(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118317302 A
(43)申请公布日 2024.07.09

(21)申请号 202310028942.X

(22)申请日 2023.01.09

(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 刘文峰 李赫 吴荣

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
专利代理师 邱英华

(51)Int.Cl.
H04W 12/06(2021.01)
H04W 12/041(2021.01)
H04W 12/0431(2021.01)
H04W 76/10(2018.01)

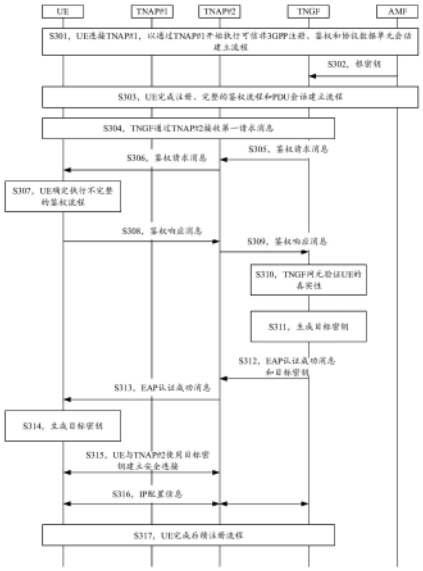
权利要求书5页 说明书31页 附图7页

(54)发明名称

鉴权方法及通信装置

(57)摘要

本申请提供一种鉴权方法及通信装置,能够解决通信中断的问题,从而提高通信效率和通信可靠性,可应用于通信系统中。该方法包括:在用户设备UE从源可信的非第三代合作伙伴计划3GPP接入点TNAP移动到目标TNAP的情况下,可信的非3GPP网关功能TNGF根据存储的与UE对应的根密钥生成中间密钥,并使用中间密钥,生成针对目标TNAP的目标密钥。以及将目标密钥发送给目标TNAP。其中,目标密钥用于保护UE与目标TNAP之间通信安全。



CN 118317302 A

1.一种鉴权方法,其特征在于,所述方法包括:

在用户设备UE从源可信的非第三代合作伙伴计划3GPP接入点TNAP移动到目标TNAP的情况下,可信的非3GPP网关功能TNGF根据存储的与所述UE对应的根密钥生成中间密钥;

所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥;以及

所述TNGF将所述目标密钥发送给所述目标TNAP;其中,所述目标密钥用于保护所述UE与所述目标TNAP之间通信安全。

2.根据权利要求1所述的方法,其特征在于,所述TNGF根据存储的与所述UE对应的根密钥生成中间密钥,包括:

所述TNGF根据第一类型识别码以及所述根密钥生成所述中间密钥;其中,所述第一类型识别码用于标识生成中间密钥。

3.根据权利要求1或2所述的方法,其特征在于,在所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥之前,所述方法包括:

所述TNGF通过所述目标TNAP向所述UE发送鉴权请求消息,所述鉴权请求消息包括第一验证参数以及第一新鲜性参数;其中,所述第一验证参数由所述TNGF根据所述中间密钥和所述第一新鲜性参数生成;

所述TNGF接收来自所述UE的鉴权响应消息,其中,所述鉴权响应消息包括第二验证参数以及第二新鲜性参数;

所述TNGF根据所述中间密钥和所述第二新鲜性参数,得到第三验证参数;

所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥,包括:

在所述第三验证参数与所述第二验证参数匹配的情况下,所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥。

4.根据权利要求1或2所述的方法,其特征在于,在所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥之前,所述方法包括:

所述TNGF通过所述目标TNAP向所述UE发送鉴权请求消息,所述鉴权请求消息包括第一验证参数以及第一新鲜性参数;其中,所述第一验证参数由所述TNGF根据所述根密钥和所述第一新鲜性参数生成;

所述TNGF接收来自所述UE的鉴权响应消息,其中,所述鉴权响应消息包括第二验证参数以及第二新鲜性参数;

所述TNGF根据所述根密钥和所述第二新鲜性参数,得到第三验证参数;

所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥,包括:

在所述第三验证参数与所述第二验证参数匹配的情况下,所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥。

5.根据权利要求1或2所述的方法,其特征在于,在所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥之后,以及所述TNGF将所述目标密钥发送给所述目标TNAP之前,所述方法还包括:

所述TNGF通过所述目标TNAP向所述UE发送鉴权请求消息,所述鉴权请求消息包括第一验证参数以及第一新鲜性参数;其中,所述第一验证参数由所述TNGF根据所述中间密钥和所述第一新鲜性参数生成;

所述TNGF接收来自所述UE的鉴权响应消息,其中,所述鉴权响应消息包括第二验证参

数以及第二新鲜性参数；

所述TNGF根据所述中间密钥和所述第二新鲜性参数，得到第三验证参数；

所述TNGF将所述目标密钥发送给所述目标TNAP，包括：

在所述第三验证参数与所述第二验证参数匹配的情况下，所述TNGF将所述目标密钥发送给所述目标TNAP。

6.根据权利要求1或2所述的方法，其特征在于，在所述TNGF使用所述中间密钥，生成针对所述目标TNAP的目标密钥之后，以及所述TNGF将所述目标密钥发送给所述目标TNAP之前，所述方法还包括：

所述TNGF通过所述目标TNAP向所述UE发送鉴权请求消息，所述鉴权请求消息包括第一验证参数以及第一新鲜性参数；其中，所述第一验证参数由所述TNGF根据所述根密钥、和所述第一新鲜性参数生成；

所述TNGF接收来自所述UE的鉴权响应消息，其中，所述鉴权响应消息包括第二验证参数以及第二新鲜性参数；

所述TNGF根据所述根密钥和所述第二新鲜性参数，得到第三验证参数；

所述TNGF将所述目标密钥发送给所述目标TNAP，包括：

在所述第三验证参数与所述第二验证参数匹配的情况下，所述TNGF将所述目标密钥发送给所述目标TNAP。

7.根据权利要求1或2所述的方法，其特征在于，在所述TNGF使用所述中间密钥，生成针对所述目标TNAP的目标密钥之前，所述方法还包括：

所述TNGF通过所述目标TNAP向所述UE发送鉴权请求消息#1；其中，所述鉴权请求消息#1中包括所述UE的标识；

所述TNGF接收来自所述UE的鉴权响应消息#1，其中，所述鉴权响应消息#1包括第二验证参数以及第二新鲜性参数；

所述TNGF根据所述中间密钥、所述第二新鲜性参数，得到第三验证参数；

所述TNGF使用所述中间密钥，生成针对所述目标TNAP的目标密钥，包括：

在所述第三验证参数与所述第二验证参数匹配的情况下，所述TNGF使用所述中间密钥，生成针对所述目标TNAP的目标密钥；

在所述TNGF将所述目标密钥发送给所述目标TNAP之后，所述方法还包括：

所述TNGF通过所述目标TNAP向所述UE发送鉴权请求消息#2，所述鉴权请求消息#2包括第一验证参数以及第一新鲜性参数；其中，所述第一验证参数由所述TNGF根据所述中间密钥和所述第一新鲜性参数生成；

所述TNGF通过所述目标TNAP接收来自所述UE的鉴权响应消息#2；所述鉴权响应消息#2用于指示所述TNGF发送认证成功消息。

8.根据权利要求1或2所述的方法，其特征在于，在所述TNGF使用所述中间密钥，生成针对所述目标TNAP的目标密钥之前，所述方法还包括：

所述TNGF向所述UE发送鉴权请求消息#1；其中，鉴权请求消息#1中包括所述UE的标识；

所述TNGF接收来自所述UE的鉴权响应消息#1，其中，所述鉴权响应消息#1包括第二验证参数以及第二新鲜性参数；

所述TNGF根据所述根密钥和所述第二新鲜性参数，得到第三验证参数；

所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥,包括:

在所述第三验证参数与所述第二验证参数匹配的情况下,所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥;

在所述TNGF将所述目标密钥发送给所述目标TNAP之后,所述方法还包括:

所述TNGF通过所述目标TNAP向所述UE发送鉴权请求消息#2,所述鉴权请求消息#2包括第一验证参数以及第一新鲜性参数;其中,所述第一验证参数由所述TNGF根据所述根密钥和所述第一新鲜性参数生成;

所述TNGF通过所述目标TNAP接收来自所述UE的鉴权响应消息#2;所述鉴权响应消息#2用于指示所述TNGF发送认证成功消息。

9.根据权利要求1-8中任一项所述的方法,其特征在于,所述TNGF使用所述中间密钥,生成针对所述目标TNAP的目标密钥,包括:

所述TNGF根据第二类型识别码和所述中间密钥生成所述目标密钥;其中,所述第二类型识别码用于生成目标密钥。

10.根据权利要求1-9中任一项所述的方法,其特征在于,在所述TNGF根据存储的与所述UE对应的根密钥生成中间密钥之前,所述方法还包括:

所述TNGF接收来自所述目标TNAP的第一请求消息;

响应于所述第一请求消息,所述TNGF确定需要执行自身与所述UE之间的鉴权流程。

11.根据权利要求10所述的方法,其特征在于,所述TNGF根据所述UE的标识,确定所述UE从所述源TNAP移动到所述目标TNAP。

12.根据权利要求1-11中任一项所述的方法,其特征在于,在所述TNGF根据存储的与所述UE对应的根密钥生成中间密钥之前,所述方法还包括:

所述TNGF根据所述UE的标识,确定所述根密钥。

13.一种鉴权方法,其特征在于,所述方法应用于通信装置从源可信的非第三代合作伙伴计划3GPP接入点TNAP移动到目标TNAP的场景下,包括:

所述通信装置根据自身与可信的非3GPP网关功能TNGF之间的根密钥,生成中间密钥;其中,所述TNGF为所述源TNAP和所述目标TNAP的管理网元,以及

所述通信装置使用所述中间密钥,生成针对所述目标TNAP的目标密钥;其中,所述目标密钥用于保护所述通信装置与所述目标TNAP之间通信安全。

14.根据权利要求13所述的方法,其特征在于,所述通信装置根据自身与TNGF之间的根密钥,生成中间密钥,包括:

所述通信装置根据第一类型识别码以及所述根密钥生成所述中间密钥;其中,所述第一类型识别码用于标识生成所述中间密钥。

15.根据权利要求13或14所述的方法,其特征在于,在所述通信装置根据自身与TNGF之间的根密钥,生成中间密钥之前,所述方法包括:

所述通信装置通过所述目标TNAP接收来自所述TNGF的鉴权请求消息;所述鉴权请求消息包括第一验证参数以及第一新鲜性参数;其中,所述第一验证参数由所述TNGF根据所述中间密钥和所述第一新鲜性参数生成;

所述通信装置使用所述中间密钥和所述第一新鲜性参数,得到第四验证参数;

在所述第四验证参数与所述第一验证参数匹配的情况下,所述通信装置向所述TNGF发

送鉴权响应消息;其中,所述鉴权响应消息包括所述通信装置的标识,第二验证参数以及第二新鲜性参数。

16.根据权利要求13或14所述的方法,其特征在于,在所述通信装置根据自身与TNGF之间的根密钥,生成中间密钥之前,所述方法包括:

所述通信装置通过所述目标TNAP接收来自所述TNGF的鉴权请求消息;所述鉴权请求消息包括第一验证参数以及第一新鲜性参数;其中,所述第一验证参数由所述TNGF根据所述根密钥和所述第一新鲜性参数以及生成;

所述通信装置使用所述根密钥和所述第一新鲜性参数,得到第四验证参数;

在所述第四验证参数与所述第一验证参数匹配的情况下,所述通信装置向所述TNGF发送鉴权响应消息;其中,所述鉴权响应消息包括第二验证参数以及第二新鲜性参数。

17.根据权利要求13或14所述的方法,其特征在于,在所述通信装置根据自身与TNGF之间的根密钥,生成中间密钥之前,所述方法包括:

所述通信装置通过所述目标TNAP接收来自所述TNGF的鉴权请求消息;所述鉴权请求消息包括第一验证参数以及第一新鲜性参数;其中,所述第一验证参数由所述TNGF根据所述根密钥和所述第一新鲜性参数以及生成;

所述通信装置使用所述中间密钥和所述第一新鲜性参数,得到第四验证参数;

所述通信装置根据自身与TNGF之间的根密钥,生成中间密钥,包括:在所述第四验证参数与所述第一验证参数匹配的情况下,所述通信装置根据自身与TNGF之间的根密钥,生成中间密钥;

在所述通信装置使用所述中间密钥,生成针对所述目标TNAP的目标密钥之后,所述方法还包括:

所述通信装置向所述TNGF发送鉴权响应消息;其中,所述鉴权响应消息包括所述通信装置的标识,第二验证参数以及第二新鲜性参数。

18.根据权利要求13或14所述的方法,其特征在于,在所述通信装置根据自身与TNGF之间的根密钥,生成中间密钥之前,所述方法包括:

所述通信装置通过所述目标TNAP接收来自所述TNGF的鉴权请求消息;所述鉴权请求消息包括第一验证参数以及第一新鲜性参数;其中,所述第一验证参数由所述TNGF根据所述根密钥和所述第一新鲜性参数生成;

所述通信装置使用所述根密钥和所述第一新鲜性参数,得到第四验证参数;

所述通信装置根据自身与TNGF之间的根密钥,生成中间密钥,包括:在所述第四验证参数与所述第一验证参数匹配的情况下,所述通信装置根据自身与所述TNGF之间的根密钥,生成中间密钥;

在所述通信装置使用所述中间密钥,生成针对所述目标TNAP的目标密钥之后,所述方法还包括:

所述通信装置向所述TNGF发送鉴权响应消息;其中,所述鉴权响应消息包括所述通信装置的标识,第二验证参数以及第二新鲜性参数。

19.根据权利要求13-18中任一项所述的方法,其特征在于,所述通信装置使用所述中间密钥,生成针对所述目标TNAP的目标密钥,包括:

所述通信装置根据第二类型识别码和所述中间密钥生成所述目标密钥;其中,所述第

二类型识别码用于标识生成目标密钥。

20.根据权利要求19所述的方法，其特征在于，在所述通信装置根据自身与TNGF之间的根密钥，生成中间密钥之前，所述方法还包括：

所述通信装置向所述目标TNAP发送第一请求消息。

21.根据权利要求20所述的方法，其特征在于，所述第一请求消息包括所述通信装置的标识。

22.根据权利要求13-21中任一项所述的方法，其特征在于，在所述通信装置根据自身与TNGF之间的根密钥，生成中间密钥之前，所述方法还包括：

所述通信装置根据TNGF的标识，确定根密钥。

23.一种通信装置，其特征在于，所述通信装置包括：用于执行如权利要求1-22中任一项所述的鉴权方法的模块。

24.一种通信装置，其特征在于，所述通信装置包括：用于执行如权利要求1-12中任一项所述的鉴权方法的模块。

25.一种通信装置，其特征在于，所述通信装置包括：用于执行如权利要求13-22中任一项所述的鉴权方法的模块。

26.一种通信装置，其特征在于，所述通信装置包括：处理器；其中，

所述处理器，用于执行如权利要求1-22中任一项所述的鉴权方法。

27.一种通信装置，其特征在于，包括：处理器和存储器；所述存储器用于存储计算机指令，当所述处理器执行该指令时，以使所述通信装置执行如权利要求1-22中任一项所述的鉴权方法。

28.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质包括计算机程序或指令，当所述计算机程序或指令在计算机上运行时，使得所述计算机执行如权利要求1-22中任一项所述的鉴权方法。

29.一种计算机程序产品，其特征在于，所述计算机程序产品包括：计算机程序或指令，当所述计算机程序或指令在计算机上运行时，使得所述计算机执行如权利要求1-22中任一项所述的鉴权方法。

鉴权方法及通信装置

技术领域

[0001] 本申请涉及通信领域,尤其涉及一种鉴权方法及通信装置。

背景技术

[0002] 用户装置(user equipment,UE),如终端设备可以通过第三代合作伙伴计划(the 3rd generation partner project,3GPP)接入网或者可信非3GPP接入网(trusted non-3GPP access network,TNAN)注册到核心网。

[0003] 目前,3GPP不支持UE在同一可信非3GPP接入网内的不同可信非3GPP接入点(trusted non-3GPP access point,TNAP)之间的移动性。为了通信安全,UE通过不同的TNAP建立接入网络时,均需要执行完整的认证流程,以获得用于建立UE与TNAP之间安全连接的密钥。基于此,UE从已经与UE建立通信连接的TNAP1切换至尚未与UE建立通信连接的TNAP2时,也需要执行完整的认证流程,以获取UE与TNAP2之间的建立安全连接的密钥。由于UE与TNAP之间的认证流程需要UE、可信非3GPP接入点(trusted non-3GPP access point,TNAP)、(trusted non-3GPP gateway function,TNGF)网元、接入和移动性管理功能(core access and mobility management function,AMF)网元以及认证服务器功能(authentication server function,AUSF)网元之间进行信息交互,以完成认证流程,交互流程复杂,这样,就会导致UE的服务被中断。

[0004] 因此,如何提高该场景下的生成UE与TNAP2之间的密钥效率,成为亟需解决的问题。

发明内容

[0005] 本申请实施例提供一种鉴权方法及通信装置,能够解决UE的服务被中断的问题,从而提高通信效率和可靠性。

[0006] 为达到上述目的,本申请采用如下技术方案:

[0007] 第一方面,提供一种鉴权方法。该鉴权方法包括:在用户设备UE从源可信的非第三代合作伙伴计划3GPP接入点TNAP移动到目标TNAP的情况下,可信的非3GPP网关功能TNGF根据存储的)根密钥生成中间密钥。TNGF使用中间密钥,生成针对目标TNAP的目标密钥。以及TNGF将目标密钥发送给目标TNAP。其中,目标密钥用于保护UE与目标TNAP之间通信安全。

