPPNASenc、K-N3GPP NASint
4114：发送K_{N3IWF}
4116：生成K_{N3IWF}

图14B

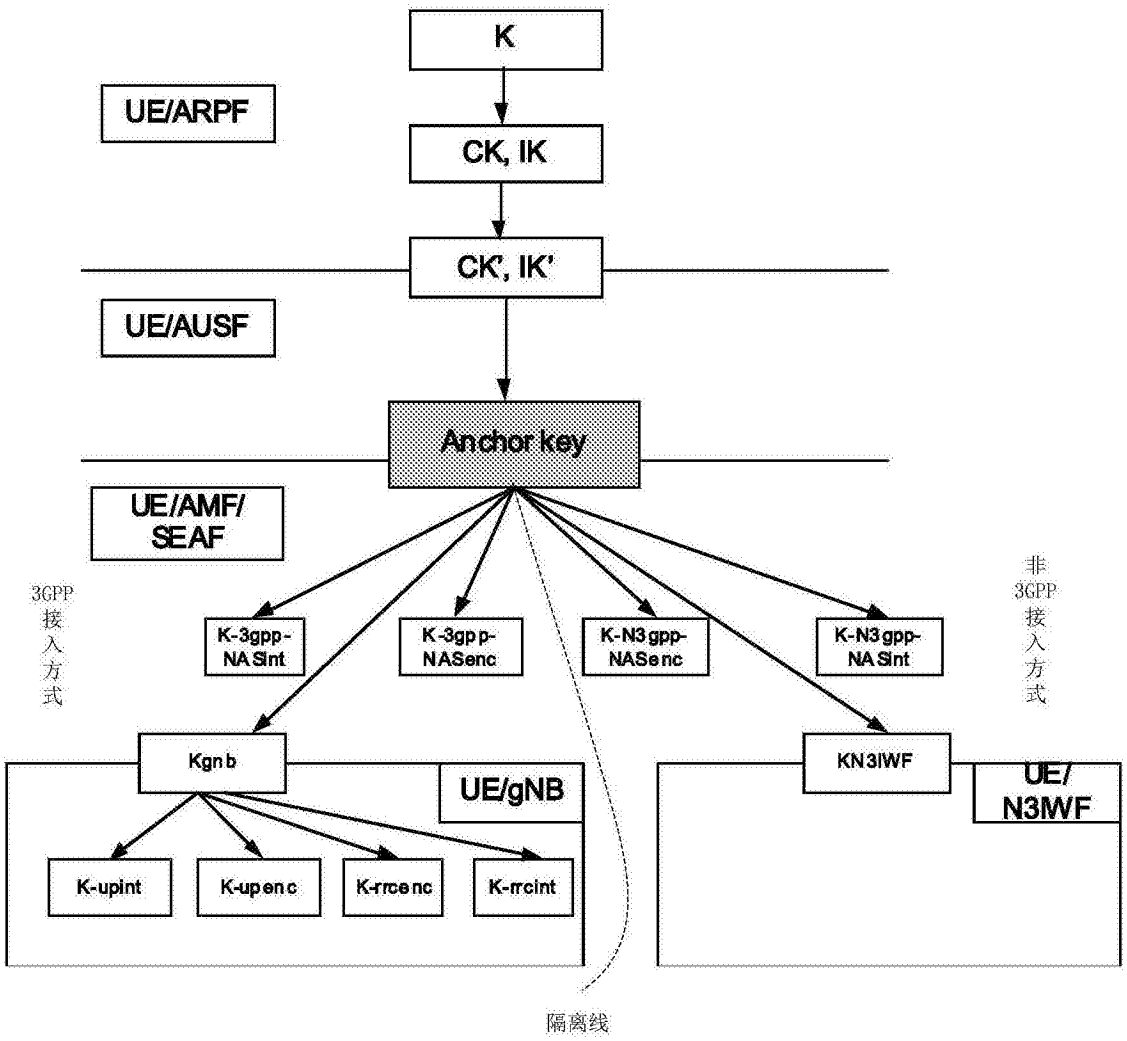

K
UE/ARPF
CK, IK
CK', IK'
UE/AUSF
Anchor key
UE/AMF/
SEAF
3GPP
接
入
方
式
K-3gpp-
NASint
K-3gpp-
NASenc
K-N3gpp-
NASenc
K-N3gpp-
NASint
非
3GPP
接
入
方
式
Kgnb
UE/gNB
KN3IWF
UE/
N3IWF
K-upint
K-upenc
K-rrcenc
K-rrcint
隔离线

