

密钥生成方法及装置

技术领域

5 本申请涉及通信技术领域，尤其涉及一种密钥生成方法及装置。

背景技术

10 为了减轻有线传输网络的建设负担，提供灵活和密集的新空口（new radio, NR）部署，第五代（5th generation, 5G）移动通信系统使用接入回传一体化（integrated access backhaul, IAB）技术。基于 IAB 技术，基站可以分为 IAB 节点（node）和 IAB 宿主基站（donor）。IAB donor 用于提供到核心网的用户设备接口，以及支持 IAB node 无线回传功能。IAB node 能够支持终端设备的无线接入和数据的无线回传。由于 IAB donor 和 IAB node 之间可以通过无线回传链路进行数据交互，因此 IAB donor 和 IAB node 之间可以不用铺设线缆。这使得 IAB node 的部署更加灵活。

15 为了保证 IAB node 和 IAB donor 之间的 F1 接口的通信安全，IAB node 与 IAB donor 之间可以建立安全隧道（例如互联网安全协议（internet protocol security, IPsec）安全隧道）。在建立安全隧道的过程中，IAB node 与 IAB donor 之间需要使用相同的 IAB 密钥  $K_{IAB}$  来作为认证凭证。

20 为了保障网络的覆盖性能以及业务传输可靠性的要求，可以使 IAB node 支持双连接（dual connectivity, DC），以应对无线回传链路可能发生的异常情况，例如无线回传链路中断或者阻塞等。

25 目前，对于除了演进的移动通信系统陆地无线接入（evolved-universal mobile telecommunications system terrestrial radio access, EUTRA）-NR 双连接（EUTRA-NR dual connection, EN-DC）之外的其他双连接类型，例如 NR-EUTRA 双连接（NR-EUTRA dual connection, NE-DC）、NR-DC 等，业界并未提供  $K_{IAB}$  生成方案。这样一来，可能会导致 IAB node 生成的  $K_{IAB}$  与 IAB donor 生成的  $K_{IAB}$  不相同，从而使得 IAB node 与 IAB donor 之间不能正常建立安全隧道。

发明内容

本申请提供一种密钥生成方法及装置，用于在双连接场景下保证 IAB donor 与 IAB node 生成相同的  $K_{IAB}$ 。

30 第一方面，提供一种密钥生成方法，包括：第一接入网设备确定通过第一接入网设备注册到 5G 核心网的第一设备为 IAB node；在需要为第一设备选择辅基站的情况下，第一接入网设备判断自身是否具备 IAB donor 功能；若第一接入网设备不具备 IAB donor 功能，则第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站；第一接入网设备获取与第二接入网设备关联的第一密钥输入参数；第一接入网设备根据主基站密钥和第一密钥输入参数，生成第一 IAB 密钥  $K_{IAB1}$ ，主基站密钥用于对主基站（第一接入网设备）与第一设备之间的通信进行安全保护， $K_{IAB1}$  用于建立第二接入网设备与第一设备之间的安全隧道；第一接入网设备向第二接入网设备发送  $K_{IAB1}$ 。

基于上述技术方案，在 IAB node（例如第一设备）通过第一接入网设备接入 5G

核心网之后，第一接入网设备可以在自身不具备 IAB donor 功能的情况下为第一设备选择具备 IAB donor 功能的第二接入网设备作为辅基站，以保证双连接场景下存在一个接入网设备作为 IAB donor 为第一设备提供相应的服务。并且，在 NE-DC、NR-DC 或者 NGEN-DC 等双连接场景下，第一接入网设备根据主基站密钥和第一密钥输入参数，生成第一 IAB 密钥  $K_{IAB1}$ ，并将  $K_{IAB1}$  发送给第一接入网设备。这样一来，IAB node 和 IAB donor 之间统一使用以主基站密钥生成的 IAB 密钥，从而保证 IAB node 和 IAB donor 之间能够以相同的 IAB 密钥作为认证凭证来建立安全隧道。

一种可能的设计中，第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站，包括：第一接入网设备向第二设备发送第一请求消息，第一请求消息包括第一设备的标识；第一接入网设备接收第二设备发送的第一响应消息，第一响应消息包括第二接入网设备的标识。

一种可能的设计中，第一密钥输入参数包括第一 IP 地址和第二 IP 地址，第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址，第二 IP 地址为第二接入网设备用于与 IAB node 通信的 IP 地址。

一种可能的设计中，第一接入网设备获取与第二接入网设备关联的第一密钥输入参数，包括：第一接入网设备向第二接入网设备发送辅基站配置消息，辅基站配置消息用于配置第二接入网设备为第一设备的辅基站，辅基站配置消息包括第一指示信息和/或第二指示信息，第一指示信息用于请求第一 IP 地址，第二指示信息用于请求第二 IP 地址；第一接入网设备接收第二接入网设备发送的辅基站配置响应消息，辅基站配置响应消息包括第一 IP 地址和/或第二 IP 地址。基于该设计，在第一 IP 地址由第二接入网设备负责分配的情况下，第一接入网设备通过复用现有的流程来获取第一密钥输入参数，有利于节省信令开销，以及简化操作流程。

一种可能的设计中，辅基站配置消息包括由主基站密钥推演得到的辅基站密钥，辅基站密钥用于对辅基站和第一设备之间的通信进行安全保护。

一种可能的设计中，上述密钥生成方法还包括：第一接入网设备向第一设备发送第一 IP 地址。

一种可能的设计中，第一接入网设备获取与第二接入网设备关联的第一密钥输入参数，包括：第一接入网设备接收第一设备发送的 IP 地址通知消息，IP 地址通知消息包括第一 IP 地址；第一接入网设备向第二接入网设备发送辅基站配置消息，辅基站配置消息用于配置第二接入网设备为第一设备的辅基站，辅基站配置消息包括第二指示信息，第二指示信息用于请求第二 IP 地址；第一接入网设备接收第二接入网设备发送的辅基站配置响应消息，辅基站配置响应消息包括第二 IP 地址。基于该设计，在第一 IP 地址由第二设备负责分配的情况下，第一接入网设备可以通过第一设备获取到第一 IP 地址，通过第二接入网设备获取到第二 IP 地址。

一种可能的设计中，上述密钥生成方法还包括：若第一接入网设备具备 IAB donor 功能，则第一接入网设备选择第三接入网设备作为第一设备的辅基站；第一接入网设备获取与第一接入网设备关联的第二密钥输入参数；第一接入网设备根据主基站密钥和第二密钥输入参数，生成第二 IAB 密钥  $K_{IAB2}$ ， $K_{IAB2}$  用于建立第一接入网设备与第一设备之间的安全隧道。

一种可能的设计中, 第二密钥输入参数包括: 第一 IP 地址和第三 IP 地址, 第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址, 第三 IP 地址为第一接入网设备用于与 IAB node 通信的 IP 地址。

5 一种可能的设计中, 第一接入网设备获取与第一接入网设备关联的第二密钥输入参数, 包括: 第一接入网设备为第一设备分配第一 IP 地址; 第一接入网设备从数据库中获取第三 IP 地址。

一种可能的设计中, 第一接入网设备获取与第一接入网设备关联的第二密钥输入参数, 包括: 第一接入网设备接收第一设备发送的 IP 地址通知消息, IP 地址通知消息包括第一 IP 地址; 第一接入网设备从数据库中获取第三 IP 地址。

10 第二方面, 提供一种密钥生成方法, 包括: 第二接入网设备接收第一接入网设备发送的辅基站配置消息, 辅基站配置消息用于配置第二接入网设备作为第一设备的辅基站; 当辅基站配置消息包括第三指示信息时, 第二接入网设备确定自身是否具备 IAB donor 功能, 第三指示信息用于指示第一设备为 IAB 节点; 当第二接入网设备具备 IAB 宿主功能时, 第二接入网设备从第一接入网设备获取第一 IAB 密钥  $K_{IAB1}$ , 所述  $K_{IAB1}$  用于建立所述第二接入网设备与所述第一设备之间的安全隧道, 所述  $K_{IAB1}$  是根据主  
15 基站密钥生成的, 所述主基站密钥用于对所述第一接入网设备和所述第一设备之间的通信进行安全保护。

基于上述技术方案, 通过以具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站, 从而保证在双连接场景下存在接入网设备作为 IAB donor 为 IAB node (也  
20 即第一设备) 提供相应的服务。第二接入网设备通过接收第一接入网设备发送的  $K_{IAB1}$ , 从而使得 IAB node 和 IAB donor 之间统一使用以主基站密钥生成的 IAB 密钥, 进而保证 IAB node 和 IAB donor 之间能够以相同的 IAB 密钥作为认证凭证来建立安全隧道。

一种可能的设计中,  $K_{IAB1}$  是根据主基站密钥生成的, 包括:  $K_{IAB1}$  是根据主基站密钥和第一密钥输入参数生成的。第一密钥输入参数包括第一 IP 地址和第二 IP 地址,  
25 第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址, 第二 IP 地址为第二接入网设备用于与 IAB node 通信的 IP 地址。