[0008] 基于第一方面所提供的鉴权方法,在UE从源TNAP切换至目标TNAP的情况下,TNGF可以根据存储的与UE对应的根密钥生成中间密钥,并生成针对目标TNAP的目标密钥,以及将目标密钥发送给目标TNAP,以用于UE与TNAP之间的安全通信。如此,在切换TNAP的情况下,根据TNGF存储的与UE对应的根密钥生成目标密钥,可以避免执行完整的认证流程,即能够简化交互流程,从而提高通信效率和可靠性。

[0009] 一种可能的设计方案中,TNGF根据存储的与UE对应的根密钥生成中间密钥,可以包括:TNGF根据第一类型识别码以及根密钥生成中间密钥。其中第一类型识别码用于标识生成中间密钥。

[0010] 一种可能的设计方案中，在TNGF使用中间密钥，生成针对目标TNAP的目标密钥之前，第一方面所提供的方法可以包括：TNGF通过目标TNAP向UE发送鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。该第一验证参数由TNGF根据中间密钥和第一新鲜性参数生成。TNGF接收来自UE的鉴权响应消息。其中，鉴权响应消息包括第二验证参数以及第二新鲜性参数。TNGF根据中间密钥和第二新鲜性参数，得到第三验证参数。TNGF使用中间密钥，生成针对目标TNAP的目标密钥，可以包括：在第三验证参数与第二验证参数匹配的情况下，TNGF使用中间密钥，生成针对目标TNAP的目标密钥。如此，通过第一验证参数和第二验证参数对UE的身份进行验证，可以避免不合法的UE接入，从而进一步提高通信安全性。

[0011] 一种可能的设计方案中，在TNGF使用中间密钥，生成针对目标TNAP的目标密钥之前，第一方面所提供的方法可以包括：TNGF通过目标TNAP向UE发送鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。TNGF接收来自UE的鉴权响应消息。其中，鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。TNGF根据根密钥和第二新鲜性参数，得到第三验证参数。TNGF使用中间密钥，生成针对目标TNAP的目标密钥，可以包括：在第三验证参数与第二验证参数匹配的情况下，TNGF使用中间密钥，生成针对目标TNAP的目标密钥。如此，通过第一验证参数和第二验证参数对UE的身份进行验证，可以避免不合法的UE接入，从而进一步提高通信安全性。

[0012] 一种可能的设计方案中，在TNGF使用中间密钥，生成针对目标TNAP的目标密钥之后，以及TNGF将目标密钥发送给目标TNAP之前，第一方面所提供的方法还可以包括：TNGF通过目标TNAP向UE发送鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据中间密钥和第一新鲜性参数生成。TNGF接收来自UE的鉴权响应消息，其中，鉴权响应消息包括第二验证参数以及第二新鲜性参数。TNGF根据中间密钥和第二新鲜性参数，得到第三验证参数。TNGF将目标密钥发送给目标TNAP，可以包括：在第三验证参数与第二验证参数匹配的情况下，TNGF将目标密钥发送给目标TNAP。如此，通过第一验证参数和第二验证参数对UE的身份进行验证，可以避免不合法的UE接入，从而进一步提高通信安全性。

[0013] 一种可能的设计方案中，在TNGF使用中间密钥，生成针对目标TNAP的目标密钥之后，以及TNGF将目标密钥发送给目标TNAP之前，第一方面所提供的方法还可以包括：TNGF通过目标TNAP向UE发送鉴权请求消息，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。TNGF接收来自UE的鉴权响应消息。其中，鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。TNGF根据根密钥和第二新鲜性参数，得到第三验证参数。TNGF将目标密钥发送给目标TNAP，可以包括：在第三验证参数与第二验证参数匹配的情况下，TNGF将目标密钥发送给目标TNAP。如此，通过第一验证参数和第二验证参数对UE的身份进行验证，可以避免不合法的UE接入，从而进一步提高通信安全性。

[0014] 一种可能的设计方案中，在TNGF使用中间密钥，生成针对目标TNAP的目标密钥之前，第一方面所提供的方法还可以包括：TNGF通过目标TNAP向UE发送鉴权请求消息#1；其中，鉴权请求消息#1中包括UE的标识。TNGF接收来自UE的鉴权响应消息#1。其中，鉴权响应

消息#1可以包括第二验证参数以及第二新鲜性参数。TNGF根据中间密钥和第二新鲜性参数，得到第三验证参数。TNGF使用中间密钥，生成针对目标TNAP的目标密钥，可以包括：在第三验证参数与第二验证参数匹配的情况下，TNGF使用中间密钥，生成针对目标TNAP的目标密钥。在TNGF将目标密钥发送给目标TNAP之后，第一方面所提供的方法还可以包括：TNGF通过目标TNAP向UE发送鉴权响应请求消息#2，鉴权响应请求消息#2包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据中间密钥和第一新鲜性参数生成。TNGF通过目标TNAP接收来自UE的鉴权响应消息#2；鉴权响应消息#2用于指示TNGF发送认证成功消息。如此，通过第一验证参数和第二验证参数对UE的身份进行验证，可以避免不合法的UE接入，从而进一步提高通信安全性。

[0015] 一种可能的设计方案中，在TNGF使用中间密钥，生成针对目标TNAP的目标密钥之前，第一方面所提供的方法还可以包括：TNGF向所述UE发送鉴权请求消息#1；其中，鉴权请求消息#1中包括UE的标识。TNGF接收来自UE的鉴权响应消息#1，其中，鉴权响应消息#1包括第二验证参数以及第二新鲜性参数。TNGF根据根密钥和第二新鲜性参数，得到第三验证参数。TNGF使用中间密钥，生成针对目标TNAP的目标密钥，可以包括：在第三验证参数与第二验证参数匹配的情况下，TNGF使用中间密钥，生成针对目标TNAP的目标密钥。在TNGF将目标密钥发送给目标TNAP之后，第一方面所提供的方法还可以包括：TNGF通过目标TNAP向UE发送鉴权请求消息#2，鉴权请求消息#2可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。TNGF通过目标TNAP接收来自UE的鉴权响应消息#2；鉴权响应消息#2用于指示TNGF发送认证成功消息如此，通过第一验证参数和第二验证参数对UE的身份进行验证，可以避免不合法的UE接入，从而进一步提高通信安全性。

[0016] 一种可能的设计方案中，TNGF使用中间密钥，生成针对目标TNAP的目标密钥，可以包括：TNGF根据第二类型识别码和中间密钥生成目标密钥。其中，第二类型识别码用于标识生成中间密钥。

[0017] 一种可能的设计方案中，在TNGF根据存储的与UE对应的根密钥生成中间密钥之前，第一方面所提供的方法还可以包括：TNGF接收来自目标TNAP的第一请求消息。响应于第一请求消息，TNGF确定需要执行自身与UE之间的鉴权流程。如此，可以通过第一请求消息触发UE与TNGF之间的鉴权流程。

[0018] 可选地，第一请求消息可以包括UE的标识。TNGF根据UE的标识，确定UE从所述源TNAP移动到所述目标TNAP。示例性地，在第一请求消息中UE的标识和已经连接源TNAP的UE的标识相同。

[0019] 一种可能的设计方案中，在TNGF根据存储的与UE对应的根密钥生成中间密钥之前，第一方面所提供的方法还可以包括：TNGF根据UE的标识，确定根密钥。

[0020] 第二方面，提供一种鉴权方法该鉴权方法应用于通信装置从源可信的非第三代合作伙伴计划3GPP接入点TNAP移动到目标TNAP的场景下，包括：通信装置根据自身与可信的非3GPP网关功能TNGF之间的根密钥，生成中间密钥。其中，TNGF为源TNAP和目标TNAP的管理网元，以及，通信装置使用中间密钥，生成针对目标TNAP的目标密钥。其中，目标密钥用于保护通信装置与目标TNAP之间通信安全。

[0021] 基于第二方面所提供的鉴权方法，在通信装置，如UE从源TNAP切换至目标TNAP的

场景下,通信装置可以根据存储的与UE对应的根密钥生成中间密钥,并生成针对目标TNAP的目标密钥,以用于通信装置与TNAP之间的安全通信。如此,在通信装置切换TNAP的情况下,根据TNGF存储的与UE对应的根密钥生成目标密钥,可以避免执行完整的认证流程,能够简化交互流程,从而提高通信效率和可靠性。

[0022] 可理解,在本申请中,第二方面所述的通信装置可以为终端设备,或者可设置于该终端设备中的芯片(系统)或其他部件或组件。也就是说,第二方面所述的鉴权方法,可以由终端设备执行,或者由终端设备中的芯片(系统)或其他部件或组件执行。

[0023] 一种可能的设计方案中,通信装置根据自身与TNGF之间的根密钥,生成中间密钥,可以包括:通信装置根据第一类型识别码以及根密钥生成中间密钥。其中,第一类型识别码用于标识生成中间密钥。

[0024] 一种可能的设计方案中,在通信装置根据自身与TNGF之间的根密钥,生成中间密钥之前,第二方面所提供的方法可以包括:通过目标TNAP接收来自TNGF的鉴权请求消息。其中,鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中,第一验证参数由TNGF根据中间密钥和第一新鲜性参数生成。通信装置使用中间密钥和第一新鲜性参数,得到第四验证参数。在第四验证参数与第一验证参数匹配的情况下,通信装置向TNGF发送鉴权响应消息。其中,鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。

[0025] 一种可能的设计方案中,在通信装置根据自身与TNGF之间的根密钥,生成中间密钥之前,第二方面所提供的方法可以包括:通信装置通过目标TNAP接收来自TNGF的鉴权请求消息。其中,鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中,第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。通信装置使用根密钥和第一新鲜性参数,得到第四验证参数。在第四验证参数与第一验证参数匹配的情况下,通信装置向TNGF发送鉴权响应消息。其中,鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。

[0026] 一种可能的设计方案中,在通信装置根据自身与TNGF之间的根密钥,生成中间密钥之前,第二方面所提供的方法可以包括:通信装置通过目标TNAP接收来自TNGF的鉴权请求消息。鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中,第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。通信装置使用中间密钥和第一新鲜性参数,得到第四验证参数。通信装置根据自身与TNGF之间的根密钥,生成中间密钥,可以包括:在第四验证参数与第一验证参数匹配的情况下,通信装置根据自身与TNGF之间的根密钥,生成中间密钥。在通信装置使用中间密钥,生成针对目标TNAP的目标密钥之后,方法还可以包括:通信装置向TNGF发送鉴权响应消息。其中,鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。

[0027] 一种可能的设计方案中,在通信装置根据自身与TNGF之间的根密钥,生成中间密钥之前,第二方面所提供的方法可以包括:通信装置通过目标TNAP接收来自TNGF的鉴权请求消息。其中,鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中,第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。通信装置使用根密钥和第一新鲜性参数,得到第四验证参数。通信装置根据自身与TNGF之间的根密钥,生成中间密钥,可以包括:在第四验证参数与第一验证参数匹配的情况下,通信装置根据自身与TNGF之间的根密钥,生成中间密钥。在通信装置使用中间密钥,生成针对目标TNAP的目标密钥之后,第二方面所提供的方法还可以包括:通信装置向TNGF发送鉴权响应消息。其中,鉴权响应消息可以包括第

二验证参数以及第二新鲜性参数。

[0028] 一种可能的设计方案中，通信装置使用中间密钥，生成针对目标TNAP的目标密钥，可以包括：通信装置根据第二类型识别码和中间密钥生成目标密钥。其中，第二类型识别码用于标识生成目标密钥。

[0029] 可选地，在通信装置根据自身与TNGF之间的根密钥，生成中间密钥之前，第二方面所提供的方法还可以包括：通信装置向目标TNAP发送第一请求消息。进一步地，第一请求消息可以包括通信装置的标识。

[0030] 一种可能的设计方案中，在通信装置根据自身与TNGF之间的根密钥，生成中间密钥之前，方法还包括：通信装置根据TNGF的标识，确定根密钥。

[0031] 第三方面，提供一种通信装置。该通信装置包括：用于执行第一方面中任一项所述的鉴权方法的模块，如收发模块和处理模块。

[0032] 可选地，第三方面所述的通信装置还可以包括存储模块，该存储模块存储有程序或指令。当该处理模块执行该程序或指令时，使得该通信装置可以执行第一方面所述的鉴权方法。

[0033] 需要说明的是，第三方面所述的通信装置可以是网络设备，例如可信的非3GPP网关功能，也可以是可设置于网络设备中的芯片(系统)或其他部件或组件，还可以是包含网络设备的装置，本申请对此不做限定。

[0034] 此外，第三方面所述的通信装置的技术效果可以参考第一方面所述的鉴权方法的技术效果，此处不再赘述。

[0035] 第四方面，提供一种通信装置。该通信装置包括：用于执行第二方面中任一项所述的鉴权方法的模块，如收发模块和处理模块。

[0036] 可选地，第四方面所述的通信装置还可以包括存储模块，该存储模块存储有程序或指令。当该处理模块执行该程序或指令时，使得该通信装置可以执行第二方面所述的鉴权方法。

[0037] 需要说明的是，第四方面所述的通信装置可以是终端设备，如用户设备，也可以是可设置于终端设备中的芯片(系统)或其他部件或组件，本申请对此不做限定。通信装置也可以称为用户设备。

[0038] 此外，第四方面所述的通信装置的技术效果可以参考第二方面所述的鉴权方法的技术效果，此处不再赘述。

[0039] 第五方面，提供一种通信装置。该通信装置包括：处理器，该处理器用于执行第一方面至第二方面中任意一种可能的实现方式所述的鉴权方法。

[0040] 在一种可能的设计方案中，第五方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第五方面所述的通信装置与其他通信装置通信。

[0041] 在一种可能的设计方案中，第五方面所述的通信装置还可以包括存储器。该存储器可以与处理器集成在一起，也可以分开设置。该存储器可以用于存储第一方面至第二方面中任一方面所述的鉴权方法所涉及的计算机程序和/或数据。

[0042] 此外，第五方面所述的通信装置的技术效果可以参考第一方面或第二方面中任意一种实现方式所述的鉴权方法的技术效果，此处不再赘述。

[0043] 第六方面，提供一种通信装置。该通信装置包括：处理器，该处理器与存储器耦合，该处理器用于执行存储器中存储的计算机程序，以使得该通信装置执行第一方面至第二方面中任意一种可能的实现方式所述的鉴权方法。

[0044] 在一种可能的设计方案中，第六方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第六方面所述的通信装置与其他通信装置通信。

[0045] 此外，第六方面所述的通信装置的技术效果可以参考第一方面或第二方面中任意一种实现方式所述的鉴权方法的技术效果。

[0046] 第七方面，提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机程序，当该处理器执行该计算机程序时，以使该通信装置执行第一方面至第二方面中的任意一种实现方式所述的鉴权方法。

[0047] 在一种可能的设计方案中，第七方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第七方面所述的通信装置与其他通信装置通信。

[0048] 此外，第七方面所述的通信装置的技术效果可以参考第一方面或第二方面中任意一种实现方式所述的鉴权方法的技术效果；

[0049] 第八方面，提供了一种通信装置，包括：处理器；所述处理器用于与存储器耦合，并读取存储器中的计算机程序之后，根据该计算机程序执行如第一方面至第五方面中的任意一种实现方式所述的鉴权方法。

[0050] 在一种可能的设计方案中，第八方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第八方面所述的通信装置与其他通信装置通信。

[0051] 此外，第八方面所述的通信装置的技术效果可以参考第一方面或第二方面中任意一种实现方式所述的鉴权方法的技术效果。

[0052] 第九方面，提供一种处理器。其中，处理器用于执行第一方面至第五方面中任意一种可能的实现方式所述的鉴权方法。

[0053] 第十方面，提供一种通信系统。该通信系统包括一个或多个终端设备，以及一个或多个网络设备。

[0054] 第十一方面，提供一种计算机可读存储介质，包括：计算机程序或指令；当该计算机程序或指令在计算机上运行时，使得该计算机执行第一方面至第二方面中任意一种可能的实现方式所述的鉴权方法。

[0055] 第十二方面，提供一种计算机程序产品，包括计算机程序或指令，当该计算机程序或指令在计算机上运行时，使得该计算机执行第一方面至第二方面中任意一种可能的实现方式所述的鉴权方法。

附图说明

[0056] 图1为本申请实施例提供的核心网的架构示意图；

[0057] 图2为本申请实施例提供的通信系统的架构示意图；

[0058] 图3为本申请实施例提供的鉴权方法的流程示意图一；

[0059] 图4为本申请实施例提供的目标密钥生成示意图一；

[0060] 图5为本申请实施例提供的目标密钥生成示意图二；

[0061] 图6为本申请实施例提供的鉴权方法的流程示意图二；

[0062] 图7为本申请实施例提供的鉴权方法的流程示意图三；

[0063] 图8为本申请实施例提供的鉴权方法的流程示意图四；

[0064] 图9为本申请实施例提供的通信装置的流程示意图一；

[0065] 图10为本申请实施例提供的通信装置的流程示意图二。

具体实施方式

[0066] 为便于理解，下面先介绍本申请实施例所涉及的技术术语。

[0067] 1、第五代(5th generation，5G)移动通信系统(简称5G系统(5G system，5GS))：

[0068] 图1为5GS的架构示意图。如图1所示，5GS包括：接入网(access network，AN)和核心网(core network，CN)，还可以包括：终端设备。

[0069] 其中，CN可以包括用户面功能(user plane function，UPF)网元(简称用户面网元)、接入和移动性管理功能(core access and mobility management function，AMF)网元、会话管理功能(session management function，SMF)网元(简称为会话管理网元)、认证服务器功能(authentication server function，AUSF)网元、可信非3GPP接入点(trusted non-3GPP access point，TNAP)、可信非3GPP网关功能(trusted non-3GPP gateway function，TNGF)网元、网络数据分析功能(network data analytics function，NWDAF)网元(简称网络数据分析网元)、网络开放功能(network exposure function，NEF)网元、网络功能存储功能(network exposure function Repository Function，NRF)网元、策略控制功能(policy control function，PCF)网元(简称策略控制网元)、统一数据管理(unified data management，UDM)网元(简称数据管理网元)、应用功能(application function，AF)网元或者服务通信代理(service communication proxy，SCP)网元等。