图15

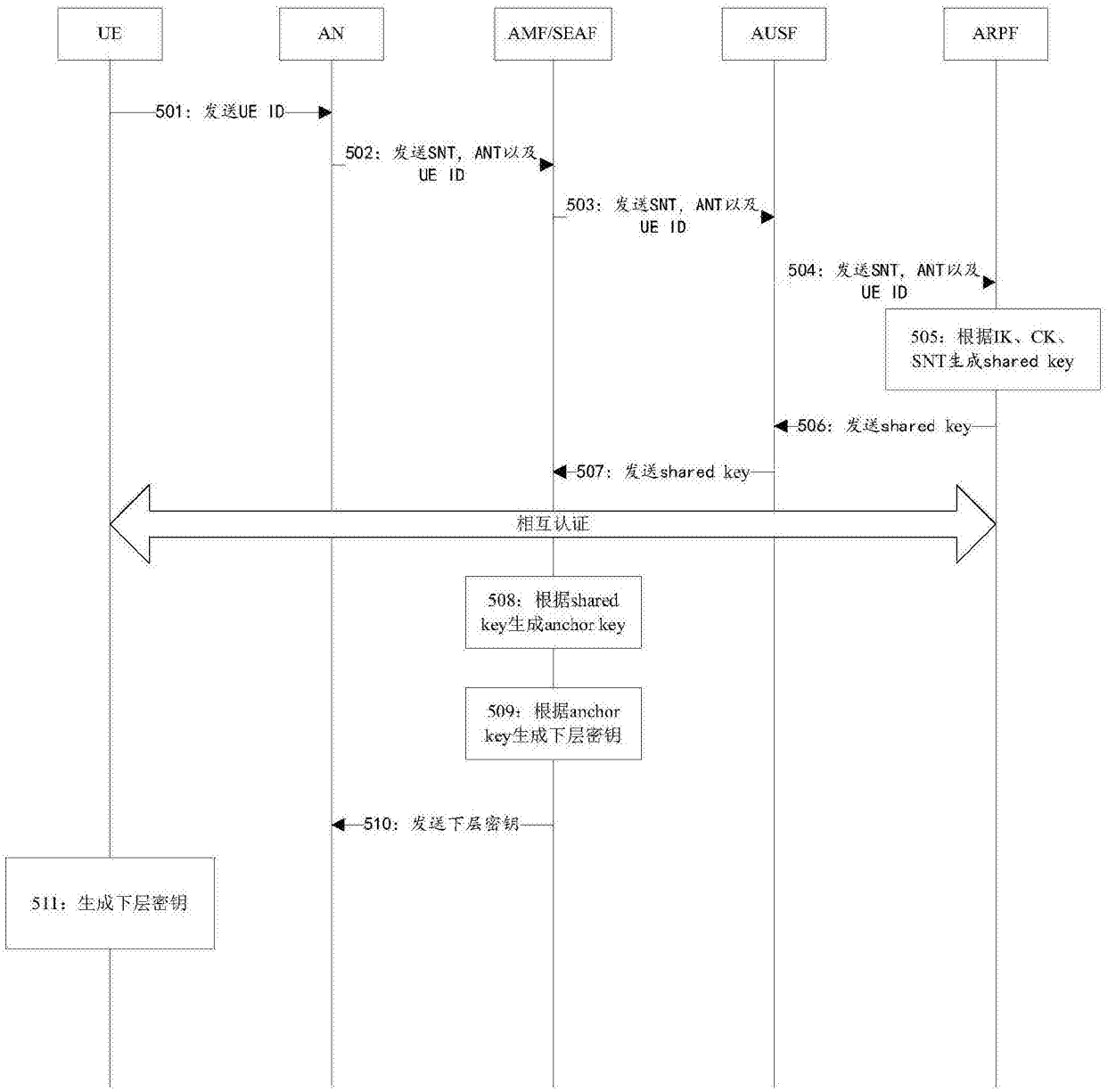

UE
AN
AMF/SEAF
AUSF
ARPF
501：发送UE ID
502：发送SNT，ANT以及UE ID
503：发送SNT，ANT以及UE ID
504：发送SNT，ANT以及UE ID
505：根据IK、CK、SNT生成shared key
506：发送shared key
507：发送shared key
相互认证
508：根据shared key生成anchor key
509：根据anchor key生成下层密钥
510：发送下层密钥
511：生成下层密钥

