(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 108012266 A
(43)申请公布日 2018.05.08

(21)申请号 201610926805.8

(22)申请日 2016.10.31

(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 菲利普·金兹伯格 瓦特里·尼米 张博

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
H04W 12/06(2009.01)

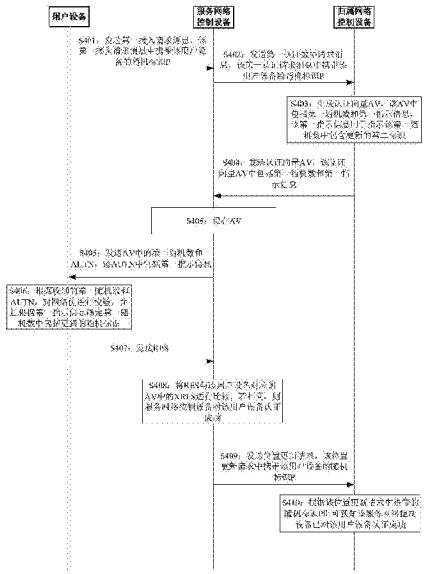
权利要求书7页 说明书29页 附图7页

(54)发明名称

一种数据传输方法及相关设备

(57)摘要

本发明公开了一种数据传输方法及相关设备，其中，该方法包括：归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息，所述第一认证数据请求消息中包括用户设备对应的第一标识；所述归属网络控制设备通过所述服务网络控制设备向所述第一标识对应的所述用户设备发送第一随机数和第一指示信息，所述第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据，所述第一数据组包括所述用户设备对应的随机标识，所述第一指示信息用于指示所述用户设备根据所述第一指示信息确定所述第一随机数中包含所述随机标识。采用本发明，可以节省用户设备确定接收到的随机数中包含更新的随机标识的计算量，节约用户设备的开销。



CN 108012266 A

1.一种数据传输方法,其特征在于,包括:

归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息,所述第一认证数据请求消息中包括用户设备对应的第一标识;

所述归属网络控制设备生成所述用户设备对应的第一随机标识;

所述归属网络控制设备通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息,所述第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据,所述第一数据组包括所述第一随机标识,所述第一指示信息用于指示所述用户设备根据所述第一指示信息确定所述第一随机数中包含所述第一随机标识。

2.根据权利要求1所述的方法,其特征在于,所述第一随机数中还包括采用第二共享密钥对所述第一加密数据进行完整性保护得到的第一完整性保护数据。

3.根据权利要求2所述的方法,其特征在于,所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥;或者所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识完整性密钥,所述随机标识完整性密钥用于对所述用户设备的随机标识进行完整性保护。

4.根据权利要求1至3任一项所述的方法,其特征在于,所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥;或者所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识加密密钥,所述随机标识加密密钥用于对所述用户设备的随机标识进行加密。

5.根据权利要求1或2所述的方法,其特征在于,所述归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之前,还包括:

所述归属网络控制设备接收所述服务网络控制设备发送的第二认证数据请求消息,所述第二认证数据请求消息中包括所述用户设备对应的第二标识;

所述归属网络控制设备采用第一密钥派生参数生成所述第一共享密钥;

所述归属网络控制设备通过所述服务网络控制设备向所述用户设备发送第二指示信息,所述第二指示信息用于指示所述用户设备采用所述第一密钥派生参数生成所述第一共享密钥。

6.根据权利要求2所述的方法,其特征在于,所述归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之前,还包括:

所述归属网络控制设备接收所述服务网络控制设备发送的第二认证数据请求消息,所述第二认证数据请求消息中包括所述用户设备对应的第二标识;

所述归属网络控制设备采用第二密钥派生参数生成所述第二共享密钥;

所述归属网络控制设备通过所述服务网络控制设备向所述用户设备发送第二指示信息,所述第二指示信息用于指示所述用户设备采用所述第二密钥派生参数生成所述第二共享密钥。

7.根据权利要求1或2所述的方法,其特征在于,所述归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之后,所述归属网络控制设备通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息之前,还包括:

所述归属网络控制设备采用第一密钥派生参数生成所述第一共享密钥;所述第一指示信息还用于指示所述用户设备采用所述第一密钥派生参数生成所述第一共享密钥。

8.根据权利要求2所述的方法，其特征在于，所述归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之后，所述归属网络控制设备通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息之前，还包括：

所述归属网络控制设备采用第二密钥派生参数生成所述第二共享密钥；所述第一指示信息还用于指示所述用户设备采用所述第二密钥派生参数生成所述第二共享密钥。

9.根据权利要求1至8任一项所述的方法，其特征在于，所述归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之后，还包括：

所述归属网络控制设备采用第三密钥派生参数生成第三共享密钥，所述第三共享密钥用于所述归属网络控制设备后续向所述用户设备发送更新的第二随机标识时对所述第二随机标识进行加密；所述第一指示信息还用于指示所述用户设备采用所述第三密钥派生参数生成所述第三共享密钥。

10.根据权利要求1至8任一项所述的方法，其特征在于，所述归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之后，还包括：

所述归属网络控制设备采用第四密钥派生参数生成第四共享密钥，所述第四共享密钥用于所述归属网络控制设备后续向所述用户设备发送所述第二随机标识时对所述第二随机标识进行完整性保护；所述第一指示信息还用于指示所述用户设备采用所述第四密钥派生参数生成所述第四共享密钥。

11.一种数据传输方法，其特征在于，包括：

用户设备向服务网络控制设备发送第一接入请求消息，所述第一接入请求消息中包括所述用户设备对应的第一标识；

所述用户设备接收归属网络控制设备通过上述服务网络控制设备发送的第一随机数和第一指示信息，所述第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据，所述第一数据组包括所述用户设备对应的第一随机标识；

所述用户设备根据所述第一指示信息确定所述第一随机数中包含所述第一随机标识；

所述用户设备采用所述第一共享密钥对所述第一加密数据进行解密，得到所述第一随机标识。

12.根据权利要求11所述的方法，其特征在于，所述第一随机数中还包括采用第二共享密钥对所述第一加密数据进行完整性保护得到的第一完整性保护数据；所述用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，还包括：

所述用户设备采用所述第二共享密钥对所述第一完整性保护数据进行完整性验证。

13.根据权利要求12所述的方法，其特征在于，所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥；或者所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识完整性密钥，所述随机标识完整性密钥用于对所述用户设备的随机标识进行完整性保护。

14.根据权利要求11至13任一项所述的方法，其特征在于，所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥；或者所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识加密密钥，所述随机标识加密密钥用于对所述用户设备的随机标识进行加密。

15.根据权利要求11或12所述的方法，其特征在于，所述用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之前，还包括：

所述用户设备向所述服务网络控制设备发送第二接入请求消息，所述第二接入请求消息中包括所述用户设备对应的第二标识；

所述用户设备接收所述归属网络控制设备通过所述服务网络控制设备发送的第二指示信息；

所述用户设备根据所述第二指示信息采用第一密钥派生参数生成所述第一共享密钥。

16.根据权利要求12所述的方法，其特征在于，所述用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之前，还包括：

所述用户设备向所述服务网络控制设备发送第二接入请求消息，所述第二接入请求消息中包括所述用户设备对应的第二标识；

所述用户设备接收所述归属网络控制设备通过所述服务网络控制设备发送的第二指示信息；

所述用户设备根据所述第二指示信息采用第二密钥派生参数生成所述第二共享密钥。

17.根据权利要求11或12所述的方法，其特征在于，所述第一指示信息还用于指示所述用户设备采用第一密钥派生参数生成所述第一共享密钥；所述用户设备采用所述第一共享密钥对所述第一加密数据进行解密，得到所述第一随机标识之前，还包括：

所述用户设备根据所述第一指示信息，采用所述第一密钥派生参数生成所述第一共享密钥。

18.根据权利要求12所述的方法，其特征在于，所述第一指示信息还用于指示所述用户设备采用第二密钥派生参数生成所述第二共享密钥；所述用户设备采用所述第一共享密钥对所述第一加密数据进行解密，得到所述第一随机标识之前，还包括：

所述用户设备根据所述第一指示信息，采用所述第二密钥派生参数生成所述第二共享密钥。

19.根据权利要求11至18任一项所述的方法，其特征在于，所述第一指示信息还用于指示所述用户设备采用第三密钥派生参数生成第三共享密钥，所述第三共享密钥用于所述归属网络控制设备后续向所述用户设备发送更新的第二随机标识时对所述第二随机标识进行加密；所述用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，还包括：

所述用户设备采用所述第三密钥派生参数生成所述第三共享密钥。

20.根据权利要求11至18任一项所述的方法，其特征在于，所述第一指示信息还用于指示所述用户设备采用第四密钥派生参数生成第四共享密钥，所述第四共享密钥用于所述归属网络控制设备后续向所述用户设备发送所述第二随机标识时对所述第二随机标识进行完整性保护；所述用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，还包括：

所述用户设备采用所述第四密钥派生参数生成所述第四共享密钥。

21.一种数据传输方法，其特征在于，包括：

归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息，所述第一认证数据请求消息中包括用户设备对应的第一标识；

所述归属网络控制设备生成第一随机数，并采用所述第一随机数和标识派生参数生成所述用户设备对应的第一随机标识；

所述归属网络控制设备判断所述第一随机标识是否未被其他用户设备使用；

若是，所述归属网络控制设备通过所述服务网络控制设备向所述用户设备发送所述第一随机数和第一指示信息，所述第一指示信息用于指示所述用户设备采用所述第一随机数和所述标识派生参数生成所述第一随机标识。

22.根据权利要求21所述的方法，其特征在于，所述归属网络控制设备判断所述第一随机标识是否未被其他用户设备使用之后，还包括：

若否，所述归属网络控制设备重新生成第二随机数，并采用所述第二随机数和所述标识派生参数生成第二随机标识；

所述归属网络控制设备判断所述第二随机标识是否未被其他用户设备使用。

23.一种数据传输方法，其特征在于，包括：

用户设备向服务网络控制设备发送接入请求消息，所述接入请求消息中包括所述用户设备对应的第一标识；

所述用户设备接收归属网络控制设备通过所述服务网络控制设备发送的第一随机数和第一指示信息；

所述用户设备根据所述第一指示信息，采用所述第一随机数和标识派生参数生成第一随机标识。

24.一种归属网络控制设备，其特征在于，包括：

接收单元，用于接收服务网络控制设备发送的第一认证数据请求消息，所述第一认证数据请求消息中包括用户设备对应的第一标识；

处理单元，用于生成所述用户设备对应的第一随机标识；

发送单元，用于通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息，所述第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据，所述第一数据组包括所述第一随机标识，所述第一指示信息用于指示所述用户设备根据所述第一指示信息确定所述第一随机数中包含所述第一随机标识。

25.根据权利要求24所述的归属网络控制设备，其特征在于，所述第一随机数中还包括采用第二共享密钥对所述第一加密数据进行完整性保护得到的第一完整性保护数据。

26.根据权利要求25所述的归属网络控制设备，其特征在于，所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥；或者所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识完整性密钥，所述随机标识完整性密钥用于对所述用户设备的随机标识进行完整性保护。

27.根据权利要求24至26任一项所述的归属网络控制设备，其特征在于，所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥；或者所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识加密密钥，所述随机标识加密密钥用于对所述用户设备的随机标识进行加密。

28.根据权利要求24或25所述的归属网络控制设备，其特征在于，在所述接收单元接收服务网络控制设备发送的第一认证数据请求消息之前，

所述接收单元，还用于接收所述服务网络控制设备发送的第二认证数据请求消息，所

述第二认证数据请求消息中包括所述用户设备对应的第二标识；

所述处理单元，还用于采用第一密钥派生参数生成所述第一共享密钥；

所述发送单元，还用于通过所述服务网络控制设备向所述用户设备发送第二指示信息，所述第二指示信息用于指示所述用户设备采用所述第一密钥派生参数生成所述第一共享密钥。

29.根据权利要求25所述的归属网络控制设备，其特征在于，在所述接收单元接收服务网络控制设备发送的第一认证数据请求消息之前，

所述接收单元，还用于接收所述服务网络控制设备发送的第二认证数据请求消息，所述第二认证数据请求消息中包括所述用户设备对应的第二标识；

所述处理单元，还用于采用第二密钥派生参数生成所述第二共享密钥；

所述发送单元，还用于通过所述服务网络控制设备向所述用户设备发送第二指示信息，所述第二指示信息用于指示所述用户设备采用所述第二密钥派生参数生成所述第二共享密钥。

30.根据权利要求24或25所述的归属网络控制设备，其特征在于，在所述接收单元接收服务网络控制设备发送的第一认证数据请求消息之后，在所述发送单元通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息之前，

所述处理单元，还用于采用第一密钥派生参数生成所述第一共享密钥；所述第一指示信息还用于指示所述用户设备采用所述第一密钥派生参数生成所述第一共享密钥。

31.根据权利要求25所述的归属网络控制设备，其特征在于，在所述接收单元接收服务网络控制设备发送的第一认证数据请求消息之后，在所述发送单元通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息之前，

所述处理单元，还用于采用第二密钥派生参数生成所述第二共享密钥；所述第一指示信息还用于指示所述用户设备采用所述第二密钥派生参数生成所述第二共享密钥。

32.根据权利要求24至31任一项所述的归属网络控制设备，其特征在于，在所述接收单元接收服务网络控制设备发送的第一认证数据请求消息之后，

所述处理单元，还用于采用第三密钥派生参数生成第三共享密钥，所述第三共享密钥用于所述归属网络控制设备后续向所述用户设备发送更新的第二随机标识时对所述第二随机标识进行加密；所述第一指示信息还用于指示所述用户设备采用所述第三密钥派生参数生成所述第三共享密钥。

33.根据权利要求24至31任一项所述的归属网络控制设备，其特征在于，在所述接收单元接收服务网络控制设备发送的第一认证数据请求消息之后，

所述处理单元，还用于采用第四密钥派生参数生成第四共享密钥，所述第四共享密钥用于所述归属网络控制设备后续向所述用户设备发送所述第二随机标识时对所述第二随机标识进行完整性保护；所述第一指示信息还用于指示所述用户设备采用所述第四密钥派生参数生成所述第四共享密钥。

34.一种用户设备，其特征在于，包括：

发送单元，用于向服务网络控制设备发送接入请求消息，所述接入请求消息中包括所述用户设备对应的第一标识；

接收单元，用于接收归属网络控制设备通过上述服务网络控制设备发送的第一随机数

和第一指示信息，所述第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据，所述第一数据组包括所述用户设备对应的第一随机标识；

处理单元，用于根据所述第一指示信息确定所述第一随机数中包含所述第一随机标识；

所述处理单元，还用于采用所述第一共享密钥对所述第一加密数据进行解密，得到所述第一随机标识。

35.根据权利要求34所述的用户设备，其特征在于，所述第一随机数中还包括采用第二共享密钥对所述第一加密数据进行完整性保护得到的第一完整性保护数据；在所述接收单元接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，

所述处理单元，还用于采用所述第二共享密钥对所述第一完整性保护数据进行完整性验证。

36.根据权利要求35所述的用户设备，其特征在于，所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥；或者所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识完整性密钥，所述随机标识完整性密钥用于对所述用户设备的随机标识进行完整性保护。

37.根据权利要求34至36任一项所述的用户设备，其特征在于，所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥；或者所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识加密密钥，所述随机标识加密密钥用于对所述用户设备的随机标识进行加密。

38.根据权利要求34或35所述的用户设备，其特征在于，在所述接收单元接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之前，

所述接收单元，还用于接收所述归属网络控制设备通过所述服务网络控制设备发送的第二指示信息；

所述处理单元，还用于根据所述第二指示信息采用第一密钥派生参数生成所述第一共享密钥。

39.根据权利要求35所述的用户设备，其特征在于，在所述接收单元接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之前，

所述接收单元，还用于接收所述归属网络控制设备通过所述服务网络控制设备发送的第二指示信息；

所述处理单元，还用于根据所述第二指示信息采用第二密钥派生参数生成所述第二共享密钥。

40.根据权利要求34或35所述的用户设备，其特征在于，所述第一指示信息还用于指示所述用户设备采用第一密钥派生参数生成所述第一共享密钥；在所述处理单元采用所述第一共享密钥对所述第一加密数据进行解密，得到所述第一随机标识之前，

所述处理单元，还用于根据所述第一指示信息，采用所述第一密钥派生参数生成所述第一共享密钥。

41.根据权利要求35所述的用户设备，其特征在于，所述第一指示信息还用于指示所述用户设备采用第二密钥派生参数生成所述第二共享密钥；在所述处理单元采用所述第一共享密钥对所述第一加密数据进行解密，得到所述第一随机标识之前，

所述处理单元，还用于根据所述第一指示信息，采用所述第二密钥派生参数生成所述第二共享密钥。

42.根据权利要求34至41任一项所述的用户设备，其特征在于，所述第一指示信息还用于指示所述用户设备采用第三密钥派生参数生成第三共享密钥，所述第三共享密钥用于所述归属网络控制设备后续向所述用户设备发送更新的第二随机标识时对所述第二随机标识进行加密；在所述接收单元接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，

所述处理单元，还用于采用所述第三密钥派生参数生成所述第三共享密钥。

43.根据权利要求34至41任一项所述的用户设备，其特征在于，所述第一指示信息还用于指示所述用户设备采用第四密钥派生参数生成第四共享密钥，所述第四共享密钥用于所述归属网络控制设备后续向所述用户设备发送所述第二随机标识时对所述第二随机标识进行完整性保护；在所述接收单元接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，

所述处理单元，还用于采用所述第四密钥派生参数生成所述第四共享密钥。

44.一种归属网络控制设备，其特征在于，包括：

接收单元，用于接收服务网络控制设备发送的第一认证数据请求消息，所述第一认证数据请求消息中包括用户设备对应的第一标识；

处理单元，用于生成第一随机数，并采用所述第一随机数和标识派生参数生成所述用户设备对应的第一随机标识；

所述处理单元，还用于判断所述第一随机标识是否未被其他用户设备使用；

若所述处理单元判断的结果为是，发送单元，用于通过所述服务网络控制设备向所述用户设备发送所述第一随机数和第一指示信息，所述第一指示信息用于指示所述用户设备采用所述第一随机数和所述标识派生参数生成所述第一随机标识。