[0070] 需要说明的是，图1仅是示例性给出了5G网络中网元或实体的一些举例，该5G网络还可以包括统一数据存储(unified data repository，UDR)网元、网络切片选择功能(network slice selection function，NSSF)网元、计费功能(charging function，CHF)网元等一些图1中未示意出的网元或实体，本申请实施例对此不做具体限定。

[0071] 其中，如图1所示，终端设备通过AN设备接入5G网络，终端设备通过N1接口(简称N1)与AMF网元通信；RAN设备通过N2接口(简称N2)与AMF网元通信；终端设备通过Yt接口与TNAP通信，TNAP通过Ta接口与TNGF网元通信；TNGF网元通过N2接口与AMF网元通信；TNGF网元还通过N3接口与UPF网元通信；RAN设备通过N3接口(简称N3)与UPF网元通信；SMF网元通过N4接口(简称N4)与UPF网元通信，UPF网元通过N6接口(简称N6)接入数据网络(data network，DN)。此外，图1所示的AUSF网元、AMF网元、SMF网元、NEF网元、NRF网元、PCF网元、UDM网元、UDR网元、AF网元、NWDAF网元或者SCP网元等控制面功能采用服务化接口进行交互。比如，AUSF网元对外提供的服务化接口为Nausf；AMF网元对外提供的服务化接口为Namf；SMF网元对外提供的服务化接口为Nsmf；NEF网元对外提供的服务化接口为Nnef；NRF网元对外提供的服务化接口为Nnrf；PCF网元对外提供的服务化接口为Npcf；UDM网元对外提供的服务化接口为Nudm；AF网元对外提供的服务化接口为Naf。此外，UDR网元对外提供的

服务化接口为Nudr;NSSF网元对外提供的服务化接口为Nnssf;CHF网元对外提供的服务化接口为Nchf;相关功能描述以及接口描述可以参考23501标准中的5G系统架构(5G system architecture)图,在此不予赘述。

[0072] 下面对上述网络架构中涉及的各个部分或网元在5G网络中的功能示例性的分别进行说明。

[0073] (1)、终端可以为具有收发功能的终端,或为可设置于该终端的芯片或芯片系统。该终端也可以称为用户装置(uesr equipment,UE)、接入终端、用户单元(subscriber unit)、用户站、移动站(mobile station,MS)、移动台、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。本申请的实施例中的终端可以是手机(mobile phone)、蜂窝电话(cellular phone)、智能电话(smart phone)、平板电脑(Pad)、无线数据卡、个人数字助理电脑(personal digital assistant,PDA)、无线调制解调器(modem)、手持设备(handset)、膝上型电脑(laptop computer)、机器类型通信(machine type communication,MTC)终端、带无线收发功能的电脑、虚拟现实(virtual reality,VR)终端、增强现实(augmented reality,AR)终端、工业控制(industrial control)中的无线终端、无人驾驶(self driving)中的无线终端、远程医疗(remote medical)中的无线终端、智能电网(smart grid)中的无线终端、运输安全(transportation safety)中的无线终端、智慧城市(smart city)中的无线终端、智慧家庭(smart home)中的无线终端、车载终端、具有终端功能的路边单元(road side unit,RSU)等。本申请的终端还可以是作为一个或多个部件或者单元而内置于车辆的车载模块、车载模组、车载部件、车载芯片或者车载单元。

[0074] (2)、AN网元用于实现接入有关的功能,可以为特定区域的授权终端提供入网功能,并能够根据终端的级别,业务的需求等使用不同质量的传输隧道。AN在网元终端与CN之间转发控制信号和用户数据。本申请中的AN网元,可以为无线接入网(radio access network,RAN)网元。RAN网元能够管理无线资源,为终端设备提供接入服务,进而完成控制信号和终端数据在终端和核心网之间的转发,RAN网元也可以理解为传统网络中的基站。例如,可以负责空口侧的无线资源管理、服务质量(quality of service,QoS)管理、数据压缩和加密等功能。

[0075] RAN网元可以是无线网络中的设备。RAN网元也可以称为无线RAN网元或者网络设备或者无线网络节点。目前,一些RAN网元的举例为:5G系统中的下一代节点B(The Next Generation Node B,gNB)、传输接收点(transmission reception point,TRP)、长期演进(long term evolution,LTE)系统中的演进型节点B(evolved Node B,eNB)、无线网络控制器(radio network controller,RNC)、节点B(Node B,NB)、基站控制器(base station controller,BSC)、基站收发台(base transceiver station,BTS)、家庭基站(例如,home evolved NodeB,或home Node B,HNB)、基带单元(base band unit,BBU),或无线保真(wireless fidelity,Wifi)接入点(access point,AP)等。在一种网络结构中,网络设备可以包括集中单元(centralized unit,CU)节点、或分布单元(distributed unit,DU)节点、或包括CU节点和DU节点的RAN网元。RAN网元还可以是无线回传设备,车载设备,可穿戴设备以及未来5G网络中的网络设备或者未来演进的PLMN网络中的网络设备等。在第三代(3rd generation,3G)系统中,称为节点B(Node B)等。

[0076] (3)、移动管理网元,属于核心网网元,主要负责信令处理部分,例如:接入控制、移

动性管理、附着与去附着以及网关选择等功能。移动管理网元为终端的会话提供服务的情况下，会为该会话提供控制面的存储资源，以存储会话标识、与会话标识关联的SMF网元标识等。在5G通信系统中，该移动管理网元可以是接入和移动性管理功能(access and mobility management function，AMF)网元。在未来通信系统中，移动管理网元仍可以是AMF网元，或者，还可以有其它的名称，本申请不做限定。

[0077] (4)、会话管理网元，用于移动网络中的会话管理，例如负责用户面网元选择，用户面网元重定向，因特网协议(internet protocol，IP)地址分配，承载的建立、修改和释放以及QoS控制。会话管理、终端的IP地址分配和管理、选择可管理用户平面功能、策略控制和收费功能接口的终结点以及下行数据通知等。在5G通信系统中，该会话管理网元可以是SMF网元。在未来通信系统中，会话管理网元仍可以是SMF网元，或者，还可以有其它的名称，本申请不做限定。

[0078] (5)、用户面网元用于分组路由和转发，用户面数据的服务质量(quality of service，QoS)处理等。在5G通信系统中，用户面网元所对应的网元或实体可以为5G网络架构中的用户平面功能(user plane function，UPF)网元，在未来通信系统中，用户面网元仍可以是UPF网元，或者用户面网元有其它名称，本申请实施例对此不作限定。

[0079] (6)、认证服务器功能网元，主要提供认证功能，支持第三代合作伙伴计划(3rd generation partnership project，3GPP)接入和Non-3GPP接入的认证，具体可参考3GPP TS 33.501。在5G通信系统中，认证服务器功能网元可以是认证服务器功能(authentication server function，AUSF)网元，在未来通信系统中，认证服务器功能网元仍可以是AUSF网元，或者认证服务器功能网元有其它名称，本申请实施例对此不作限定。

[0080] (7)TNAP，用于提供UE接入功能。

[0081] (8)TNGF网元，用于作为可信非3GPP接入网的网关。

[0082] (9)、数据管理网元，用于处理用户标识、接入鉴权、注册、或移动性管理等。在5G通信系统中，数据管理网元所对应的网元或者实体可以为5G网络架构中的统一数据管理(unified data management，UDM)网元，其中Nudm是UDM网元提供的基于服务的接口，UDM网元可以通过Nudm与其他的网络功能通信。在未来通信系统中，数据管理网元仍可以是UDM网元，或者数据管理网元有其它名称，本申请实施例对此不作限定。

[0083] (10)、网络开放功能网元，主要提供的服务使得第三代合作伙伴计划(3rd generation partnership project，3GPP)网络能够安全地向第三方的业务提供者应用功能网元207提供网络业务能力。在5G通信系统中，网络开放功能网元可以是(network exposure function，NEF)网元，Nnef是NEF网元提供的基于服务的接口，NEF网元可以通过Nnef与其他的网络功能通信，在未来通信系统中，网络开放功能网元仍可以是NEF网元，或者有其它名称，本申请实施例对此不作限定。

[0084] (11)、策略控制网元，包含用户签约数据管理功能、策略控制功能、计费策略控制功能、QoS控制等，用于指导网络行为的统一策略框架，为控制平面功能网元(例如AMF网元等)提供策略规则信息等。在5G通信系统中，策略控制网元可以是PCF网元。在未来通信系统中，策略控制功能网元仍可以是PCF网元，或者有其它名称，本申请实施例对此不作限定。

[0085] (12)、应用功能网元，主要用于向3GPP网络提供应用层信息。在5G通信系统中，应用功能网元207可以是应用功能(application function，AF)网元，Naf是AF网元提供的基

于服务的接口，AF网元可以通过Naf与其他的网络功能通信，在未来通信系统中，应用功能网元仍可以是AF网元，或者有其它名称，本申请实施例对此不作限定。示例性的，AF网元例如可以包括业务能力服务器(services capability server，SCS)或者应用服务器(application server，AS)。

[0086] (13)、数据网络，指的是为终端提供数据传输服务的网络，如IMS(IP Multi-media Service，IP多媒体业务)、Internet等。

[0087] 终端通过建立终端到RAN网元到UPF网元到DN网元之间的PDD会话，来访问数据网络。

[0088] (14)网络数据分析功能网元，用于提供基于大数据和人工智能等技术的网络数据采集和分析功能。在5G系统中，网络数据分析功能网元可以是NWDAF网元。在未来通信系统中，网络数据分析功能网元仍可以是NWDAF网元，或者，还可以有其它的名称，本申请不做限定。

[0089] (15)、切片选择功能网元，用于为终端选择网络切片等。在5G通信系统中，切片选择功能网元可以是NSSF网元。在未来通信系统中，网络切片选择功能网元仍可以是NSSF网元，或者有其它名称，本申请实施例对此不作限定。

[0090] (16)、统一数据存储网元，主要负责存储结构化数据，存储的内容包括签约数据和策略数据、对外暴露的结构化数据和应用相关的数据。在5G通信系统中，该统一数据存储网元可以是UDR网元。在未来通信系统中，统一数据存储网元仍可以是UDR网元，或者，还可以有其它的名称，本申请不做限定。

[0091] 需要说明，下述实施例中，TNGF网元均简称为TNGF，AMF网元均简称为AMF，AUSF网元均简称为AUSF，UPF网元均简称为UPF，终端设备均以UE进行说明，后续不再赘述。

[0092] UE可以通过第三代合作伙伴计划(the 3rd generation partner project，3GPP)接入网或者可信非3GPP接入网(trusted non-3GPP access network，TNAN)注册到核心网。

[0093] 目前，3GPP不支持UE在同一可信非3GPP接入网内的不同可信非3GPP接入点(trusted non-3GPP access point，TNAP)之间的移动性。为了通信安全，UE通过不同的TNAP接入网络时，均需要执行完整的认证流程，以获得用于建立UE与TNAP之间安全连接的密钥。基于此，UE从已经与UE建立通信连接的TNAP1切换至尚未与UE建立通信连接的TNAP2时，也需要执行完整的认证流程，以获取UE与TNAP2之间的建立安全连接的密钥。由于UE与TNAP之间的认证流程需要UE、可信非3GPP接入点(trusted non-3GPP access point，TNAP)、(trusted non-3GPP gateway function，TNGF)、接入和移动性管理功能(core access and mobility management function，AMF)以及认证服务器功能(authentication server function，AUSF)之间进行信息交互，以完成认证流程，交互流程复杂，这样，就会导致UE的服务被中断。

[0094] 因此，如何提高该场景下的生成UE与TNAP2之间的密钥效率，成为亟需解决的问题。

[0095] 综上，针对上述技术问题，本申请实施例提出了如下技术方案，用以避免UE切换TNAP时通信流程中断的问题，以提高通信效率和通信可靠性。以下简单介绍本申请实施例的方案。本申请实施例中，在TNAP从源TNAP切换至目标TNAP的情况下，TNGF可以基于存储的与UE对应的根密钥生成中间密钥，进而根据中间密钥生成针对目标TNAP的目标密钥，并向

目标TNAP发送该目标密钥。UE也可以存储与TNGF对应的的根密钥生成中间密钥，进而根据中间密钥生成针对目标TNAP的目标密钥。如此，根据UE和TNGF均可以根据自身存储的根密钥生成用目标密钥，可以避免UE切换TNAP时，执行完整的认证流程，即能够简化交互流程，从而提高通信效率和可靠性。

[0096] 本申请实施例的技术方案可以应用于各种通信系统，例如无线保真(wireless fidelity，WiFi)系统，车到任意物体(vehicle to everything，V2X)通信系统、设备间(device-todevie，D2D)通信系统、车联网通信系统、第4代(4th generation，4G)移动通信系统，如长期演进(long term evolution，LTE)系统、全球互联微波接入(worldwide interoperability for microwave access，WiMAX)通信系统、第五代(5th generation，5G)移动通信系统，如新空口(new radio，NR)系统，以及未来的通信系统，如第六代(6th generation，6G)移动通信系统等。

[0097] 本申请将围绕可包括多个设备、组件、模块等的系统来呈现各个方面、实施例或特征。应当理解和明白的是，各个系统可以包括另外的设备、组件、模块等，并且/或者可以并不包括结合附图讨论的所有设备、组件、模块等。此外，还可以使用这些方案的组合。

[0098] 另外，在本申请实施例中，“示例地”、“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用示例的一词旨在以具体方式呈现概念。

[0099] 本申请实施例中，“信息(information)”，“信号(signal)”，“消息(message)”，“信道(channel)”、“信令(singaling)”有时可以混用，应当指出的是，在不强调其区别时，其所要表达的含义是一致的。“的(of)”，“相应的(corresponding，relevant)”和“对应的(corresponding)”有时可以混用，应当指出的是，在不强调其区别时，其所要表达的含义是一致的。

[0100] 本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

[0101] 为便于理解本申请实施例，首先以图2中示出的通信系统为例详细说明适用于本申请实施例的通信系统。示例性地，图2为本申请实施例提供的鉴权方法所适用的一种通信系统的架构示意图。

[0102] 如图2所示，该通信系统包括UE、3GPP接入网、可信非3GPP接入网(trusted non-3GPP access network，TNAN)和AMF。

[0103] UE可以通过3GPP接入网进行3GPP接入，UE可以通过TNAN进行non-3GPP接入。其中TNAN包括TNAP#1、TNAP#2和TNGF。示例性地，UE与TNAP#1之间可以通过Yt接口通信连接，UE与TNGF之间可以通过NWt接口通信连接。UE还可以通过N1接口与AMF通信连接。UE与TNAP#2之间可以通过Yt接口通信连接，UE与TNGF之间可以通过NWt接口通信连接。UE还可以通过N1接口与AMF通信连接。在此情况下，TNGF为TNAP#1、TNAP#2的管理网元。TNGF为TNAP的管理网元，是指TNGF与该TNAP建立有连接，并且TNGF生成用于该TNAP与UE之间建立安全通信的密钥，并发送给TNAP。

[0104] 此外，图2所示的通信系统中还可以包括SMF、UPF、和数据网络。

[0105] 其中,SMF与AMF之间可以通过N11接口通信,UPF与SMF之间可以通过N4接口通信连接,UPF与TNGF之间可以通过N3接口通信连接,数据网络和UPF之间可以通过N6接口通信连接。3GPP接入网可以通过N2接口与AMF通信连接。3GPP接入网可以包括RAN。

[0106] 需要说明的是,本申请实施例提供的鉴权方法,可以适用于图2所示的UE、TNAP#1、TNAP#2和TNGF之间具体实现可以参考下述方法实施例,此处不再赘述。

[0107] 应当指出的是,本申请实施例中的方案还可以应用于其他通信系统中,相应的名称也可以用其他通信系统中的对应功能的名称进行替代。

[0108] 应理解,图2仅为便于理解而示例的简化示意图,该通信系统中还可以包括其他网络设备,如AUSF等,图2中未予以画出。

[0109] 下面结合本申请实施例所应用的各种场景分别说明本申请实施例所提供的方案。下面实施例中,均以TNAP#1作为源TNAP,TNAP#2作为目标TNAP进行说明。

[0110] 示例性地,图3为本申请实施例提供的鉴权方法的流程示意图一,该鉴权方法主要适用于UE在同一TNGF下切换TNAP的情况下,TNGF和UE均在完成对对侧设备的身份认证后,确定用于UE与切换后的TNAP之间通信的K_{TNAP}密钥。例如,在UE从同一TNGF所连接的TNAP#1切换至TNAP#2的情况下,确定用于UE与TNAP#2之间通信安全的K_{TNAP}密钥。以下结合UE从TNAP#1和TNAP#2说明图3所示鉴权方法的通信流程。

[0111] S301,UE连接TNAP#1,以通过TNAP#1开始执行可信非3GPP注册、鉴权和协议数据单元(protocol data unit,PDU)会话建立流程。