图16

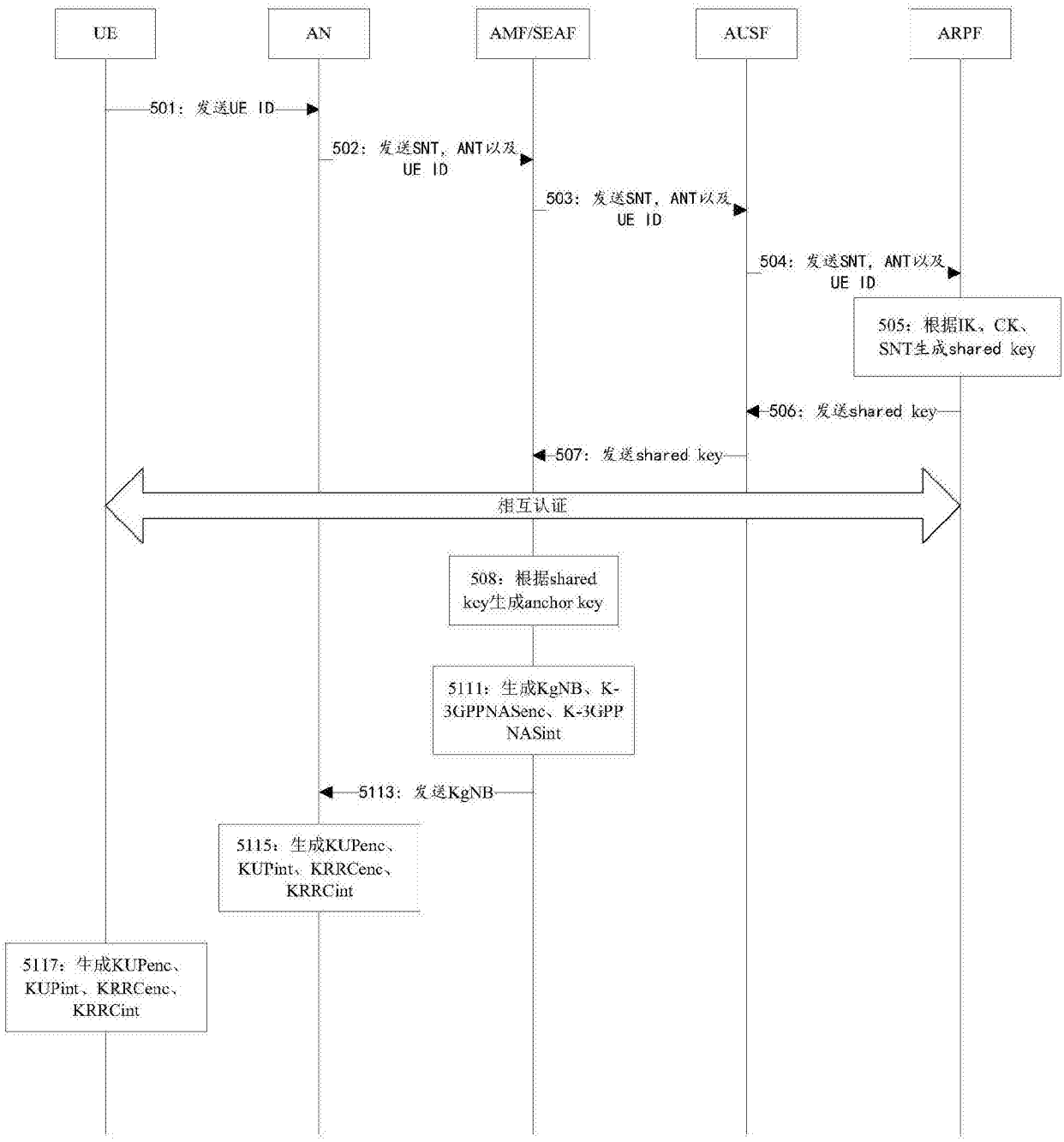

UE
AN
AMF/SEAF
AUSF
ARPF
501：发送UE ID
502：发送SNT，ANT以及UE ID
503：发送SNT，ANT以及UE ID
504：发送SNT，ANT以及UE ID
505：根据IK、CK、SNT生成shared key
506：发送shared key
507：发送shared key
相互认证
508：根据shared key生成anchor key
5111：生成KgNB、K-3GPPNASenc、K-3GPP NASint
5113：发送KgNB
5115：生成KUPenc、KUPint、KRRCenc、KRRCint
5117：生成KUPenc、KUPint、KRRCenc、KRRCint