45.根据权利要求44所述的归属网络控制设备，其特征在于，在所述处理单元判断所述第一随机标识是否未被其他用户设备使用之后，

若所述处理单元判断的结果为否，所述处理单元，还用于重新生成第二随机数，并采用所述第二随机数和所述标识派生参数生成第二随机标识；

所述处理单元，还用于判断所述第二随机标识是否未被其他用户设备使用。

46.一种用户设备，其特征在于，包括：

发送单元，用于向服务网络控制设备发送接入请求消息，所述接入请求消息中包括所述用户设备对应的第一标识；

接收单元，用于接收归属网络控制设备通过所述服务网络控制设备发送的第一随机数和第一指示信息；

处理单元，用于根据所述第一指示信息，采用所述第一随机数和标识派生参数生成第一随机标识。

一种数据传输方法及相关设备

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种数据传输方法及相关设备。

背景技术

[0002] 对于第三代移动通信系统(英文:3rd Generation,简称:3G)及其长期演进(英文:Long Term Evolution,简称:LTE)系统,为了保障数据传输的安全性,用户设备(英文:User Equipment,简称:UE)在向网络侧传输数据之前,必须要进行UE与网络侧之间的安全认证和密钥协商过程。目前在LTE系统中采用认证和密钥协商(英文:Authentication and Key Agreement,简称:AKA)协议来完成UE和网络侧之间的安全认证和密钥协商过程。

[0003] AKA过程是在UE进行初始接入时完成的,UE在向网络侧发送接入请求时,接入请求中会携带UE的永久性标识:国际移动用户识别号(英文:International Mobile Subscriber Identity,简称:IMSI)。网络侧会基于UE的IMSI找到该UE的根密钥K,进而基于根密钥K实现UE与网络侧之间的相互认证过程。

[0004] 由于在UE初始接入过程中,接入请求中携带的IMSI是未做任何的加密和完整性保护,任何第三方攻击者都可以通过空口窃听此接入请求,获得UE的IMSI,从而对该UE进行跟踪,因此,存在较大的安全隐患。

[0005] 为了避免在接入过程中泄露UE的IMSI,可以采用随机标识代替UE的永久标识,来对UE进行识别。在该方式中,每次UE进行初始接入都可以采用随机标识,而不再采用UE的永久标识IMSI,因此,攻击者从空口仅仅获得随机标识,并不能确定该随机标识是标识哪个UE的,因此,提高了UE的安全性。

[0006] 请参见图1,是现有技术中的AKA过程的流程示意图。在LTE系统中参与AKA过程的网元主要包括:UE、演进的基站(英文:evolved Node B,简称:eNB)、移动管理实体(英文:Mobility Management Entity,简称:MME)和归属签约用户服务器(英文:Home Subscriber Server,简称:HSS)。UE和HSS之间预共享根密钥K和随机标识,假设UE的初始随机标识为P,该随机标识P用于在UE和网络侧之间识别该UE。并且,随机标识P可以进行更新。该AKA过程包括以下步骤。

[0007] S101:UE通过eNB向MME发送接入请求消息,该接入请求消息中携带了该UE对应的随机标识P以及归属网络标识(ID),归属网络标识用于指示该UE归属于哪个运营商。

[0008] S102:MME根据接入请求消息中携带的归属网络标识找到对应的HSS,向该HSS发送认证数据请求消息,该认证数据请求消息中携带UE的随机标识P。

[0009] S103:HSS收到认证数据请求消息后,查找随机标识P对应的根密钥K,根据根密钥K生成该UE对应的认证向量(英文:Authentication Vector,简称:AV)。

[0010] 具体的,若HSS确定不需要更新UE的随机标识P,则HSS随机产生一个随机数RAND,然后根据RAND、自身当前保存的鉴权序列号SQN、根密钥K以及其它信息生成该UE对应的AV,其中AV包括:RAND、认证令牌(英文:Authentication Token,简称:AUTN)、期望的响应数(英文:Expected response,简称:XRES)和K_{ASME}。需要说明的是,这里是以LTE中的AV向量为例

进行的说明，3G的AV向量中包括加密密钥CK和完整性密钥IK，而不包括K_{ASME}，K_{ASME}是由CK和IK推衍生成的。

[0011] 其中，AUTN是由SQN与匿名密钥(英文：Anonymity Key，简称：AK)进行异或运算得到的值、认证管理域(英文：Authentication Management Field，简称：AMF)以及消息认证码(英文：Message Authentication Code，简称：MAC)这三个内容组成的。其中AK是根据RAND和K计算得到的。MAC是根据RAND、K、AMF和SQN计算得到的，用来让UE认证网络侧。

[0012] 若HSS确定需要更新UE的随机标识P，则HSS对RAND进行重新定义，RAND由Enc(P')、MAC(SQN)和随机字符串三部分内容组成，且这三部分内容分别占用不同的字段，例如，RAND的长度为128比特(bit)，其中，第1至第40位代表Enc(P')，第41至第56位代表MAC(SQN)，第57至第76位代表随机字符串。其中，P'表示更新的随机标识，Enc(P')是对P'进行加密后得到的密文，MAC(SQN)是对SQN进行完整性保护后得到的参数。随机字符串是HSS生成的随机数。其中Enc(P')是采用该UE的根密钥K进行加密运算得到的，MAC(SQN)是采用该UE的根密钥K进行完整性保护运算得到的。然后根据RAND、SQN、根密钥K以及其它信息生成该UE对应的AV，AV的内容可参见上述相关描述，此处不再赘述。

[0013] S104：HSS向MME发送认证数据响应消息，该认证数据响应消息中携带该UE的AV，MME将收到的该UE的AV进行保存。

[0014] S105：MME向UE发送用户认证请求消息，该用户认证请求消息中携带了该UE认证向量中的RAND和AUTN。

[0015] S106：UE收到用户认证请求消息后，根据收到的RAND和AUTN，对网络侧进行校验。

[0016] 校验过程包括：UE根据RAND和根密钥K计算得到AK，再根据AK以及AUTN中的SQN与AK进行异或运算得到的值计算得到SQN，接着根据RAND、SQN、AUTN中的AMF和根密钥K共同计算出一个XMAC，并将XMAC和认证响应消息中的MAC做比较，如果相同，则接着校验收到的SQN是否等于本地保存的SQN，以防止重放攻击。如果是，则该UE成功地认证了网络。UE接着根据该RAND和K计算得到RES和K_{ASME}，其中RES是用来让网络认证UE的参数。

[0017] 并且，UE根据根密钥K和AUTN中的SQN，对RAND中对应MAC(SQN)的字段进行完整性验证，若验证成功，则表明RAND中包含新的随机标识，进而根据根密钥K，对RAND中对应Enc(P')的字段进行解密，得到更新的随机标识P'。若UE对RAND中对应MAC(SQN)的字段验证失败，则表明RAND中不包含新的随机标识。

[0018] S107：UE向MME发送用户认证响应消息，该用户认证响应消息中携带RES。

[0019] S108：MME接收到用户认证响应消息后，将用户认证响应消息中携带的RES与该UE对应的认证向量中的XRES进行比较，若相同，则MME对UE认证通过。

[0020] 至此，UE和网络侧完成了AKA过程。之后，UE再接入网络时就可以使用更新的随机标识P'，以保障UE的安全。

[0021] 由上可知，在现有技术中，HSS利用RAND中的MAC(SQN)来通知UE发送的RAND中是否包含新的随机标识，UE需要对RAND进行额外的计算才能确定接收到的RAND中是否包含新的随机标识，增加了UE的计算量，不利于节约UE开销。

发明内容

[0022] 本发明实施例提供了一种数据传输方法及相关设备，可以节省用户设备确定接收

到的随机数中包含更新的随机标识的计算量，进而节约用户设备的开销。

[0023] 第一方面，本发明实施例提供了一种数据传输方法，该方法包括：归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息，第一认证数据请求消息中包括用户设备对应的第一标识；归属网络控制设备生成用户设备对应的第一随机标识；归属网络控制设备通过服务网络控制设备向用户设备发送第一随机数和第一指示信息，第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据，第一数据组包括第一随机标识，第一指示信息用于指示用户设备根据第一指示信息确定第一随机数中包含第一随机标识。

[0024] 归属网络控制设备可以通过第一指示信息明确告知用户设备第一随机数中包括更新的随机标识，而非生成消息认证码让用户设备根据消息认证码以确定第一随机数中包括更新的随机标识，节省了归属网络控制设备的处理复杂度。并且用户设备通过解析第一指示信息就可以直接确认出接收到的第一随机数中包括更新的随机标识，无需进行额外的计算处理过程，节省了用户设备的开销，降低了用户设备的处理复杂度。

[0025] 在一种可能的设计中，第一随机数中还包括采用第二共享密钥对第一加密数据进行完整性保护得到的第一完整性保护数据。通过归属网络控制设备对第一加密数据进行完整性保护，可以提高第一随机标识传输的安全性。

[0026] 在一种可能的设计中，第二共享密钥为用户设备与归属网络控制设备之间预共享的根密钥；或者第二共享密钥为用户设备与归属网络控制设备之间预共享的随机标识完整性密钥，随机标识完整性密钥用于对用户设备的随机标识进行完整性保护。归属网络控制设备与用户设备之间可以预共享第二共享密钥，从而在数据传输过程中，归属网络控制设备可以采用第二共享密钥对第一加密数据进行完整性保护得到第一完整性保护数据，提高了第一随机标识传输的安全性。

[0027] 在一种可能的设计中，第一共享密钥为用户设备与归属网络控制设备之间预共享的根密钥；或者第一共享密钥为用户设备与归属网络控制设备之间预共享的随机标识加密密钥，随机标识加密密钥用于对用户设备的随机标识进行加密。归属网络控制设备与用户设备之间可以预共享第一共享密钥，从而在数据传输过程中，归属网络控制设备可以采用第一共享密钥对用户设备的第一随机标识进行加密，提高了第一随机标识传输的安全性。

[0028] 在一种可能的设计中，归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之前，还包括：归属网络控制设备接收服务网络控制设备发送的第二认证数据请求消息，第二认证数据请求消息中包括用户设备对应的第二标识；归属网络控制设备采用第一密钥派生参数生成第一共享密钥；归属网络控制设备通过服务网络控制设备向用户设备发送第二指示信息，第二指示信息用于指示用户设备采用第一密钥派生参数生成第一共享密钥。归属网络控制设备在向用户设备发送加密的第一随机标识之前，可以通过第二指示信息通知用户设备生成第一共享密钥，使得归属网络控制设备在后续向用户设备发送第一随机标识时，采用第一共享密钥对第一随机标识进行加密，提高第一随机标识传输的安全性。

[0029] 在一种可能的设计中，归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之前，还包括：归属网络控制设备接收服务网络控制设备发送的第二认证数据请求消息，第二认证数据请求消息中包括用户设备对应的第二标识；归属网络控制设备

采用第二密钥派生参数生成第二共享密钥;归属网络控制设备通过服务网络控制设备向用户设备发送第二指示信息,第二指示信息用于指示用户设备采用第二密钥派生参数生成第二共享密钥。归属网络控制设备在向用户设备发送加密的第一随机标识之前,可以通过第二指示信息通知用户设备生成第二共享密钥,使得归属网络控制设备在后续向用户设备发送第一随机标识时,采用第二共享密钥对第一加密数据进行完整性保护,提高第一随机标识传输的安全性。

[0030] 在一种可能的设计中,归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之后,归属网络控制设备通过服务网络控制设备向用户设备发送第一随机数和第一指示信息之前,还包括:归属网络控制设备采用第一密钥派生参数生成第一共享密钥;第一指示信息还用于指示用户设备采用第一密钥派生参数生成第一共享密钥。归属网络控制设备在向用户设备发送加密的第一随机标识时,可以通过第一指示信息直接通知用户设备生成第一共享密钥,从而用户设备可以基于第一共享密钥对第一加密数据解密得到第一随机标识。

[0031] 在一种可能的设计中,第一密钥派生参数为归属网络控制设备与用户设备之间预共享的。

[0032] 在一种可能的设计中,归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之后,归属网络控制设备通过服务网络控制设备向用户设备发送第一随机数和第一指示信息之前,还包括:归属网络控制设备采用第二密钥派生参数生成第二共享密钥;第一指示信息还用于指示用户设备采用第二密钥派生参数生成第二共享密钥,第二共享密钥用于归属网络控制设备对第一加密数据进行完整性保护。归属网络控制设备在向用户设备发送加密的第一随机标识时,可以通过第一指示信息直接通知用户设备生成第二共享密钥,从而用户设备可以基于第二共享密钥对第一完整性保护数据进行完整性验证。

[0033] 在一种可能的设计中,第二密钥派生参数为归属网络控制设备与用户设备之间预共享的。

[0034] 在一种可能的设计中,归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之后,还包括:归属网络控制设备采用第三密钥派生参数生成第三共享密钥,第三共享密钥用于归属网络控制设备后续向用户设备发送更新的第二随机标识时对第二随机标识进行加密;第一指示信息还用于指示用户设备采用第三密钥派生参数生成第三共享密钥。

[0035] 在一种可能的设计中,第三密钥派生参数为归属网络控制设备与用户设备之间预共享的。

[0036] 在一种可能的设计中,归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息之后,还包括:归属网络控制设备采用第四密钥派生参数生成第四共享密钥,第四共享密钥用于归属网络控制设备后续向用户设备发送第二随机标识时对第二随机标识进行完整性保护;第一指示信息还用于指示用户设备采用第四密钥派生参数生成第四共享密钥。

[0037] 在一种可能的设计中,第四密钥派生参数为归属网络控制设备与用户设备之间预共享的。

[0038] 在一种可能的设计中,归属网络控制设备生成用户设备对应的第一随机标识之

后，还包括：归属网络控制设备接收该服务网络控制设备发送的认证成功消息，该认证成功消息用于指示该服务网络控制设备已对该用户设备认证成功；该归属网络控制设备根据该认证成功消息，保存用户设备与第一随机标识的映射关系，并保存用户设备与第一标识的映射关系。可以避免以下情况的发生：若归属网络控制设备在生成了新的随机标识之后，就释放旧的随机标识，若第三方攻击者通过伪造接入请求消息，触发归属网络控制设备释放合法用户的旧的随机标识，从而造成合法用户不能接入网络。

[0039] 在一种可能的设计中，该认证成功消息中包括该用户设备对应的第一标识或者该用户设备对应的第一随机标识。

[0040] 在一种可能的设计中，该第一密钥派生参数和/或该第三密钥派生参数包括该用户设备的根密钥、基于该用户设备的根密钥衍生的共享密钥、该第一随机数、鉴权序列号、加密算法标识、归属网络标识和服务网络标识中的至少一项。

[0041] 在一种可能的设计中，该第二密钥派生参数和/或该第四密钥派生参数包括该用户设备的根密钥、基于该用户设备的根密钥衍生的共享密钥、该第一随机数、鉴权序列号、完整性保护算法标识、归属网络标识和服务网络标识中的至少一项。

[0042] 在一种可能的设计中，该第一数据组还包括序列码，该序列码用于表征该用户设备对应的随机标识更新的总次数。

[0043] 第二方面，本发明实施例提供了一种数据传输方法，该方法包括：用户设备向服务网络控制设备发送第一接入请求消息，该第一接入请求消息中包括该用户设备对应的第一标识；该用户设备接收归属网络控制设备通过该服务网络控制设备发送的第一随机数和第一指示信息，第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据，第一数据组包括用户设备对应的第一随机标识；用户设备根据第一指示信息确定第一随机数中包含第一随机标识；用户设备采用第一共享密钥对第一加密数据进行解密，得到第一随机标识。用户设备通过解析第一指示信息就可以直接确认出接收到的第一随机数中包括更新的随机标识，无需进行额外的计算处理过程，节省了用户设备的开销，降低了用户设备的处理复杂度。

[0044] 在一种可能的设计中，第一随机数中还包括采用第二共享密钥对第一加密数据进行完整性保护得到的第一完整性保护数据；用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，还包括：用户设备采用第二共享密钥对第一完整性保护数据进行完整性验证。通过对第一完整性保护数据进行完整性验证，可以验证第一加密数据是否未被第三方篡改，可以提高第一随机标识传输的安全性。

[0045] 在一种可能的设计中，第二共享密钥为用户设备与归属网络控制设备之间预共享的根密钥；或者第二共享密钥为用户设备与归属网络控制设备之间预共享的随机标识完整性密钥，随机标识完整性密钥用于对用户设备的随机标识进行完整性保护。归属网络控制设备与用户设备之间可以预共享第二共享密钥，从而在数据传输过程中，归属网络控制设备可以采用第二共享密钥对第一加密数据进行完整性保护得到第一完整性保护数据，提高了第一随机标识传输的安全性。

[0046] 在一种可能的设计中，第一共享密钥为用户设备与归属网络控制设备之间预共享的根密钥；或者第一共享密钥为用户设备与归属网络控制设备之间预共享的随机标识加密密钥，随机标识加密密钥用于对用户设备的随机标识进行加密。归属网络控制设备与用户

设备之间可以预共享第一共享密钥，从而在数据传输过程中，归属网络控制设备可以采用第一共享密钥对用户设备的第一随机标识进行加密，提高了第一随机标识传输的安全性。

[0047] 在一种可能的设计中，用户设备向服务网络控制设备发送第一接入请求消息之前，还包括：用户设备向该服务网络控制设备发送第二接入请求消息，该第二接入请求消息中包括该用户设备对应的第二标识；该用户设备接收该归属网络控制设备通过该服务网络控制设备发送的第二指示信息；该用户设备根据该第二指示信息采用第一密钥派生参数生成第一共享密钥。用户设备在接收归属网络控制设备发送的加密的第一随机标识之前，可以根据归属网络控制设备发送的第二指示信息，生成第一共享密钥，使得后续用户设备接收到归属网络控制设备发送的加密的第一随机标识，采用第一共享密钥对第一随机标识进行加密，提高第一随机标识传输的安全性。