[0112] 需要说明的是,S301执行过程中,包括两次鉴权流程,两次鉴权流程分别包括第一鉴权流程,即主鉴权流程(以下在不做特殊说明的情况下,均称为主鉴权流程),以及第二鉴权流程。其中,主鉴权流程中,鉴权服务器(authentication server)是AUSF,鉴权方(authenticator)是AMF,被鉴权方是UE。主鉴权流程使用的方法是可扩展认证协议(extensible authentication protocol,EAP)-认证与密钥协商'(authentication and key management',AKA'),即EAP-AKA'方法或者5G-AKA方法,此处不再赘述。第二鉴权流程中,鉴权服务器是TNGF,鉴权方是TNAP#1,被鉴权方是UE。其中,主鉴权流程和第二鉴权流程执行的时间之间的关系如下:UE先触发第二鉴权流程,在第二鉴权流程执行过程中,由AMF触发第一鉴权流程,在第一鉴权流程成功完成后,第二鉴权流程才会完成。完整执行第一鉴权流程和第二鉴权流程的鉴权流程,可以称为完整的鉴权流程。在只执行第二鉴权流程,且在第二鉴权流程执行过程中没有执行第一鉴权流程的鉴权流程,叫做不完整的鉴权流程。本实施例就是提供一种不完整的鉴权流程的方法。可选地,S301交互的信息中,可以包括UE的标识,其中,UE的标识可以是5G全球唯一临时标识(5G-globally unique temporary UE identity,5G-GUTI)和/或用户隐藏标识符(subscription concealed identifier,SUCI)。其中,UE的标识的格式为网络访问标识符(network access identifier,NAI)格式,如username@realm格式。

[0113] 关于S301的具体实现可以参考协议版本TS 33.501版本17.7.0章节7.2A.2.1中定义的流程,此处不再赘述。

[0114] S302,AMF向TNGF发送根密钥。相应地,TNGF接收来自AMF的根密钥。

[0115] 其中,根密钥可以携带在N2初始上下文建立请求消息中。

[0116] 关于S302的具体实现原理可以参考协议版本TS 33.501版本17.7.0中的7A.2.1中

的相关介绍，此处不再赘述。

[0117] S303，UE完成注册、完整的鉴权流程和PDU会话建立流程。

[0118] 在此过程中，UE与TNAP#1建立连接。

[0119] 其中，S303中的信元可以包括初始身份标识(initator identifier，IDi)和初始身份标识(responser Idenifier，IDr)。IDi中可以包括5G-GUTI和/或SUCI。

[0120] S303包括如下步骤：步骤1a，TNGF生成根密钥K_{TNGF}，并使用K_{TNGF}生成针对TNAP#1的K_{TNAP1}。

[0121] 步骤2a，TNGF向TNAP#1发送K_{TNAP1}。相应地，TNAP#1接收来自TNGF的K_{TNAP1}。

[0122] 步骤3a，UE根据生成根密钥K_{TNGF}，并使用K_{TNGF}生成针对TNAP#1的K_{TNAP1}。

[0123] 步骤4a，UE与TNAP#1使用K_{TNAP1}建立安全连接。

[0124] 关于S303具体实现原理可以参考协议版本TS 33.501版本17.7.0中的7A.2.1中定义的流程，此处不再赘述。

[0125] S304，TNGF通过TNAP#2接收第一请求消息。

[0126] 示例性地，S304包括，在UE从TNAP#1移动到TNAP#2的情况下，TNGF通过TNAP#2接收第一请求消息。

[0127] 一种可能的设计方案中，第一请求消息可以包括UE的标识。该第一请求消息可以用于通知TNGF该UE从TNAP#1移动到了TNAP#2。UE的标识可以包括UE在S301中携带的5G-GUTI，或SUCI，或者SS303中携带的信元，如初始身份标识(initator identifier，IDi)，或者NAI格式的标识，或者UE的网络协议(internet protocal，IP)地址等其他TNGF可以识别UE的身份，或者用于TNGF确定TNGF中存储与UE对应的的根密钥(以下均简称为TNGF中存储的密钥)与UE中存储的根密钥(以下均简称为UE中存储的根密钥)相同的标识信息。本实施例不对UE的标识做具体限定。

[0128] 本申请实施例中，第一请求消息可以有多种不同的实现方法。如下述情形1.1和下述情形1.2。

[0129] 情形1.1，第一请求消息可以由TNAP#2生成。在这种情况下，S304可以包括：TNAP#2生成第一请求消息。UE与TNAP#2之间已经建立通信连接。TNAP#2基于该通信连接向TNGF发送第一请求消息。

[0130] 情形1.2，第一请求消息由UE生成。在此情况下，S303可以包括：UE生成第一请求消息，并通过TNAP#2将第一请求消息发送给TNGF，相应地，TNGF接收来自TNAP#2的第一请求消息。关于情形1.2的实现原理可以参考下述图6所示的S607和S608。

[0131] 示例性地，第一请求消息可以是EAP身份响应消息(EAP-RES/Identity)消息，或者EAP-RES/5G-NAS(non-access stratum)消息，或者EAP-RES/5G-ReAUTH(re-authentication)消息，或者EAP-RES/ReAUTH消息等。本实施例对消息名称做不具体限定。

[0132] 示例性地，第一请求消息可以是EAP-RES/Identity消息。该消息由UE发送，消息中携带的UE标识。比如，UE的标识为NAI格式的标识。该NAI格式的标识可以与UE在S301中携带的UE的标识的相同。

[0133] S305，响应于第一请求消息，TNGF向TNAP#2发送鉴权请求消息。相应地，TNAP#2接收来自TNGF的鉴权请求消息。

[0134] 其中，鉴权请求消息包括第一验证参数以及第一新鲜性参数。

[0135] 其中,第一新鲜性参数是TNGF生成的随机数、或者计数器值,本实施例不做具体限定。

[0136] 可选地,鉴权请求消息还可以包括TNGF的标识。

[0137] 其中,鉴权请求消息用于UE在不同的TNAP之间切换时,对UE进行重新认证。TNGF的标识可以是如下的一种或多种:TNGF的IP地址,TNGF的身份标识,S303中携带的初始身份标识(responser Idenifier,IDr),或者用于UE确定UE存储的根密钥与TNGF存储的与UE对应的根密钥相同的标识信息。

[0138] 鉴权请求消息可以是EAP-REQ/Restart消息,或者EAP-REQ/5G-Restart消息,或者EAP-REQ/5G-NAS消息,或者EAP-REQ/5G/Notification消息,或者EAP-REQ/5G-AN消息,或者EAP-REQ/5G-ReAUTH消息,或者EAP-REQ/ReAUTH消息等。本实施例不对鉴权请求消息的名称做具体限定。

[0139] 可选地,在发送鉴权请求消息之前,图3所提供的方法还可以包括:响应于第一请求消息,TNGF确定执行不完整的鉴权流程。示例性地,TNGF根据第一请求消息中的信息确定需要对UE进行鉴权。在一种可能的实现方式中,若第一请求消息中只包括接入网参数(access network parameter,AN parameter),TNGF确定执行不完整的鉴权流程。在另一种可能的实现方式中,第一请求消息中包括用于指示需要执行不完整的鉴权流程的指示信息,此时,TNGF根据第一请求消息中携带的指示信息确定执行不完整鉴权流程。指示信息可以由UE生成,也可以由TNAP#1生成,本实施例不做具体限定。示例性地,指示信息可以通过一个或多个比特位(bit)指示。在又一种可能的实现方式中,第一请求消息中包括UE的标识,此时,TNGF可以根据第一请求消息中的UE的标识,确定TNGF存储有UE对应的安全上下文,进而确定执行不完整鉴权流程。

[0140] 在TNGF确定触发不完整的鉴权流程后,TNGF根据第一请求消息中的UE的标识,确定根密钥,该根密钥与UE的标识对应,即确定与UE对应的根密钥。可理解,TNGF中可以存储或配置有不同UE的标识与不同根密钥的第一对应关系。TNGF可以根据UE的标识,确定与UE对应的根密钥。

[0141] 其中,根密钥可以是K_{TNGF},或者K_{TNAP},或者K_{TIPSec}等密钥。本实施例对根密钥不做具体限定。生成参数可以包括以下至少一种:TNGF的标识、或第一新鲜性参数。在生成参数包括TNGF标识的情况下,鉴权请求消息中还可以包括TNGF标识。

[0142] 对于UE而言,K_{TNGF}是UE与TNGF在通过TNAP#1接入时UE自己生成的。对于TNGF而言,K_{TNGF}是TNGF从AMF得到的密钥。K_{TNGF}在UE和TNGF侧相同。K_{TNAP}是TNGF和UE分别各自使用K_{TNGF}和第二类型识别码生成的密钥,TNGF在生成K_{TNAP}后,将K_{TNAP}发送给TNAP,K_{TNAP}用于UE与TNAP之间建立安全连接。例如,TNAP#1与UE之间的K_{TNAP}可以是K_{TNAP1},K_{TNAP1}用于保护UE与TNAP#1之间建立安全。K_{TIPSec}是TNGF和UE分别各自使用K_{TNGF}和第三类型识别码生成的用于建立IPsec的密钥。类型识别码用于标识生成密钥的类型,生成密钥的类型也可以用于表征密钥的用处,比如第二类型识别码用于表征生成的密钥用于TNAP#2,即目标密钥。第三类型识别码用于表征生成的密钥用于IPsec。

[0143] 在确定与UE对应的根密钥后,TNGF可以使用与UE对应的根密钥、生成参数和生成算法计算得到第一验证参数。

[0144] TNGF使用与UE对应的根密钥生成第一验证参数有多种实现方式。以下结合方式1、

方式2说明。

[0145] 方式1,TNGF使用与UE对应的根密钥生成中间密钥,再使用中间密钥生成第一验证参数。例如,与UE对应的根密钥为K_{TNGF},则TNGF使用K_{TNGF}生成中间密钥K_{TNGF}',再使用K_{TNGF}'生成第一验证参数。TNGF使用与UE对应的根密钥生成中间密钥的流程可以在执行S304前生成。比如,可以在执行S304前,以及在生成与UE对应的根密钥后生成中间密钥;也可以在TNGF确定触发不完整的鉴权流程后再生成。本实施例不限制具体的生成时间。示例性地,TNGF可以根据与UE对应的根密钥、TNGF的IP地址和第一新鲜性参数计算得到第一验证参数。或者,TNGF可以根据与UE对应的根密钥和TNGF的身份标识计算得到第一验证参数。或者,TNGF可以根据与UE对应的根密钥和TNGF生成的随机数,计算得到第一验证参数。

[0146] 方式2,TNGF使用与UE对应的根密钥直接生成第一验证参数。示例性地,TNGF可以使用与UE对应的根密钥和生成算法生成第一验证参数。生成算法可以叫做密钥导出函数(key derivation function,KDF),生成算法可以是基于散列信息认证码(hash-based message authentication code,HMAC)的方法,比如,散列信息认证码(hash-based message authentication code,HMAC)-安全散列算法(-secure hash algorithm,SHA)-256。本实施例不对具体的HMAC方法做限定。

[0147] 示例性地,TNGF可以根据与UE对应的根密钥生成中间密钥,使用中间密钥、TNGF的IP地址和第一新鲜性参数计算得到第一验证参数。或者,TNGF可以根据与UE对应的根密钥生成中间密钥,使用中间密钥和TNGF的标识计算得到第一验证参数。或者,TNGF可以根据与UE对应的根密钥生成中间密钥,使用中间密钥和TNGF生成的随机数,计算得到第一验证参数。

[0148] 需要说明的是,生成参数,如第一验证参数以及第一新鲜性参数可以携带在EAP认证成功消息中发送,在此情况下,可以不单独执行S305。UE可以根据携带第一验证参数以及第一新鲜性参数的EAP认证成功消息(EAP-success消息)对TNGF进行验证。

[0149] S306,TNAP#2向UE发送鉴权请求消息。相应地,UE接收来自TNAP#2的鉴权请求消息。

[0150] 示例性地,若S306鉴权请求消息封装在验证、授权和计费(authentication,authorization,accounting,AAA)消息中,则TNAP#2可以解封装AAA消息,得到鉴权请求消息,并可以将鉴权请求消息封装为层二(layer,L2)消息,再向UE发送封装有鉴权请求消息的L2消息。

[0151] S307,UE确定执行不完整的鉴权流程。

[0152] 关于不完整的鉴权流程,可以参考S301中的相关介绍,此处不再赘述。

[0153] UE确定执行不完整的鉴权流程有多种实现方式。以下结合情形2.1至情形2.3。

[0154] 情形2.1,在先执行S305-S306,再执行S307的情况下,当UE收到鉴权请求消息的时候,UE根据鉴权请求消息的内容确定执行不完整的鉴权流程。比如,UE在同一时刻只会与一个TNGF连接,因此当UE收到的一条来自于TNAP#2的消息时,并且该消息与鉴权相关(比如是EAP消息),则UE可以进一步根据消息中携带了鉴权参数,确定执行不完整的鉴权流程。

[0155] 情形2.2,先执行S307,再执行S304-S306的情况下,或者S307是S304中的一个步骤的情况下,在UE确定从TNAP#1移动到TNAP#2,且用于管理TNAP#1的TNGF和用于管理TNAP#2的TNGF相同的情况下,UE确定执行不完整的鉴权流程。比如,若UE根据TNAP的标识确定UE从

TNAP#1移动到了TNAP#2，又根据TNAP#2携带的TNGF信息确定TNGF用于管理TNAP#1的TNGF和用于管理TNAP#2TNGF相同，那么，UE确定执行不完整的鉴权流程。TNGF信息可以与TNGF标识相同，也可以不相同，本实施例不做具体限定。或者，当UE确定从TNAP#1移动到TNAP#2后，UE提供相同的realm或者服务器标识集(service set identifier，SSID)，使得TNAP#2选择到与TNAP#1相同的TNGF。比如，UE收到TNAP#2发送的EAP-REQ/Identity消息和TNGF信息。UE根据TNGF信息确定TNGF没有改变，则UE可以发送EAP-RES/Identity消息，并且在消息中携带UE的标识。此时，S304的第一请求消息为EAP-RES/Identity消息。

[0156] 情形2.3，UE收到来自于TNGF的消息，并根据该消息确定执行不完整鉴权流程。比如，UE可以根据该消息的消息名称确定执行不完整鉴权流程。此时，消息名称具有指示作用，UE根据不同的消息名称，便可以确定流程。例如，UE中存储有消息名称和流程之间的第二对应关系，UE根据不同的消息名称和第二对应关系便可以确定流程。也就是说，可以按照隐式的方式确定是否执行不完整鉴权流程，或者说根据提前规定好的与消息对应执行方式确定是否执行不完整鉴权流程。再比如，UE可以根据该来自于TNGF的消息中携带的参数的情况，如是否携带指示信息，或者具有指示作用的其他参数，确定执行不完整鉴权流程。在该来自于TNGF的消息中携带了指示信息，或者具有指示作用的参数的情况下，UE可以确定执行不完整的鉴权流程。

[0157] 其中，来自于TNGF的消息可以是EAP-REQ/Restart消息，或者EAP-REQ/5G-Restart消息，或者EAP-REQ/5G-NAS消息，或者EAP-RES/5G/Notification消息，或者EAP-REQ/5G-AN消息，或者EAP-REQ/5G-ReAUTH消息，或者EAP-REQ/ReAUTH消息等。本实施例不对消息名称做具体限定。

[0158] 在UE接收到来自TNAP#2的鉴权请求消息的情况下，本申请实施例提供的鉴权方法包括步骤1a。

[0159] 步骤1a，UE可以验证第一验证参数是否正确，即验证第四验证参数与第一验证参数是否匹配。或者说，UE验证TNGF的真实性。具体地，由于UE已经通过TNAP#1与TNGF建立过连接，因此，UE中存储有与TNGF对应的根密钥(也可以称为UE与TNGF之间的根密钥)，与TNGF对应的根密钥与前述与UE对应的根密钥相同。UE可以通过收到的TNGF的信息，或者TNGF标识，或者根据消息来源(比如，UE在同一时刻只会与一个TNGF连接，因此当UE收到的一条消息来自于TNAP#2时)，确定与TNGF对应的根密钥。再根据与TNGF对应的根密钥，生成第四验证参数。关于生成第四验证参数的原理与生成第一验证参数的原理类似，此处不再赘述。之后，UE将第一验证参数与第四验证参数进行对比，如果第一验证参数与第四验证参数相同，则表明第一验证参数与第四验证参数是匹配的，即表明对TNGF的鉴权成功。在第一验证参数与第四验证参数相匹配的情况下，UE使用第二新鲜性参数生成第二验证参数。关于使用第二新鲜性参数生成第二验证参数的原理可以参考S305中生成第一验证参数的原理，此处不再赘述。

[0160] 示例性地，UE根据与TNGF对应的根密钥和TNGF的IP地址，第一新鲜度参数计算得到第四验证参数，并将第四验证参数与第一验证参数进行对比。或者，UE根据与TNGF对应的根密钥和TNGF的身份标识计算得到第四验证参数。并将第四验证参数与第一验证参数进行对比。或者，TNGF根据与TNGF对应的根密钥和TNGF生成的随机数，计算得到第四验证参数，并将第四验证参数与第一验证参数进行对比。或者，TNGF根据与TNGF对应的根密钥生成中

间密钥，如使用K_{TNGF}'、TNGF的IP地址，以及第一新鲜性参数计算得到第四验证参数，并将第四验证参数与第一验证参数进行对比。或者，TNGF根据与TNGF对应的根密钥生成中间密钥，使用中间密钥和TNGF的身份标识计算得到第四验证参数，并将第四验证参数与第一验证参数进行对比。或者，TNGF根据与TNGF对应的根密钥生成中间密钥，使用中间密钥和TNGF生成的随机数，计算得到第四验证参数，并将第四验证参数与第一验证参数进行对比。

[0161] S308，UE向TNAP#2发送鉴权响应消息。相应地，TNAP#2接收来自UE的鉴权响应消息。

[0162] 其中，鉴权响应消息包括第二验证参数以及第二新鲜性参数。可选地，鉴权响应消息还可以包括UE的标识。

[0163] S308可以发生在S305-S306之前，也可以发生在S305-S306之后。以下结合情形3.1和情形3.2说明。

[0164] 情形3.1，若S308之前执行步骤5a，S308发生在S305-S306之后。

[0165] 在此情况下，在S308可以包括：在本申请实施例提供的鉴权方法包括步骤1a，且第一验证参数验证正确的情况后，执行S308。

[0166] 在这种情况下，鉴权响应消息为EAP-RES/Restart消息，或者EAP-RES/5G-Restart消息，或者EAP-RES/5G-NAS消息，或者EAP-RES/5G/Notification消息，或者EAP-RESXU/5G-AN消息，或者EAP-REQ/5G-ReAUTH消息，或者EAP-REQ/ReAUTH消息等。本实施例不对消息名称做具体限定。