图17A

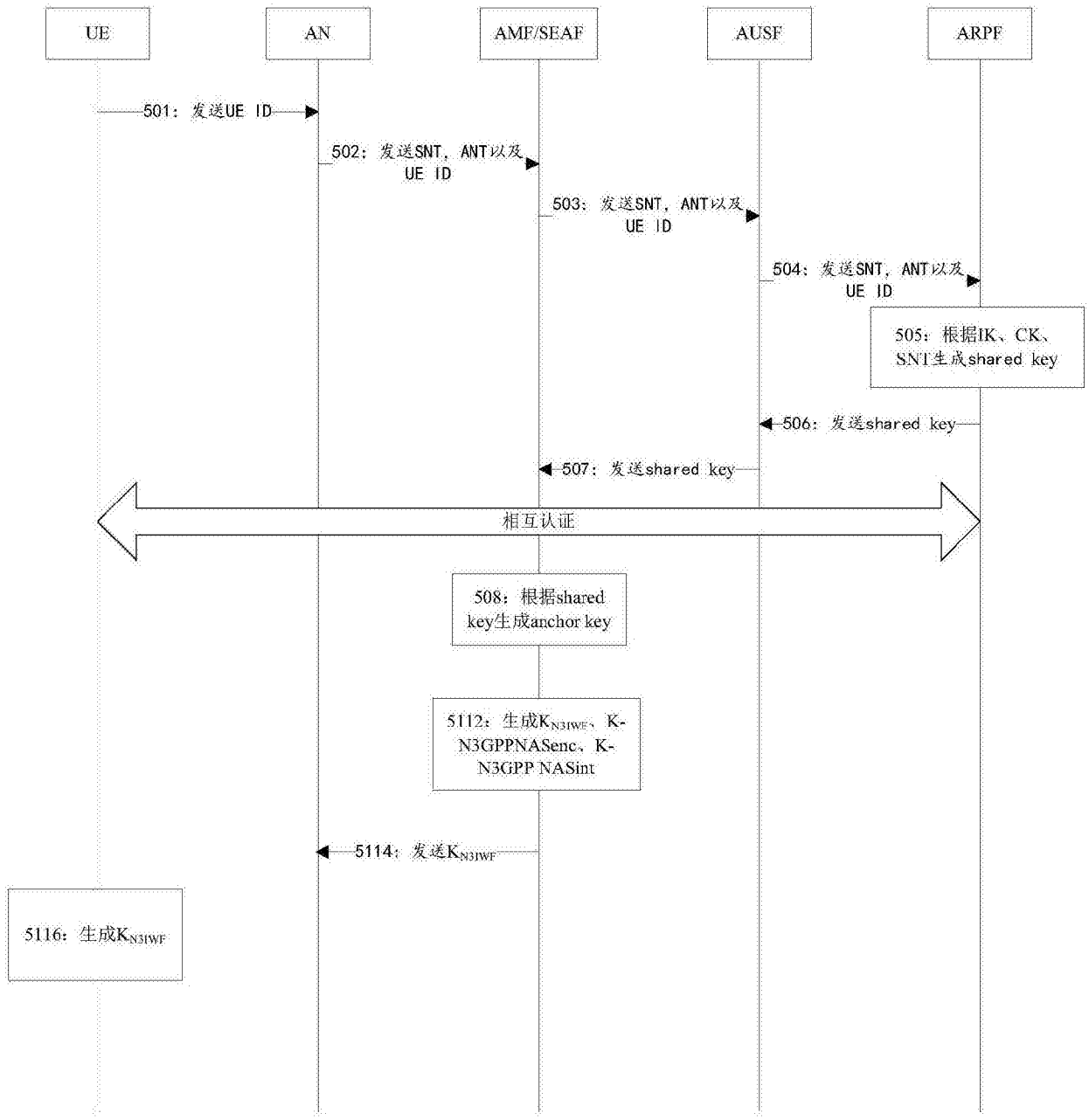

UE
AN
AMF/SEAF
AUSF
ARPF
501：发送UE ID
502：发送SNT，ANT以及UE ID
503：发送SNT，ANT以及UE ID
504：发送SNT，ANT以及UE ID
505：根据IK、CK、SNT生成shared key
506：发送shared key
507：发送shared key
相互认证
508：根据shared key生成anchor key
5112：生成K_N3IWF、K-N3GPPNASenc、K-N3GPP NASint
5114：发送K_N3IWF
5116：生成K_N3IWF