一种可能的设计中, 辅基站配置消息还包括第一指示信息和/或第二指示信息, 第一指示信息用于请求第一 IP 地址, 第二指示信息用于请求第二 IP 地址。

30 一种可能的设计中, 上述密钥生成方法还包括: 第二接入网设备向第一接入网设备发送辅基站配置响应消息, 辅基站配置响应消息包括第一 IP 地址和/或第二 IP 地址。

一种可能的设计中, 所述第二接入网设备从所述第一接入网设备获取  $K_{IAB1}$ , 包括: 所述第二接入网设备接收所述第一接入网设备发送的辅基站重配置完成消息, 所述辅基站重配置完成消息包括所述  $K_{IAB1}$ 。

一种可能的设计中, 所述第二接入网设备从所述第一接入网设备获取  $K_{IAB1}$ , 包括:  
35 所述第二接入网设备向所述第一接入网设备发送密钥请求消息, 所述密钥请求消息用于请求所述  $K_{IAB1}$ ; 所述第二接入网设备接收所述第一接入网设备发送的密钥响应消息, 所述密钥响应消息包括所述  $K_{IAB1}$ 。

一种可能的设计中, 所述密钥请求消息还包括所述第一 IP 地址和/或第二 IP 地址。

第三方面, 提供一种密钥生成方法, 应用于第一设备连接主基站和辅基站的场景,

第一设备具备 IAB node 功能。该密钥生成方法包括：第一设备根据主基站支持的通信制式、辅基站支持的通信制式以及核心网支持的通信制式，确定双连接的类型；当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据主基站密钥，生成 IAB 密钥  $K_{IAB}$ ，所述主基站密钥用于对所述第一设备与主基站之间的通信安全进行安全保护。

基于上述技术方案，IAB node 通过确定双连接的类型，从而在 NE-DC、NR-DC 或者 NGEN-DC 场景下，IAB node 使用主基站密钥，生成 IAB 密钥  $K_{IAB}$ ，从而使得 IAB node 和 IAB donor 之间统一使用以主基站密钥生成的 IAB 密钥，进而保证 IAB node 和 IAB donor 之间能够以相同的 IAB 密钥作为认证凭证来建立安全隧道。

一种可能的设计中，上述密钥生成方法还包括：第一设备接收主基站的广播消息；第一设备根据广播消息中的配置参数，确定主基站支持的通信制式，配置参数包括以下一项或者多项：基站标识、逻辑小区标识、物理小区标识、上行频点或下行频点。

一种可能的设计中，第一设备根据广播消息中的配置参数，确定主基站支持的通信制式，包括：当广播消息中的配置参数属于 5G 通信系统时，第一设备确定主基站支持 5G 通信制式；或者，当广播消息中的配置参数属于 4G 通信系统时，第一设备确定主基站支持 4G 通信制式。

一种可能的设计中，上述密钥生成方法还包括：第一设备接收主基站发送的 RRC 重配置消息，RRC 重配置消息包括辅小区组配置信息；第一设备根据辅小区组配置信息，确定辅基站支持的通信制式。

一种可能的设计中，第一设备根据 RRC 重配置消息，确定辅基站支持的通信制式，包括：当辅小区组配置信息属于 5G 通信制式时，第一设备确定辅基站支持 5G 通信制式；或者，当辅小区组配置信息属于 4G 通信制式时，第一设备确定辅基站支持 4G 通信制式。

一种可能的设计中，上述密钥生成方法还包括：第一设备接收主基站发送的广播消息；第一设备根据广播消息中的小区配置信息，确定核心网支持的通信制式。

一种可能的设计中，第一设备根据广播消息中的小区配置信息，确定核心网支持的通信制式，包括：当小区配置信息属于 5G 通信制式时，第一设备确定核心网支持 5G 通信制式；或者，当小区配置信息属于 4G 通信制式时，第一设备确定核心网支持 4G 通信制式。

一种可能的设计中，第一设备根据主基站支持的通信制式、辅基站支持的通信制式以及核心网支持的通信制式，确定双连接的类型，包括：当主基站支持 5G 网络制式，辅基站支持 4G 网络制式，核心网支持 5G 网络制式时，第一设备确定双连接类型为 NE-DC；或者，当主基站支持 5G 网络制式，辅基站支持 5G 网络制式，核心网支持 5G 网络制式时，第一设备确定双连接类型为 NR-DC；或者，当主基站支持 4G 网络制式，辅基站支持 5G 网络制式，核心网支持 5G 网络制式时，第一设备确定双连接类型为 NGEN-DC；或者，当主基站支持 4G 网络制式，辅基站支持 5G 网络制式，核心网支持 4G 网络制式时，第一设备确定双连接类型为 EN-DC。

第四方面，提供一种密钥生成方法，方法包括：第一接入网设备确定通过第一接入网设备注册到网络的第一设备为 IAB node；若第一接入网设备具备 IAB donor 功能，

则第一接入网设备选择第三接入网设备作为第一设备的辅基站；第一接入网设备根据辅基站密钥，生成第二 IAB 密钥  $K_{IAB2}$ ， $K_{IAB2}$  用于建立第一接入网设备与第一设备之间的安全隧道，所述辅基站密钥用于对所述辅基站和所述第一设备之间的通信进行安全保护。

5       基于上述技术方案，由于第一接入网设备确定第一设备为 IAB node，并且第一接入网设备具备 IAB donor 功能，因此第一接入网设备可以作为第一设备的 IAB donor。进而，在双连接场景下，第一接入网设备根据辅基站密钥，生成  $K_{IAB2}$ ，从而保证 IAB node 和 IAB donor 之间统一使用以辅基站密钥生成的 IAB 密钥，进而保证 IAB node 和 IAB donor 之间能够以相同的 IAB 密钥作为认证凭证来建立安全隧道。

10       一种可能的设计中，辅基站密钥是根据主基站密钥推演得到的，所述主基站密钥用于对第一接入网设备和第一设备之间的通信进行安全保护。

一种可能的设计中，在第一接入网设备根据辅基站密钥，生成  $K_{IAB2}$  之后，方法还包括：第一接入网设备向第二接入网设备发送辅基站配置消息，辅基站配置消息包括辅基站密钥；第一接入网设备接收第二接入网设备发送的辅基站配置响应消息。

15       一种可能的设计中，第一接入网设备根据辅基站密钥，生成  $K_{IAB2}$ ，包括：第一接入网设备在发送辅基站配置消息之后，根据辅基站密钥，生成  $K_{IAB2}$ 。

一种可能的设计中，第一接入网设备根据辅基站密钥，生成  $K_{IAB2}$ ，包括：第一接入网设备在接收到辅基站配置响应消息之后，根据辅基站密钥，生成  $K_{IAB2}$ 。

20       一种可能的设计中，上述密钥生成方法还包括：若第一接入网设备不具备 IAB donor 功能，则第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站；第一接入网设备向第二接入网设备发送辅基站配置消息，辅基站配置消息包括辅基站密钥。

第五方面，提供一种密钥生成方法，应用于第一设备连接主基站和辅基站的场景，第一设备具备 IAB node 功能。该密钥生成方法包括：第一设备根据主基站支持的通信制式、辅基站支持的通信制式以及核心网支持的通信制式，确定双连接的类型；当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据辅基站密钥，生成 IAB 密钥  $K_{IAB}$ ，所述辅基站密钥用于对所述第一设备与辅基站之间的通信安全进行安全保护。

30       基于上述技术方案，IAB node 通过确定双连接的类型，从而在 NE-DC、NR-DC 或者 NGEN-DC 场景下，IAB node 使用辅基站密钥，生成 IAB 密钥  $K_{IAB}$ ，从而使得 IAB node 和 IAB donor 之间统一使用以辅基站密钥生成的 IAB 密钥，进而保证 IAB node 和 IAB donor 之间能够以相同的 IAB 密钥作为认证凭证来建立安全隧道。

一种可能的设计中，上述密钥生成方法还包括：第一设备接收主基站的广播消息；第一设备根据广播消息中的配置参数，确定主基站支持的通信制式，配置参数包括以下一项或者多项：基站标识、逻辑小区标识、物理小区标识、上行频点或下行频点。

35       一种可能的设计中，第一设备根据广播消息中的配置参数，确定主基站支持的通信制式，包括：当广播消息中的配置参数属于 5G 通信系统时，第一设备确定主基站支持 5G 通信制式；或者，当广播消息中的配置参数属于 4G 通信系统时，第一设备确定主基站支持 4G 通信制式。

一种可能的设计中,上述密钥生成方法还包括:第一设备接收主基站发送的 RRC 重配置消息, RRC 重配置消息包括辅小区组配置信息;第一设备根据辅小区组配置信息,确定辅基站支持的通信制式。

- 5 一种可能的设计中,第一设备根据 RRC 重配置消息,确定辅基站支持的通信制式,包括:当辅小区组配置信息属于 5G 通信制式时,第一设备确定辅基站支持 5G 通信制式;或者,当辅小区组配置信息属于 4G 通信制式时,第一设备确定辅基站支持 4G 通信制式。