[0167] 情形3.2，S308发生在S305-S306之前。鉴权响应消息可以是EAP-RES/Restart消息，或者EAP-RES/5G-Restart消息，或者EAP-RES/5G-NAS消息，或者EAP-RES/5G-Notification消息(EAP-5G通知请求消息)，或者EAP-RES/5G-AN消息，或者EAP-REQ/5G-ReAUTH消息，或者EAP-REQ/ReAUTH消息，或者只携带接入网参数的EAP-5G消息等。本实施例不对消息名称做具体限定。

[0168] 可以理解，在S308之前，本申请实施例所提供的方法还可以包括步骤2a。

[0169] 步骤2a，UE生成第二新鲜性参数和第二验证参数。示例性地，UE可以生成第二新鲜性参数，并根据第二新鲜性参数和与TNGF对应的根密钥生成第二验证参数，或者根据第二新鲜性参数生成第二验证参数。其中，第二新鲜性参数是TNGF生成的随机数、或者计数器值，本实施例不做具体限定。

[0170] S309，TNAP#2向TNGF发送鉴权响应消息。相应地，TNGF接收来自TNAP#2的鉴权响应消息。

[0171] TNAP#2可以对鉴权响应消息做透传，此处对TNAP#2发送鉴权响应消息的方式不作限定。

[0172] S310，TNGF验证UE的真实性。

[0173] 示例性地，S310可以包括：TNGF使用第二新鲜性参数生成第三验证参数。生成第三验证参数的原理可以参考S305中生成第一验证参数的相关介绍。TNGF将第三验证参数与第二验证参数进行对比，如果第三验证参数与第二验证参数相同，则表明第三验证参数与第二验证参数是匹配的，即表明对UE的鉴权成功。

[0174] 需要说明的是，本申请实施例中，上述S304到S310有多种不同的可能的执行顺序，步骤的执行顺序可以根据具体情况对应。

[0175] 在一种可能的实现方式中，可以按照S304到S310的顺序依次执行。

[0176] 在另一种可能的实现方式中，执行顺序为S304，S307，S308，S309，S305-S306，最后再执行S310。需要说明的是，此时S308中不同情形的步骤可以被插入到了不同的位置执行。在此情况下，在S308之前，TNGF还可以向UE发送与鉴权请求消息类型相同的信息，如下述图7所示的鉴权请求消息#1。在S306之后，UE还可以通过TNAP向TNGF发送与鉴权响应消息类型相同的信息。

[0177] 在又一种可能的实现方式中，执行顺序为S307，S304，S308，S309，S305-S306，最后S310。

[0178] 可理解，

[0179] 在对TNGF的鉴权成功的情况下，可以继续执行S311。

[0180] S311，TNGF生成目标密钥。

[0181] 其中，目标密钥用于保护UE与TNAP#2之间通信安全，或者说用于UE与TNAP#2，即目标密钥之间建立安全连接。

[0182] 一种可能的设计方案中，S311可以包括：TNGF可以根据与UE对应的根密钥直接生成目标密钥。在此情况下，TNGF可以按照以下方式一或方式二生成目标密钥。

[0183] 方式一，TNGF根据与UE对应的根密钥生成中间密钥，再根据中间密钥生成目标密钥。如下步骤6a和步骤7a。

[0184] 步骤6a，TNGF根据与UE对应的根密钥和第一类型识别码(usage type distinguisher)生成中间密钥。

[0185] 步骤7a，TNGF根据中间密钥和第二类型识别码生成目标密钥。

[0186] 其中，第二类型识别码与第一类型识别码不同。

[0187] 示例性地，如图4所示，TNGF可以将与UE对应的根密钥和第一类型识别码输入密钥生成函数(key derivation function，KDF)，如此便可以得到中间密钥。将中间密钥和第二类型识别码输入密钥生成函数，便可以得到目标密钥。其中，第一类型识别码用于标识生成密钥的类型，如中间密钥。示例性地，第一类型识别码可以是0x03。第二类型识别码用于标识生成密钥的类型，如目标密钥。第二类型识别码可以是0x02。

[0188] 可理解，密钥生成函数的输入参数还可以包括固定码，如0x84。

[0189] 可理解，在S311包括步骤6a和步骤7a的情况下，步骤S304至S309中的一个或多个步骤的执行顺序还可以位于步骤6a和步骤7a之间。关于S304至S310，以及S311与步骤6a和步骤7a之间的顺序，不作限定。一种可能的设计方案中，步骤7a可以在TNGF确定与UE对应的根密钥之后执行。

[0190] 方式二：与UE对应的根密钥和计数参数结合生成目标密钥。

[0191] TNGF根据与UE对应的根密钥、第三类型识别码和计数参数确定目标密钥。其中，计数参数可以是计数器的计数值，该计数值可以根据UE切换TNAP的次数确定，如计数值为UE切换TNAP的次数。

[0192] 示例性地，如图5所示，TNGF可以将中间密钥和第三类型识别码和计数参数输入密钥生成函数，如此便可以得到密钥目标密钥。

[0193] 可理解，密钥生成函数的输入参数还可以包括固定码，如0x84。

[0194] 例如，第二类型识别码为0x02。

[0195] 可理解，S311中的密钥生成函数沿用TS33.501 A22中定义的密钥生成函数，此处不再赘述。

[0196] 另一种可能的设计方案中，TNGF根据与UE对应的根密钥生成目标密钥，可以包括：TNGF根据与UE对应的根密钥和第一新鲜性参数、第二新鲜性参数成中间密钥；TNGF根据中间密钥和第二类型识别码生成目标密钥；其中，第二类型识别码与第一类型识别码不同。比如，第二类型识别码取值为0x02。

[0197] 再一种可能的设计方案中，S311，TNGF根据与UE对应的根密钥生成目标密钥，可以包括：TNGF根据与UE对应的根密钥，如K_{TNGF}和第一新鲜性参数、第二新鲜性参数成目标密钥。

[0198] 可理解，在一些可能的实施例中，S311可以在S301至S304之后，以及S305之前执行。

[0199] S312，TNGF向TNAP#2发送EAP认证成功消息(EAP-Success消息)和目标密钥。

[0200] 关于认证成功消息的实现原理可以参考TS 33.501版本17.7.0中章节7.2A.1中的相关介绍。关于S312的实现原理可以参考TS 33.501版本17.7.0中章节7.2A.1中的相关介绍，此处不再赘述。

[0201] S313，TNAP#2向UE发送EAP认证成功消息。相应地，UE接收来自TNAP#2的认证成功消息。

[0202] 一种可能的设计方案中，在S313之前，还包括：在TNAP#2收到EAP认证成功消息和目标密钥后，可以存储目标密钥，再向UE发送EAP认证成功消息。

[0203] 关于S314的实现原理可以参考TS 33.501版本17.7.0中章节7.2A.1中的相关介绍。

[0204] S314，UE生成目标密钥。

[0205] UE生成目标密钥的方法可以参考S311中的相关介绍，此处不再赘述。

[0206] S315，UE与TNAP#2使用目标密钥建立安全连接。

[0207] 关于S315的实现原理可以参考TS 33.501版本17.7.0中章节7.2A.1中的步骤12的相关介绍。

[0208] IP配置信息用于指示TNGF与UE通信的IP地址。

[0209] 关于S316的实现原理可以参考TS 33.501版本17.7.0中章节7.2A.1中的步骤12。

[0210] S317，UE完成后续注册流程。

[0211] 关于S317的实现原理可以参考TS 33.501版本17.7.0中章节7.2A.1中的步骤13-19。

[0212] 为便于理解，以下结合具体场景说明本申请实施例的鉴权方法的流程。

[0213] 可理解，本申请实施例中，在不同的场景下，图3中的S304与S315之间的步骤还可以存在其他执行顺序，此处不再赘述。

[0214] 场景1：

[0215] 图6为本申请实施例提供的鉴权方法的流程示意图二，该鉴权方法主要适用于UE在同一TNGF下切换TNAP的情况下，UE和TNGF侧均执行鉴权流程，并在验证通过的情况下，生成目标密钥。以下结合UE从TNAP#1和TNAP#2说明图6所示鉴权方法的通信流程。

[0216] S601，UE连接TNAP#1，以通过TNAP#1开始执行可信非3GPP注册、鉴权和PDU会话建

立流程。

[0217] 其中,S301交互的信息中,可以包括UE的标识。关于UE的标识的实现原理,可以参考S301中的相关介绍,此处不再赘述。

[0218] 关于S601的具体实现可以参考上述S301,此处不再赘述。

[0219] 需要说明的是,步骤S601中分为多个子步骤,在不同的子步骤中携带了不同的UE标识。比如,在其中的一步中,UE通过TNAP#1发送EAP-REQ/Identity消息给TNGF,该消息中携带一个NAI格式的UE的标识。在另一个步骤中,UE通过TNAP#1向发送EAP-5G/NAS消息,消息中携带AN parameter,AN parameter携带了UE的标识为5G-GUTI或者SUCI。

[0220] S602,AMF向TNGF发送根密钥。相应地,TNGF接收来自AMF的根密钥。

[0221] 关于S602的具体实现原理可以参考S302中的相关介绍,此处不再赘述。

[0222] S603,UE完成注册、完整的鉴权流程和PDU会话建立流程。

[0223] 具体实现原理可以参考上述S303中的相关介绍,此处不再赘述,此处不再赘述。

[0224] S604,UE连接TNAP#2。

[0225] 关于S303具体实现原理可以参考协议版本TS 33.501版本17.7.0中的7A.2.1中定义的流程,此处不再赘述。

[0226] S605,TNAP#2向UE发送EAP响应消息。相应地,UE接收来自TNAP#2的EAP响应消息。

[0227] EAP响应消息由TNAP#2生成,比如是EAP-RES/Identity消息。EAP响应消息用于向UE请求UE的标识。

[0228] S606,UE确定执行不完整的鉴权流程。

[0229] 关于S606的实现原理可以参考上述S307中的情形2.2或情形2.3的相关介绍,此处不再赘述。

[0230] S607,UE向TNAP#2发送第一请求消息。相应地,TNAP#2接收来自UE的第一请求消息。

[0231] 其中,第一请求消息中,可以包括UE的标识。

[0232] 第一请求消息可以是EAP-REQ/Identity消息。该消息可以包括UE在步骤S601中发送的至少一种UE的标识。

[0233] 关于S607的实现原理可以参考上述S304中情形1.2的相关介绍,此处不再赘述。

[0234] S608,TNAP#2向TNGF发送第一请求消息。相应地,TNGF接收来自TNAP#2的第一请求消息。

[0235] TNGF接收到第一请求消息后,TNGF根据第一请求消息确定触发不完整的鉴权流程。

[0236] 关于TNGF根据第一请求消息确定触发不完整的鉴权流程的实现原理,可以参考S305中的相关介绍,此处不再赘述。

[0237] S609,TNGF根据一请求消息中UE的标识确定与UE对应的根密钥。

[0238] 关于S609的实现原理,可以参考S305中的TNGF根据第一请求消息中的UE的标识,确定与UE对应的根密钥的相关介绍,此处不再赘述。

[0239] S610,TNGF根据与UE对应的根密钥生成第一新鲜性参数和第一验证参数。

[0240] 关于S610的实现原理,可以参考S305中的方式1和方式2的相关介绍,此处不再赘述。

[0241] S611,响应于第一请求消息,TNGF通过向TNAP#2发送鉴权请求消息。相应地,TNAP#2接收来自TNGF的鉴权请求消息。

[0242] 关于S611的实现原理,可以参考S305中的相关介绍,此处不再赘述。可选地,该消息中携带TNGF的标识。具体地,如果在步骤S604中没有携带TNGF的标识,则一种情况是鉴权请求消息中携带TNGF的标识,以确保UE可以找到与TNGF对应的根密钥;另一种情况是:如果该UE在某一个时刻只会与一个TNGF连接,那么TNGF的标识可以不携带。此时,UE可以根据的鉴权响应消息的来源确定是否进行非3GPP接入。若鉴权响应消息来自于TNAP#2,则UE可以确定是进行非3GPP接入,因此就可以找到所有非3GPP接入的安全上下文,即可以确定出与TNGF对应的根密钥。

[0243] S612,TNAP#2向UE发送鉴权请求消息。相应地,UE接收来自TNAP#2的鉴权请求消息。

[0244] 关于S612的实现原理,可以参考S306中的相关介绍,此处不再赘述。

[0245] S613,UE生成目标密钥。

[0246] 关于S613的实现原理,可以参考S314中的相关介绍,此处不再赘述。

[0247] S614,UE通过向TNAP#2发送鉴权响应消息。相应地,TNAP#2接收来自UE的鉴权响应消息。

[0248] 关于S614的实现原理,可以参考S308中的相关介绍,此处不再赘述。

[0249] S615,TNAP#2向TNGF发送鉴权响应消息。相应地,TNGF接收来自TNAP#2的鉴权响应消息。

[0250] 关于S615的实现原理,可以参考S309中的相关介绍,此处不再赘述。

[0251] S616,TNGF生成目标密钥。

[0252] 关于S616的实现原理,可以参考S311中的相关介绍,此处不再赘述。

[0253] S617,TNGF向TNAP#2发送EAP认证成功消息(EAP-Success消息)和目标密钥。

[0254] 关于S617的实现原理,可以参考S312中的相关介绍,此处不再赘述。

[0255] S618,TNAP#2向UE发送EAP认证成功消息。相应地,UE接收来自TNAP#2的认证成功消息。

[0256] 关于S618的实现原理,可以参考S313中的相关介绍,此处不再赘述。

[0257] S619,UE与TNAP#2使用目标密钥建立安全连接。

[0258] 关于S619的实现原理,可以参考S315中的相关介绍,此处不再赘述。

[0259] S620,UE接收来自TNGF的IP配置信息。相应地,UE接收来自TNGF的IP配置信息。

[0260] IP配置信息用于指示TNGF与UE通信的IP地址。

[0261] 关于S620的实现原理,可以参考S316中的相关介绍,此处不再赘述。

[0262] S621,UE完成后续注册流程。

[0263] 关于S621的实现原理,可以参考S317中的相关介绍,此处不再赘述。

[0264] 场景2:

[0265] 图7为本申请实施例提供的鉴权方法的流程示意图二,该鉴权方法主要适用于UE在同一TNGF下切换TNAP的情况下,在TNGF侧和UE侧均进行鉴权,且在UE和TNGF的鉴权流程完成后,UE和TNGF再生成目标密钥。以下结合UE从TNAP#1和TNAP#2说明图7所示鉴权方法的通信流程。

[0266] S701,UE连接TNAP#1,以通过TNAP#1开始执行可信非3GPP注册、鉴权和PDU会话建立流程。

[0267] 关于S701的实现原理,可以参考S301中的相关介绍,此处不再赘述。

[0268] S702,AMF向TNGF发送根密钥。相应地,TNGF接收来自AMF的根密钥。

[0269] 关于S702的实现原理,可以参考S302中的相关介绍,此处不再赘述。

[0270] S703,UE完成注册、完整的鉴权流程和PDU会话建立流程。

[0271] 关于S703的实现原理,可以参考S303中的相关介绍,此处不再赘述。

[0272] S704,TNGF通过TNAP#2接收第一请求消息。

[0273] 关于S704的实现原理,可以参考S304中情形2.2的相关介绍,此处不再赘述。

[0274] S705,UE确定执行不完整的鉴权流程。

[0275] 关于S705的实现原理,可以参考S307中的相关介绍,此处不再赘述。

[0276] S706,UE通过向TNAP#2发送鉴权响应消息#1。相应地,TNAP#2接收来自UE的鉴权响应消息#1。

[0277] 其中,鉴权响应消息#1包括第二验证参数以及第二新鲜性参数。

[0278] 可选地,鉴权响应消息#1还可以包括UE的标识。

[0279] 关于S706的实现原理,可以参考S308中情形3.2的相关介绍,此处不再赘述。

[0280] 可理解,在发送鉴权请求消息#1之前,UE还可以通过TNAP#2向TNGF发送鉴权请求消息#1。该鉴权请求消息#1用于将UE的标识发送给TNGF。鉴权响应消息#1可以是只包含AN parameter的EAP-RES/5G-NAS消息,或者鉴权响应消息#1可以是EAP-RES/Identity消息。

[0281] S707,TNAP#2向TNGF发送鉴权响应消息#1。相应地,TNGF接收来自TNAP#2的鉴权响应消息#1。

[0282] 鉴权响应消息#1可以参考图3中的鉴权响应消息的相关介绍,关于S707的实现原理,可以参考S309中的相关介绍,此处不再赘述。

[0283] S708,TNGF验证UE的真实性。

[0284] 关于S708的实现原理,可以参考S310中的相关介绍,此处不再赘述。

[0285] S709,TNGF向TNAP#2发送鉴权请求消息#2。相应地,TNAP#2接收来自TNGF的鉴权请求消息#2。

[0286] 关于鉴权请求消息#2的实现原理可以参考S305中鉴权请求消息的相关介绍,关于S708的实现原理,可以参考S305中的相关介绍,此处不再赘述。

[0287] S710,TNAP#2向UE发送鉴权请求消息#2。相应地,UE接收来自TNAP#2的鉴权请求消息#2。

[0288] 关于S710的实现原理,可以参考S306中的相关介绍,此处不再赘述。

[0289] S711,UE验证TNGF的真实性。

[0290] 关于S711的实现原理,可以参考S308情形3.1中的相关介绍,此处不再赘述。

[0291] S712,UE通过向TNAP#2发送鉴权响应消息#2。相应地,TNAP#2接收来自UE的鉴权响应消息#2。

[0292] 鉴权响应消息#2用于指示TNGF发送认证成功消息,如EAP认证响应消息。可选地,鉴权响应消息中携带有用于指示UE对TNGF认证成功的指示信息。鉴权响应消息#2可以是EAP-RES/ReAUTH消息,或者EAP-RES/5G-NAS/ReAUTH消息。鉴权响应消息#2与鉴权请求消