[0048] 在一种可能的设计中，用户设备向服务网络控制设备发送第一接入请求消息之前，还包括：用户设备向该服务网络控制设备发送第二接入请求消息，该第二接入请求消息中包括该用户设备对应的第二标识；用户设备接收归属网络控制设备通过服务网络控制设备发送的第二指示信息；用户设备根据第二指示信息采用第二密钥派生参数生成第二共享密钥。用户设备在接收归属网络控制设备发送的加密的第一随机标识之前，可以根据归属网络控制设备发送的第二指示信息，生成第二共享密钥，使得后续用户设备接收到归属网络控制设备发送的第一完整性保护数据时，采用第二共享密钥对第一完整性保护数据进行完整性验证，提高第一随机标识传输的安全性。

[0049] 在一种可能的设计中，第一指示信息还用于指示用户设备采用第一密钥派生参数生成第一共享密钥；该用户设备接收归属网络控制设备通过该服务网络控制设备发送的第一随机数和第一指示信息之后，用户设备采用第一共享密钥对第一加密数据进行解密，得到第一随机标识之前，还包括：用户设备根据第一指示信息，采用第一密钥派生参数生成第一共享密钥。用户设备可以根据第一指示信息，确定生成第一共享密钥，从而用户设备可以基于第一共享密钥对第一加密数据解密得到第一随机标识。

[0050] 在一种可能的设计中，第一指示信息还用于指示用户设备采用第二密钥派生参数生成第二共享密钥；该用户设备接收归属网络控制设备通过该服务网络控制设备发送的第一随机数和第一指示信息之后，用户设备采用第一共享密钥对第一加密数据进行解密，得到第一随机标识之前，还包括：用户设备根据第一指示信息，采用第二密钥派生参数生成第二共享密钥。用户设备可以根据第一指示信息，确定生成第二共享密钥，从而用户设备可以基于第二共享密钥对第一完整性保护数据进行完整性验证。

[0051] 在一种可能的设计中，第一指示信息还用于指示用户设备采用第三密钥派生参数生成第三共享密钥，第三共享密钥用于归属网络控制设备后续向用户设备发送更新的第二随机标识时对第二随机标识进行加密；用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，还包括：用户设备采用第三密钥派生参数生成第三共享密钥。

[0052] 在一种可能的设计中，第一指示信息还用于指示用户设备采用第四密钥派生参数生成第四共享密钥，第四共享密钥用于归属网络控制设备后续向用户设备发送第二随机标识时对第二随机标识进行完整性保护；用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，还包括：用户设备采用第四密钥派生参数生

成第四共享密钥。

[0053] 在一种可能的设计中，用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，还包括：用户设备保存用户设备与第一随机标识的映射关系，并保存用户设备与第一标识的映射关系。用户设备既保存新的第一随机标识，又保存旧的第一标识，以使得在接入过程中如果不能通过新的第一随机标识成功接入网络，还可以采用旧的第一标识接入网络，提高了用户设备成功接入网络的几率。

[0054] 在一种可能的设计中，该第一密钥派生参数和/或该第三密钥派生参数包括该用户设备的根密钥、基于该用户设备的根密钥衍生的共享密钥、该第一随机数、鉴权序列号、加密算法标识、归属网络标识和服务网络标识中的至少一项。

[0055] 在一种可能的设计中，该第二密钥派生参数和/或该第四密钥派生参数包括该用户设备的根密钥、基于该用户设备的根密钥衍生的共享密钥、该第一随机数、鉴权序列号、完整性保护算法标识、归属网络标识和服务网络标识中的至少一项。

[0056] 在一种可能的设计中，该第一数据组还包括序列码，该序列码用于表征该用户设备对应的随机标识更新的总次数。

[0057] 第三方面，本发明实施例提供了一种数据传输方法，该方法包括：服务网络控制设备向归属网络控制设备发送认证成功消息，该认证成功消息用于指示该归属网络控制设备该服务网络控制设备已对用户设备认证成功。

[0058] 在一种可能的设计中，该认证成功消息中包括该用户设备对应的第一标识或者该用户设备对应的第一随机标识。

[0059] 第四方面，本发明实施例提供了一种数据传输方法，该方法包括：归属网络控制设备接收服务网络控制设备发送的第一认证数据请求消息，该第一认证数据请求消息中包括用户设备对应的第一标识；该归属网络控制设备生成第一随机数，并采用该第一随机数和标识派生参数生成该用户设备对应的第一随机标识；该归属网络控制设备判断该第一随机标识是否未被其他用户设备使用；若是，该归属网络控制设备通过该服务网络控制设备向该用户设备发送该第一随机数和第一指示信息，该第一指示信息用于指示该用户设备采用该第一随机数和该标识派生参数生成该第一随机标识。

[0060] 归属网络控制设备采用生成的第一随机标识来生成第一随机数，若第一随机数未被其他用户设备使用，则归属网络控制设备将该第一随机标识分配给该用户设备，向该用户设备发送第一指示信息，指示用户设备采用第一随机数生成该第一随机标识，因此，第一随机标识是归属网络控制设备与用户设备之间基于相同的参数派生的，无需进行随机标识的传输，提高了用户设备的随机标识的安全性。

[0061] 在一种可能的设计中，该归属网络控制设备判断该第一随机标识是否未被其他用户设备使用之后，还包括：若否，该归属网络控制设备重新生成第二随机数，并采用该第二随机数和该标识派生参数生成第二随机标识；该归属网络控制设备判断该第二随机标识是否未被其他用户设备使用。

[0062] 在一种可能的设计中，该标识派生参数为该归属网络控制设备与该用户设备之间预共享的。归属网络控制设备与用户设备可以基于预共享的参数来生成第一随机标识。

[0063] 第五方面，本发明实施例提供了一种数据传输方法，该方法包括：用户设备接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息；所述用户设备

根据所该第一指示信息，采用该第一随机数和标识派生参数生成该第一随机标识。用户设备采用归属网络控制设备发送的第一随机数生成该第一随机标识，因此，第一随机标识是归属网络控制设备与用户设备之间基于相同的参数派生的，无需进行随机标识的传输，提高了用户设备的随机标识的安全性。

[0064] 在一种可能的设计中，该标识派生参数为该归属网络控制设备与该用户设备之间预共享的。归属网络控制设备与用户设备可以基于预共享的参数来生成第一随机标识。

[0065] 第六方面，本发明实施例提供了一种归属网络控制设备，该归属网络控制设备具有实现上述第一方面或第四方面中归属网络控制设备行为的功能。功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的模块。

[0066] 在一个可能的设计中，该归属网络控制设备的结构中包括处理器和存储器，存储器用于存储支持该归属网络控制设备执行上述方法的程序，处理器被配置为用于执行存储器中存储的程序。该归属网络控制设备还可以包括通信接口，用于该归属网络控制设备与其他设备或通信网络通信。

[0067] 第七方面，本发明实施例提供了一种用户设备，该用户设备具有实现上述第二方面或第五方面中用户设备行为的功能。功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的模块。

[0068] 在一个可能的设计中，该用户设备的结构中包括处理器和存储器，存储器用于存储支持该用户设备执行上述方法的程序，处理器被配置为用于执行存储器中存储的程序。该用户设备还可以包括通信接口，用于该用户设备与其他设备或通信网络通信。

[0069] 第八方面，本发明实施例提供了一种服务网络控制设备，该服务网络控制设备具有实现上述第三方面中服务网络控制设备行为的功能。功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的模块。

[0070] 在一个可能的设计中，该服务网络控制设备的结构中包括处理器和存储器，存储器用于存储支持该服务网络控制设备执行上述方法的程序，处理器被配置为用于执行存储器中存储的程序。该服务网络控制设备还可以包括通信接口，用于该服务网络控制设备与其他设备或通信网络通信。

[0071] 第九方面，本发明提供了一种归属网络控制设备，该归属网络控制设备包括用于执行上述第一方面或第四方面所描述的数据传输方法的模块或单元。

[0072] 第十方面，本发明提供了一种用户设备，该用户设备包括用于执行上述第二方面或第五方面所描述的数据传输方法的模块或单元。

[0073] 第十一方面，本发明提供了一种服务网络控制设备，该服务网络控制设备包括用于执行上述第三方面所描述的数据传输方法的模块或单元。

[0074] 第十二方面，本发明提供了一种通信系统，包括归属网络控制设备、用户设备和服务网络控制设备，其中，归属网络控制设备为第六方面或第九方面所描述的归属网络控制设备，用户设备为第七方面或第十方面所描述的用户设备，服务网络控制设备为第八方面或第十一方面所描述的服务网络控制设备。

[0075] 第十三方面，本发明实施例提供了一种计算机存储介质，用于储存为上述归属网络控制设备所用的计算机软件指令，其包含用于执行上述第一方面或第四方面为归属网络

控制设备所设计的程序。

[0076] 第十四方面，本发明实施例提供了一种计算机存储介质，用于储存为上述用户设备所用的计算机软件指令，其包含用于执行上述第二方面或第五方面为用户设备所设计的程序。

[0077] 第十五方面，本发明实施例提供了一种计算机存储介质，用于储存为上述服务网络控制设备所用的计算机软件指令，其包含用于执行上述第三方面为服务网络控制设备所设计的程序。

[0078] 本发明的这些方面或其他方面在以下实施例的描述中会更加简明易懂。

附图说明

[0079] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍。

[0080] 图1是现有技术中AKA过程的信令流程示意图；

[0081] 图2是本发明实施例提供的一种通信系统的架构示意图；

[0082] 图3所示为本发明实施例提供的计算机设备示意图；

[0083] 图4为本发明实施例提供的一种数据传输方法的流程示意图；

[0084] 图5为本发明实施例提供的另一种数据传输方法的流程示意图；

[0085] 图6为本发明实施例提供的另一种数据传输方法的流程示意图；

[0086] 图7为本发明实施例提供的另一种数据传输方法的流程示意图；

[0087] 图8为本发明实施例提供的一种归属网络控制设备的结构示意图；

[0088] 图9为本发明实施例提供的一种用户设备的结构示意图；

[0089] 图10为本发明实施例提供的一种服务网络控制设备的结构示意图。

具体实施方式

[0090] 本发明的实施方式部分使用的术语仅用于对本发明的具体实施例进行解释，而非旨在限定本发明。下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚地描述。

[0091] 请参见图2，是本发明实施例提供的一种通信系统的架构示意图。该通信系统20包括用户设备201、接入网设备202、服务网络控制设备203和归属网络控制设备204。

[0092] 其中，用户设备201也可以称为移动台、接入终端、用户单元、用户站、移动站、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置等。该用户设备201可以是手机、平板电脑、笔记本电脑、掌上电脑、移动互联网设备(英文：Mobile Internet Device，简称：MID)、可穿戴设备(例如智能手表(如iWatch)等)等具备通用用户标识模块(英文：Universal Subscriber Identity Module，简称：USIM)/用户识别模块(英文：Subscriber Identity Module，简称：SIM)的终端设备。

[0093] 可选的，用户设备201由两部分组成，分别是：USIM/SIM模块和移动设备(英文：Mobile Equipment，简称：ME)。其中，USIM/SIM模块是运营商颁发的智能卡，与归属网络控制设备204之间共享一个永久性对称根密钥K，这个K是在制造USIM/SIM模块时一次性写入的，并且受到USIM/SIM的安全机制保护，无法被读出。USIM/SIM模块具有AKA的认证和计算

能力。ME为用户设备201中除了USIM模块之外的硬件设备，可以执行安全运算。

[0094] 或者，用户设备201为一个独立的设备，该设备具备上述所述的USIM/SIM模块和ME的功能。

[0095] 接入网设备202可以是通过无线方式与用户设备201进行通信的设备，例如：基站(英文：NodeB，简称：NB)、eNB、无线保真(英文：Wireless Fidelity，简称：WiFi)中的无线接入点、未来5G网络中的无线接入网设备等等；同时，接入网设备202也可以是通过有线方式与用户设备201进行通信的设备，例如：网关，服务器，控制网关等等。有线的传输方式包括但不限于：IP、基于内容的网络、基于身份的网络等等。为方便表述，以下实施例中将采用无线接入网设备进行表述。

[0096] 服务网络控制设备203属于认证处理节点。服务网络控制设备203包括但不限于：移动管理实体(英文：Mobility Management Entity，简称：MME)、认证服务器功能实体(英文：Authentication Server Function简称：AUSF)、安全锚点函数网元(英文：Security Anchor Function简称：SEAF)、安全上行文管理网元(英文：Security Context Management Function简称：SCMF)、引导服务器功能网元(英文：Bootstrapping Server Function简称：BSF)、呼叫会话控制功能实体(英文：Call Session Control Function简称：CSCF)或新配置与网络认证相关的功能设备(为了方便描述后续可称为网络认证服务器)。以下以该服务网络控制设备203包括MME为例来进行描述。当该服务网络控制设备203只包括一个设备时，后续描述到的服务网络控制设备203所执行的操作均由该一个设备完成；当该服务网络控制设备203包括多个设备时，后续描述到的服务网络控制设备203所执行的操作由该多个设备协作完成，即该多个设备中不同设备各执行一些操作，执行操作所产生的数据、参数均可以根据需要在该多个设备之间传输。

[0097] 归属网络控制设备204是运营商维护的设备，存储有用户的签约信息等。归属网络控制设备204与用户设备201之间共享根密钥K。或者，归属网络控制设备204与用户设备201中的USIM/SIM模块之间共享根密钥K。归属网络控制设备204可以是归属签约用户服务器(英文：Home Subscriber Server，简称：HSS)，也可以是认证授权计费(英文：Authentication，Authorization and Accounting，简称：AAA)认证中心，等等。

[0098] 归属网络控制设备204可以将更新的随机标识进行加密和/或完整性保护，然后将加密和/或完整性保护后的随机标识以及第一指示信息发送给服务网络控制设备203，服务网络控制设备203再将该加密和/或完整性保护后的随机标识以及第一指示信息发送给无线接入网设备202，无线接入网设备202再将该加密和/或完整性保护后的随机标识以及第一指示信息发送给用户设备201，用户设备201接收无线接入网设备202发送的该加密和/或完整性保护后的随机标识以及第一指示信息。用户设备201根据该第一指示信息就可以确定出无线接入网设备202返回的消息中携带了更新的随机标识，因此用户设备201对加密数据进行解密，从而获得更新的随机标识，或者用户设备201先对加密数据进行完整性验证，再对加密数据进行解密，从而获得更新的随机标识。

[0099] 可选的，归属网络控制设备204与用户设备201之间可以预共享随机标识加密密钥和/或随机标识完整性密钥。或者，归属网络控制设备204与用户设备201中的USIM/SIM模块之间预共享随机标识加密密钥和/或随机标识完整性密钥。其中，随机标识加密密钥用于对用户设备的随机标识进行加密性保护，随机标识完整性密钥用于对用户设备的随机标识进

行完整性保护，或者用于随机标识传输过程中的完整性保护。为了方便描述，后续统一用CKP来表示随机标识加密密钥，用IKP来表示随机标识完整性密钥。

[0100] 可选的，随机标识加密密钥和/或随机标识完整性密钥还可以是归属网络控制设备204发送给用户设备201的，也即是说，用户设备201或者用户设备201中的USIM/SIM模块初始并不会存储随机标识加密密钥和/或随机标识完整性密钥，当归属网络控制设备204确定对更新的随机标识进行加密和/或完整性保护时，会先将随机标识加密密钥和/或随机标识完整性密钥发送给用户设备201，使得用户设备201可以正确地解密得到更新的随机标识。

[0101] 需要说明的是，本发明实施例中所描述的随机标识为具有随机性的字符串，可以部分字符串内容都是随机选择，也有可能全部字符串是随机选择。包括但不限于以下两种可能：可能性一：随机标识是一个随机的字符串。可能性二：随机标识由三部分组成，包括移动国家码(英文：Mobile Network Code，简称：MNC)、移动网号(英文：Mobile Country Code，简称：MCC)和随机的字符串。

[0102] 如图3所示，图2中的归属网络控制设备204或者用户设备201或者服务网络控制设备203可以以图3中的计算机设备(或系统)的方式来实现。

[0103] 图3所示为本发明实施例提供的计算机设备示意图。计算机设备300包括至少一个处理器301，通信总线302，存储器303以及至少一个通信接口304。

[0104] 处理器301可以是一个通用中央处理器(英文：Central Processing Unit，简称：CPU)，微处理器，特定应用集成电路(英文：Application-Specific Integrated Circuit，简称：ASIC)，或一个或多个用于控制本发明方案程序执行的集成电路。

[0105] 通信总线302可包括一通路，在上述组件之间传送信息。所述通信接口304，使用任何收发器一类的装置，用于与其他设备或通信网络通信，如以太网，无线接入网(英文：Radio Access Technology，简称：RAN)，无线局域网(英文：Wireless Local Area Networks，简称：WLAN)等。

[0106] 存储器303可以是只读存储器(英文：Read-Only Memory，简称：ROM)或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器(英文：Random Access Memory，简称：RAM)或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器(英文：Electrically Erasable Programmable Read-Only Memory，简称：EEPROM)、只读光盘(英文：Compact Disc Read-Only Memory，简称：CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器可以是独立存在，通过总线与处理器相连接。存储器也可以和处理器集成在一起。

[0107] 其中，所述存储器303用于存储执行本发明方案的程序代码，并由处理器301来控制执行。所述处理器301用于执行所述存储器303中存储的程序代码。

[0108] 在具体实现中，作为一种实施例，处理器301可以包括一个或多个CPU，例如图3中的CPU0和CPU1。

[0109] 在具体实现中，作为一种实施例，计算机设备300可以包括多个处理器，例如图3中的处理器301和处理器308。这些处理器中的每一个可以是一个单核(single-CPU)处理器，

也可以是一个多核(multi-CPU)处理器。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据(例如计算机程序指令)的处理核。