一种可能的设计中,上述密钥生成方法还包括:第一设备接收主基站发送的广播消息;第一设备根据广播消息中的小区配置信息,确定核心网支持的通信制式。

- 10 一种可能的设计中,第一设备根据广播消息中的小区配置信息,确定核心网支持的通信制式,包括:当小区配置信息属于 5G 通信制式时,第一设备确定核心网支持 5G 通信制式;或者,当小区配置信息属于 4G 通信制式时,第一设备确定核心网支持 4G 通信制式。

- 15 一种可能的设计中,第一设备根据主基站支持的通信制式、辅基站支持的通信制式以及核心网支持的通信制式,确定双连接的类型,包括:当主基站支持 5G 网络制式,辅基站支持 4G 网络制式,核心网支持 5G 网络制式时,第一设备确定双连接类型为 NE-DC;或者,当主基站支持 5G 网络制式,辅基站支持 5G 网络制式,核心网支持 5G 网络制式时,第一设备确定双连接类型为 NR-DC;或者,当主基站支持 4G 网络制式,辅基站支持 5G 网络制式,核心网支持 5G 网络制式时,第一设备确定双连接类型为 NGEN-DC;或者,当主基站支持 4G 网络制式,辅基站支持 5G 网络制式,核心网支持 4G 网络制式时,第一设备确定双连接类型为 EN-DC。

- 25 第六方面,提供一种密钥生成方法,应用于第一设备连接主基站和辅基站的场景下,第一设备具备 IAB node 功能。该密钥生成方法包括:第一设备获知主基站或者辅基站作为 IAB donor;当主基站为 IAB donor 时,第一设备根据主基站密钥和密钥输入参数,生成 IAB 密钥, IAB 密钥用于建立 IAB node 和 IAB donor 之间的安全隧道,主基站密钥用于对第一设备与主基站之间的通信进行安全保护;或者,当辅基站为 IAB donor 时,第一设备根据辅基站密钥和密钥输入参数,生成 IAB 密钥,辅基站密钥用于对第一设备与辅基站之间的通信进行安全保护。

- 30 基于上述技术方案,在主基站作为 IAB donor 的情况下,保证 IAB node 和 IAB donor 均采用主基站密钥来生成 IAB 密钥。在辅基站作为 IAB donor 的情况下,保证 IAB node 和 IAB donor 均采用辅基站密钥来生成 IAB 密钥。这样一来,保证在双连接场景下, IAB donor 和 IAB node 之间能够以相同的 IAB 密钥作为认证凭证来建立安全隧道。

- 35 一种可能的设计中,第一设备获知主基站或者辅基站作为 IAB donor,包括:当第一设备接收到第四指示信息时,第一设备获知主基站为 IAB donor,第四指示信息用于指示主基站为 IAB donor;或者,当第一设备接收到第五指示信息时,第一设备获知辅基站为 IAB donor,第五指示信息用于指示辅基站为 IAB donor。

一种可能的设计中,第一设备获知主基站或者辅基站作为 IAB donor,包括:当第一设备与主基站之间建立无线回程链路时,第一设备获知主基站为 IAB donor;或者,

当第一设备与辅基站之间建立无线回程链路时，第一设备获知辅基站为 IAB donor。

一种可能的设计中，第一设备获知主基站或者辅基站作为 IAB donor，包括：第一设备获取主基站支持的频段以及辅基站支持的频段；当主基站支持的频段高于辅基站支持的频段时，第一设备获知主基站为 IAB donor；或者，当主基站支持的频段低于辅

5 基站支持的频段时，第一设备获知辅基站为 IAB donor。

一种可能的设计中，第一设备获知主基站或者辅基站作为 IAB donor，包括：当第一设备接收主基站广播的第六指示信息时，第一设备获知主基站为 IAB donor；或者，当第一设备接收辅基站广播的第六指示信息时，第一设备获知辅基站为 IAB donor；其中，第六指示信息用于指示基站具有 IAB donor 功能。

10 第七方面，提供一种通信装置，应用于第一接入网设备。所述通信装置包括：处理模块和通信模块。处理模块，用于确定注册到 5G 核心网的第一设备为 IAB node；在需要为第一设备选择辅基站的情况下，判断自身是否具备 IAB donor 功能；若不具备 IAB donor 功能，则选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站；获取与第二接入网设备关联的第一密钥输入参数；根据主基站密钥和第一密钥

15 输入参数，生成第一 IAB 密钥  $K_{IAB1}$ ，主基站密钥用于对主基站（第一接入网设备）与第一设备之间的通信进行安全保护， $K_{IAB1}$  用于建立第二接入网设备与第一设备之间的安全隧道。通信模块，用于向第二接入网设备发送  $K_{IAB1}$ 。

一种可能的设计中，通信模块，还用于向第二设备发送第一请求消息，第一请求消息包括第一设备的标识；接收第二设备发送的第一响应消息，第一响应消息包括第二接入网设备的标识。

20

一种可能的设计中，第一密钥输入参数包括第一 IP 地址和第二 IP 地址，第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址，第二 IP 地址为第二接入网设备用于与 IAB node 通信的 IP 地址。

一种可能的设计中，通信模块，用于向第二接入网设备发送辅基站配置消息，辅基站配置消息用于配置第二接入网设备为第一设备的辅基站，辅基站配置消息包括第一指示信息和/或第二指示信息，第一指示信息用于请求第一 IP 地址，第二指示信息用于请求第二 IP 地址；接收第二接入网设备发送的辅基站配置响应消息，辅基站配置响应消息包括第一 IP 地址和/或第二 IP 地址。

25

一种可能的设计中，辅基站配置消息包括由主基站密钥推演得到的辅基站密钥，辅基站密钥用于对辅基站和第一设备之间的通信进行安全保护。

30

一种可能的设计中，通信模块，还用于向第一设备发送第一 IP 地址。

一种可能的设计中，通信模块，还用于接收第一设备发送的 IP 地址通知消息，IP 地址通知消息包括第一 IP 地址；向第二接入网设备发送辅基站配置消息，辅基站配置消息用于配置第二接入网设备为第一设备的辅基站，辅基站配置消息包括第二指示信息，第二指示信息用于请求第二 IP 地址；接收第二接入网设备发送的辅基站配置响应消息，辅基站配置响应消息包括第二 IP 地址。

35

一种可能的设计中，处理模块，还用于若自身具备 IAB donor 功能，则选择第三接入网设备作为第一设备的辅基站；获取与第一接入网设备关联的第二密钥输入参数；根据主基站密钥和第二密钥输入参数，生成第二 IAB 密钥  $K_{IAB2}$ ， $K_{IAB2}$  用于建立自身

与第一设备之间的安全隧道。

一种可能的设计中，第二密钥输入参数包括：第一 IP 地址和第三 IP 地址，第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址，第三 IP 地址为第一接入网设备用于与 IAB node 通信的 IP 地址。

- 5 一种可能的设计中，处理模块，还用于为第一设备分配第一 IP 地址；从数据库中获取第三 IP 地址。

一种可能的设计中，通信模块，还用于接收第一设备发送的 IP 地址通知消息，IP 地址通知消息包括第一 IP 地址。处理模块，还用于从数据库中获取第三 IP 地址。

- 10 第八方面，提供一种通信装置，应用于第二接入网设备。所述通信装置包括：通信模块和处理模块。通信模块，用于接收第一接入网设备发送的辅基站配置消息，辅基站配置消息用于配置第二接入网设备作为第一设备的辅基站。处理模块，用于当辅基站配置消息包括第三指示信息时，确定自身是否具备 IAB donor 功能，第三指示信息用于指示第一设备为 IAB 节点。通信模块，还用于当自身具备 IAB 宿主功能时，从第一接入网设备获取第一 IAB 密钥  $K_{IAB1}$ ，所述  $K_{IAB1}$  用于建立所述第二接入网设备与  
15 所述第一设备之间的安全隧道，所述  $K_{IAB1}$  是根据主基站密钥生成的，所述主基站密钥用于对所述第一接入网设备和所述第一设备之间的通信进行安全保护。

- 一种可能的设计中， $K_{IAB1}$  是根据主基站密钥生成的，包括： $K_{IAB1}$  是根据主基站密钥和第一密钥输入参数生成的。第一密钥输入参数包括第一 IP 地址和第二 IP 地址，第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址，第二 IP 地址为第二接入网设备用于与 IAB node 通信的 IP 地址。  
20

一种可能的设计中，辅基站配置消息还包括第一指示信息和/或第二指示信息，第一指示信息用于请求第一 IP 地址，第二指示信息用于请求第二 IP 地址。

一种可能的设计中，通信模块，还用于向第一接入网设备发送辅基站配置响应消息，辅基站配置响应消息包括第一 IP 地址和/或第二 IP 地址。

- 25 一种可能的设计中，通信模块，具体用于接收所述第一接入网设备发送的辅基站重配置完成消息，所述辅基站重配置完成消息包括所述  $K_{IAB1}$ 。

一种可能的设计中，通信模块，具体用于向所述第一接入网设备发送密钥请求消息，所述密钥请求消息用于请求所述  $K_{IAB1}$ ；接收所述第一接入网设备发送的密钥响应消息，所述密钥响应消息包括所述  $K_{IAB1}$ 。