息#2对应。其中，鉴权响应消息#2可以是EAP-RES/ReAUTH消息，或者EAP-RES/5G-NAS/ReAUTH消息。

[0293] S713，TNAP#2向TNGF发送鉴权响应消息#2。相应地，TNGF接收来自TNAP#2的鉴权响应消息#2。

[0294] S714，TNGF生成目标密钥。

[0295] 关于S714的实现原理，可以参考S311中的相关介绍，此处不再赘述。

[0296] 可选地，TNGF根据步骤S712和S713消息中携带的指示信息确定UE对TNGF认证成功，则生成目标密钥。

[0297] S715，TNGF向TNAP#2发送EAP认证成功消息和目标密钥。

[0298] 关于S715的实现原理，可以参考S312中的相关介绍，此处不再赘述。

[0299] S716，TNAP#2向UE发送EAP认证成功消息。相应地，UE接收来自TNAP#2的认证成功消息。

[0300] 关于S716的实现原理，可以参考S313中的相关介绍，此处不再赘述。

[0301] S717，UE生成目标密钥。

[0302] 关于S717的实现原理，可以参考S314中的相关介绍，此处不再赘述。

[0303] S718，UE与TNAP#2使用目标密钥建立安全连接。

[0304] 关于S718的实现原理，可以参考S315中的相关介绍，此处不再赘述。

[0305] S719，UE接收来自TNGF的IP配置信息。相应地，UE接收来自TNGF的IP配置信息。

[0306] 关于S719的实现原理，可以参考S316中的相关介绍，此处不再赘述。

[0307] S720，UE完成后续注册流程。

[0308] 关于S720的实现原理，可以参考S317中的相关介绍，此处不再赘述。

[0309] 场景3

[0310] 图8为本申请实施例提供的鉴权方法的流程示意图四，该鉴权方法主要适用于UE在同一TNGF下切换TNAP的情况下，在TNGF侧对UE进行鉴权，TNGF对UE进行鉴权后，与UE进行信息交互后，UE再生成密钥。以下结合UE从TNAP#1和TNAP#2说明图6所示鉴权方法的通信流程。

[0311] S801，UE连接TNAP#1，以通过TNAP#1开始执行可信非3GPP注册、鉴权和PDU会话建立流程。

[0312] 关于S801的实现原理，可以参考S301中的相关介绍，此处不再赘述。

[0313] S802，AMF向TNGF发送根密钥。相应地，TNGF接收来自AMF的根密钥。

[0314] 关于S802的实现原理，可以参考S302中的相关介绍，此处不再赘述。

[0315] S803，UE完成注册、完整的鉴权流程和PDU会话建立流程。

[0316] 关于S803的实现原理，可以参考S303中的相关介绍，此处不再赘述。

[0317] S804，TNGF通过TNAP#2接收第一请求消息。

[0318] 关于S804的实现原理，可以参考S304中的相关介绍，此处不再赘述。

[0319] S805，响应于第一请求消息，TNGF向TNAP#2发送鉴权请求消息。相应地，TNAP#2接收来自TNGF的鉴权请求消息。

[0320] 关于S805的实现原理，可以参考S305中的相关介绍，此处不再赘述。

[0321] S806，TNAP#2向UE发送鉴权请求消息。相应地，UE接收来自TNAP#2的鉴权请求消

息。

[0322] 关于S806的实现原理,可以参考S306中的相关介绍,此处不再赘述。

[0323] S807,UE确定执行不完整的鉴权流程。

[0324] 关于S807的实现原理,可以参考S307中的相关介绍,此处不再赘述。

[0325] S808,UE向TNAP#2发送鉴权响应消息。相应地,TNAP#2接收来自UE的鉴权响应消息。

[0326] 关于S808的实现原理,可以参考S308中的相关介绍,此处不再赘述。

[0327] S809,TNAP#2向TNGF发送鉴权响应消息。相应地,TNGF接收来自TNAP#2的鉴权响应消息。

[0328] 关于S809的实现原理,可以参考S309中的相关介绍,此处不再赘述。

[0329] S810,TNGF验证UE的真实性。

[0330] 关于S810的实现原理,可以参考S310中的相关介绍,此处不再赘述。

[0331] S811,TNGF生成目标密钥。

[0332] 关于S811的实现原理,可以参考S311中的相关介绍,此处不再赘述。可理解,在S311包括步骤8a和步骤7a的情况下,步骤6a和步骤7a依次执行,且步骤6a可以在S810之后,步骤7a可以在S812之前。

[0333] S812,TNGF向TNAP#2发送EAP认证成功消息和目标密钥。

[0334] 关于S812的实现原理,可以参考S312中的相关介绍,此处不再赘述。

[0335] S813,TNAP#2向UE发送EAP认证成功消息。相应地,UE接收来自TNAP#2的认证成功消息。

[0336] 关于S813的实现原理,可以参考S313中的相关介绍,此处不再赘述。

[0337] S814,UE生成目标密钥。

[0338] 关于S814的实现原理,可以参考S314中的相关介绍,此处不再赘述。

[0339] S815,UE与TNAP#2使用目标密钥建立安全连接。

[0340] 关于S815的实现原理,可以参考S315中的相关介绍,此处不再赘述。

[0341] S816,UE接收来自TNGF的IP配置信息。相应地,UE接收来自TNGF的IP配置信息。

[0342] 关于S816的实现原理,可以参考S316中的相关介绍,此处不再赘述。

[0343] S817,UE完成后续注册流程。

[0344] 关于S817的实现原理,可以参考S317中的相关介绍,此处不再赘述。

[0345] 基于上述图3、图6、图7中任一所提供的通鉴权法,在UE从源TNAP切换至目标TNAP的情况下,TNGF可以根据存储的根密钥生成中间密钥,并生成针对目标TNAP的目标密钥,以及将目标密钥发送给目标TNAP,以用于UE与TNAP之间的安全通信。如此,在切换TNAP的情况下,根据TNGF存储的根密钥生成目标密钥,可以避免执行完整的认证流程,即能够简化交互流程,从而提高通信效率和可靠性。

[0346] 以上结合图3-图8详细说明了本申请实施例提供的鉴权方法。以下结合图9-图10详细说明用于执行本申请实施例提供的鉴权方法的通信装置。

[0347] 示例性地,图9是本申请实施例提供的通信装置900的结构示意图一。如图9所示,通信装置900包括:处理模块901和收发模块902。为了便于说明,图9仅示出了该通信装置900的主要部件。

[0348] 一些实施例中，通信装置900可适用于图2中所示出的通信系统中，执行图3、图6、图7或图9中任一所示出的鉴权方法中TNGF的功能。

[0349] 处理模块901，用于在用户设备UE从源可信的非第三代合作伙伴计划3GPP接入点TNAP移动到目标TNAP的情况下，根据存储的与UE对应的根密钥生成中间密钥，并使用中间密钥，生成针对目标TNAP的目标密钥。

[0350] 收发模块902，用于将目标密钥发送给目标TNAP。

[0351] 其中，目标密钥用于保护UE与目标TNAP之间通信安全。

[0352] 一种可能的设计方案中，处理模块901，具体用于根据第一类型识别码以及根密钥生成中间密钥。其中第一类型识别码用于标识生成中间密钥。

[0353] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP向UE发送鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。该第一验证参数由通信装置900根据中间密钥和第一新鲜性参数生成。收发模块902，还用于接收来自UE的鉴权响应消息。其中，鉴权响应消息包括第二验证参数以及第二新鲜性参数。处理模块901，还用于根据中间密钥和第二新鲜性参数，得到第三验证参数。处理模块901，具体用于在第三验证参数与第二验证参数匹配的情况下，通信装置900使用中间密钥，生成针对目标TNAP的目标密钥。

[0354] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP向UE发送鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由通信装置900根据根密钥和第一新鲜性参数生成。收发模块902，还用于接收来自UE的鉴权响应消息。其中，鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。处理模块901，还用于根据根密钥和第二新鲜性参数，得到第三验证参数。处理模块901，具体用于在第三验证参数与第二验证参数匹配的情况下，使用中间密钥，生成针对目标TNAP的目标密钥。

[0355] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP向UE发送鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由通信装置900根据中间密钥和第一新鲜性参数生成。收发模块902，还用于接收来自UE的鉴权响应消息，其中，鉴权响应消息包括第二验证参数以及第二新鲜性参数。通信装置900根据中间密钥和第二新鲜性参数，得到第三验证参数。通信装置900将目标密钥发送给目标TNAP，可以包括：在第三验证参数与第二验证参数匹配的情况下，通信装置900将目标密钥发送给目标TNAP。

[0356] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP向UE发送鉴权请求消息，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由通信装置900根据根密钥和第一新鲜性参数生成。收发模块902，还用于接收来自UE的鉴权响应消息。其中，鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。处理模块901，还用于根据根密钥和第二新鲜性参数，得到第三验证参数。收发模块902，具体用于在第三验证参数与第二验证参数匹配的情况下，将目标密钥发送给目标TNAP。

[0357] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP向UE发送鉴权请求消息#1；其中，鉴权请求消息#1中包括UE的标识，以及接收来自UE的鉴权响应消息#1。其中，鉴权响应消息#1可以包括第二验证参数以及第二新鲜性参数。处理模块901，还用于根据中间

密钥和第二新鲜性参数，得到第三验证参数。处理模块901，具体用于在第三验证参数与第二验证参数匹配的情况下，使用中间密钥，生成针对目标TNAP的目标密钥。收发模块902，还用于通过目标TNAP向UE发送鉴权请求消息#2，鉴权请求消息#2包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由通信装置900根据中间密钥和第一新鲜性参数生成。所述收发模块902，还用于通过目标TNAP接收来自UE的鉴权响应消息#2；鉴权响应消息#2用于指示TNGF发送认证成功消息。

[0358] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP向UE发送鉴权请求消息#1；其中，鉴权请求消息#1中包括UE的标识，以及接收来自UE的鉴权响应消息#1。其中，鉴权响应消息#1包括第二验证参数以及第二新鲜性参数。处理模块901，还用于根据根密钥和第二新鲜性参数，得到第三验证参数。处理模块901，具体用于在第三验证参数与第二验证参数匹配的情况下，使用中间密钥，生成针对目标TNAP的目标密钥。收发模块，还用于通过目标TNAP向UE发送鉴权请求消息#2。鉴权请求消息#2可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由通信装置900根据根密钥和第一新鲜性参数生成所述收发模块902，还用于通过目标TNAP接收来自UE的鉴权响应消息#2；鉴权响应消息#2用于指示TNGF发送认证成功消息。

[0359] 一种可能的设计方案中，处理模块901，具体用于根据第二类型识别码和中间密钥生成目标密钥。其中，第二类型识别码用于标识生成中间密钥。

[0360] 一种可能的设计方案中，收发模块902，还用于接收来自目标TNAP的第一请求消息。处理模块901，还用于响应于第一请求消息，确定需要执行通信装置900与UE之间的鉴权流程。

[0361] 可选地，第一请求消息可以包括UE的标识。处理模块901，具体用于第一请求消息中UE的标识和已经连接源TNAP的UE的标识相同。

[0362] 一种可能的设计方案中，处理模块901，还用于根据UE的标识，确定根密钥。

[0363] 可选地，收发模块902可以包括接收模块和发送模块(图9中未示出)。其中，收发模块902用于实现通信装置900的发送功能和接收功能。

[0364] 可选地，通信装置900还可以包括存储模块(图9中未示出)，该存储模块存储有程序或指令。当处理模块901执行该程序或指令时，使得通信装置900可以执行图3、图6、图7或图8中任一项所示出的鉴权方法中TNGF的功能。

[0365] 应理解，通信装置900中涉及的处理模块901可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块902可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

[0366] 需要说明的是，通信装置900可以是网络设备，如TNGF，也可以是可设置于网络设备中的芯片(系统)或其他部件或组件，还可以是包含网络设备的装置，本申请对此不做限定。

[0367] 此外，通信装置900的技术效果可以参考图3、图6、图7或图8中任一项所示出的鉴权方法的技术效果，此处不再赘述。

[0368] 另一些实施例中，通信装置900可适用于图2中所示出的通信系统中，执行图3、图6、图7或图8中任一所示出的鉴权方法中通信装置900的功能。该通信装置900可以应用于通信装置900从源可信的非第三代合作伙伴计划3GPP接入点TNAP移动到目标TNAP的场景。

[0369] 其中，处理模块901，用于根据自身与可信的非3GPP网关功能TNGF之间的根密钥，生成中间密钥。其中，TNGF为源TNAP和目标TNAP的管理网元，以及，处理模块901，用于使用中间密钥，生成针对目标TNAP的目标密钥。其中，目标密钥用于保护通信装置900与目标TNAP之间通信安全。

[0370] 一种可能的设计方案中，处理模块901，具体用于根据第一类型识别码以及根密钥生成中间密钥。其中，第一类型识别码用于标识生成中间密钥。

[0371] 一种可能的设计方案中，收发模块902，用于通过目标TNAP接收来自TNGF的鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据中间密钥和第一新鲜性参数生成。处理模块901，还用于使用中间密钥和第一新鲜性参数，得到第四验证参数。收发模块902，还用于在第四验证参数与第一验证参数匹配的情况下，向TNGF发送鉴权响应消息。其中，鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。

[0372] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP接收来自TNGF的鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。处理模块901，还用于使用根密钥和第一新鲜性参数，得到第四验证参数。收发模块902，还用于在第四验证参数与第一验证参数匹配的情况下，向TNGF发送鉴权响应消息。其中，鉴权响应消息可以包括第二验证参数以及第二新鲜性参数。

[0373] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP接收来自TNGF的鉴权请求消息。鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。处理模块901，还用于使用中间密钥和第一新鲜性参数，得到第四验证参数。处理模块901，具体用于在第四验证参数与第一验证参数匹配的情况下，根据该通信装置900与TNGF之间的根密钥，生成中间密钥。收发模块902，还可以用于向TNGF发送鉴权响应消息。其中，鉴权响应消息可以包括通信装置900的标识、第二验证参数以及第二新鲜性参数。

[0374] 一种可能的设计方案中，收发模块902，还用于通过目标TNAP接收来自TNGF的鉴权请求消息。其中，鉴权请求消息可以包括第一验证参数以及第一新鲜性参数。其中，第一验证参数由TNGF根据根密钥和第一新鲜性参数生成。处理模块901，用于使用根密钥和第一新鲜性参数，得到第四验证参数。处理模块901，具体用于在第四验证参数与第一验证参数匹配的情况下，根据自身与TNGF之间的根密钥，生成中间密钥。收发模块902，还用于向TNGF发送鉴权响应消息。其中，鉴权响应消息可以包括通信装置900的标识，第二验证参数以及第二新鲜性参数。

[0375] 一种可能的设计方案中，处理模块901，具体用于根据第二类型识别码和中间密钥生成目标密钥。其中，第二类型识别码用于标识生成中间密钥。

[0376] 可选地，收发模块902，还用于向目标TNAP发送第一请求消息。进一步地，第一请求消息可以包括通信装置900的标识。

[0377] 一种可能的设计方案中，处理模块901，还用于根据TNGF的标识，确定根密钥。

[0378] 可选地，收发模块902可以包括接收模块和发送模块(图9中未示出)。其中，收发模块902用于实现通信装置900的发送功能和接收功能。

[0379] 可选地,通信装置900还可以包括存储模块(图9中未示出),该存储模块存储有程序或指令。当处理模块901执行该程序或指令时,使得通信装置900可以执行图3、图6、图7或图8中任一项所示出的鉴权方法中TNGF的功能。

[0380] 应理解,通信装置900中涉及的处理模块901可以由处理器或处理器相关电路组件实现,可以为处理器或处理单元;收发模块902可以由收发器或收发器相关电路组件实现,可以为收发器或收发单元。

[0381] 需要说明的是,通信装置900可以是终端设备,也可以是可设置于终端设备中的芯片(系统)或其他部件或组件,还可以是包含终端设备的装置,本申请对此不做限定。

[0382] 此外,通信装置900的技术效果可以参考图3、图6、图7或图8中任一项所示出的鉴权方法的技术效果,此处不再赘述。

[0383] 示例性地,图10为本申请实施例提供的通信装置的结构示意图二。该通信装置可以是终端设备或网络设备,也可以是可设置于终端设备或网络设备的芯片(系统)或其他部件或组件。如图10所示,通信装置1000可以包括处理器1001。可选地,通信装置1000还可以包括存储器1002和/或收发器1003。其中,处理器1001与存储器1002和收发器1003耦合,如可以通过通信总线连接。

[0384] 下面结合图10对通信装置1000的各个构成部件进行具体的介绍:

[0385] 其中,处理器1001是通信装置1000的控制中心,可以是一个处理器,也可以是多个处理元件的统称。例如,处理器1001是一个或多个中央处理器(central processing unit,CPU),也可以是特定集成电路(application specific integrated circuit,ASIC),或者是被配置成实施本申请实施例的一个或多个集成电路,例如:一个或多个数字信号处理器(digital signal processor,DSP),或,一个或者多个现场可编程门阵列(field programmable gate array,FPGA)。