图17B

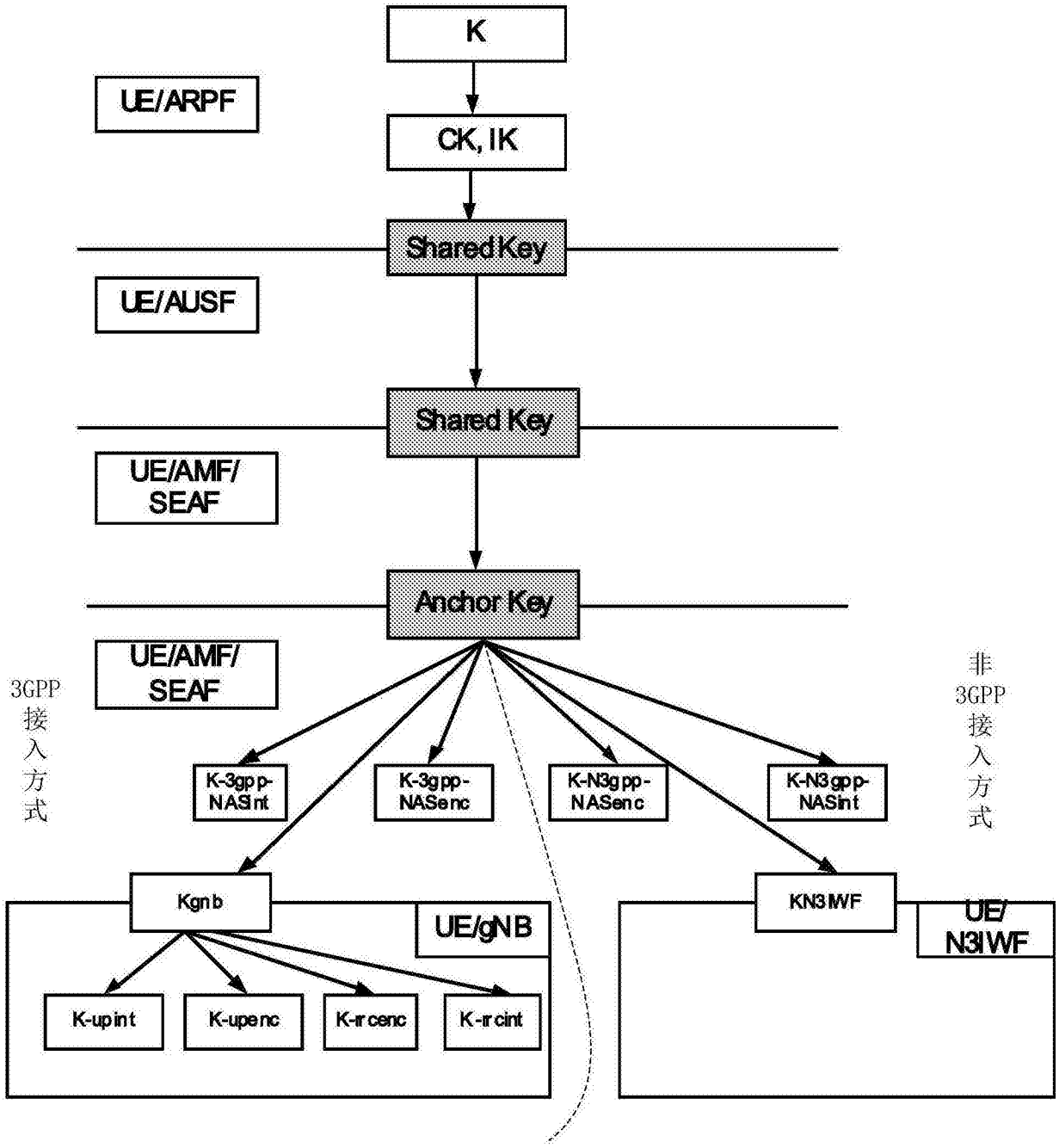

K
UE/ARPF
CK, IK
Shared Key
UE/AUSF
Shared Key
UE/AMF/
SEAF
Anchor Key
UE/AMF/
SEAF
3GPP
接
入
方
式
非
3GPP
接
入
方
式
K-3gpp-
NASint
K-3gpp-
NASenc
K-N3gpp-
NASenc
K-N3gpp-
NASint
Kgnb
UE/gNB
KN3IWF
UE/
N3IWF
K-upint
K-upenc
K-rrcenc
K-rrcint
隔离线