- 30 一种可能的设计中，所述密钥请求消息还包括所述第一 IP 地址和/或第二 IP 地址。

- 第九方面，提供一种通信装置，应用于第一设备。所述通信装置包括：处理模块。处理模块，用于根据主基站支持的通信制式、辅基站支持的通信制式以及核心网支持的通信制式，确定双连接的类型；当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，根据主基站密钥和密钥输入参数，生成  $K_{IAB}$ ，所述主基站密钥用于对所述第一设备与主基站之间的通信安全进行安全保护。  
35

一种可能的设计中，通信装置还包括通信模块。通信模块，用于接收主基站的广播消息。处理模块，还用于根据广播消息中的配置参数，确定主基站支持的通信制式，配置参数包括以下一项或者多项：基站标识、逻辑小区标识、物理小区标识、上行频点或下行频点。

一种可能的设计中，处理模块，具体用于当广播消息中的配置参数属于 5G 通信系统时，确定主基站支持 5G 通信制式；或者，当广播消息中的配置参数属于 4G 通信系统时，确定主基站支持 4G 通信制式。

5 一种可能的设计中，通信装置还包括通信模块。通信模块，用于接收主基站发送的 RRC 重配置消息，RRC 重配置消息包括辅小区组配置信息。处理模块，用于根据辅小区组配置信息，确定辅基站支持的通信制式。

一种可能的设计中，处理模块，具体用于当辅小区组配置信息属于 5G 通信制式时，确定辅基站支持 5G 通信制式；或者，当辅小区组配置信息属于 4G 通信制式时，确定辅基站支持 4G 通信制式。

10 一种可能的设计中，通信装置还包括通信模块。通信模块，用于接收主基站发送的广播消息。处理模块，用于根据广播消息中的小区配置信息，确定核心网支持的通信制式。

一种可能的设计中，处理模块，具体用于当小区配置信息属于 5G 通信制式时，确定核心网支持 5G 通信制式；或者，当小区配置信息属于 4G 通信制式时，确定核心网支持 4G 通信制式。

15 一种可能的设计中，处理模块，具体用于当主基站支持 5G 网络制式，辅基站支持 4G 网络制式，核心网支持 5G 网络制式时，确定双连接类型为 NE-DC；或者，当主基站支持 5G 网络制式，辅基站支持 5G 网络制式，核心网支持 5G 网络制式时，确定双连接类型为 NR-DC；或者，当主基站支持 4G 网络制式，辅基站支持 5G 网络制式，核心网支持 5G 网络制式时，确定双连接类型为 NGEN-DC；或者，当主基站支持 4G 网络制式，辅基站支持 5G 网络制式，核心网支持 4G 网络制式时，确定双连接类型为 EN-DC。

20 第十方面，提供一种通信装置，应用于第一接入网设备。所述通信装置包括：处理模块。处理模块，用于确定注册到网络的第一设备为 IAB node；在需要为第一设备选择辅基站的情况下，判断自身是否具备 IAB donor 功能；若自身具备 IAB donor 功能，则选择第三接入网设备作为第一设备的辅基站；根据辅基站密钥，生成 IAB 密钥  $K_{IAB}$ ， $K_{IAB}$  用于建立自身与第一设备之间的安全隧道，所述辅基站密钥用于对所述辅基站和所述第一设备之间的通信进行安全保护。

25 一种可能的设计中，辅基站密钥是根据主基站密钥推演得到的，所述主基站密钥用于对第一接入网设备和第一设备之间的通信进行安全保护。

一种可能的设计中，通信装置还包括通信模块。通信模块，用于在处理模块生成  $K_{IAB}$  之后，向第二接入网设备发送辅基站配置消息，辅基站配置消息包括辅基站密钥；接收第二接入网设备发送的辅基站配置响应消息。

30 一种可能的设计中，处理模块，具体用于在通信模块发送辅基站配置消息之后，根据辅基站密钥，生成  $K_{IAB}$ 。

一种可能的设计中，处理模块，具体用于在接收到辅基站配置响应消息之后，根据辅基站密钥，生成  $K_{IAB}$ 。

一种可能的设计中，处理模块，还用于若自身不具备 IAB donor 功能，则选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站；向第二接入网设备发送

辅基站配置消息，辅基站配置消息包括辅基站密钥。

第十一方面，提供一种通信装置，应用于第一设备。所述通信装置包括：处理模块。处理模块，用于根据主基站支持的通信制式、辅基站支持的通信制式以及核心网支持的通信制式，确定双连接的类型；当双连接的类型为 NE-DC、NR-DC 或者  
5 NGEN-DC 时，根据辅基站密钥，生成  $K_{IAB}$ ，所述辅基站密钥用于对所述第一设备与辅基站之间的通信安全进行安全保护。

一种可能的设计中，通信装置还包括通信模块。通信模块，用于接收主基站的广播消息。处理模块，还用于根据广播消息中的配置参数，确定主基站支持的通信制式，配置参数包括以下一项或者多项：基站标识、逻辑小区标识、物理小区标识、上行频  
10 点或下行频点。

一种可能的设计中，处理模块，具体用于当广播消息中的配置参数属于 5G 通信系统时，确定主基站支持 5G 通信制式；或者，当广播消息中的配置参数属于 4G 通信系统时，确定主基站支持 4G 通信制式。

一种可能的设计中，通信装置还包括通信模块。通信模块，用于接收主基站发送的 RRC 重配置消息，RRC 重配置消息包括辅小区组配置信息。处理模块，用于根据  
15 辅小区组配置信息，确定辅基站支持的通信制式。

一种可能的设计中，处理模块，具体用于当辅小区组配置信息属于 5G 通信制式时，确定辅基站支持 5G 通信制式；或者，当辅小区组配置信息属于 4G 通信制式时，确定辅基站支持 4G 通信制式。

一种可能的设计中，通信装置还包括通信模块。通信模块，用于接收主基站发送的广播消息。处理模块，用于根据广播消息中的小区配置信息，确定核心网支持的通信制式。  
20

一种可能的设计中，处理模块，具体用于当小区配置信息属于 5G 通信制式时，确定核心网支持 5G 通信制式；或者，当小区配置信息属于 4G 通信制式时，确定核心网支持 4G 通信制式。  
25

一种可能的设计中，处理模块，具体用于当主基站支持 5G 网络制式，辅基站支持 4G 网络制式，核心网支持 5G 网络制式时，确定双连接类型为 NE-DC；或者，当主基站支持 5G 网络制式，辅基站支持 5G 网络制式，核心网支持 5G 网络制式时，确定双连接类型为 NR-DC；或者，当主基站支持 4G 网络制式，辅基站支持 5G 网络制式，核心网支持 5G 网络制式时，确定双连接类型为 NGEN-DC；或者，当主基站支持 4G 网络制式，辅基站支持 5G 网络制式，核心网支持 4G 网络制式时，确定双连接类型为 EN-DC。  
30

第十二方面，提供一种通信装置，应用于第一设备，所述第一设备具备 IAB node 功能。所述通信装置包括：处理模块。处理模块，用于获知主基站或者辅基站作为 IAB donor；当主基站为 IAB donor 时，根据主基站密钥和密钥输入参数，生成 IAB 密钥，IAB 密钥用于建立 IAB node 和 IAB donor 之间的安全隧道；或者，当辅基站为 IAB donor 时，根据辅基站密钥和密钥输入参数，生成 IAB 密钥。  
35

一种可能的设计中，处理模块，具体用于当接收到第四指示信息时，获知主基站为 IAB donor，第四指示信息用于指示主基站为 IAB donor；或者，当接收到第五指示

信息时，获知辅基站为 IAB donor，第五指示信息用于指示辅基站为 IAB donor。

一种可能的设计中，处理模块，具体用于当通信装置与主基站之间建立无线回程链路时，获知主基站为 IAB donor；或者，当通信装置与辅基站之间建立无线回程链路时，获知辅基站为 IAB donor。

- 5 一种可能的设计中，处理模块，具体用于获取主基站支持的频段以及辅基站支持的频段；当主基站支持的频段高于辅基站支持的频段时，获知主基站为 IAB donor；或者，当主基站支持的频段低于辅基站支持的频段时，获知辅基站为 IAB donor。

- 10 一种可能的设计中，处理模块，具体用于当接收主基站广播的第六指示信息时，获知主基站为 IAB donor；或者，当接收辅基站广播的第六指示信息时，获知辅基站为 IAB donor；其中，第六指示信息用于指示基站具有 IAB donor 功能。

第十三方面，提供一种通信装置，包括处理器和通信端口，处理器用于执行计算机程序指令，使得通信装置实现第一方面至第六方面中任一方面所提供的任一种设计所涉及的方法。

- 15 第十四方面，提供一种计算机可读存储介质，该计算机可读存储介质存储有指令，当指令在计算机上运行时，使得计算机实现第一方面至第六方面中任一方面所提供的任一种设计所涉及的方法。

第十五方面，提供一种计算机程序产品，该计算机程序产品包括指令，当计算机程序产品在计算机上运行时，使得计算机实现第一方面至第六方面中任一方面所提供的任一种设计所涉及的方法。