[0386] 可选地,处理器1001可以通过运行或执行存储在存储器1002内的软件程序,以及调用存储在存储器1002内的数据,执行通信装置1000的各种功能。

[0387] 在具体的实现中,作为一种实施例,处理器1001可以包括一个或多个CPU,例如图10中所示出的CPU0和CPU1。

[0388] 在具体实现中,作为一种实施例,通信装置1000也可以包括多个处理器,例如图10中所示的处理器1001和处理器1004。这些处理器中的每一个可以是一个单核处理器(single-CPU),也可以是一个多核处理器(multi-CPU)。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。

[0389] 其中,所述存储器1002用于存储执行本申请方案的软件程序,并由处理器1001来控制执行,具体实现方式可以参考上述方法实施例,此处不再赘述。

[0390] 可选地,存储器1002可以是只读存储器(read-only memory,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(random access memory,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(electrically erasable programmable read-only memory,EEPROM)、只读光盘(compact disc read-only memory,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1002可以和处理器1001集成在一起，也可以独立存在，并通过通信装置1000的接口电路(图10中未示出)与处理器1001耦合，本申请实施例对此不作具体限定。

[0391] 收发器1003，用于与其他通信装置之间的通信。例如，通信装置1000为终端设备，收发器1003可以用于与网络设备通信，或者与另一个终端设备通信。又例如，通信装置1000为网络设备，收发器1003可以用于与终端设备通信，或者与另一个网络设备通信。

[0392] 可选地，收发器1003可以包括接收器和发送器(图10中未单独示出)。其中，接收器用于实现接收功能，发送器用于实现发送功能。

[0393] 可选地，收发器1003可以和处理器1001集成在一起，也可以独立存在，并通过通信装置1000的接口电路(图10中未示出)与处理器1001耦合，本申请实施例对此不作具体限定。

[0394] 需要说明的是，图10中示出的通信装置1000的结构并不构成对该通信装置的限定，实际的通信装置可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0395] 此外，通信装置1000的技术效果可以参考上述方法实施例所述的鉴权方法的技术效果，此处不再赘述。

[0396] 应理解，在本申请实施例中的处理器可以是中央处理单元(central processing unit，CPU)，该处理器还可以是其他通用处理器、数字信号处理器(digital signal processor，DSP)、专用集成电路(application specific integrated circuit，ASIC)、现成可编程门阵列(field programmable gate array，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0397] 还应理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(read-only memory，ROM)、可编程只读存储器(programmable ROM，PROM)、可擦除可编程只读存储器(erasable PROM，EPROM)、电可擦除可编程只读存储器(electrically EPROM，EEPROM)或闪存。易失性存储器可以是随机存取存储器(random access memory，RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的随机存取存储器(random access memory，RAM)可用，例如静态随机存取存储器(static RAM，SRAM)、动态随机存取存储器(DRAM)、同步动态随机存取存储器(synchronous DRAM，SDRAM)、双倍数据速率同步动态随机存取存储器(double data rate SDRAM，DDR SDRAM)、增强型同步动态随机存取存储器(enhanced SDRAM，ESDRAM)、同步连接动态随机存取存储器(synchlink DRAM，SLDRAM)和直接内存总线随机存取存储器(direct rambus RAM，DR RAM)。

[0398] 上述实施例，可以全部或部分地通过软件、硬件(如电路)、固件或其他任意组合来实现。当使用软件实现时，上述实施例可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令或计算机程序。在计算机上加载或执行所述计算机指令或计算机程序时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以为通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中

心通过有线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集合的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质。半导体介质可以是固态硬盘。

[0399] 应理解,本文中术语“和/或”,仅仅是一种描述关联对象的关联关系,表示可以存在三种关系,例如,A和/或B,可以表示:单独存在A,同时存在A和B,单独存在B这三种情况,其中A,B可以是单数或者复数。另外,本文中字符“/”,一般表示前后关联对象是一种“或”的关系,但也可能表示的是一种“和/或”的关系,具体可参考前后文进行理解。

[0400] 本申请中,“至少一个”是指一个或者多个,“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达,是指的这些项中的任意组合,包括单项(个)或复数项(个)的任意组合。例如,a,b,或c中的至少一项(个),可以表示:a,b,c,a-b,a-c,b-c,或a-b-c,其中a,b,c可以是单个,也可以是多个。

[0401] 应理解,在本申请的各种实施例中,上述各过程的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不应对本申请实施例的实施过程构成任何限定。

[0402] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

[0403] 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统、装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0404] 在本申请所提供的几个实施例中,应该理解到,所揭露的系统、装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0405] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0406] 另外,在本申请各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。

[0407] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个

人计算机,服务器,或者网络设备等)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(read-only memory,ROM)、随机存取存储器(random access memory,RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0408] 以上所述,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。因此,本申请的保护范围应以所述权利要求的保护范围为准。

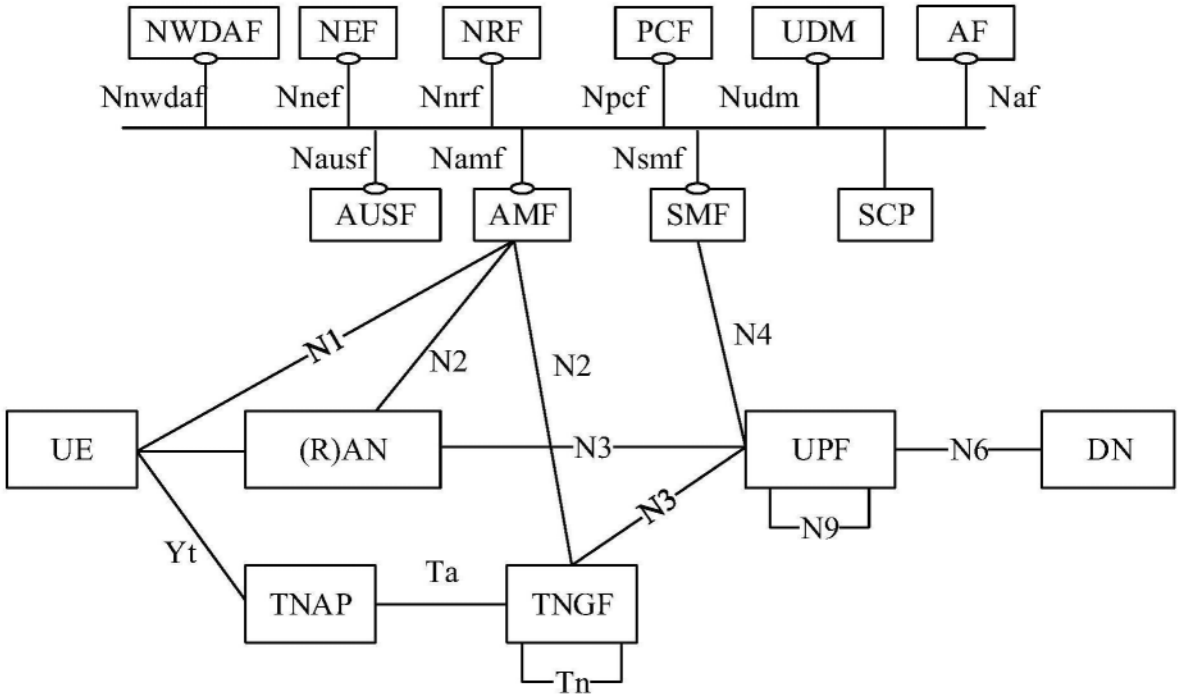

NWDAF
NEF
NRF
PCF
UDM
AF
Nnwdaf
Nnef
Nnrf
Npcf
Nudm
Naf
Nausf
Namf
Nsmf
AUSF
AMF
SMF
SCP
N1
N2
N2
N4
UE
(R)AN
N3
UPF
N6
DN
N3
N9
Yt
Ta
TNAP
TNGF
Tn

图1

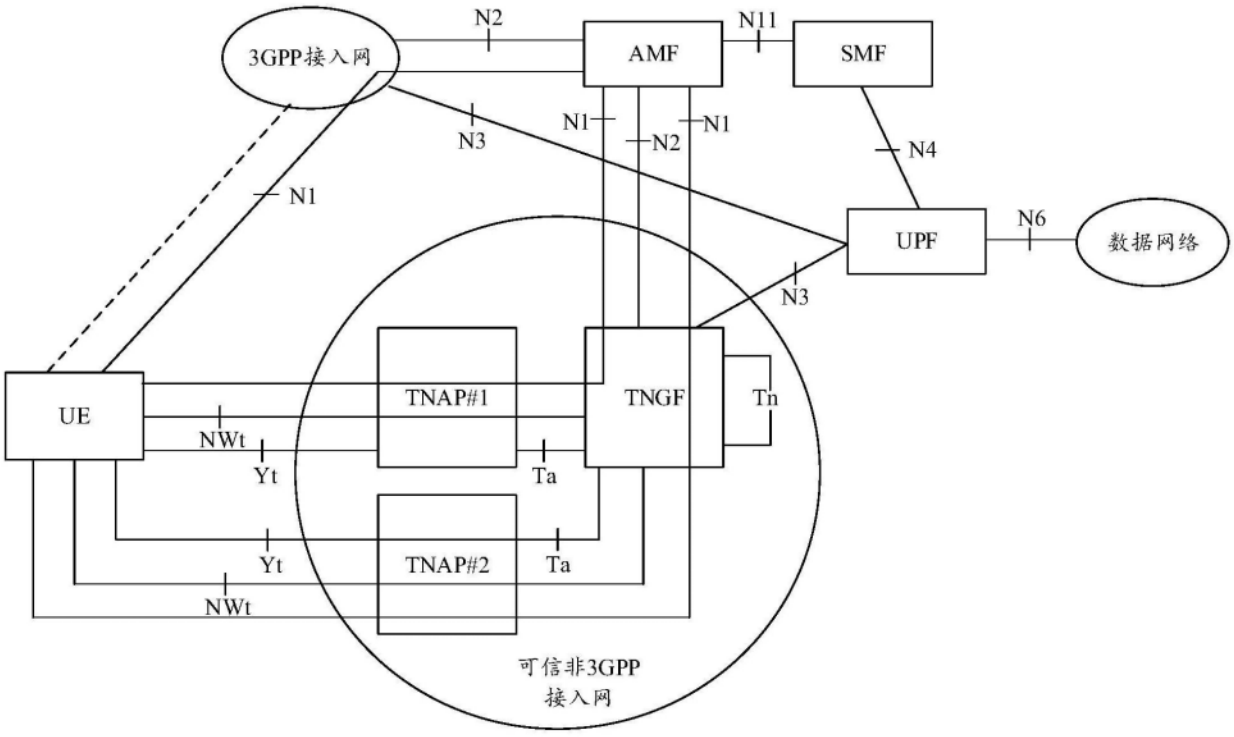

3GPP接入网
N2
AMF
N11
SMF
N3
N1
N2
N1
N4
N1
UPF
N6
数据网络
N3
UE
TNAP#1
TNGF
Tn
NWt
Yt
Ta
Yt
TNAP#2
Ta
NWt
可信非3GPP
接入网

图2

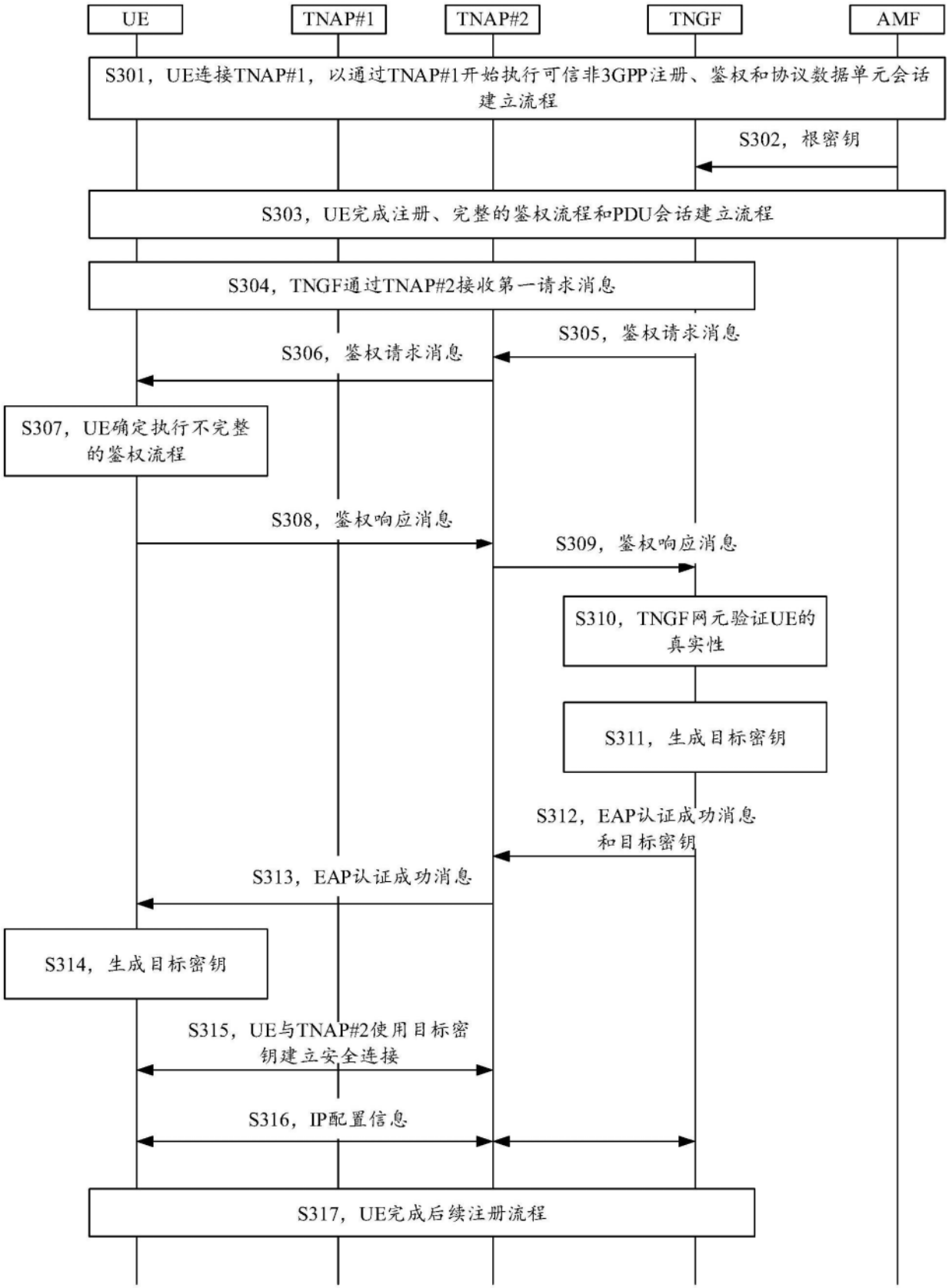

UE
TNAP#1
TNAP#2
TNGF
AMF
S301，UE连接TNAP#1，以通过TNAP#1开始执行可信非3GPP注册、鉴权和协议数据单元会话建立流程
S302，根密钥
S303，UE完成注册、完整的鉴权流程和PDU会话建立流程
S304，TNGF通过TNAP#2接收第一请求消息
S305，鉴权请求消息
S306，鉴权请求消息
S307，UE确定执行不完整的鉴权流程
S308，鉴权响应消息
S309，鉴权响应消息
S310，TNGF网元验证UE的真实性
S311，生成目标密钥
S312，EAP认证成功消息和目标密钥
S313，EAP认证成功消息
S314，生成目标密钥
S315，UE与TNAP#2使用目标密钥建立安全连接
S316，IP配置信息
S317，UE完成后续注册流程