[0110] 在具体实现中,作为一种实施例,计算机设备300还可以包括输出设备305和输入设备306。输出设备305和处理器301通信,可以以多种方式来显示信息。例如,输出设备305可以是液晶显示器(英文:Liquid Crystal Display,简称:LCD),发光二级管(英文:Light Emitting Diode,简称:LED)显示设备,阴极射线管(英文:Cathode Ray Tube,简称:CRT)显示设备,或投影仪(projector)等。输入设备306和处理器301通信,可以以多种方式接受用户的输入。例如,输入设备406可以是鼠标、键盘、触摸屏设备或传感设备等。

[0111] 上述的计算机设备300可以是一个通用计算机设备或者是一个专用计算机设备。在具体实现中,计算机设备300可以是台式机、便携式电脑、网络服务器、掌上电脑(英文:Personal Digital Assistant,简称:PDA)、移动手机、平板电脑、无线终端设备、通信设备、嵌入式设备或有图3中类似结构的设备。本发明实施例不限定计算机设备300的类型。

[0112] 如图2中的归属网络控制设备204也可以为图3所示的设备,归属网络控制设备204的存储器中存储了一个或多个软件模块(如交互模块和处理模块)。如图2中的用户设备201可以为图3所示的设备,用户设备201的存储器中存储了一个或多个软件模块(如交互模块和处理模块)。如图2中的服务网络控制设备203可以为图3所示的设备,服务网络控制设备203的存储器中存储了一个或多个软件模块(如交互模块和处理模块)。归属网络控制设备或者用户设备或者服务网络控制设备可以通过处理器以及存储器中的程序代码来实现软件模块,执行下述图4至图7方法实施例所述的流程。

[0113] 基于上述图2所述的通信架构示意图,图4为本发明实施例提供的一种数据传输方法的流程示意图,该数据传输方法包括如下步骤。

[0114] S401:用户设备向服务网络控制设备发送第一接入请求消息,该第一接入请求消息中携带该用户设备的随机标识P。

[0115] 本发明实施例以第一接入请求消息携带用户设备对应的随机标识P为例进行说明,除了随机标识P,第一接入请求消息中还可以携带其他标识来标识该用户设备,该标识包括但不限于:国际移动用户标识(英文:International Mobile Subscriber Identity,简称:IMSI)、国际移动设备标识(英文:International Mobile Equipment Identity,简称:IMEI)、互联网协议(英文:Internet Protoco,简称:IP)多媒体私有标识(英文:IP Multimedia Private Identity,简称:IMPI)、IP多媒体公有标识(英文:IP Multimedia Public Identity,简称:IMPU)、临时移动用户标识(英文:Temporary Mobile Subscriber Identity,简称:TMSI)、媒体访问控制(英文:Media Access Control,简称:MAC)地址、IP地址、手机号码和全球唯一临时UE标识(英文:Globally Unique Temporary UE Identity,简称:GUTI)。具体的,当用户设备第一次执行初始接入过程时,标识可以为该用户设备对应的IMSI或IMPI,当用户设备执行第二次或第N次接入过程时,标识可以为该用户设备对应的上述标识中的任意一个。

[0116] 在一种应用场景中,用户设备与该用户设备所属的归属网络控制设备之间可以预先共享一个初始随机标识P。该随机标识P可以唯一识别出该用户设备。因此,当用户设备执行初始接入过程(或者初始注册过程)时,在第一接入请求消息(或者注册请求消息,本发明实施例以接入请求消息为例进行说明)中就可以携带随机标识P,因此,在空口中就可以不

再传输用户设备的IMSI了，提高了用户设备的隐私性和安全性。例如，可以在用户设备的存储器中存储随机标识P，同时，归属网络控制设备中也存储有该用户设备对应的随机标识P以及该用户设备对应的IMSI的映射关系。

[0117] 在另一种应用场景中，用户设备与该用户设备所属的归属网络控制设备之间没有预先共享一个初始随机标识P，那么当用户设备执行初始接入过程时，在第一接入请求消息中需要携带IMSI，该IMSI可以唯一识别出该用户设备。之后，归属网络控制设备会向该用户设备发送一个随机标识P，用户设备在后续初始接入时，就可以不再携带IMSI，而是携带随机标识P。

[0118] 本发明实施例以第一种场景为例进行说明，在后续实施例中，统一用随机标识P来表示该用户设备的标识。相应的，在第二种场景中，标识可以是用户设备的IMSI，且后续执行过程可以参考针对第一种场景的步骤描述，不再赘述。

[0119] 可选的，该第一接入请求消息中还可以携带归属网络标识，用于指示该用户设备归属于哪一个网络，以使服务网络控制设备接收到第一接入请求消息后，根据该归属网络标识确定该用户设备属于哪一个归属网络，例如：中国移动网络、中国联通网络、中国电信网络等。在漫游场景中：服务网络控制设备需要基于归属网络标识才能知道该用户设备所属的归属网络控制设备。

[0120] 可选的，若随机标识P是由MNC、MCC和随机字符串组成的，则第一接入请求消息中可以不携带归属网络标识，根据MNC和MCC就可以确定出该用户设备归属于哪一个网络。

[0121] 可选的，用户设备向无线接入网设备发送该第一接入请求消息，无线接入网设备接收用户设备发送的该第一接入请求消息。无线接入网设备再将该第一接入请求消息发送给服务网络控制设备，服务网络控制设备接收无线接入网设备发送的第一接入请求消息。

[0122] 可选的，用户设备可以直接发送第一接入请求消息至服务网络控制设备。

[0123] S402：服务网络控制设备接收用户设备发送的第一接入请求消息，向该用户设备所属的归属网络控制设备发送第一认证数据请求消息，该第一认证数据请求消息中携带该用户设备的随机标识P。

[0124] 具体的，服务网络控制设备接收用户设备发送的第一接入请求消息，根据该第一接入请求消息中携带的归属网络标识，找到对应的归属网络控制设备，并向该归属网络控制设备发送携带随机标识P的第一认证数据请求消息。

[0125] 可选的，该第一认证数据请求消息中还可以包括本服务网的网络标识(英文：Serving Network ID，简称：SNID)，SNID用于指示UE所接入的服务网络控制设备所属的服务网络，例如：中国移动网络、中国联通网络、中国电信网络等。

[0126] 若所述第一接入消息包含归属网络标识，则服务网络控制设备可以根据该归属网络标识找到对应的归属网络控制设备，从而向该归属网络控制设备发送第一认证数据请求消息。

[0127] 可选的，若随机标识中包含MNC和MCC，则服务网络控制设备可以根据MNC和MCC确定归属网络控制设备，从而向该归属网络控制设备发送第一认证数据请求消息。

[0128] S403：归属网络控制设备接收服务网络控制设备发送的携带随机标识P的第一认证数据请求消息，生成认证向量AV，该AV中包括第一随机数和第一指示信息，该第一指示信息用于指示该第一随机数中包含更新的随机标识。

[0129] 归属网络控制设备根据第一认证数据请求消息中携带的随机标识P，在本端数据库中查找该随机标识P对应的根密钥K，该根密钥K也就是该用户设备的根密钥。具体的，归属网络控制设备中存储有随机标识P和根密钥K的映射表。该映射表中记录有随机标识P与根密钥K的映射关系，此外，该映射表中还可以记录有用户设备的永久标识，例如IMSI。该映射表可如表1所示。

[0130] 表1

[0131]

IMSI	随机标识P	根密钥K
460011418603055	01	111111
460030912121001	02	000000

[0132] 由表1可知，随机标识为01的用户设备对应的根密钥K为111111，随机标识为02的用户设备对应的根密钥K为000000。

[0133] 归属网络控制设备获取到该用户设备对应的根密钥K后，首先确定是否需要更新该用户设备的随机标识。如果确定不需要更新该用户设备的随机标识P，则归属网络控制设备会随机产生一个第一随机数，然后根据第一随机数、自身当前保存的鉴权序列号SQN、根密钥K以及其它信息生成该用户设备对应的AV，其中AV包括：第一随机数、AUTN、XRES和共享密钥K_{ASME}。需要说明的是，这里是以LTE中的AV向量为例进行的说明，3G的AV向量中包括加密密钥CK和完整性密钥IK，而不包括K_{ASME}，K_{ASME}是由CK和IK推衍生成的，其中，CK用于对用户数据进行加密，IK用于对用户数据进行完整性保护。其中，AUTN是由SQN与AK进行异或运算得到的值、AMF以及MAC这三个内容组成的。未来5G系统中AV所包括的内容在此不作限定。

[0134] 如果归属网络控制设备确定需要更新该用户设备的随机标识P，则归属网络控制设备首先生成新的随机标识(为了便于描述，本发明实施例以随机标识P'作为新的随机标识)，然后重新定义第一随机数，将新的随机标识P'携带在第一随机数中。具体的，将第一随机数定义为：由X、Y和随机字符串三部分组成的字符串。其中，随机字符串是由归属网络控制设备随机生成的字符串。X＝Enc(P')，Enc为采用密钥CKP的加密算法，Enc(P')表示采用CKP对随机标识P'进行加密之后得到的加密数据。Y＝MAC(X)，MAC为采用IKP的完整性保护算法，MAC(X)表示采用IKP对随机标识P'的加密数据进行完整性保护之后得到的完整性保护数据。MAC(X)是用来让用户设备认证接收到的Enc(P')是否未被第三方篡改。可选的，X还可以是Enc(P'||C)，其中，||表示级联，C表示计数器，可以每个用户设备的计数器都不同，也即是说，每个用户设备都维护一个计数器，归属网络控制设备也为每个用户设备维护一个计数器，该计数器记录的数值是该用户设备的随机标识更新的总次数。或者，C表示归属网络控制设备自己的计数器。C的作用是为了统计随机标识处理的次数。可选的，Y还可以是MAC(X||C)，关于C的描述与上述相同。可选的，Y还可以是MAC(P')，所述Y为针对P'计算的完整性保护数据。可选的，Y还可以是MAC(P'||C)，关于C的描述与上述相同。可选的，第一随机数还可以只由X和随机字符串两部分组成。也即是说，第一随机数中可以只包括随机标识P'对应的加密数据以及一串随机字符串，而不包括完整性保护数据。本发明实施例中以第一随机数中包括X、Y以及随机字符串三部分并且X＝Enc(P')、Y＝MAC(X)为例进行说明，即第一随机数中包括随机标识P'对应的加密数据、随机标识P'对应的完整性保护数据以及一串随机字符串。

[0135] 可选的，在本发明实施例中用户设备与归属网络控制设备之间可以预先协商第一随机数中的各个参数的长度以及位置。比如：第一随机数的长度为128比特，其中，随机标识P'的长度为40比特，Enc(P')的长度为40比特，MAC(Enc(P'))的长度为16比特，随机字符串的长度为16比特。例如，第一随机数中的第1至第40位代表Enc(P')，第41至第56位代表MAC(Enc(P'))，第57至第76位代表随机字符串。因此，用户设备在接收到第一随机数后，可以从第一随机数中解析出各个参数。

[0136] 然后归属网络控制设备根据第一随机数、自身当前保存的鉴权序列号SQN、根密钥K以及其它信息生成该用户设备对应的AV。其中AV包括：第一随机数、AUTN、XRES和共享密钥K_{ASME}。该过程可以参考上述描述，此处不再赘述。

[0137] 此外，归属网络控制设备还会在AUTN中的AMF中携带第一指示信息，用来指示第一随机数中包含更新的随机标识P'。该第一指示信息可以通过AMF中的一个比特(bit)来指示，也可以通过两个或者更多个比特来指示。例如，AMF是由16个比特组成的字符串，其中每个比特都有不同的定义，16个比特中的八位用于标准化使用，另外的八位用于特定运算符使用。归属网络控制设备可以将其中未使用的比特做新的定义。假设初始AMF中未使用的比特都为0，定义其中预设的一个比特置为1时，表示第一随机数中包含更新的随机标识P'，当这一位比特置为0时，表示第一随机数中不包含更新的随机标识P'。或者，假设初始AMF中未使用的比特都为0，定义其中预设的两个比特作为第一指示信息的标志位，当这两位被置为11时，表示第一随机数中包含更新的随机标识P'，当这两位被置为10时，表示第一随机数中不包含更新的随机标识P'。可选的，假设AMF中未使用的比特都为1，定义其中预设的一个比特置为0时，表示第一随机数中包含更新的随机标识P'，当这一位比特置为1时，表示第一随机数中不包含更新的随机标识P'。需要说明的是，用户设备与归属网络控制设备需要预先协商好通过AMF中的哪一个比特或者哪几个比特来作为第一指示信息的比特位，这样的话，用户设备在接收到AMF后，就可以通过解析这一个比特或者这几个比特的值，来确定出第一随机数中是否包括更新的随机标识P'。

[0138] 可选的，在本发明实施例中用户设备与归属网络控制设备之间可以预先协商AUTN中的各个参数的长度和位置。比如：AUTN的长度为128比特，其中，SQN的长度为48比特，AMF的长度为16比特，MAC的长度为16比特。例如，AUTN中的第1至第48位代表SQN与AK的异或值，第49至第64位代表AMF，第65至第80位代表MAC。因此，用户设备在接收到AUTN后，可以从AUTN中解析出各个参数。

[0139] 需要说明的是，本发明实施例是以第一指示信息通过AUTN中的AMF中的比特来指示的，在其他可选的实现方式中，第一指示信息还可以通过其他字段来指示，例如，通过第一随机数中的一个比特或者两个比特或者多个比特来指示，本发明实施例对此不作限定。

[0140] S404：归属网络控制设备向该服务网络控制设备发送认证向量AV，该认证向量AV中包括第一随机数和第一指示信息。

[0141] S405：服务网络控制设备接收归属网络控制设备发送的AV，并向该用户设备发送AV中的第一随机数和AUTN，该AUTN中包括第一指示信息。

[0142] 可选的，服务网络控制设备将第一随机数和AUTN发送给无线接入网设备，无线接入网设备接收服务网络控制设备发送的第一随机数和AUTN。无线接入网设备再将该第一随机数和AUTN发送给用户设备，用户设备接收无线接入网设备发送的第一随机数和AUTN。

[0143] S406:用户设备接收服务网络控制设备发送的第一随机数和AUTN,根据第一随机数和AUTN对网络侧进行校验,并且根据AUTN中的第一指示信息确定第一随机数中是否包括更新的随机标识。

[0144] 用户设备接收到第一随机数和AUTN后,根据自身存储的根密钥K和第一随机数验证AUTN的正确性,从而对网络侧进行校验。验证过程具体可以是:用户设备根据第一随机数和根密钥K计算得到AK,再根据AK以及AUTN中的SQN与AK进行异或运算得到的值计算得到SQN,接着根据第一随机数、SQN、AUTN中的AMF和根密钥K共同计算出一个XMAC,并将XMAC和接入响应消息中的MAC做比较,如果相同,则接着校验收到的SQN是否等于本地保存的SQN,如果是,则该用户设备成功地认证了网络,执行步骤S407。用户设备接着根据该第一随机数和根密钥K计算得到RES和K_{ASME},其中RES用于网络认证该用户设备。

[0145] 并且,用户设备验证AMF中的预设的比特是否置为1,若否,则表明接收到的第一随机数中未携带更新的随机标识P';若是,则表明第一随机数中携带了更新的随机标识P'。若确定出第一随机数中携带了更新的随机标识P',用户设备需要从第一随机数中解析出更新的随机标识P'。具体的,若第一随机数中包括X、Y和随机字符串三部分,则用户设备需要对第一随机数进行拆分,按照预先协商的第一随机数的组成结构将第一随机数拆分为三部分,分别对应Enc(P')、MAC(Enc(P'))和随机字符串。用户设备根据密钥IKP和Enc(P')对MAC(Enc(P'))进行完整性验证,具体的,用户设备根据IKP和Enc(P')生成一个MAC,验证这个MAC是否与MAC(Enc(P'))相同,若是,则表明Enc(P')未被篡改。之后,用户设备采用CKP对Enc(P')进行解密,得到更新的随机标识P'。可选的,用户设备还可以先对Enc(P')进行解密,再对MAC(Enc(P'))进行完整性验证。

[0146] 或者,若第一随机数只包括X和随机字符串,则用户设备需要对第一随机数进行拆分,按照预先协商的第一随机数的组成结构将第一随机数拆分为两部分,分别对应Enc(P')和随机字符串。用户设备采用CKP对Enc(P')进行解密,从而得到更新的随机标识P'。

[0147] 或者,若第一随机数中携带的X为Enc(P'||C),则用户设备采用CKP对Enc(P'||C)进行解密,得到更新的随机标识P'和C,用户设备可以基于自身存储的计数器与C进行比较,若相同,则表示用户设备与网络侧的随机标识更新次数相同,是同步的。其中,该计数器记录的是该用户设备的随机标识更新的总次数,C的初始值可以为0。可选,随机标识更新后,C加1。或者用户设备接收到消息后,C加1,之后再对比与解密得到的C是否相同。或者,第一随机数中Y=MAC(X||C)包含其他形式,则采用C和X一起验证Y是否正确。或者Y=MAC(P'),则解密得到P'后再验证Y是否正确。或者Y=MAC(P'||C),则解密得到P'后,与C一起验证Y是否正确。

[0148] 用户设备得到更新的随机标识P'后,保存新的随机标识P',并释放旧的随机标识P。或者,用户设备还可以既保存新的随机标识P',又保存旧的随机标识P,以使得在接入过程中如果不能通过新的随机标识P'成功接入网络,还可以采用旧的随机标识P接入网络,提高了用户设备成功接入网络的几率。

[0149] S407:用户设备向服务网络控制设备发送RES。

[0150] 可选的,用户设备向无线接入网设备发送RES,无线接入网设备接收用户设备发送的RES。无线接入网设备向服务网络控制设备发送RES,服务网络控制设备接收无线接入网设备发送的RES。

[0151] S408:服务网络控制设备接收用户设备发送的RES,将RES与该用户设备对应的AV中的XRES进行比较,若相同,则服务网络控制设备对该用户设备认证成功。