图18

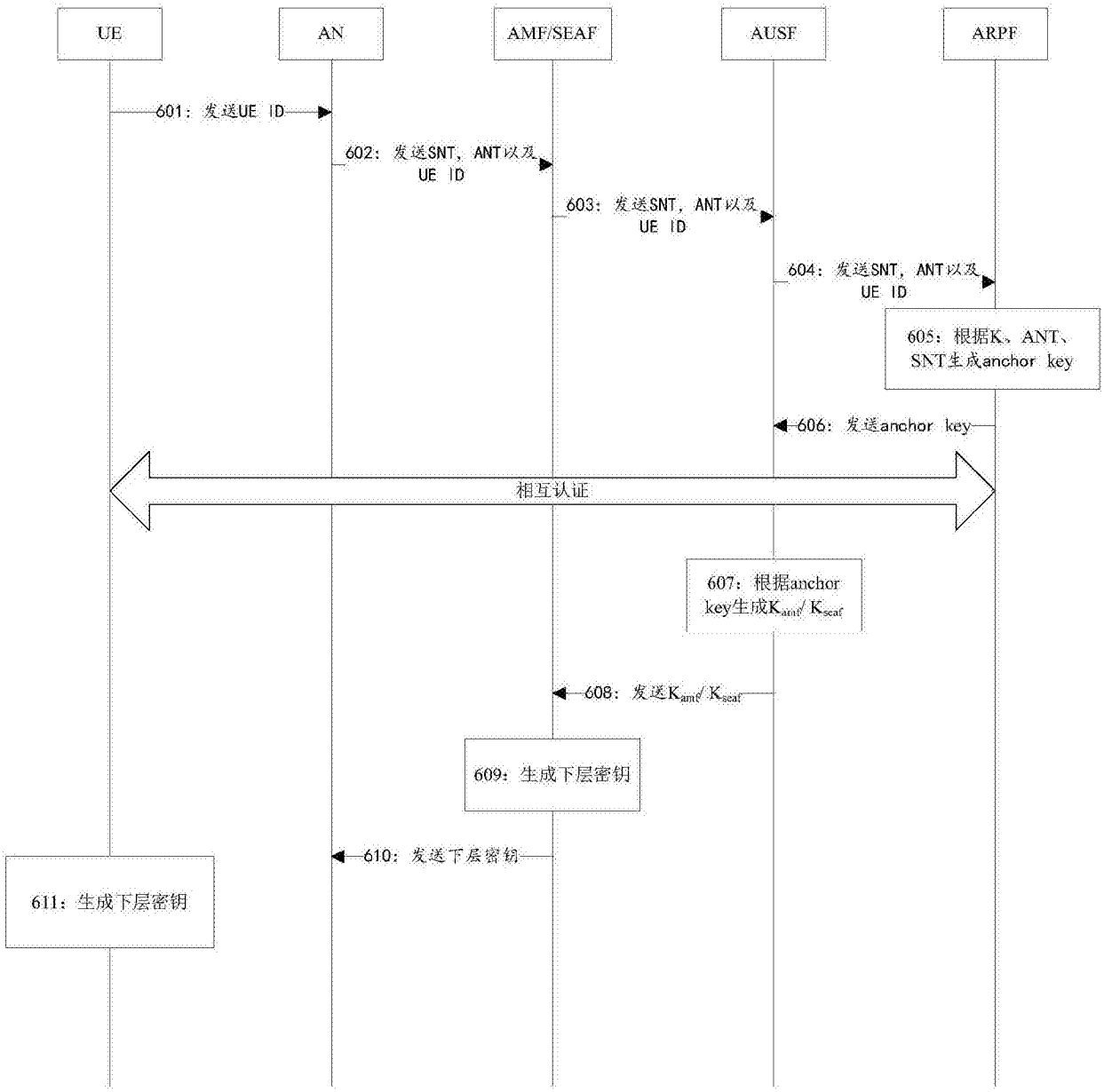

UE
AN
AMF/SEAF
AUSF
ARPF
601：发送UE ID
602：发送SNT，ANT以及UE ID
603：发送SNT，ANT以及UE ID
604：发送SNT，ANT以及UE ID
605：根据K、ANT、SNT生成anchor key
606：发送anchor key
相互认证
607：根据anchor key生成Kamf/Kseaf
608：发送Kamf/Kseaf
609：生成下层密钥
610：发送下层密钥
611：生成下层密钥