图3

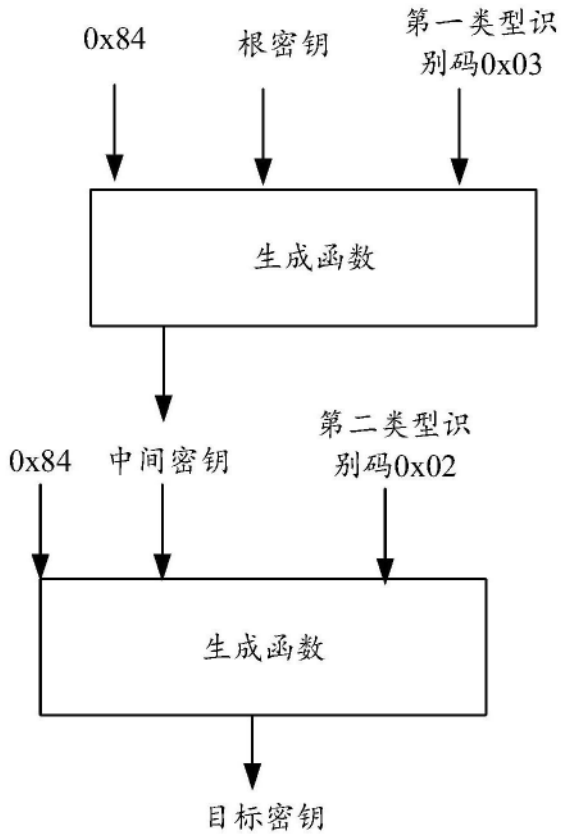

0x84
根密钥
第一类型识别码0x03
生成函数
0x84
中间密钥
第二类型识别码0x02
生成函数
目标密钥

图4

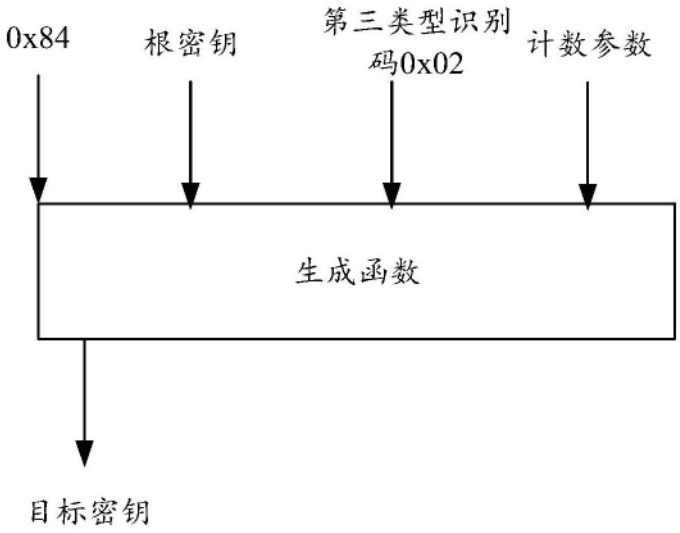

0x84
根密钥
第三类型识别码0x02
计数参数
生成函数
目标密钥

图5

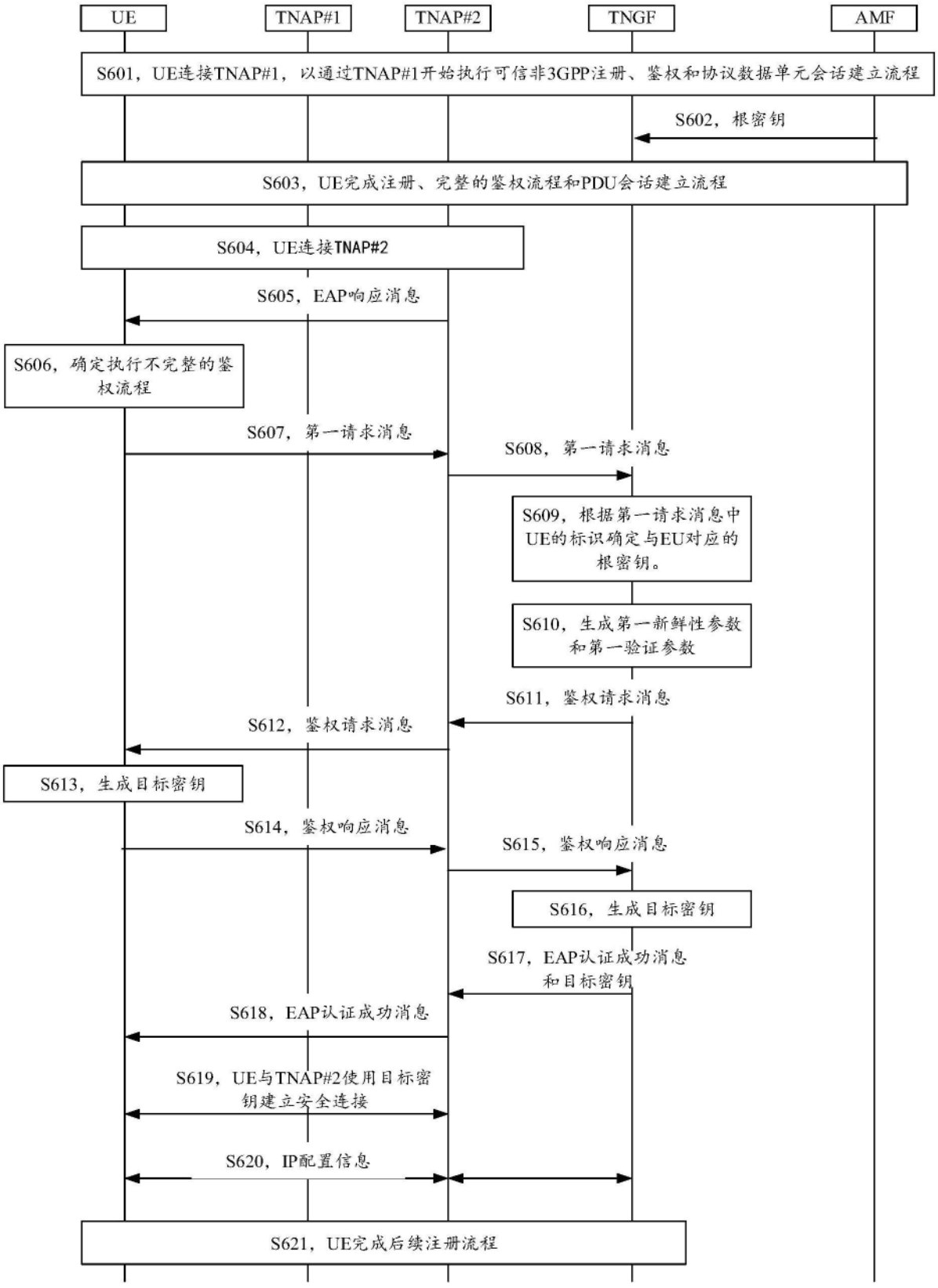

UE
TNAP#1
TNAP#2
TNGF
AMF
S601，UE连接TNAP#1，以通过TNAP#1开始执行可信非3GPP注册、鉴权和协议数据单元会话建立流程
S602，根密钥
S603，UE完成注册、完整的鉴权流程和PDU会话建立流程
S604，UE连接TNAP#2
S605，EAP响应消息
S606，确定执行不完整的鉴权流程
S607，第一请求消息
S608，第一请求消息
S609，根据第一请求消息中UE的标识确定与EU对应的根密钥。
S610，生成第一新鲜性参数和第一验证参数
S611，鉴权请求消息
S612，鉴权请求消息
S613，生成目标密钥
S614，鉴权响应消息
S615，鉴权响应消息
S616，生成目标密钥
S617，EAP认证成功消息和目标密钥
S618，EAP认证成功消息
S619，UE与TNAP#2使用目标密钥建立安全连接
S620，IP配置信息
S621，UE完成后续注册流程

图6

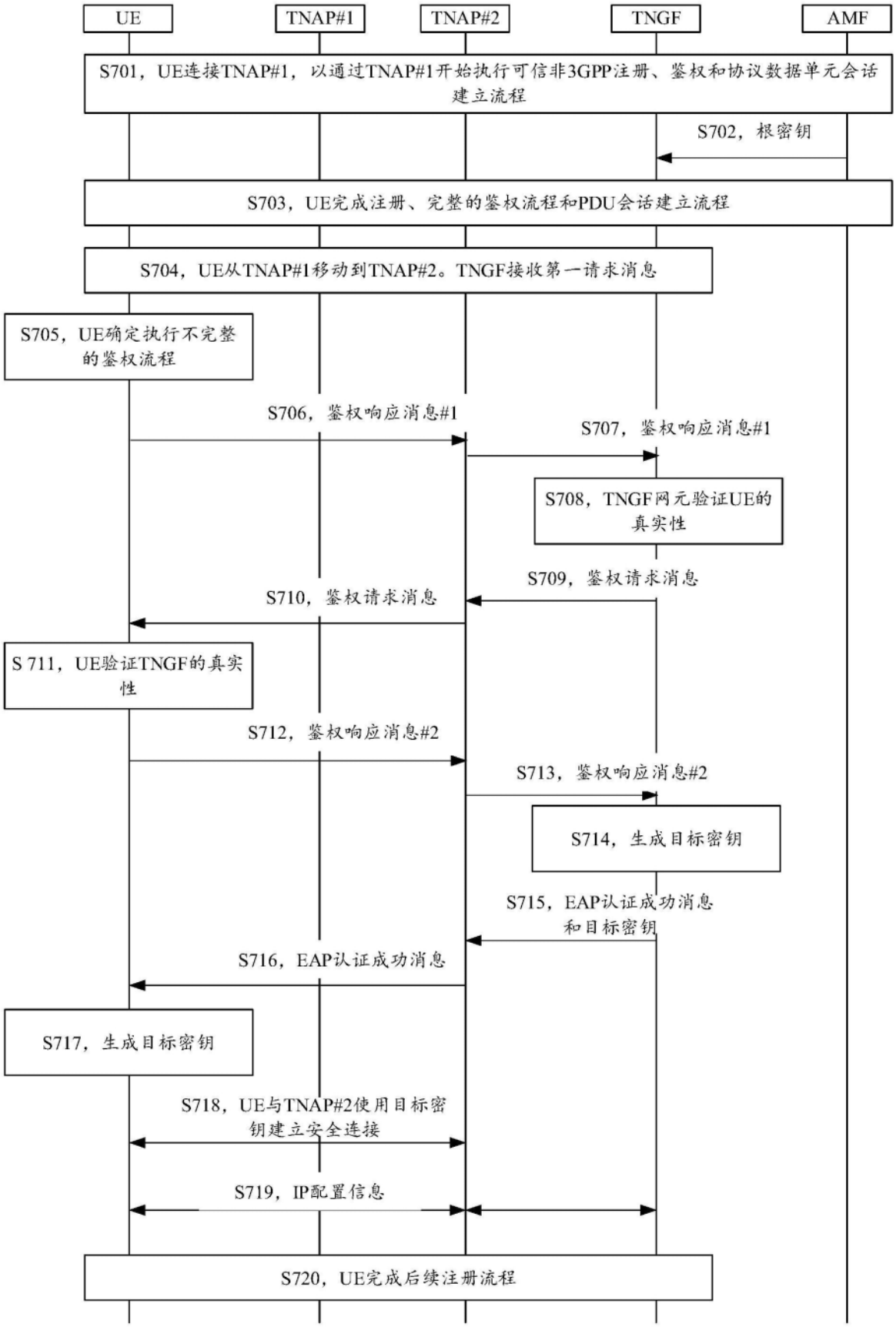

UE
TNAP#1
TNAP#2
TNGF
AMF
S701，UE连接TNAP#1，以通过TNAP#1开始执行可信非3GPP注册、鉴权和协议数据单元会话建立流程
S702，根密钥
S703，UE完成注册、完整的鉴权流程和PDU会话建立流程
S704，UE从TNAP#1移动到TNAP#2。TNGF接收第一请求消息
S705，UE确定执行不完整的鉴权流程
S706，鉴权响应消息#1
S707，鉴权响应消息#1
S708，TNGF网元验证UE的真实性
S709，鉴权请求消息
S710，鉴权请求消息
S 711，UE验证TNGF的真实性
S712，鉴权响应消息#2
S713，鉴权响应消息#2
S714，生成目标密钥
S715，EAP认证成功消息和目标密钥
S716，EAP认证成功消息
S717，生成目标密钥
S718，UE与TNAP#2使用目标密钥建立安全连接
S719，IP配置信息
S720，UE完成后续注册流程

图7

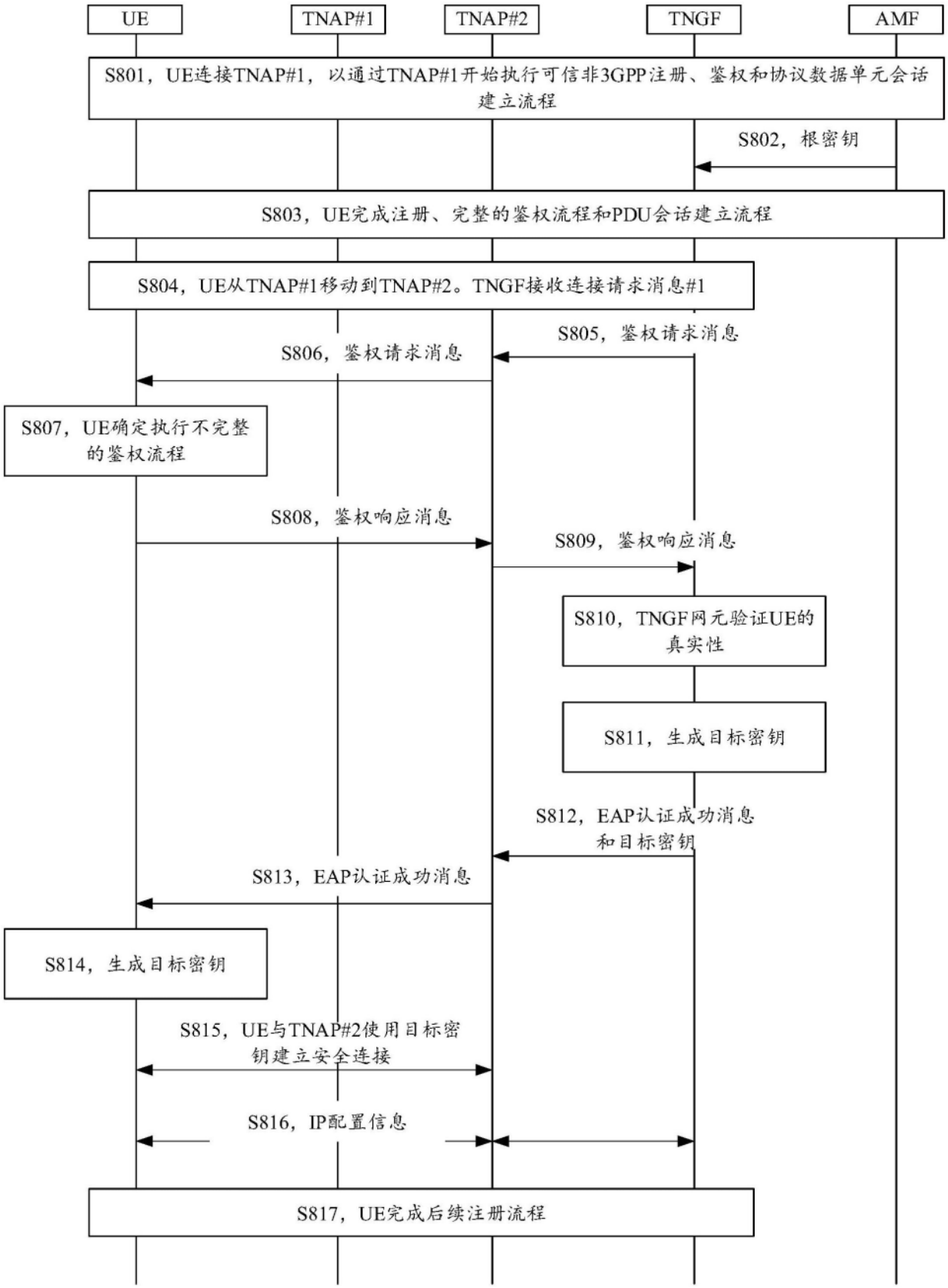

UE
TNAP#1
TNAP#2
TNGF
AMF
S801，UE连接TNAP#1，以通过TNAP#1开始执行可信非3GPP注册、鉴权和协议数据单元会话建立流程
S802，根密钥
S803，UE完成注册、完整的鉴权流程和PDU会话建立流程
S804，UE从TNAP#1移动到TNAP#2。TNGF接收连接请求消息#1
S805，鉴权请求消息
S806，鉴权请求消息
S807，UE确定执行不完整的鉴权流程
S808，鉴权响应消息
S809，鉴权响应消息
S810，TNGF网元验证UE的真实性
S811，生成目标密钥
S812，EAP认证成功消息和目标密钥
S813，EAP认证成功消息
S814，生成目标密钥
S815，UE与TNAP#2使用目标密钥建立安全连接
S816，IP配置信息
S817，UE完成后续注册流程

图8

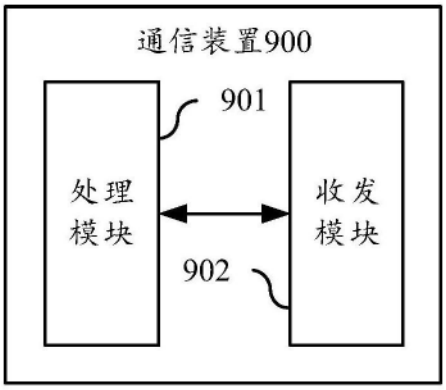

通信装置900
901
处理模块
收发模块
902

图9

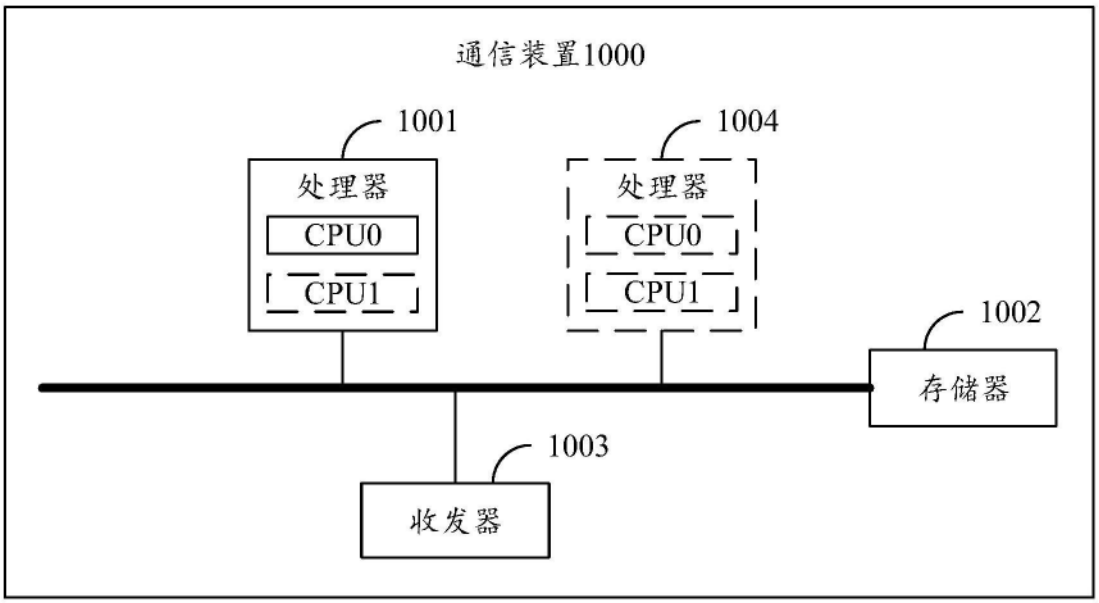

通信装置1000
1001
处理器
CPU0
CPU1
1004
处理器
CPU0
CPU1
1002
存储器
1003
收发器

图10