[0152] S409:服务网络控制设备向该用户设备所属的归属网络控制设备发送位置更新请求,该位置更新请求中携带该用户设备的随机标识P,该位置更新请求用于通知该归属网络控制设备该服务网络控制设备已对该用户设备认证成功。

[0153] 需要说明的是,本发明实施例中是以服务网络控制设备向该用户设备所属的归属网络控制设备发送位置更新请求为例,来通知该归属网络控制设备该服务网络控制设备已对该用户设备认证成功这一事件的,其中,位置更新请求是现有的接入过程中的信令,用于指示归属网络控制设备该用户设备的位置发生了更新。在其他可选的实现方式中,服务网络控制设备还可以向该用户设备所属的归属网络控制设备发送其他的信令消息来通知该归属网络控制设备该服务网络控制设备已对该用户设备认证成功这一事件,本发明实施例对此不作具体限定。例如,服务网络控制设备通过新定义的请求消息来通知该归属网络控制设备该服务网络控制设备已对该用户设备认证成功这一事件。可选的,服务网络控制设备不发送随机标识P,而发送其他消息(例如,字符串"OK")至归属网络控制设备,以通知归属网络控制设备已对用户设备认证成功。归属网络控制设备可以通过与服务网络控制设备之间的第S402和S406的通话标识确定是哪一个用户认证成功。

[0154] S410:归属网络控制设备接收该服务网络控制设备发送的位置更新请求,根据该位置更新请求中携带的随机标识P即可获知该服务网络控制设备已对该用户设备认证成功。

[0155] 作为一种实现方式,归属网络控制设备确定该服务网络控制设备已对该用户设备认证成功后,保存该用户设备对应的新的随机标识P',并且释放该用户设备对应的旧的随机标识P。

[0156] 作为另一种实现方式,归属网络控制设备确定该服务网络控制设备已对该用户设备认证成功后,同时保存该用户设备对应的新的随机标识P'和旧的随机标识P。这样做的好处在于可以避免以下情况的发生:若归属网络控制设备在生成了新的随机标识P'之后,就释放旧的随机标识P,若第三方攻击者通过伪造接入请求消息,触发归属网络控制设备释放合法用户的旧的随机标识P,从而造成合法用户不能接入网络。

[0157] 可选的,归属网络控制设备执行完上述步骤之后,还可以向该服务网络控制设备发送位置更新确认消息。

[0158] 需要说明的是,本发明实施例中的位置更新确认消息是现有的接入过程中的信令,用于指示该服务网络控制设备已对该用户设备的位置进行了更新。在其他可选的实现方式中,归属网络控制设备还可以通过其他信令消息来通知该服务网络控制设备已对该用户设备的位置进行了更新这一事件,本发明实施例对此不作具体限定。例如,归属网络控制设备通过新定义的确认消息来通知该服务网络控制设备已对该用户设备的位置进行了更新这一事件。

[0159] 通过执行本发明实施例,归属网络控制设备可以通过第一指示信息明确告知用户设备第一随机数中包括更新的随机标识,用户设备通过解析第一指示信息就可以直接确认出接收到的第一随机数中包括更新的随机标识,无需进行额外的计算处理过程,节省了用户设备的开销,降低了用户设备的处理复杂度。

[0160] 可选的，用户设备可以划分为USIM/SIM模块和ME两部分，结合图5针对这两个模块来对图4中的步骤S406和步骤S407进行详细描述。该过程包括如下步骤。

[0161] S501：ME接收服务网络控制设备发送的第一随机数和AUTN，该AUTN中包括第一指示信息。

[0162] S502：ME向USIM/SIM模块发送第一随机数和AUTN。

[0163] S503：USIM/SIM模块接收ME发送的第一随机数和AUTN，根据收到的第一随机数和AUTN，对网络侧进行校验。

[0164] 具体的，USIM/SIM模块存储有根密钥K，根据根密钥K和第一随机数验证AUTN的正确性。验证成功，则USIM/SIM计算RES和K_{ASME}。

[0165] 可选的，USIM/SIM模块还可以与归属网络控制设备预共享一个随机标识P，在初始接入过程中，USIM/SIM模块将随机标识P发送给ME，ME向服务网络控制设备发送携带随机标识P的第一接入请求消息。

[0166] 可选的，USIM/SIM模块中也存储IMSI，并存储随机标识P与IMSI的映射关系。在随机标识P不能接入网络时，USIM/SIM模块可采用IMSI接入网络。

[0167] 可选的，ME还可以与归属网络控制设备预共享一个随机标识P，在初始接入过程中，ME向服务网络控制设备发送携带随机标识P的第一接入请求消息。

[0168] S504：USIM/SIM模块向ME发送RES。

[0169] S505：ME接收USIM/SIM模块发送的RES，根据第一指示信息确定第一随机数中是否包括更新的随机标识P’。

[0170] 具体的，ME验证AMF中的预设的比特是否置为1，若是，则表明接入响应消息中的第一随机数中携带了更新的随机标识P’，则ME采用随机标识加密密钥CKP从第一随机数中获取更新的随机标识P’，获取随机标识P’的方式可参见图4所示实施例中的步骤S406中的描述，此处不再赘述。

[0171] 其中，ME可以与归属网络控制设备预共享CKP和IKP，这种情况下，USIM/SIM模块可以不需要升级，节省了成本；或者，USIM/SIM模块与归属网络控制设备预共享CKP和IKP，这种情况下，在上述步骤S504中，USIM/SIM模块需要将CKP和IKP发送给ME，使得ME可以采用CKP从第一随机数中获取更新的随机标识P’。ME得到新的随机标识P’之后，保存此随机标识P’，并释放旧的随机标识P，或者，ME保存新的随机标识P’，同时也保存旧的随机标识P。

[0172] 或者，采用CKP从第一随机数中获取更新的随机标识P’这一动作还可以在USIM/SIM模块中执行，此时，ME不需要再执行该动作。

[0173] S505：ME向服务网络控制设备发送RES。

[0174] 上述实施例中所描述的随机标识保护密钥可以是用户设备与归属网络控制设备之间预共享的，还可以是用户设备与归属网络控制设备之间采用相同的密钥派生参数派生的，还可以是归属网络控制设备生成并下发给用户设备的，以下分别对这三种情况进行描述。本发明实施例中以随机标识保护密钥既包括CKP又包括IKP来进行描述，如果归属网络控制设备向用户设备发送的第一随机数中只包括X和随机字符串，而不包括Y，那么用户设备与归属网络控制设备之间也就不需要预共享IKP，也不需要派生IKP，因此，在这种场景中，只涉及CKP的生成。

[0175] 第一种情况：CKP和IKP可以是用户设备与归属网络控制设备之间预共享的，例如，

在制造用户设备，或者在制造USIM/SIM模块时可以将CKP和IKP一次性写入，同时在归属网络控制设备中也存储该CKP和IKP，用于后续过程中，归属网络控制设备向该用户设备发送更新的随机标识时，采用该CKP和IKP对更新的随机标识进行加密以及完整性保护，同时，用户设备接收到归属网络控制设备发送的更新的随机标识时，可以通过该CKP和IKP对该更新的随机标识进行解密以及完整性验证，从而获得更新的随机标识。

[0176] 第二种情况，CKP和IKP是用户设备与归属网络控制设备之间采用相同的密钥派生参数派生的，在这种情况下，在图4所示的数据传输过程之前，归属网络控制设备利用AKA的流程，派生CKP和IKP，用户设备在这个过程中也会派生CKP和IKP，从而实现用户设备与归属网络控制设备之间CKP和IKP的共享。因此，在后续过程中，如果归属网络控制设备向用户设备发送随机标识，就可以采用CKP和IKP对该随机标识进行加密和完整性保护，从而提高随机标识传输的安全性。结合图6来描述该过程，该过程具体包括如下步骤。

[0177] S601：用户设备向服务网络控制设备发送第二接入请求消息，该第二接入请求消息中携带该用户设备的随机标识P。

[0178] 本发明实施例以第二接入请求消息携带用户设备对应的随机标识P为例进行说明，除了随机标识P，第二接入请求消息中还可以携带其他标识来标识该用户设备，该标识包括但不限于：IMSI、IMEI、IMPI、IMPU、TMSI、MAC地址、IP地址、手机号码和GUTI。

[0179] S602：服务网络控制设备接收用户设备发送的第二接入请求消息，向该用户设备所属的归属网络控制设备发送第二认证数据请求消息，该第二认证数据请求消息中携带该用户设备的随机标识P。

[0180] 本发明实施例中的步骤S601和S602可以参考图4所示实施例中的步骤S401和S402，此处不再赘述。

[0181] S603：归属网络控制设备接收服务网络控制设备发送的携带随机标识P的第二认证数据请求消息，生成认证向量AV，该AV中包括第二随机数和第二指示信息，该第二指示信息用于指示该用户设备需要派生CKP和IKP。

[0182] 具体的，本发明实施例中的第二随机数未做重新定义，即第二随机数是归属网络控制设备随机生成的一组字符串。步骤S603与图4所示实施例中的步骤S403的区别在于AMF。归属网络控制设备会在AUTN中的AMF中携带第二指示信息，用来指示用户设备是否需要生成CKP和IKP。该第二指示信息可以通过AMF中的一个比特来指示，也可以通过两个或者更多个比特来指示。例如，AMF是由16个比特组成的字符串，其中每个比特都有不同的定义，16个比特中的八位用于标准化使用，另外的八位用于特定运算符使用。归属网络控制设备可以将其中未使用的比特做新的定义。假设初始AMF中未使用的比特都为0，定义其中预设的一个比特置为1时，表示用户设备需要用户设备生成CKP和IKP。其中，本发明实施例第二指示信息与图4所示实施例中的第一指示信息可以分别占用AMF中不同的比特来进行区分。

[0183] 需要说明的是，本发明实施例是以第二指示信息通过AUTN中的AMF中的比特来指示的，在其他可选的实现方式中，第二指示信息还可以通过其他字段来指示，例如，通过第二随机数中的一个比特或者两个比特或者多个比特来指示，本发明实施例对此不作限定。

[0184] 此外，归属网络控制设备还会采用密钥派生参数和密钥派生算法生成CKP和IKP，该密钥派生参数和密钥派生算法是用户设备与归属网络控制设备之间预先协商好的。例如，生成CKP和IKP的公式如下：CKP＝KDF((K、CK、IK和K_{ASME}中的至少一项)，(第二随机数、

SQN、加密算法标识、归属网络控制设备ID和SNID中的至少一项)。其中,KDF为密钥推演函数(英文:Key Derivation Function)。IKP=KDF((K、CK、IK和K_{ASME}中的至少一项),(第二随机数、SQN、完整性保护算法标识、归属网络控制设备ID和SNID中的至少一项)。

[0185] S604:归属网络控制设备向该服务网络控制设备发送认证向量AV,该认证向量AV中包括第二随机数和第二指示信息。

[0186] S605:服务网络控制设备接收归属网络控制设备发送的AV,保存该AV,并向该用户设备发送AV中的第二随机数和AUTN,该AUTN中包括第二指示信息。

[0187] S606:用户设备接收服务网络控制设备发送的第二随机数和AUTN,根据收到的第二随机数和AUTN,对网络侧进行校验,并且根据第二指示信息确定需要派生CKP和IKP。

[0188] 其中,验证过程可参见图4所示实施例中的步骤S406,此处不再赘述。

[0189] 具体的,用户设备验证AMF中的预设的比特是否置为1,若否,则表明不需要派生CKP和IKP;若是,则表明需要派生CKP和IKP。如果确定出需要判断CKP和IKP,则用户设备采用与归属网络控制设备预先协商好的密钥派生参数和密钥派生算法派生CKP和IKP。生成CKP和IKP的公式可以参见步骤S604。

[0190] 需要说明的是,若CKP和IKP的密钥派生参数中包括K_{ASME},则用户设备需要先使用CK和IK生成K_{ASME}。若CKP和IKP的密钥派生参数中不包括根密钥K,则CKP和IKP的生成过程可以由用户设备中的ME执行,因此,在一种可选的实现方式中,ME与归属网络控制设备预先协商密钥派生参数和密钥派生算法。若CKP和IKP的生成需要根密钥K,则CKP和IKP的生成过程可以由USIM/SIM模块执行。这种方式中,USIM/SIM模块将生成的CKP和IKP发送给ME。

[0191] S607:用户设备向服务网络控制设备发送RES。

[0192] S608:服务网络控制设备接收用户设备发送的RES,将RES与该用户设备对应的AV中的XRES进行比较,若相同,则服务网络控制设备对该用户设备认证成功。

[0193] S609:服务网络控制设备向该用户设备所属的归属网络控制设备发送位置更新请求,该位置更新请求中携带该用户设备的随机标识P,该位置更新请求用于通知该归属网络控制设备该服务网络控制设备已对该用户设备认证成功。

[0194] 其中,步骤S607-S609可参见图4所示实施例中的步骤S407-S409,此处不再赘述。

[0195] 并且,图6所示实施例中的AKA过程是在图4所示实施例中的AKA过程之前执行的,也即是说,在执行图4所示的AKA过程之前,用户设备与归属网络控制设备就已经进行了相互鉴权认证的过程,因此,执行完图6所示实施例之后,再执行图4所示实施例的时候,就可以不需要再次进行相互鉴权认证的过程了,在图4所示的初始接入过程中,归属网络控制设备只需要将用户设备更新的随机标识下发给用户设备即可。

[0196] 或者,归属网络控制设备还可以在一次AKA过程中同时将更新后的随机标识P'以及用于指示用户设备派生CKP和IKP的指示信息发送给用户设备。其中,归属网络控制设备采用该CKP和IKP对该随机标识P'进行了加密以及完整性保护。具体的,结合图6的过程来描述本发明实施例,本发明实施例与图6所示实施例的区别主要体现在:

[0197] 针对步骤S603:归属网络控制设备接收到服务网络控制设备发送的携带随机标识P的第二认证数据请求消息后,生成一个随机数,并基于该随机数以及该用户设备对应的根密钥K生成该用户设备对应的认证向量AV,该AV中携带第二指示信息,该第二指示信息用于指示返回的消息中携带有更新后的随机标识以及用户设备需要生成CKP和IKP。并且归属网

络控制设备基于该随机数以及密钥派生参数和密钥派生算法生成CKP和IKP，然后采用CKP对更新后的随机标识P'进行加密得到加密数据，并采用IKP对该加密数据进行完整性保护得到完整性保护数据，其中，密钥派生参数和密钥派生算法可以参见步骤S603，此处不再赘述。

[0198] 具体的，第二指示信息可以采用AMF中的一个比特或者多个比特来指示。假设初始AMF中未使用的比特都为0，定义其中预设的一个比特置为1时，表示返回的消息中携带有更新后的随机标识以及用户设备需要生成CKP和IKP，当这一位比特置为0时，表示返回的消息中未携带有更新后的随机标识以及用户设备不需要生成CKP和IKP。

[0199] 针对步骤S604：归属网络控制设备向服务网络控制设备发送认证向量AV、采用CKP对更新后的随机标识P'进行加密得到的加密数据以及采用IKP对该加密数据进行完整性保护得到的完整性保护数据。服务网络控制设备接收归属网络控制设备发送的认证向量AV、采用CKP对更新后的随机标识P'进行加密得到的加密数据以及采用IKP对该加密数据进行完整性保护得到的完整性保护数据。保存该认证向量AV，并向该用户设备发送认证向量AV中的随机数、采用CKP对更新后的随机标识P'进行加密得到的加密数据以及采用IKP对该加密数据进行完整性保护得到的完整性保护数据。用户设备接收服务网络控制设备发送的随机数、采用CKP对更新后的随机标识P'进行加密得到的加密数据以及采用IKP对该加密数据进行完整性保护得到的完整性保护数据。根据AV中携带的第二指示信息确定出返回的消息中携带有更新后的随机标识以及用户设备需要生成CKP和IKP，因此，用户设备基于密钥派生参数和密钥派生算法生成CKP和IKP，并采用生成的CKP对加密数据进行加密，采用生成的IKP对完整性保护数据进行校验，从而获取到更新后的随机标识P'。

[0200] 本发明实施例中的其他过程与图6所示实施例中的类此，此处不再赘述。

[0201] 第三种情况：CKP和IKP是由归属网络控制设备生成并下发给用户设备的，在这种情况中，在第一种实现方式中，归属网络控制设备可以通过一次AKA过程将自身生成的CKP和IKP发送给用户设备，之后再通过一次AKA过程将更新的随机标识P'发送给用户设备。在第二种实现方式中，归属网络控制设备可以在同一次AKA过程中将更新的随机标识P'以及下一次发送新的随机标识时需要使用的CKP和IKP一同发送给用户设备。

[0202] 针对第三种情况中的第一种实现方式，归属网络控制设备在图4所示的数据传输过程之前，通过AKA流程将自身生成的CKP和IKP发送给用户设备。具体的，结合图6来描述归属网络控制设备将自身生成的CKP和IKP发送给用户设备。

[0203] 本发明实施例中与图6所示实施例的实现过程类似，不同点主要体现在：

[0204] 针对步骤S603，第二指示信息用于指示该第二随机数中包括CKP和IKP。

[0205] 具体的，归属网络控制设备采用密钥派生参数和密钥派生算法生成CKP和IKP。其中，密钥派生参数和密钥派生算法可以是归属网络控制设备本地配置的，例如，生成CKP和IKP的公式可以参见步骤S603中的描述。

[0206] 本发明实施例中的第二随机数需要重新定义，将归属网络控制设备生成的CKP和IKP携带在第二随机数中。具体的，将第二随机数定义为：由A、B、C、D和随机字符串五部分组成的字符串。其中，随机字符串是由归属网络控制设备随机生成的字符串。A表示采用用户设备的根密钥K对CKP进行加密得到的加密数据，B表示采用根密钥K对A进行完整性保护得到的完整性保护数据，C表示采用根密钥K对IKP进行加密得到的加密数据，D表示采用根密