- 20 第十六方面，提供一种芯片，该芯片包括处理器，当处理器执行计算机程序指令时，使得计算机实现第一方面至第六方面中任一方面所提供的任一种设计所涉及的方法。

其中，上述第七方面至第十六方面中任一种设计方式所带来的技术效果可参见上文所提供的对应的方法中的有益效果同设计方式所带来的技术效果，此处不再赘述。

## 25 附图说明

- 图 1 为相关技术提供的一种双连接配置的流程图；  
图 2 为本申请实施例提供的一种 IAB 组网场景的示意图；  
图 3 为本申请实施例提供的一种 IAB 网络中用户面协议栈的示意图；  
图 4 为本申请实施例提供的一种 IAB 网络中控制面协议栈的示意图；  
30 图 5 为本申请实施例提供的一种 IAB node 采用 EN-DC 模式的示意图；  
图 6 为本申请实施例提供的一种 EN-DC 场景下生成 IAB 密钥的流程图；  
图 7 为本申请实施例提供的一种 IAB node 采用 NE-DC 模式的示意图；  
图 8 为本申请实施例提供的一种 IAB node 采用 NR-DC 模式的示意图；  
图 9 为本申请实施例提供的一种 IAB node 采用 NGEN-DC 模式的示意图；  
35 图 10 为本申请实施例提供的一种密钥生成方法的流程图；  
图 11 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 12 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 13 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 14 为本申请实施例提供的另一种密钥生成方法的流程图；

- 图 15 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 16 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 17 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 18 为本申请实施例提供的另一种密钥生成方法的流程图；  
5 图 19 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 20 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 21 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 22 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 23 为本申请实施例提供的另一种密钥生成方法的流程图；  
10 图 24 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 25 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 26 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 27 为本申请实施例提供的另一种密钥生成方法的流程图；  
图 28 为本申请实施例提供的一种通信装置的结构示意图；  
15 图 29 为本申请实施例提供的一种通信装置的硬件结构示意图。

### 具体实施方式

- 在本申请的描述中，除非另有说明，“/”表示“或”的意思，例如，A/B 可以表示 A 或 B。本文中的“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。  
20 此外，“至少一个”是指一个或多个，“多个”是指两个或两个以上。“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并无限定一定不同。

- 需要说明的是，本申请中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其他实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”  
25 等词旨在以具体方式呈现相关概念。

为了便于理解本申请的技术方案，下面对一些技术术语进行介绍。

#### 1、双连接

- 在无线通信技术领域中，为了提升用户的吞吐率，引入了双连接(dual connectivity, DC)技术。DC 可以支持两个或两个以上基站同时为一个终端设备提供数据传输服务。  
30 这些基站中包括一个主基站以及一个或多个辅基站。

上述主基站又可以被称为主节点(master node, MN)或者主接入网设备，上述辅基站又可以被称为辅节点(secondary node, SN)或者辅接入网设备，本申请实施例对此不作限定。

- 主基站与核心网(core network, CN)之间通过 S1/NG 接口连接。主基站与核心网之间至少包括控制面连接，还可以有用户面连接。S1 接口包括 S1-U 和 S1-C。NG 接口包括 NG-U 和 NG-C。其中，S1-U/NG-U 代表用户面连接，S1-C/NG-C 代表控制面连接。  
35

辅基站与核心网之间可以具有用户面连接，也可以不具有用户面连接。当辅基站与核心网之间不具有用户面连接时，终端设备的数据可以由主基站在分组数据汇聚协

议（packet data convergence protocol, PDCP）层分流给辅基站。

依据主基站、辅基站以及主基站连接的核心网各自支持的通信制式，双连接可以有多种类型。示例性的，下面以表 1 为例对双连接的类型进行说明。

表 1

| 双连接类型   | 主基站   | 辅基站   | 核心网    |
|---------|-------|-------|--------|
| EN-DC   | 4G 基站 | 4G 基站 | 4G 核心网 |
| NE-DC   | 5G 基站 | 4G 基站 | 5G 核心网 |
| NR-DC   | 5G 基站 | 5G 基站 | 5G 核心网 |
| NGEN-DC | 4G 基站 | 4G 基站 | 5G 核心网 |

5 在双连接场景下，主基站管理一个主小区（primary cell, PCell）。其中，主小区是指部署在主频点，且在终端发起初始连接建立过程或 RRC 连接重建立过程中接入的小区，或者在切换过程中指示为主小区的小区。进一步地，除主小区外，主基站还可以管理一个或多个辅小区（secondary cell, SCell）。主基站下为终端提供服务的小区，如主小区、主基站下的辅小区，可以构成（master cell group, MCG）。

10 辅基站管理一个主辅小区（primary secondary cell, PSCell）。其中，主辅小区可以是终端向辅基站发起随机接入过程中接入的小区，或者终端在辅基站改变过程中跳过随机接入过程发起数据传输的另一辅基站上的小区，或者执行同步重配置流程时发起随机接入过程中接入的辅基站上的小区。进一步地，除主辅小区外，辅基站还可以管理一个或多个辅小区。辅基站上为终端提供服务的小区，如主辅小区、辅基站上的辅小区，可以构成辅小区组（secondary cell group, SCG）。

15 在本申请实施例中，终端设备是一种具有无线收发功能的设备。终端设备可以被部署在陆地上，包括室内或室外、手持或车载；也可以被部署在水面上（如轮船等）；还可以被部署在空中（例如飞机、气球和卫星上等）。终端设备可以是用户设备（user equipment, UE）。其中，UE 包括具有无线通信功能的手持式设备、车载设备、可穿戴设备或计算设备。示例性地，UE 可以是手机（mobile phone）、平板电脑或带无线收发功能的电脑。终端设备还可以是虚拟现实（virtual reality, VR）终端设备、增强现实（augmented reality, AR）终端设备、工业控制中的无线终端设备、无人驾驶中的无线终端设备、远程医疗中的无线终端设备、智能电网中的无线终端设备、智慧城市（smart city）中的无线终端设备、智慧家庭（smart home）中的无线终端设备等等。

25 上述主基站和辅基站可以统称为网络设备。该网络设备包括但不限于：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 Node B, 或 home Node B, HNB）、基带单元（baseband unit, BBU），无线中继节点、无线回传节点、传输点（transmission and reception point, TRP 或者 transmission point, TP）等，还可以为 5G，如，新空口（new radio, NR）系统中的 gNB，或，传输点（TRP 或 TP），5G 系统中的基站的一个或一组（包括多个天线面板）天线面板，或者，还可以为构成 gNB 或传输点的网络节点，如基带单元（baseband unit, BBU），或，分布式单元（distributed unit, 30

DU)、具有基站功能的路边单元(road side unit, RSU)等。

在本申请实施例中,网络设备可以采用集中式单元(centralized unit, CU)-DU架构。也即,网络设备可以由CU和至少一个DU构成。这种情况下,网络设备的部分功能部署在CU上,网络设备的另一部分功能部署在DU上。CU和DU是按照协议栈进行功能切分。作为一种实现方式, CU部署有协议栈中的RRC层,分组数据汇聚层协议(packet data convergence protocol, PDCP)层,以及业务数据适应协议(service data adaptation protocol, SDAP)层; DU部署有协议栈中的无线链路控制(radio link control, RLC)层,媒体接入控制(media access control, MAC)层,以及物理层(physical layer, PHY)。从而, CU具有RRC、PDCP和SDAP的处理能力。DU具有RLC、MAC和PHY的处理能力。可以理解的是,上述功能的切分仅为一个示例,不构成对CU和DU的限定。也就是说, CU和DU之间还可以有其他功能切分的方式,本申请实施例在此不予赘述。

## 2、双连接配置流程

如图1所示,相关技术中提供的一种双连接配置流程包括以下步骤:

15 S10、终端设备通过主基站注册到网络。

可选的,在终端设备注册到网络之后,主基站可以向终端设备下发测量事件,以使得终端设备向主基站上报测量报告。之后,主基站可以根据测量报告,确定是否为终端设备添加辅基站。如果确定为终端设备添加辅基站,主基站可以执行下述步骤S11。

S11、主基站确定为终端设备添加辅基站。

20 S12、主基站向辅基站发送辅节点增加/调整请求(SN addition/modification request)消息。

其中, SN addition/modification request 消息包含辅基站的相关配置信息。

需要说明的是,主基站可以生成辅基站密钥。之后,主基站发送的 SN addition/modification request 消息可以携带辅基站密钥。由于主基站不使用辅基站密钥,因此主基站可以在发送 SN addition/modification request 消息之后,删除辅基站密钥。

25 S13、辅基站向主基站发送辅节点增加/调整请求确认(SN addition/modification request ack)消息。

其中, SN addition/modification request ack 消息用于表示同意使用 SN addition/modification request 消息所携带的配置信息。

30 S14、主基站向终端设备发送RRC重配置消息。

其中, RRC重配置消息用于配置终端设备与辅基站之间的无线承载。

S15、终端设备向主基站发送RRC重配置完成消息。

S16、主基站向辅基站发送辅节点重配置完成(SN reconfiguration complete)消息。

35 之后,终端设备和辅基站可以执行随机接入流程(random access procedure)。在经过随机接入流程之后,终端设备和辅基站之间建立RRC连接。

## 3、 $K_{gNB}$

在5G网络中,  $K_{gNB}$  是终端设备和接入与移动管理功能(access and mobility management function, AMF)分别根据  $K_{AMF}$  推演得到的。AMF在推演得到  $K_{gNB}$  之后,会将  $K_{gNB}$  发送给终端设备所连接的接入网设备。这样一来,终端设备和接入网设备维