图19

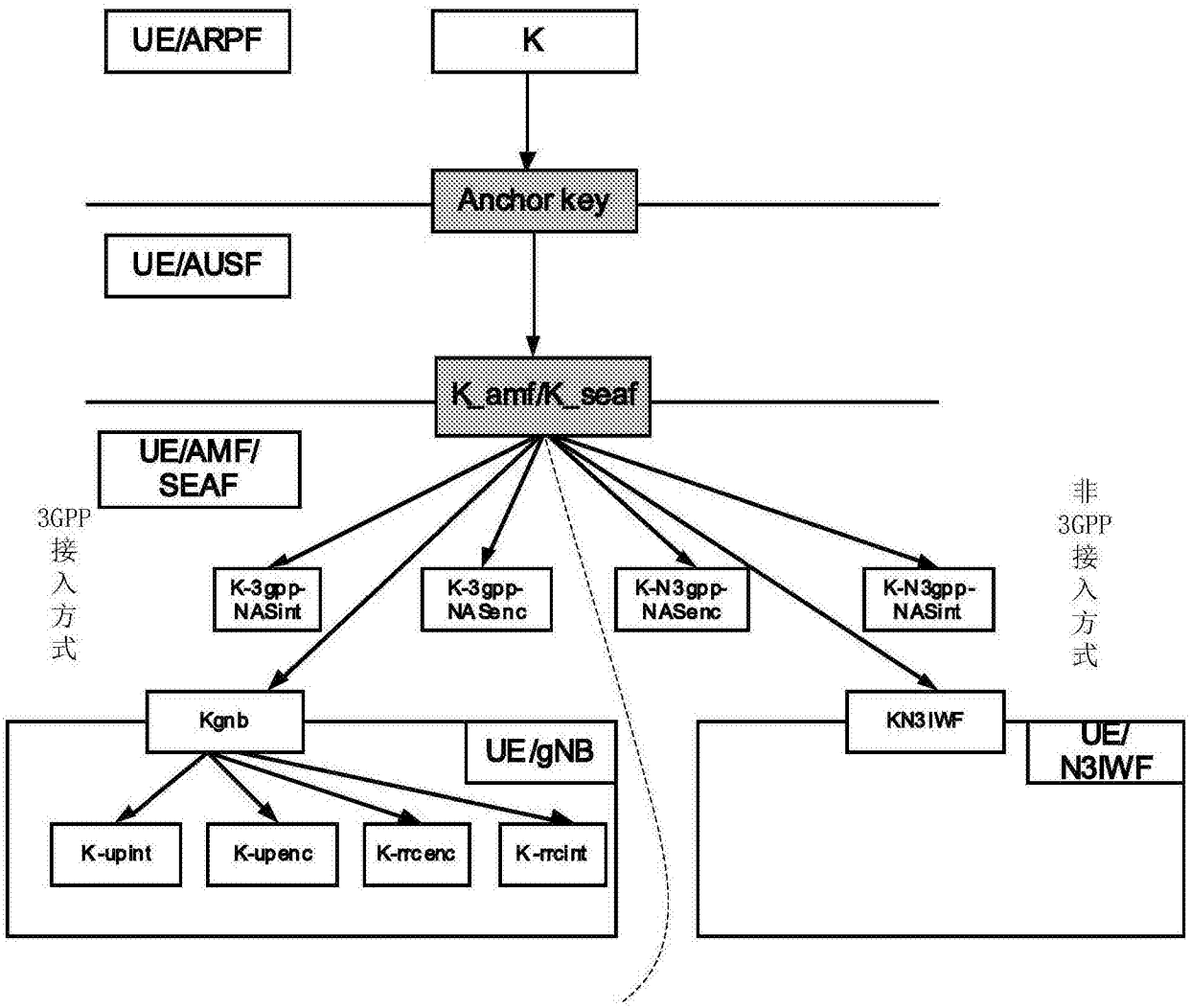

UE/ARPF
K
Anchor key
UE/AUSF
K_amf/K_seaf
UE/AMF/
SEAF
3GPP
接
入
方
式
K-3gpp-
NASint
K-3gpp-
NASenc
K-N3gpp-
NASenc
K-N3gpp-
NASint
非
3GPP
接
入
方
式