钥K对C进行完整性保护得到的完整性保护数据。这里，CKP和IKP用于在后续过程中，归属网络控制设备向用户设备发送更新的随机标识P'时所采用的加密密钥和完整性密钥。

[0207] 可选的，第二随机数还可以仅包括A、B和随机字符串三部分。其中A表示采用用户设备的根密钥K对CKP和IKP一起进行加密得到的加密数据，B表示采用根密钥K对A进行完整性保护得到的完整性保护数据。

[0208] 此外，归属网络控制设备会在AUTN中的AMF中携带第二指示信息，用来指示第二随机数中包括CKP和IKP。具体的，该第二指示信息可以通过AMF中的一个比特来指示，也可以通过两个或者更多个比特来指示。例如，AMF是由16个比特组成的字符串，其中每个比特都有不同的定义，16个比特中的八位用于标准化使用，另外的八位用于特定运算符使用。归属网络控制设备可以将其中未使用的比特做新的定义。假设初始AMF中未使用的比特都为0，定义其中预设的一个比特置为1时，表示第二随机数中包括CKP和IKP。

[0209] 针对步骤S606，用户设备根据第二指示信息确定第二随机数中包括CKP和IKP。

[0210] 具体的，用户设备验证AMF中的预设的比特是否置为1，若否，则表明第二随机数中不包括CKP和IKP；若是，则表明第二随机数中包括CKP和IKP。如果确定出第二随机数中包括CKP和IKP，则用户设备需要从第二随机数中解析出CKP和IKP。具体的，若第一随机数中包括A、B、C、D和随机字符串五部分，则用户设备需要对第二随机数进行拆分，按照预先协商的第一随机数的组成结构将第二随机数拆分为五部分，分别对应CKP的加密数据、CKP的完整性保护数据、IKP的加密数据、IKP的完整性保护数据以及随机字符串。用户设备根据根密钥K和CKP的加密数据对CKP的完整性保护数据进行完整性验证，验证成功后，采用根密钥K对CKP的加密数据进行解密，得到CKP。同样的，用户设备根据根密钥K和IKP的加密数据对IKP的完整性保护数据进行完整性验证，验证成功后，采用根密钥K对IKP的加密数据进行解密，得到IKP。

[0211] 可选的，若归属网络控制设备将新的CKP和IKP一起进行保护，即第三随机参数包含三个部分，A、B和随机字符串；则用户设备采用K和A验证B的正确性，验证成功后，再针对A执行解密动作得到CKP和IKP。

[0212] 可选的，上述流程中采用K执行加密和完整性保护。也可能，采用旧的CKP，执行机密性保护，另外采用旧的IKP执行完整性保护。对应的，用户设备可以采用旧CKP解密得到新的CKP和IKP，另外，利用旧的IKP验证完整性是否成立。

[0213] 可选的，上述流程仅执行针对新CKP和IKP的机密性保护，不执行完整性保护。

[0214] 可选的，针对旧的CKP和IKP加密和完整性保护多种可能性，可以参考图4所对应流程。此处不再赘述。

[0215] 本发明实施例中的其他过程与图6所示实施例中的执行过程一致，此处不再赘述。

[0216] 针对第三种情况中的第二种实现方式，结合图4来描述该过程。本发明实施例中与图4所示实施例的实现过程类似，不同点主要体现在：

[0217] 针对步骤S403，若归属网络控制设备判断出需要更新该用户设备的随机标识并且需要派生新的CKP'和IKP'时，归属网络控制设备执行以下几个动作：生成随机标识P'。采用旧的随机标识保护密钥加密和/或完整性保护随机标识P'。生成新的CKP'和IKP'，生成新的CKP'和IKP'时才用到的密钥派生参数和密钥派生算法可以参见图6所示实施例中的步骤S603。生成第一随机数。定义AMF中的第一指示信息，该第一指示信息用于指示第一随机数

中包括更新的随机标识以及需要用户设备派生新的CKP'和IKP'。其中，新的CKP'和IKP'用于归属网络控制设备下一次向用户设备发送更新的随机标识P"，对该随机标识P"进行加密和完整性包括，也即是说，每次传输更新的随机标识均采用新的密钥进行加密和完整性保护，进一步提高了传输的随机标识的安全性。具体的，本发明实施例中需要对第一随机数进行重新定义，第一随机数中包括：X、Y和随机字符串。其中，X＝Enc(P')，Y＝MAC(X)。

[0218] 具体的，可以通过AMF中的两个比特来指示，也可以通过更多个比特来指示。例如，AMF是由16个比特组成的字符串，其中每个比特都有不同的定义，16个比特中的八位用于标准化使用，另外的八位用于特定运算符使用。归属网络控制设备可以将其中未使用的比特做新的定义。假设初始AMF中未使用的比特都为0，定义其中预设的两个比特置为1时，表示第一随机数中包含更新的随机标识P'并且用户设备需要派生新的CKP'和IKP'，当这一位比特置为0时，表示第一随机数中不包含更新的随机标识P'并且用户设备不需要派生新的CKP'和IKP'。

[0219] 针对步骤S406，用户设备接收到服务网络控制设备发送的第一随机数和AUTN，通过识别AUTN中的AMF携带的第一指示信息，就可以确定出接收到的第一随机数中包含更新的随机标识以及需要派生新的CKP'和IKP'。具体的，用户设备验证AMF中的预设的两个比特是否置为1，若否，则表明第一随机数中未携带更新的随机标识P'并且不需要派生新的CKP'和IKP'；若是，则表明第一随机数中携带了更新的随机标识P'并且需要派生新的CKP'和IKP'。因此，用户设备采用图4所示实施例中的方法，采用旧的CKP对第一随机数中的Enc(P')进行解密，得到更新的随机标识P'，并采用旧的IKP和Enc(P')对第一随机数中的MAC(Enc(P'))进行完整性验证。并且用户设备采用图6所示实施例中的密钥派生参数以及密钥派生算法，推衍得到新的CKP'和IKP'。本发明实施例中的其他过程与图4所示实施例中的类似，此处不再赘述。

[0220] 或者，归属网络控制设备将自身生成的新的CKP'和IKP'进行加密和完整性保护，并将加密和完整性保护之后的CKP'和IKP'携带在第一随机数中发送给用户设备，此时，第一指示信息用于指示第一随机数中包括更新的随机标识P'以及新的CKP'和IKP'。

[0221] 具体的，归属网络控制设备重新定义第一随机数，第一随机数由X、Y、E、F、G、H和随机字符串组成。其中，X＝Enc(P')，Y＝MAC(X)，E＝Enc(CKP')，F＝MAC(E)，G＝Enc(IKP')，H＝MAC(G)。Enc为采用旧的密钥CKP的加密算法，MAC为采用旧的密钥IKP的完整性保护算法。Enc(CKP')表示采用CKP对新的密钥CKP'进行加密之后得到的加密数据。MAC(E)表示采用IKP对新的密钥CKP'进行完整性保护之后得到的完整性保护数据。Enc(IKP')表示采用CKP对新的密钥IKP'进行加密之后得到的加密数据。MAC(G)表示采用IKP对新的密钥IKP'进行完整性保护之后得到的完整性保护数据。需要说明的是，对新的密钥CKP'进行加密或完整性所使用的密钥、对新的密钥IKP'进行加密或完整性保护所使用的密钥与对随机标识P'进行加密或完整性保护所使用的密钥可以相同，也可以不同，并且使用的密钥需要用户设备与归属网络控制设备预先协商。

[0222] 可选的，第一随机数格式为X、Y、E、F和随机字符串。X、Y的描述与上述相同。但E和F分别为，E＝Enc(CKP'||IKP')，F＝MAC(E)。此时通过E可以将新的CKP'和IKP'同时发送给用户设备。

[0223] 可选的，第一随机数格式为X、Y、E、F和随机字符串。流程中采用K执行加密和完整

性保护。也可能，采用旧的CKP，执行机密性保护，另外采用旧的IKP执行完整性保护。对应的，用户设备可以采用旧CKP解密得到新的CKP和IKP，另外，利用旧的IKP验证完整性是否成立。

[0224] 该第一指示信息可以通过AMF中的一个比特来指示，也可以通过两个或者更多个比特来指示。例如，AMF是由16个比特组成的字符串，其中每个比特都有不同的定义，16个比特中的八位用于标准化使用，另外的八位用于特定运算符使用。归属网络控制设备可以将其中未使用的比特做新的定义。假设初始AMF中未使用的比特都为0，定义其中预设的一个比特置为1时，表示第一随机数中包括更新的随机标识P'以及新的CKP'和IKP'。

[0225] 针对步骤S406，用户设备接收到第一随机数和AUTN后，根据AUTN中携带的第一指示信息即可确定第一随机数中包括更新的随机标识P'以及新的CKP'和IKP'，从而从第一随机数中获取更新的随机标识P'以及新的CKP'和IKP'。

[0226] 具体的，用户设备验证AMF中的预设的比特是否置为1，若否，则表明第一接入响应消息中的第一随机数中未携带更新的随机标识P'以及新的CKP'和IKP'；若是，则表明第一接入响应消息中的第一随机数中携带了更新的随机标识P'以及新的CKP'和IKP'。如果确定出第一随机数中携带了更新的随机标识P'以及新的CKP'和IKP'，用户设备采用旧的密钥CKP和X对Y进行完整性验证，验证成功后，采用旧的密钥CKP对X进行解密，得到更新的随机标识P'。同样的，用户设备采用旧的密钥CKP和E对F进行完整性验证，验证成功后，采用旧的密钥CKP对E进行解密，得到新的CKP'。用户设备采用旧的密钥CKP和G对H进行完整性验证，验证成功后，采用旧的密钥CKP对G进行解密，得到新的IKP'。

[0227] 本发明实施例中的其他过程与图4所示实施例中的执行过程一致，此处不再赘述。

[0228] 通过执行上述实施例，归属网络控制设备与用户设备可以共享密钥CKP和IKP，从而实现对随机标识的加密和完整性保护，提高了随机标识的安全性。

[0229] 请参见图7，是本发明实施例提供的另一种数据传输方法的流程示意图。该数据传输方法包括如下步骤。

[0230] S701：用户设备向服务网络控制设备发送第一接入请求消息，该第一接入请求消息中携带该用户设备的随机标识P。

[0231] S702：服务网络控制设备接收用户设备发送的第一接入请求消息，向该用户设备所属的归属网络控制设备发送第一认证请求消息，该第一认证请求消息中携带该用户设备的随机标识P。

[0232] 本发明实施例中的步骤S701和S702可以参见图4所示实施例中的步骤S401和S402，此处不再赘述。

[0233] S703：归属网络控制设备接收服务网络控制设备发送的携带随机标识P的第一认证数据请求消息，若确定需要更新该用户设备的随机标识，则归属网络控制设备生成随机数，并根据该随机数生成新的随机标识。

[0234] 具体的，归属网络控制设备生成一个随机数，并结合该随机数、标识派生参数以及标识派生算法推衍得到新的随机标识。其中，标识派生参数包括但不限于CK、IK、SQN，标识派生算法包括但不限于：HMACsha256函数，或者KDF函数。

[0235] S704：归属网络控制设备判断该新的随机标识是否未被其他用户设备使用，若判断出该新的随机标识已被其他用户设备使用，返回执行步骤S703；若判断出新的随机标识

未被其他用户设备使用，执行步骤S705。

[0236] S705：归属网络控制设备保存该用户设备与该新的随机标识的对应关系，并向服务网络控制设备发送认证向量AV，该认证向量AV中包括该随机数。

[0237] 可选的，归属网络控制设备可以删除该用户设备对应的旧的随机标识，或者，归属网络控制设备也可以包括该用户设备与该用户设备对应的旧的随机标识的对应关系。

[0238] S706：服务网络控制设备接收归属网络控制设备发送的AV，保存该AV，并向该用户设备发送AV中的该随机数和AUTN。

[0239] S707：用户设备接收服务网络控制设备发送的该随机数和AUTN，根据该随机数、标识派生参数以及标识派生算法推衍得到新的随机标识，并且根据收到的该随机数和AUTN，对网络侧进行校验，验证成功后，执行步骤S708。

[0240] S708：用户设备向服务网络控制设备发送RES。

[0241] S709：服务网络控制设备接收用户设备发送的RES，将RES与该用户设备对应的AV中的XRES进行比较，若相同，则服务网络控制设备对该用户设备认证成功。

[0242] S710：服务网络控制设备向该用户设备所属的归属网络控制设备发送位置更新请求，该位置更新请求中携带该用户设备的随机标识P，该位置更新请求用于通知该归属网络控制设备该服务网络控制设备已对该用户设备认证成功。

[0243] S711：归属网络控制设备接收该服务网络控制设备发送的位置更新请求，根据该位置更新请求中携带的随机标识P即可获知该服务网络控制设备已对该用户设备认证成功。

[0244] 本发明实施例中的步骤S705-S711可以参见图4所示实施例中的步骤S404-S410，此处不再赘述。

[0245] 需要说明的是，本发明实施例是以默认每次AKA都基于随机数推衍得到新的随机标识为例进行的说明，因此不需要定义AMF动作。此外，还可以采用图4所示实施例中的第一指示信息的方法来通知用户设备需要基于收到的随机数推衍得到新的随机标识，这种方式中，如何定义AMF可以参见图4所示实施例中的相应描述，此处不再赘述。

[0246] 通过执行本发明实施例，归属网络控制设备可以派生新的随机标识，并且在确定出新的随机标识未被其他用户设备使用后，将生成该随机标识所采用的随机数发送给用户设备，用户设备基于该随机数派生该新的随机标识，因此，可以避免传输新的随机标识，进一步地提高了用户设备的隐私性和安全性。

[0247] 本发明实施例还描述了与上述图4至图7所述方法实施例属于同一发明构思下的一种归属网络控制设备的结构示意图。如图8所示，该归属网络控制设备800用于执行图4至图7所述方法实施例中归属网络控制设备的功能，包括：接收单元801，处理单元802和发送单元803。

[0248] 其中，接收单元801，用于接收服务网络控制设备发送的第一认证数据请求消息，所述第一认证数据请求消息中包括用户设备对应的第一标识；处理单元802，用于生成所述用户设备对应的第一随机标识；发送单元803，用于通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息，所述第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据，所述第一数据组包括所述第一随机标识，所述第一指示信息用于指示所述用户设备根据所述第一指示信息确定所述第一随机数中包含所述第

一随机标识。

[0249] 可选的，所述第一随机数中还包括采用第二共享密钥对所述第一加密数据进行完整性保护得到的第一完整性保护数据。

[0250] 可选的，所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥；或者所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识完整性密钥，所述随机标识完整性密钥用于对所述用户设备的随机标识进行完整性保护。

[0251] 可选的，所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥；或者所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识加密密钥，所述随机标识加密密钥用于对所述用户设备的随机标识进行加密。

[0252] 可选的，在所述接收单元801接收服务网络控制设备发送的第一认证数据请求消息之前，所述接收单元801，还用于接收所述服务网络控制设备发送的第二认证数据请求消息，所述第二认证数据请求消息中包括所述用户设备对应的第二标识；所述处理单元802，还用于采用第一密钥派生参数生成所述第一共享密钥；所述发送单元803，还用于通过所述服务网络控制设备向所述用户设备发送第二指示信息，所述第二指示信息用于指示所述用户设备采用所述第一密钥派生参数生成所述第一共享密钥。

[0253] 可选的，在所述接收单元801接收服务网络控制设备发送的第一认证数据请求消息之前，所述接收单元801，还用于接收所述服务网络控制设备发送的第二认证数据请求消息，所述第二认证数据请求消息中包括所述用户设备对应的第二标识；所述处理单元802，还用于采用第二密钥派生参数生成所述第二共享密钥；所述发送单元803，还用于通过所述服务网络控制设备向所述用户设备发送第二指示信息，所述第二指示信息用于指示所述用户设备采用所述第二密钥派生参数生成所述第二共享密钥。

[0254] 可选的，在所述接收单元801接收服务网络控制设备发送的第一认证数据请求消息之后，在所述发送单元803通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息之前，所述处理单元802，还用于采用第一密钥派生参数生成所述第一共享密钥；所述第一指示信息还用于指示所述用户设备采用所述第一密钥派生参数生成所述第一共享密钥。

[0255] 可选的，在所述接收单元801接收服务网络控制设备发送的第一认证数据请求消息之后，在所述发送单元803通过所述服务网络控制设备向所述用户设备发送第一随机数和第一指示信息之前，所述处理单元802，还用于采用第二密钥派生参数生成所述第二共享密钥；所述第一指示信息还用于指示所述用户设备采用所述第二密钥派生参数生成所述第二共享密钥。

[0256] 可选的，在所述接收单元801接收服务网络控制设备发送的第一认证数据请求消息之后，所述处理单元802，还用于采用第三密钥派生参数生成第三共享密钥，所述第三共享密钥用于所述归属网络控制设备后续向所述用户设备发送更新的第二随机标识时对所述第二随机标识进行加密；所述第一指示信息还用于指示所述用户设备采用所述第三密钥派生参数生成所述第三共享密钥。

[0257] 可选的，在所述接收单元801接收服务网络控制设备发送的第一认证数据请求消息之后，所述处理单元802，还用于采用第四密钥派生参数生成第四共享密钥，所述第四共

享密钥用于所述归属网络控制设备后续向所述用户设备发送所述第二随机标识时对所述第二随机标识进行完整性保护;所述第一指示信息还用于指示所述用户设备采用所述第四密钥派生参数生成所述第四共享密钥。

[0258] 在本实施例中,归属网络控制设备800是以功能单元的形式来呈现。这里的"单元"可以指ASIC电路,执行一个或多个软件或固件程序的处理器和存储器,集成逻辑电路,和/或其他可以提供上述功能的器件。在一个简单的实施例中,本领域的技术人员可以想到归属网络控制设备800可以采用图3所示的形式。接收单元801、处理单元802和发送单元803可以通过图3的处理器和存储器来实现。