护同一个  $K_{gNB}$ ，从而终端设备和接入网设备可以利用  $K_{gNB}$  及其推演出来的密钥进行安全通信。

#### 4、 $K_{eNB}$

- 在 4G 网络中， $K_{eNB}$  是终端设备和移动管理实体 (mobility management entity, MME) 分别根据  $K_{ASME}$  推演得到的。MME 在推演得到  $K_{eNB}$  之后，会将会将  $K_{eNB}$  发送给终端设备所连接的接入网设备。这样一来，终端设备和接入网设备维护同一个  $K_{eNB}$ ，从而终端设备和接入网设备可以利用  $K_{eNB}$  及其推演出来的密钥进行安全通信。

#### 5、安全保护

- 安全保护是指对数据进行加密/解密，和/或完整性保护/校验等处理，以避免数据泄露或者数据被篡改等风险。

1) 加密/解密: 保护数据在传输过程中的机密性 (因此又可以被称作机密性保护)，机密性是指无法被直接看出真实内容。加密保护一般可以使用密钥和加密算法对数据进行加密来实现。

- 2) 完整性保护/校验: 判断消息在传递过程中，其内容是否被更改，也可以用于作为身份验证，以确认消息的来源。

3) 防重放保护/校验: 判断消息是否被重放，以确认消息的新鲜性。

以上是对本申请实施例所涉及的技术术语的介绍，以下不再赘述。

- 相比较于 4G 移动通信系统，5G 移动通信系统针对网络各项性能指标，在全方位上都提出了更严苛的要求。例如，容量指标提升 1000 倍，更广的覆盖需求、超高可靠超低时延等。

- 一方面，为满足 5G 移动通信系统对超高容量的需求，并且考虑到高频载波频率资源丰富，运营商普遍在热点区域利用高频小站进行组网。但是，高频载波传播特性较差，受遮挡衰减严重，覆盖范围不广，故而需要大量密集部署小站。相应地，为这些大量密集部署的小站提供光纤回传的代价很高，施工难度大，因此需要经济便捷的回传方案。另一方面，从广覆盖需求的角度出发，在一些偏远地区提供网络覆盖，光纤的部署难度大，成本高，也需要设计灵活便利的接入和回传方案。

接入回传一体化 (integrated access and backhaul, IAB) 技术为解决上述两个问题提供了思路: 其接入链路 (access link) 和回传链路 (backhaul link) 皆采用无线传输方案，避免光纤部署。

- 在 IAB 网络中，IAB 节点可以为终端设备提供无线接入服务，并通过无线回传链路连接到 IAB 宿主 (donor) 传输用户的业务数据。

- IAB 节点经宿主节点通过有线链路连接到核心网。例如，在独立组网的 5G 架构下，IAB 节点经宿主节点通过有线链路连接到 5G 网络的核心网 (5G core, 5GC)。在非独立组网的 5G 架构下，IAB 节点在控制面经演进型基站 (evolved NodeB, eNB) 连接到演进分组核心网 (evolved packet core, EPC)，在用户面经宿主节点以及 eNB 连接到 EPC。

为了保证 IAB 网络的覆盖性能以及业务传输的可靠性，IAB 网络支持多跳 IAB 节点和多连接 IAB 节点组网。因此，在 IAB 节点服务的终端和宿主节点之间可能存在多条传输路径。在一条传输路径上可能包括多个节点，例如终端、一个或多个 IAB 节点、

宿主节点。IAB 节点之间，以及 IAB 节点和为 IAB 节点服务的宿主节点有确定的层级关系，每个 IAB 节点将为其提供回传服务的节点视为父节点。相应地，每个 IAB 节点可视为其父节点的子节点。

示例性的，如图 2 所示，在 IAB 独立组网场景中，IAB 节点 1 的父节点为宿主节点，IAB 节点 1 又为 IAB 节点 2 和 IAB 节点 3 的父节点，IAB 节点 2 和 IAB 节点 3 均为 IAB 节点 4 的父节点，IAB 节点 5 的父节点为 IAB 节点 2。终端的上行数据包可以经一个或多个 IAB 节点传输至宿主节点后，再由宿主节点发送至移动网关设备（例如 5G 网络中的用户面功能（user plane function, UPF）网元），下行数据包将由宿主节点从移动网关设备处接收后，再经一个或多个 IAB 节点发送至终端。

可以理解的是，在 IAB 网络中，终端和宿主节点之间的一条传输路径上，可以包含一个或多个 IAB 节点。每个 IAB 节点需要维护面向父节点的无线回传链路，还需要维护和子节点的无线链路。若一个 IAB 节点是终端接入的节点，该 IAB 节点和子节点（即终端）之间是无线接入链路。若一个 IAB 节点是为其他 IAB 节点提供回传服务的节点，该 IAB 节点和子节点（即其他 IAB 节点）之间是无线回传链路。示例性的，参见图 2，在路径“终端 1→IAB 节点 4→IAB 节点 3→IAB 节点 1→宿主节点”中。终端 1 通过无线接入链路接入 IAB 节点 4，IAB 节点 4 通过无线回传链路接入 IAB 节点 3，IAB 节点 3 通过无线回传链路接入 IAB 节点 1，IAB 节点 1 通过无线回传链路接入宿主节点。

IAB 节点可以包括移动终端（mobile terminal, MT）以及集中式单元（distributed unit, DU）。IAB 节点所包括的 MT 具有终端设备的部分或者全部功能。当 IAB 节点面向其父节点时，IAB 节点可以被看做是终端设备，也即 IAB 节点扮演 MT 的角色。当 IAB 节点面向其子节点（子节点可能是终端或另一 IAB 节点的终端部分）时，IAB 节点可以被看做是网络设备，也即 IAB 节点扮演 DU 的角色。换言之，一个 IAB 节点可以通过 MT 部分与该 IAB 节点的至少一个父节点之间建立回传连接。一个 IAB 节点的 DU 部分可以为终端设备或其他 IAB 节点的 MT 部分提供接入服务。

IAB 宿主可以是一个具有完整的实体。或者，IAB 宿主还可以是集中式单元（centralized unit, CU）（本文中简称为 Donor-CU，也可以简称为 CU）和分布式单元（distributed unit, DU）（本文中简称为 Donor-DU）分离的形态，也即 IAB 宿主由 Donor-CU 和 Donor-DU 组成。其中，Donor-CU 还可以是用户面（User plane, UP）（本文中简称为 CU-UP）和控制面（Control plane, CP）（本文中简称为 CU-CP）分离的形态，即 Donor-CU 由 CU-CP 和 CU-UP 组成。

本申请实施例中，IAB 宿主可以有其他名称，例如宿主基站、宿主节点、DgNB（即 donor gNB）等，对此不作限定。

在 IAB 节点和 IAB 宿主之间，需要建立 F1 接口。F1 接口还可以被称为 F1\*接口，对此不作限定。F1 接口支持 F1-U（或者说 F1\*-U）的用户面协议和 F1-C（或者说 F1\*-C）的控制面协议。

示例性的，图 3 为本申请实施例提供的 IAB 网络中用户面协议栈的示意图。如图 6 所示，用户面协议栈包括以下协议层中的一个或多个：通用分组无线服务（general packet radio service, GPRS）隧道协议用户面（GPRS tunnelling protocol user plane,

GTP-U), 用户数据报协议 (user datagram protocol, UDP), 因特网协议 (internet protocol, IP), 无线回传链路引入回传适配协议 (Backhaul Adaptation Protocol, BAP), 无线链路控制 (radio link control, RLC), 媒体接入控制 (media access control, MAC), 物理层 (PHY layer)。图 3 中, L2 层可以为开放式通信系统互联 (open systems interconnection, OSI) 参考模型中的数据链路层, L1 层可以为物理层。

示例性的, 图 4 为本申请实施例提供的 IAB 网络中控制面协议栈的示意图。如图 4 所示, 控制面协议栈包括以下协议层中的一个或多个: F1 应用协议 (F1 application protocol, F1AP), 流控传输协议 (stream control transport protocol, SCTP), IP, BAP, RLC, MAC, PHY 等。

为了保护 F1 接口的安全, IAB 节点和 IAB 宿主之间可以建立互联网安全协议 (internet protocol security, IPSec) 安全连接。其中, 互联网密钥交换 (internet key exchange, IKE) V2 协议中支持使用预共享密钥 (pre-shared secret key, PSK) 的方式来进行安全认证。例如, IAB 节点和 IAB 宿主可以提前配置好 PSK, 在后续 IPSec 建立过程中作为认证凭证来使用。当前, 为了省去预配置 PSK 的过程, 实现 IAB node 与 IAB donor 的即插即用, IAB node 与 IAB donor 可以通过计算  $K_{IAB}$  来作为 PSK。