Kgnb
UE/gNB
K-upint
K-upenc
K-rrcenc
K-rrcint
KN3IWF
UE/
N3IWF
隔离线

图20

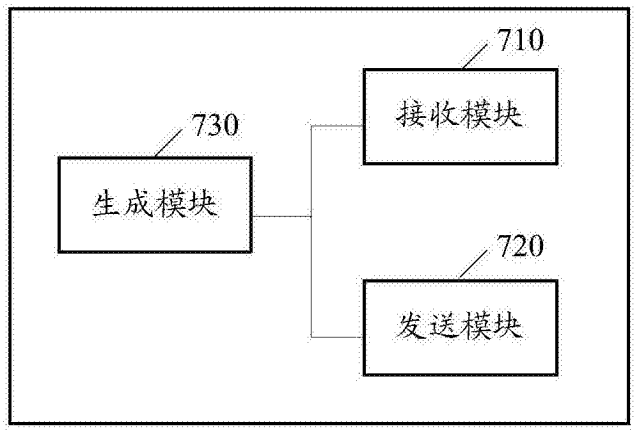

710
接收模块
730
生成模块
720
发送模块

图21

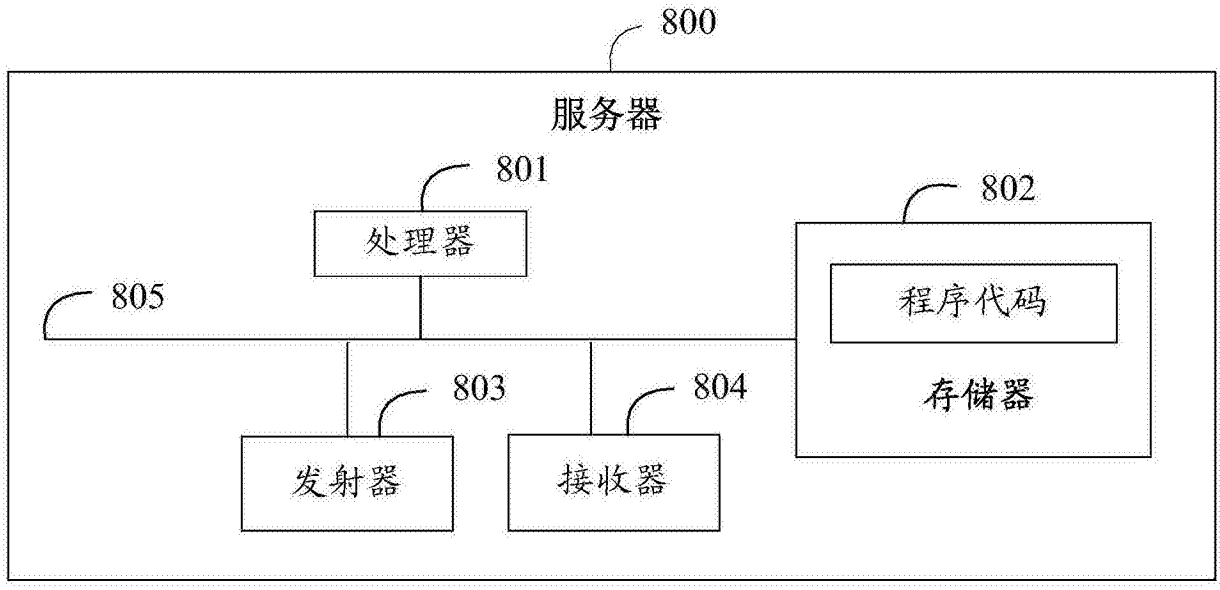


图22