[0259] 本发明实施例还描述了与上述图4至图7所述方法实施例属于同一发明构思下的一种用户设备的结构示意图。如图9所示,该用户设备900用于执行图4至图7所述方法实施例中用户设备的功能,包括:发送单元901、接收单元902和处理单元903。

[0260] 其中,发送单元901,用于向服务网络控制设备发送第一接入请求消息,所述第一接入请求消息中包括所述用户设备对应的第一标识;接收单元902,用于接收归属网络控制设备通过上述服务网络控制设备发送的第一随机数和第一指示信息,所述第一随机数中包括采用第一共享密钥对第一数据组进行加密得到的第一加密数据,所述第一数据组包括所述用户设备对应的第一随机标识;处理单元903,用于根据所述第一指示信息确定所述第一随机数中包含所述第一随机标识;所述处理单元903,还用于采用所述第一共享密钥对所述第一加密数据进行解密,得到所述第一随机标识。

[0261] 可选的,所述第一随机数中还包括采用第二共享密钥对所述第一加密数据进行完整性保护得到的第一完整性保护数据;在所述接收单元902接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后,

[0262] 所述处理单元903,还用于采用所述第二共享密钥对所述第一完整性保护数据进行完整性验证。

[0263] 可选的,所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥;或者所述第二共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识完整性密钥,所述随机标识完整性密钥用于对所述用户设备的随机标识进行完整性保护。

[0264] 可选的,所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的根密钥;或者所述第一共享密钥为所述用户设备与所述归属网络控制设备之间预共享的随机标识加密密钥,所述随机标识加密密钥用于对所述用户设备的随机标识进行加密。

[0265] 可选的,在所述接收单元902接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之前,所述发送单元901,还用于向服务网络控制设备发送第二接入请求消息,所述第二接入请求消息中包括所述用户设备对应的第二标识;所述接收单元902,还用于接收所述归属网络控制设备通过所述服务网络控制设备发送的第二指示信息;

[0266] 所述处理单元903,还用于根据所述第二指示信息采用第一密钥派生参数生成所述第一共享密钥。

[0267] 可选的,在所述接收单元902接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之前,所述发送单元901,还用于向服务网络控制设备发送第

二接入请求消息，所述第二接入请求消息中包括所述用户设备对应的第二标识；所述接收单元902，还用于接收所述归属网络控制设备通过所述服务网络控制设备发送的第二指示信息；

[0268] 所述处理单元903，还用于根据所述第二指示信息采用第二密钥派生参数生成所述第二共享密钥。

[0269] 可选的，所述第一指示信息还用于指示所述用户设备采用第一密钥派生参数生成所述第一共享密钥；在所述处理单元903采用所述第一共享密钥对所述第一加密数据进行解密，得到所述第一随机标识之前，所述处理单元903，还用于根据所述第一指示信息，采用所述第一密钥派生参数生成所述第一共享密钥。

[0270] 可选的，所述第一指示信息还用于指示所述用户设备采用第二密钥派生参数生成所述第二共享密钥；在所述处理单元903采用所述第一共享密钥对所述第一加密数据进行解密，得到所述第一随机标识之前，所述处理单元903，还用于根据所述第一指示信息，采用所述第二密钥派生参数生成所述第二共享密钥。

[0271] 可选的，所述第一指示信息还用于指示所述用户设备采用第三密钥派生参数生成第三共享密钥，所述第三共享密钥用于所述归属网络控制设备后续向所述用户设备发送更新的第二随机标识时对所述第二随机标识进行加密；在所述接收单元902接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，所述处理单元903，还用于采用所述第三密钥派生参数生成所述第三共享密钥。

[0272] 可选的，所述第一指示信息还用于指示所述用户设备采用第四密钥派生参数生成第四共享密钥，所述第四共享密钥用于所述归属网络控制设备后续向所述用户设备发送所述第二随机标识时对所述第二随机标识进行完整性保护；在所述接收单元902接收归属网络控制设备通过服务网络控制设备发送的第一随机数和第一指示信息之后，所述处理单元903，还用于采用所述第四密钥派生参数生成所述第四共享密钥。

[0273] 在本实施例中，用户设备900是以功能单元的形式来呈现。这里的“单元”可以指ASIC电路，执行一个或多个软件或固件程序的处理器和存储器，集成逻辑电路，和/或其他可以提供上述功能的器件。在一个简单的实施例中，本领域的技术人员可以想到用户设备900可以采用图3所示的形式。发送单元901、接收单元902和处理单元903可以通过图3的处理器和存储器来实现。

[0274] 本发明实施例还描述了与上述图4至图7所述方法实施例属于同一发明构思下的一种服务网络控制设备的结构示意图。如图10所示，该服务网络控制设备1000用于执行图4至图7所述方法实施例中服务网络控制设备的功能，包括：接收单元1001、发送单元1002和处理单元1003。

[0275] 其中，接收单元1001，用于接收用户设备发送的第一接入请求消息，所述第一接入请求消息中包括所述用户设备对应的第一标识；发送单元1002，用于向归属网络控制设备发送第一认证数据请求消息，所述第一认证数据请求消息包括所述第一标识；处理单元1003，用于对用户设备进行认证；所述发送单元1002，还用于在处理单元1001对该用户设备成功认证后，向归属网络控制设备发送认证成功消息，该认证成功消息用于指示该归属网络控制设备该服务网络控制设备已对用户设备认证成功。

[0276] 可选的，该认证成功消息中包括该用户设备对应的第一标识或者该用户设备对应

的第一随机标识。

[0277] 在本实施例中，服务网络控制设备1000是以功能单元的形式来呈现。这里的“单元”可以指ASIC电路，执行一个或多个软件或固件程序的处理器和存储器，集成逻辑电路，和/或其他可以提供上述功能的器件。在一个简单的实施例中，本领域的技术人员可以想到服务网络控制设备1000可以采用图3所示的形式。接收单元1001、发送单元1002和处理单元1003可以通过图3的处理器和存储器来实现。

[0278] 本发明实施例还提供了一种计算机存储介质，用于储存为上述图8所示的归属网络控制设备所用的计算机软件指令，其包含用于执行上述方法实施例所设计的程序。

[0279] 本发明实施例还提供了另一种计算机存储介质，用于储存为上述图9所述的用户设备所用的计算机软件指令，其包含用于执行上述方法实施例所设计的程序。

[0280] 本发明实施例还提供了另一种计算机存储介质，用于储存为上述图10所述的用户设备所用的计算机软件指令，其包含用于执行上述方法实施例所设计的程序。

[0281] 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流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0282] 以上实施例仅揭露了本发明中较佳实施例，不能以此来限定本发明之权利范围，本领域普通技术人员可以理解实现上述实施例的全部或部分流程，并依本发明权利要求所作的等同变化，仍属于发明所涵盖的范围。

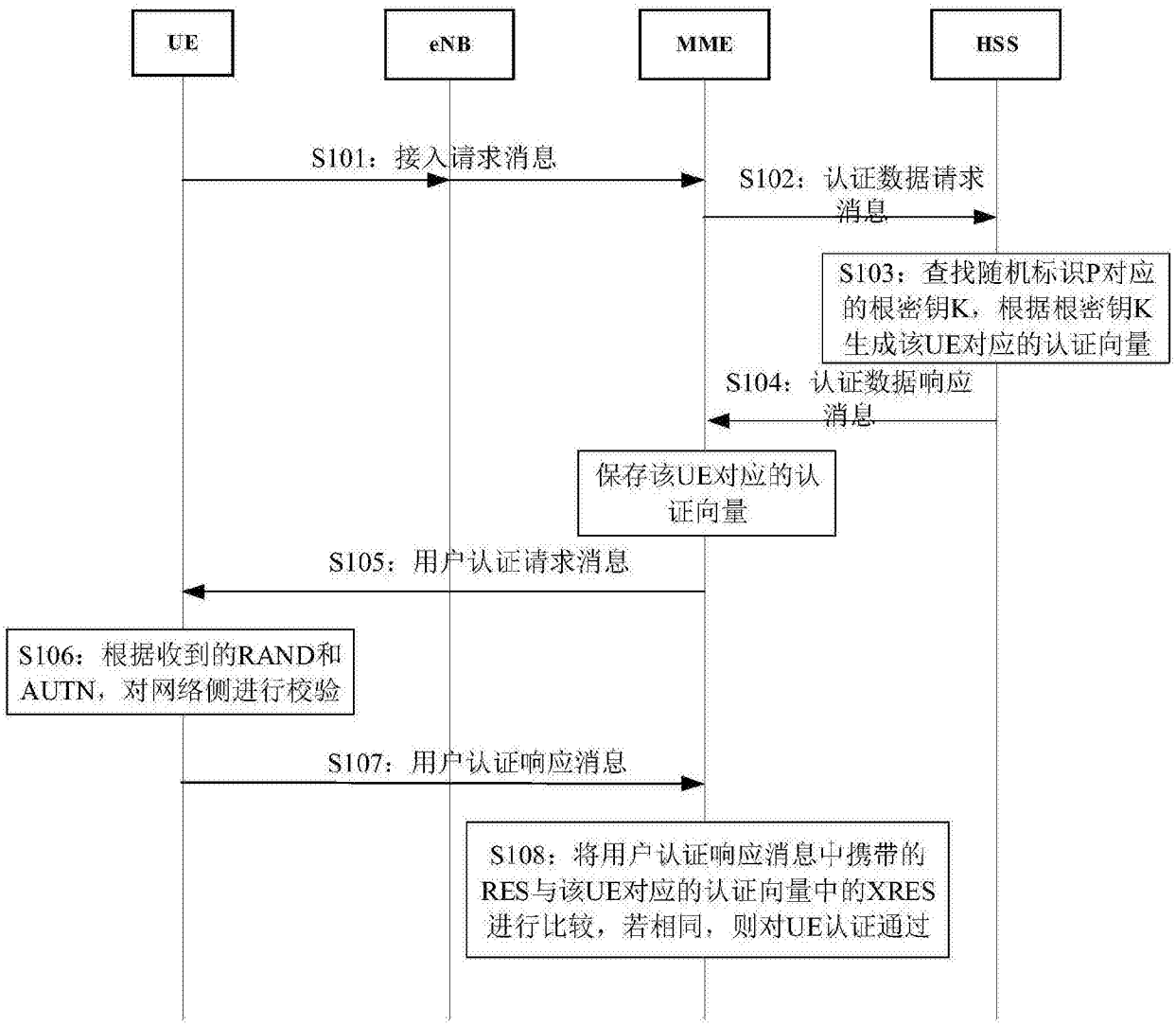

UE
eNB
MME
HSS
S101：接入请求消息
S102：认证数据请求消息
S103：查找随机标识P对应的根密钥K，根据根密钥K生成该UE对应的认证向量
S104：认证数据响应消息
保存该UE对应的认证向量
S105：用户认证请求消息
S106：根据收到的RAND和AUTN，对网络侧进行校验
S107：用户认证响应消息
S108：将用户认证响应消息中携带的RES与该UE对应的认证向量中的XRES进行比较，若相同，则对UE认证通过

图1

200

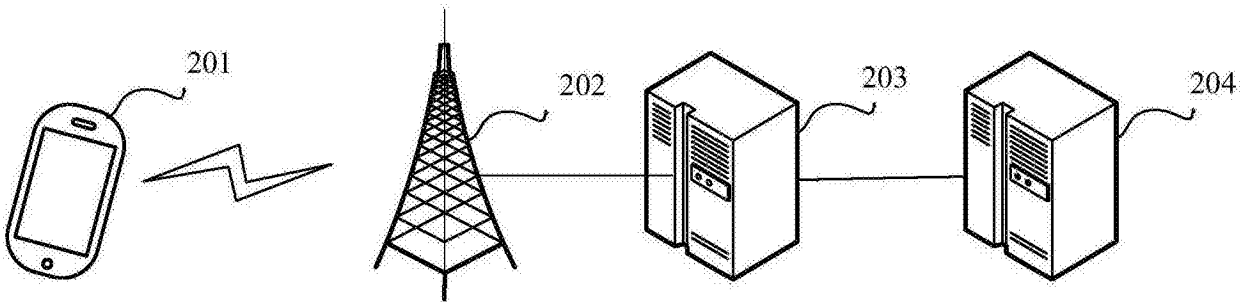

201
202
203
204

图2

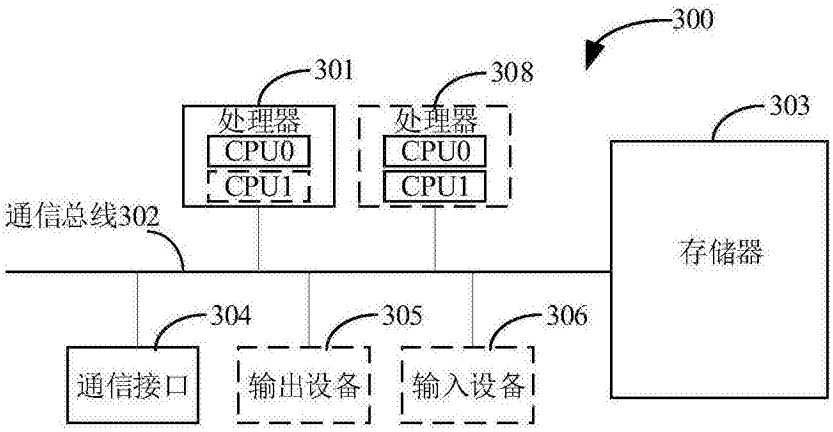

300
301
308
303
处理器
CPU0
CPU1
处理器
CPU0
CPU1
通信总线302
存储器
304
305
306
通信接口
输出设备
输入设备

图3

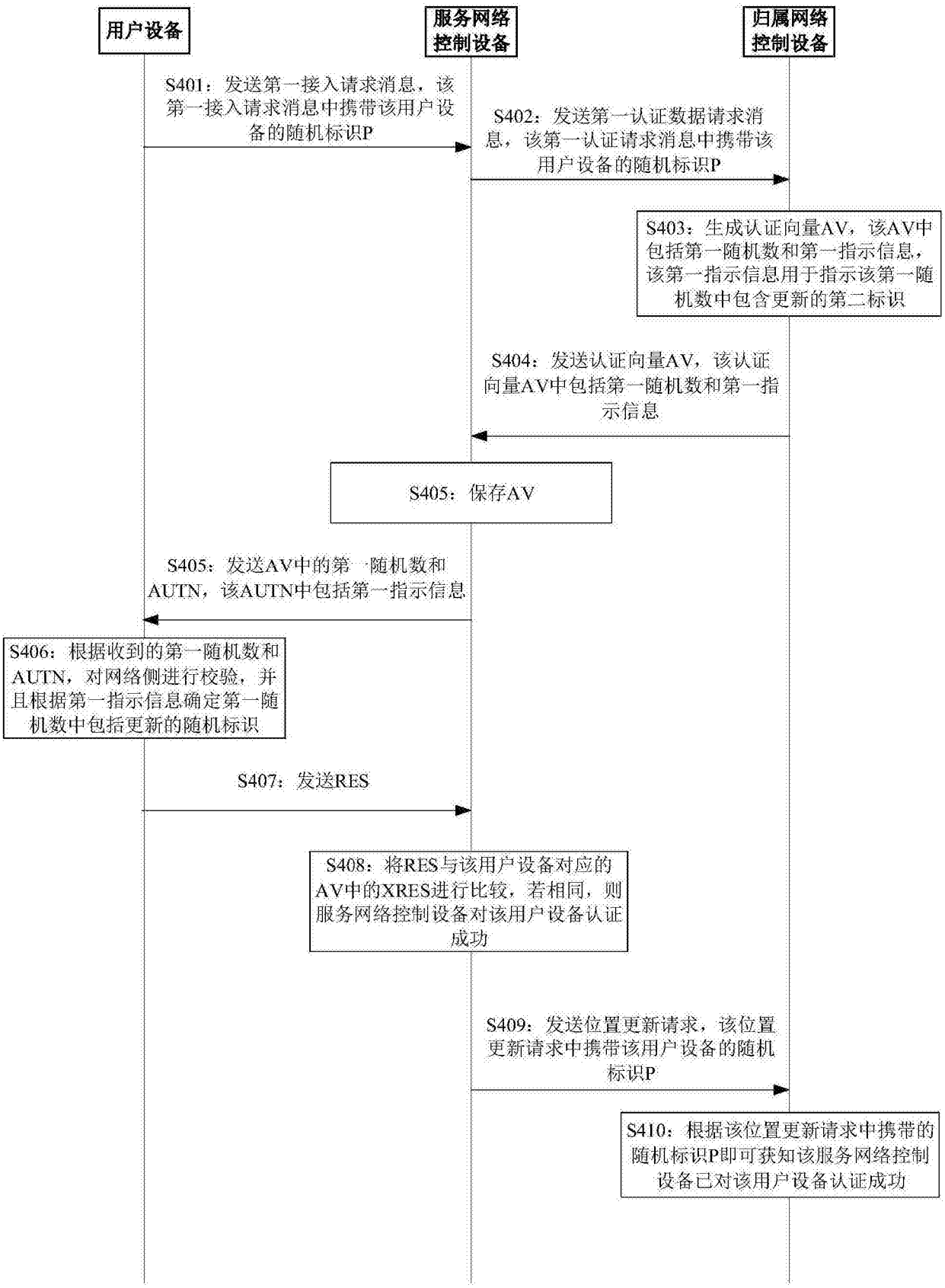

用户设备
服务网络控制设备
归属网络控制设备
S401：发送第一接入请求消息，该第一接入请求消息中携带该用户设备的随机标识P
S402：发送第一认证数据请求消息，该第一认证请求消息中携带该用户设备的随机标识P
S403：生成认证向量AV，该AV中包括第一随机数和第一指示信息，该第一指示信息用于指示该第一随机数中包含更新的第二标识
S404：发送认证向量AV，该认证向量AV中包括第一随机数和第一指示信息
S405：保存AV
S405：发送AV中的第一随机数和AUTN，该AUTN中包括第一指示信息
S406：根据收到的第一随机数和AUTN，对网络侧进行校验，并且根据第一指示信息确定第一随机数中包括更新的随机标识
S407：发送RES
S408：将RES与该用户设备对应的AV中的XRES进行比较，若相同，则服务网络控制设备对该用户设备认证成功
S409：发送位置更新请求，该位置更新请求中携带该用户设备的随机标识P
S410：根据该位置更新请求中携带的随机标识P即可获知该服务网络控制设备已对该用户设备认证成功