当前, 为了保障网络的覆盖性能以及业务传输可靠性的要求, 可以使 IAB node 支持双连接 (dual connectivity, DC), 以应对无线回传链路可能发生的异常情况, 例如无线回程链路中断或者阻塞等。

图 5 为 IAB node 采用 EN-DC 模式的示意图。如图 5 所示, 当 IAB node 工作在 EN-DC 模式时, 4G 基站 (也即 eNB) 作为主基站, IAB donor 作为辅基站。MeNB 与 IAB node 的 MT 之间有 LTE Uu 空口连接, MeNB 与 IAB donor-CU-CP 之间有 X2-C 接口连接, MeNB 通过 S1 接口连接到 4G 核心网 (evolved packet core, EPC)。可选的, IAB donor-CU-UP 可以通过 S1-U 接口连接到 EPC, 例如连接到业务网关 (serving gateway, SGW)。

目前, 在 IAB node 采用 EN-DC 模式的场景下, 如图 6 所示, IAB node 与 IAB donor 生成  $K_{IAB}$  的流程包括以下步骤:

S20、IAB node 通过 MeNB 接入核心网。

应理解, 在 IAB node 接入核心网之后, IAB node 和 MeNB 均存储相同的  $K_{eNB}$ 。

S21、在 MeNB 生成 S-Kgnb 之后, MeNB 向 IAB donor 发送 SN additional/modification request 消息。

其中, SN additional/modification request 消息包括 S-Kgnb。S-Kgnb 是根据  $K_{eNB}$  推演得到的。

可以理解的是, MeNB 在将 S-Kgnb 发送给辅基站后, 可选删除 S-Kgnb。也即, MeNB 计算 S-Kgnb 的目的是发给辅基站使用, 而 MeNB 并不使用 S-Kgnb。

S22、IAB donor 向 MeNB 发送 SN additional/modification request ACK 消息。

S23、MeNB 向 IAB node 发送 RRC 重配置消息。

应理解, 在接收到 RRC 重配置消息之后, IAB node 可以根据  $K_{eNB}$  推演得到 S-Kgnb。

S24、IAB node 向 MeNB 发送 RRC 重配置完成消息。

S25、MeNB 向 IAB donor 发送 SN reconfiguration complete 消息。

S26、IAB node 根据 S-Kgnb, 生成 IAB 密钥。

S27、IAB donor 根据 S-Kgnb, 生成 IAB 密钥。

在 EN-DC 模式下, IAB donor 能且只能是辅基站, 所以生成 IAB 密钥的输入密钥可以为 S-Kgnb, 即辅基站使用 S-Kgnb 推演 IAB 密钥。

5 这样一来, IAB node 和 IAB donor 能够以相同的 IAB 密钥作为认证凭证, 建立安全隧道。

但是, 随着通信技术的发展, IAB node 也可以采用其他类型的双连接(例如 NE-DC、NR-DC、NGEN-DC 等)。

图 7 为 IAB node 采用 NE-DC 模式的示意图。如图 7 所示, 当 IAB node 工作在  
10 NE-DC 模式时, IAB donor CU-UP 通过 NG-U 接口连接到 5G 核心网(5G core, 5GC)中的用户面网元, IAB donor CU-CP 通过 NG-C 接口连接到 5GC 中的控制面网元。SeNB 与 IAB node 中的 MT 之间有 LTE Uu 空口连接。IAB donor CU-CP 与 SeNB 之间有 X2-C 接口。

图 8 为 IAB node 采用 NR-DC 模式的示意图。如图 8 所示, 当 IAB node 工作在  
15 NR-DC 模式时, IAB node 连接一个 IAB donor 和一个 gNB。其中, IAB donor CU-UP 通过 NG-U 接口连接到 5GC 中的用户面网元, IAB donor CU-CP 通过 NG-C 接口连接到 5GC 中的控制面网元。gNB 与 IAB node 中的 MT 之间有 NR Uu 接口。

图 9 为 IAB node 采用 NGEN-DC 模式的示意图。如图 9 所示, 当 IAB node 工作在 NGEN-DC 时, IAB node 连接的主基站为 NG-eNB, IAB node 连接的辅基站为 IAB  
20 donor。其中, IAB donor CU-UP 通过 NG-U 接口连接到 5GC 中的用户面网元。IAB node 中的 MT 与 NG-eNB 之间有 LTE Uu 接口。

目前, 对于除了 EN-DC 之外的其他类型的双连接, 业界并未提供 IAB node 与 IAB donor 生成  $K_{IAB}$  的技术方案。这样一来, 可能会导致 IAB node 生成的  $K_{IAB}$  与 IAB donor 生成的  $K_{IAB}$  不相同, 从而使得 IAB node 与 IAB donor 之间不能正常建立 IPsec 安全连接。  
25

举例来说, 假设 IAB node 采用 NR-DC 接入网络中, 主基站和辅基站均为 gNB。IAB donor 可能为主基站, 也可能为辅基站。IAB node 根据 IP 地址与 IAB donor 建立连接, 但无需感知 IAB donor 为主基站还是辅基站。这样一来, 在 IAB donor 为辅基站的情况下, IAB donor 可能采用辅基站密钥来计算 IAB 密钥, 而 IAB node 可能采用  
30 主基站密钥来计算 IAB 密钥, 从而导致 IAB donor 和 IAB node 各自维护的 IAB 密钥不相同。又或者, 在 IAB donor 为主基站的情况下, IAB donor 可能采用主基站密钥来计算 IAB 密钥, 而 IAB node 可能采用辅基站密钥来计算 IAB 密钥, 从而导致 IAB donor 和 IAB node 各自维护的 IAB 密钥不相同。

为了解决上述技术问题, 本申请实施例提供三个技术方案。下面先对三个技术方案的思路进行介绍。  
35

技术方案一的思路在于: 对于除了 EN-DC 之外的其他类型的双连接(例如 NE-DC、NR-DC 或者 NGEN-DC)的场景下, IAB donor 和 IAB node 均采用主基站密钥来计算  $K_{IAB}$ 。

技术方案二的思路在于: 对于除了 EN-DC 之外的其他类型的双连接(例如 NE-DC、

NR-DC 或者 NGEN-DC) 的场景下, IAB donor 和 IAB node 均采用辅基站密钥来计算  $K_{IAB}$ 。

技术方案三的思路在于: 对于除了 EN-DC 之外的其他类型的双连接(例如 NE-DC、NR-DC 或者 NGEN-DC) 的场景下, IAB donor 和 IAB node 均根据 IAB donor 的本地  
5 密钥来计算  $K_{IAB}$ 。其中, 若主基站为 IAB donor, 则上述本地密钥为主基站密钥; 若辅基站为 IAB donor, 则本地密钥为辅基站密钥。

上述技术方案一至技术方案三, 均能保证 IAB donor 和 IAB node 维护相同的  $K_{IAB}$ 。应理解, 在实际应用中, 可以从上述技术方案一至技术方案三中选择任意一个技术方案来执行。

10 示例性的, 主基站密钥用于对主基站(例如下文中的第一接入网设备)与第一设备之间的通信进行安全保护。例如, 主基站密钥可以为  $K_{gNB}$ 、 $K_{RRCCint}$ 、 $K_{RRCCenc}$ 、 $K_{UPint}$ 、或者  $K_{UPenc}$  等。其中,  $K_{RRCCint}$ 、 $K_{RRCCenc}$ 、 $K_{UPint}$  和  $K_{UPenc}$  均是通过  $K_{gNB}$  推演得到的。 $K_{RRCCint}$  用于对主基站与第一设备之间的 RRC 信令进行完整性保护。 $K_{RRCCenc}$  用于对主基站与第一设备之间的 RRC 信令进行加密保护。 $K_{UPint}$  用于对主基站与第一设备之间的  
15 用户面数据进行完整性保护。 $K_{UPenc}$  用于对主基站与第一设备之间的用户面数据进行加密保护。在此对主基站密钥进行统一说明, 以下不再赘述。

示例性的, 辅基站密钥用于对辅基站(例如下文中的第二接入网设备或者第三接入网设备)和第一设备之间的通信进行安全保护。例如, 辅基站密钥可以为  $K_{Sb}$ 、 $S-K_{RRCCint}$ 、 $S-K_{RRCCenc}$ 、 $S-K_{UPint}$ 、或者  $S-K_{UPenc}$  等, 对此不作限定。 $S-K_{RRCCint}$ 、 $S-K_{RRCCenc}$ 、  
20  $S-K_{UPint}$ 、或者  $S-K_{UPenc}$  均通过  $K_{Sb}$  推演得到。 $S-K_{RRCCint}$  用于对辅基站与第一设备之间的 RRC 信令进行完整性保护。 $S-K_{RRCCenc}$  用于对辅基站与第一设备之间的 RRC 信令进行加密保护。 $S-K_{UPint}$  用于对辅基站与第一设备之间的用户面数据进行完整性保护。 $S-K_{UPenc}$  用于对辅基站与第一设备之间的用户面数据进行加密保护。在此对主基站密钥进行统一说明, 以下不再赘述。