图4

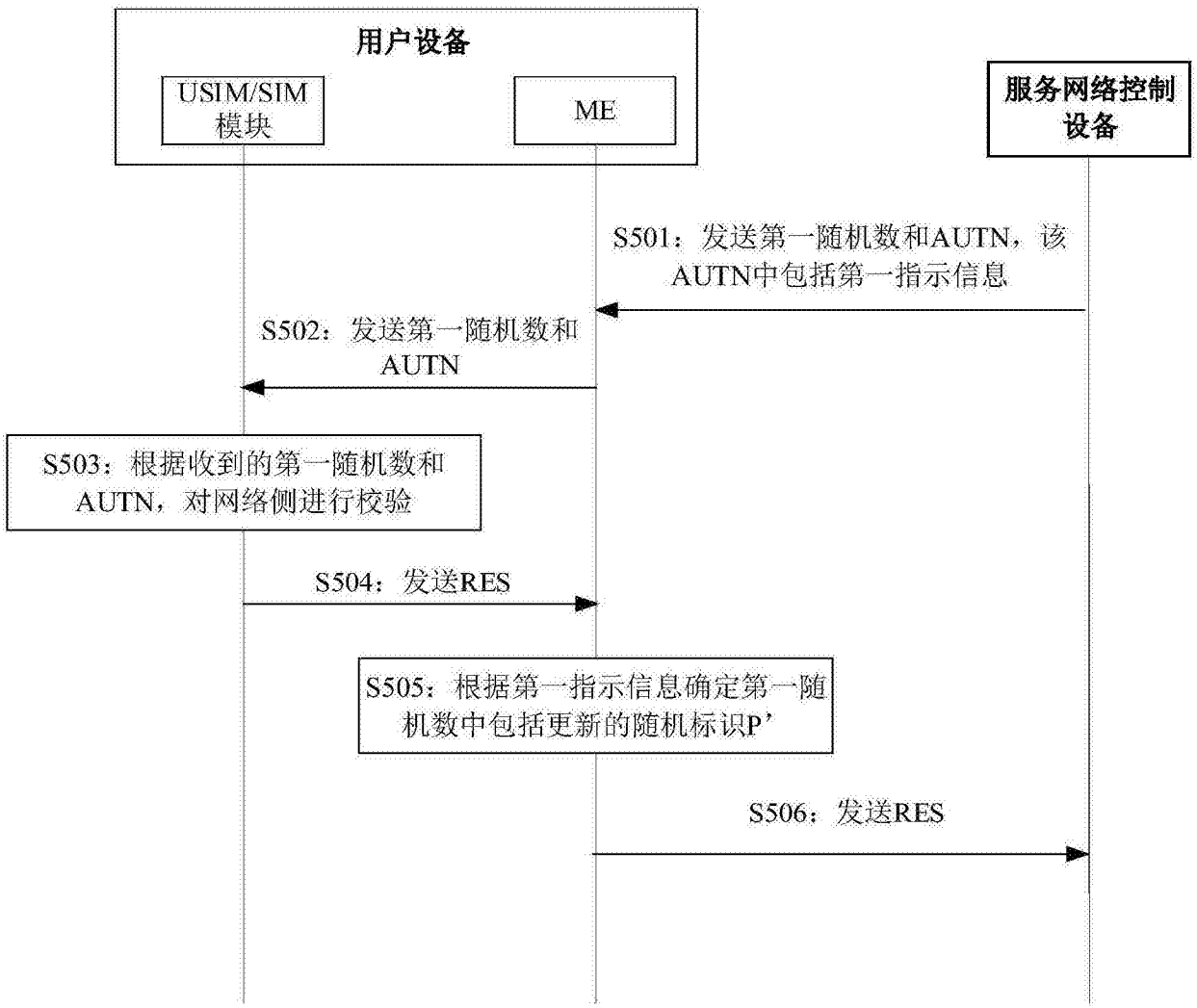

用户设备
USIM/SIM模块
ME
服务网络控制设备
S501：发送第一随机数和AUTN，该AUTN中包括第一指示信息
S502：发送第一随机数和AUTN
S503：根据收到的第一随机数和AUTN，对网络侧进行校验
S504：发送RES
S505：根据第一指示信息确定第一随机数中包括更新的随机标识P’
S506：发送RES

图5

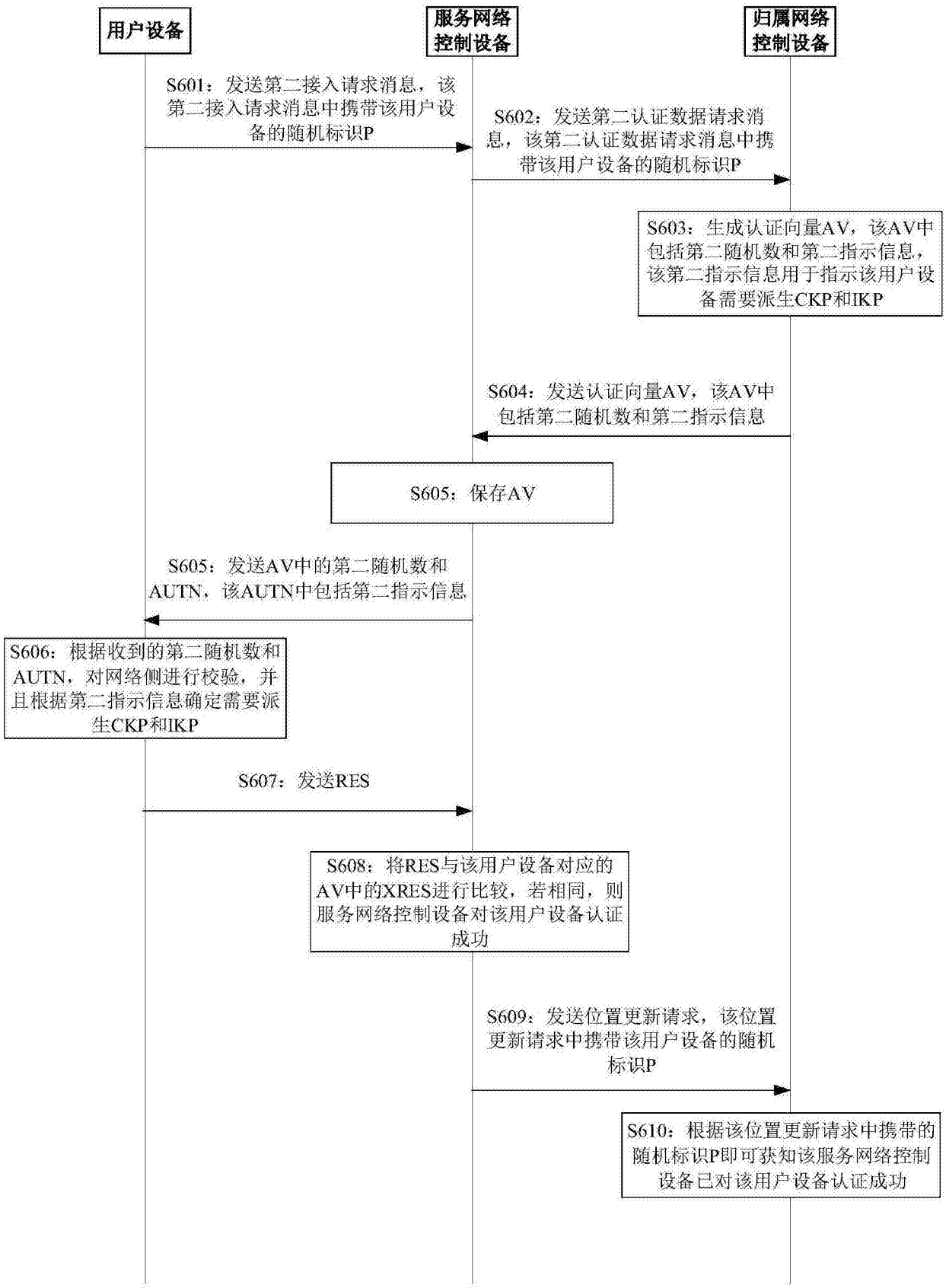

用户设备
服务网络控制设备
归属网络控制设备
S601：发送第二接入请求消息，该第二接入请求消息中携带该用户设备的随机标识P
S602：发送第二认证数据请求消息，该第二认证数据请求消息中携带该用户设备的随机标识P
S603：生成认证向量AV，该AV中包括第二随机数和第二指示信息，该第二指示信息用于指示该用户设备需要派生CKP和IKP
S604：发送认证向量AV，该AV中包括第二随机数和第二指示信息
S605：保存AV
S605：发送AV中的第二随机数和AUTN，该AUTN中包括第二指示信息
S606：根据收到的第二随机数和AUTN，对网络侧进行校验，并且根据第二指示信息确定需要派生CKP和IKP
S607：发送RES
S608：将RES与该用户设备对应的AV中的XRES进行比较，若相同，则服务网络控制设备对该用户设备认证成功
S609：发送位置更新请求，该位置更新请求中携带该用户设备的随机标识P
S610：根据该位置更新请求中携带的随机标识P即可获知该服务网络控制设备已对该用户设备认证成功

图6

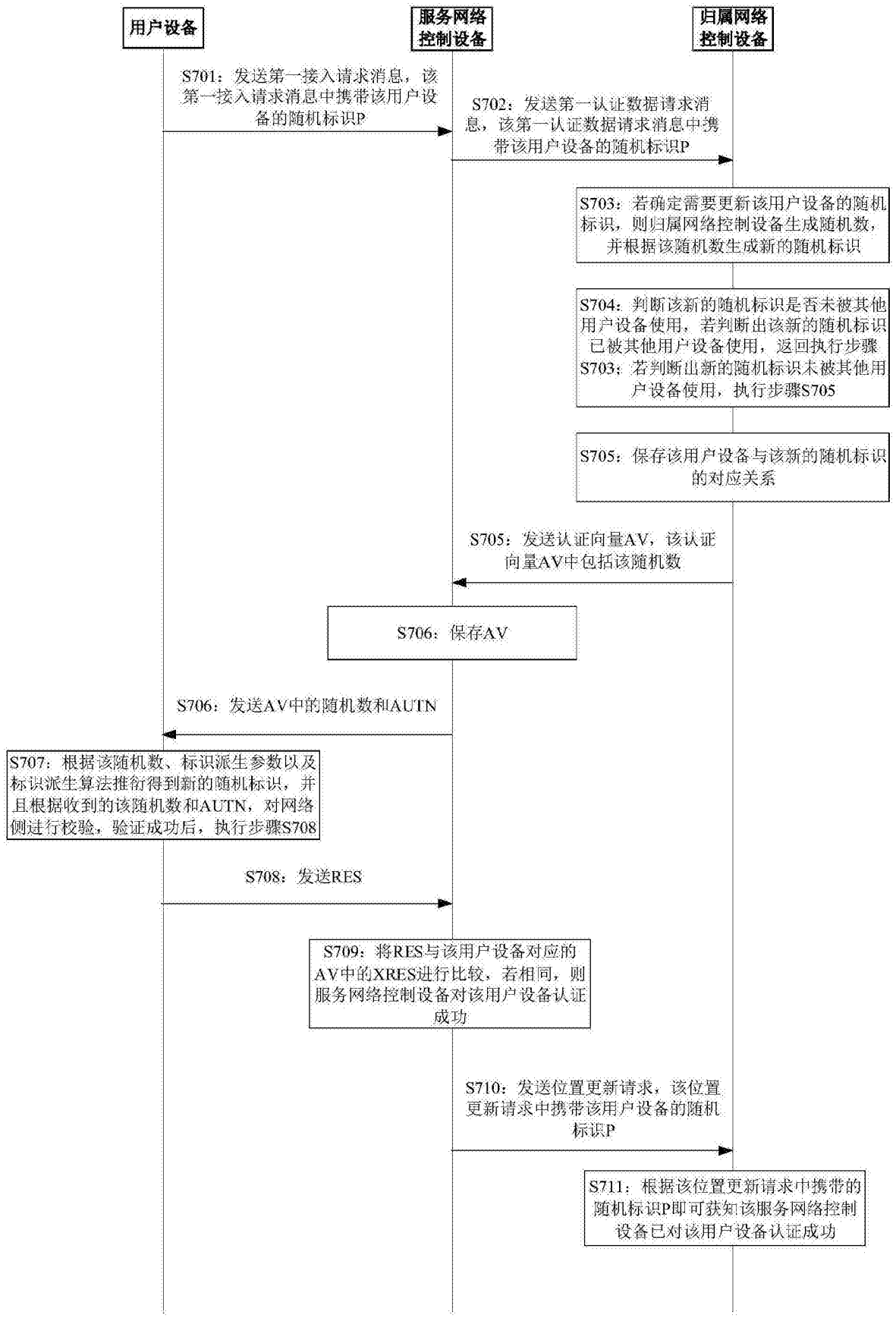

用户设备
服务网络控制设备
归属网络控制设备
S701：发送第一接入请求消息，该第一接入请求消息中携带该用户设备的随机标识P
S702：发送第一认证数据请求消息，该第一认证数据请求消息中携带该用户设备的随机标识P
S703：若确定需要更新该用户设备的随机标识，则归属网络控制设备生成随机数，并根据该随机数生成新的随机标识
S704：判断该新的随机标识是否未被其他用户设备使用，若判断出该新的随机标识已被其他用户设备使用，返回执行步骤S703；若判断出新的随机标识未被其他用户设备使用，执行步骤S705
S705：保存该用户设备与该新的随机标识的对应关系
S705：发送认证向量AV，该认证向量AV中包括该随机数
S706：保存AV
S706：发送AV中的随机数和AUTN
S707：根据该随机数、标识派生参数以及标识派生算法推衍得到新的随机标识，并且根据收到的该随机数和AUTN，对网络侧进行校验，验证成功后，执行步骤S708
S708：发送RES
S709：将RES与该用户设备对应的AV中的XRES进行比较，若相同，则服务网络控制设备对该用户设备认证成功
S710：发送位置更新请求，该位置更新请求中携带该用户设备的随机标识P
S711：根据该位置更新请求中携带的随机标识P即可获知该服务网络控制设备已对该用户设备认证成功

图7

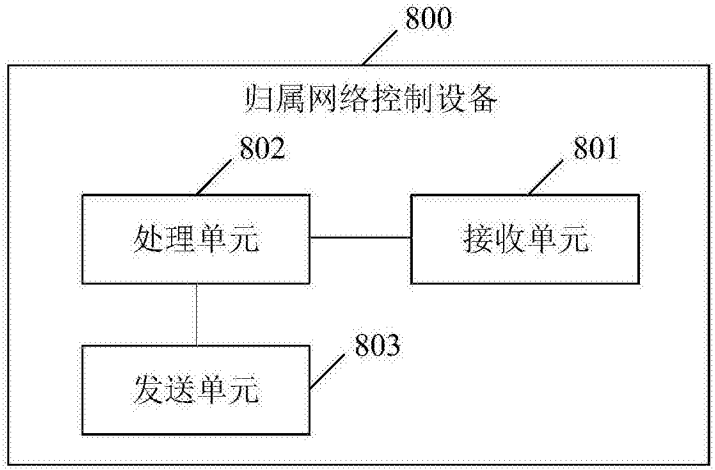

800
归属网络控制设备
802
801
处理单元
接收单元
803
发送单元

图8

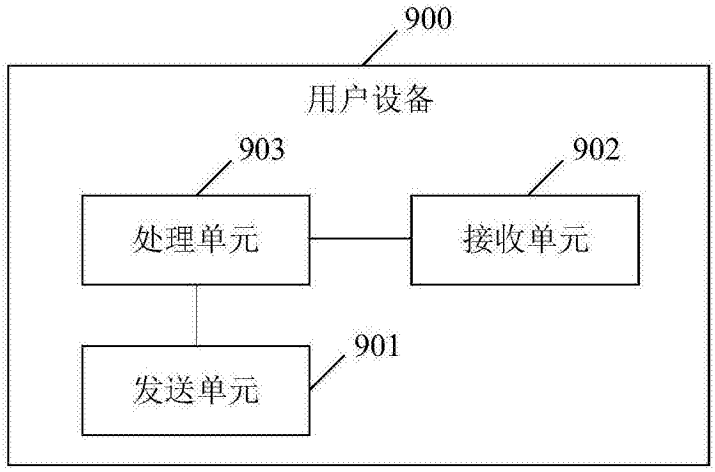

900
用户设备
903
902
处理单元
接收单元
901
发送单元

图9

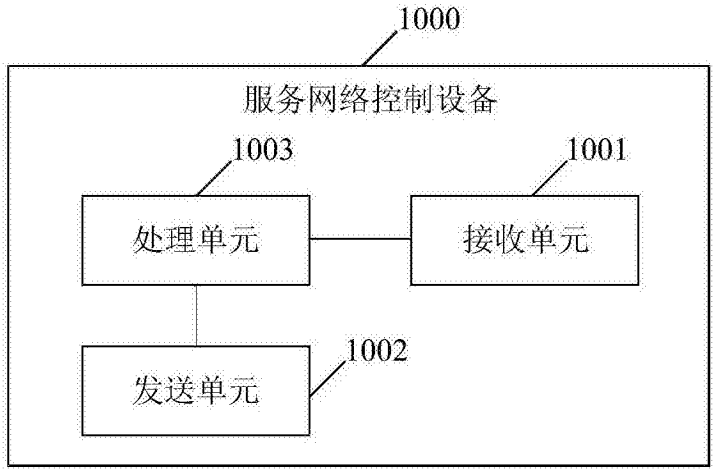

1000
服务网络控制设备
1003
1001
处理单元
接收单元
1002
发送单元

图10