25 下面结合说明书附图对三个实施例的具体实现方式进行详细说明。需要说明的是, 下述实施例中各个消息/信息的名称仅是一个示例, 具体实现中可以是其他的名称, 对此不作限定。

#### 技术方案一

在除了 EN-DC 之外的其他类型的双连接场景下, 网络侧可参照图 10 所示的实施例来获取 IAB 密钥, IAB node 可参照图 11 所示的实施例来获取 IAB 密钥。  
30

如图 10 所示, 为本申请实施例提供的一种密钥生成方法, 该方法包括以下步骤:

S101、第一接入网设备确定通过第一接入网设备注册到 5G 核心网的第一设备为 IAB node。

作为一种可能的实现方式, 第一接入网设备接收到第一设备发送的 IAB 指示信息, IAB 指示信息用于指示第一设备为 IAB node。从而, 第一接入网设备根据 IAB 指示信息, 可以获知第一设备为 IAB node。  
35

示例性的, IAB 指示信息可以记为 “IAB-indication”。

作为另一种可能的实现方式, 第一接入网设备接收到核心网网元的 IAB 授权信息, IAB 授权信息用于指示第一设备具有作为 IAB node 的权限。从而, 第一接入网设备根

据 IAB 授权信息，可以获知第一设备为 IAB node。

示例性的，IAB 授权信息可以记为 “IAB-authorized”。

应理解，核心网网元可以主动地向第一接入网设备发送 IAB 授权信息。或者，核心网网元可以根据第一接入网设备的请求，校验第一设备的签约数据，确定是否向第一接入网设备回复 IAB 授权信息。

应理解，在第一设备注册到 5G 核心网的过程中，第一接入网设备和第一设备均能获取到相同的主基站密钥。

S102、在需要为第一设备选择辅基站的情况下，第一接入网设备判断自身是否具备 IAB donor 功能。

10 作为一种可能的实现方式，第一接入网设备查找 IAB donor 配置信息中是否存在第一接入网设备的标识。当 IAB donor 配置信息存在第一接入网设备的标识时，第一接入网设备确定自身具备 IAB donor 功能。当 IAB donor 配置信息不存在第一接入网设备的标识时，第一接入网设备确定自身不具备 IAB donor 功能。

15 其中，IAB donor 配置信息用于记录一个或多个具备 IAB donor 功能的接入网设备的标识。可选的，IAB donor 配置信息可以是操作维护管理（operation administration and maintenance）系统或者其他设备配置给第一接入网设备的。

作为另一种可能的实现方式，第一接入网设备可以检查自身是否存储有 donor 配置文件。在第一接入网设备存储有 donor 配置文件时，第一接入网设备可以确定自身具备 IAB donor 功能。否则，第一接入网设备确定自身不具备 IAB donor 功能。

20 应理解，上述 donor 配置文件用于配置接入网设备作为 IAB donor 时的功能。Donor 配置文件可以是第一接入网设备本地配置的，或者 OAM 系统配置给第一接入网设备的。

25 可选的，当第一接入网设备不具备 IAB donor 功能时，第一接入网设备执行下述步骤 S103-S106。当第一接入网设备具备 IAB donor 功能时，第一接入网设备执行下述步骤 S107-S109。

S103、在第一接入网设备不具备 IAB donor 功能的情况下，第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站。

30 作为一种可能的实现方式中，第二设备预先为第一接入网设备配置了第二接入网设备的标识。从而，在需要为 IAB node（例如第一设备）添加辅基站的情况下，第一接入网设备可以根据第二接入网设备的标识，选择第二接入网设备作为辅基站。

35 作为一种可能的实现方式，第一接入网设备向第二设备发送第一请求消息，该第一请求消息包括第一设备的标识。第二设备根据第一请求消息，可以确定作为第一设备的 IAB donor 的接入网设备（也即第二接入网设备）。之后，第一接入网设备接收第二设备发送的第一响应消息，第一响应消息包括第二接入网设备的标识。从而，第一接入网设备可以选择第二接入网设备作为第一设备的辅基站。

可选的，上述第一设备的标识可以包括小区无线网络临时标识（cell-radio network temporary identifier, C-RNTI），设备编号等，对此不作限定。

可选的，上述第二接入网设备的标识可以包括 IP 地址、设备编号等，对此不作限定。

可选的，上述第二设备可以为 OAM 系统或者核心网网元，对此不作限定。

需要说明的是，第二设备根据第一请求消息，确定第二接入网设备，存在以下两种情况：

情况 1、第二设备已经预先存储第一设备与第二接入网设备之间的映射关系。从而，第二设备根据第一设备的标识，以及第一设备与第二接入网设备之间的映射关系，可以查找到第二接入网设备的标识。

情况 2、第二设备未存储第一设备与第二接入网设备之间的映射关系。从而，第二设备可以根据拓扑信息等因素，确定第二接入网设备。

应理解，由于第二设备负责确定第二接入网设备，因此第二设备可以向第一设备发送第二接入网设备用于与 IAB node 通信的 IP 地址，以便于第一设备与第二接入网设备之间能够根据 IP 地址进行通信。

在本申请实施例中，第一接入网设备在选择第二接入网设备作为辅基站之后，会向第二接入网设备发送辅基站配置消息，以使得第二接入网设备获知自身作为第一设备的辅基站。示例性的，辅基站配置消息可以为图 1 所示的双连接配置流程中的 SN addition/modification request 消息。

可选的，在第一设备为 IAB node 的情况下，辅基站配置消息可以包括第三指示信息，第三指示信息用于指示第一设备为 IAB node。从而，第二接入网设备可以根据第三指示信息，获知第一设备为 IAB node。

对于第二接入网设备来说，在辅基站配置消息包括第三指示信息的情况下，第二接入网设备判断自身是否具备 IAB donor 功能。在第二接入网设备确定自身具备 IAB donor 功能的情况下，第二接入网设备需要从第一接入网设备获取  $K_{IAB1}$ 。

其中，第二接入网设备判断自身是否具备 IAB donor 功能的具体实现方式可以参考上文中第一接入网设备判断自身是否具备 IAB donor 功能的具体实现方式，在此不再赘述。

S104、第一接入网设备获取与第二接入网设备关联的第一密钥输入参数。

其中，第一密钥输入参数包括：第一 IP 地址和/或第二 IP 地址。

第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址。由于第一设备作为 IAB node，因此第一 IP 地址也可以被称为 IAB node 的 IP 地址，或者 IAB node 中 MT 的 IP 地址。

第二 IP 地址为第二接入网设备用于与 IAB node 通信的 IP 地址。由于第二接入网设备作为第一设备的 IAB donor，因此第二 IP 地址也可以被称为 IAB donor 的 IP 地址，或者 IAB donor 中 CU 的 IP 地址。

可选的，第一接入网设备获取第一 IP 地址，可以采用以下实现方式 1-1 或者实现方式 1-2 中的任意一种：

实现方式 1-1、第一接入网设备从第二设备获取到第一 IP 地址。

例如，在第一设备的 IP 地址是由第二设备负责分配的情况下，第二设备向第一接入网设备发送的第一响应消息还可以包括第一 IP 地址。

实现方式 1-2、第一接入网设备从第二接入网设备获取到第一 IP 地址。

例如，第一接入网设备向第二接入网设备发送第一指示信息，第一指示信息用于

请求第一 IP 地址。之后，第一接入网设备接收第二接入网设备发送的第一 IP 地址。

示例性的，第一指示信息可以承载于新增的信令中。或者，第一指示信息可以承载于现有的信令中，例如 SN addition/modification request 消息。

- 示例性的，第二接入网设备发送的第一 IP 地址可以承载于新增的信令中。或者，  
5 第二接入网设备发送的第一 IP 地址可以承载于现有的信令中，例如 SN addition/modification request ACK 消息。

可选的，第一接入网设备获取第二 IP 地址，可以采用以下实现方式 2-1 至实现方式 2-3 中的任意一种：

- 实现方式 2-1、第一接入网设备从第二设备获取到第二 IP 地址。  
10 例如，若第二设备存储具备 IAB donor 功能的各个接入网设备的 IP 地址，则第二设备存储有第二 IP 地址。因此，第二设备向第一接入网设备发送的第一响应消息还可以包括第二 IP 地址。

实现方式 2-2、第一接入网设备可以以第二接入网设备的 Xn 接口的 IP 地址作为第二 IP 地址。

- 15 应理解，实现方式 2-2 一般基于通信系统默认接入网设备的 Xn 接口的 IP 地址即为接入网设备作为 IAB donor 时的 IP 地址。

实现方式 2-3、第一接入网设备从第二接入网设备获取到第二 IP 地址。

例如，第一接入网设备向第二接入网设备发送第二指示信息，第二指示信息用于请求第二 IP 地址。第一接入网设备接收第二接入网设备发送的第二 IP 地址。

- 20 示例性的，第二指示信息可以承载于新增的信令中。或者，第二指示信息可以承载于现有的信令中，例如 SN addition/modification request 消息。

- 应理解，第二指示信息和第一指示信息可以承载于同一信令中，或者不同信令中。当第二指示信息和第一指示信息承载于同一信令时，第二指示信息和第一指示信息可以集成为一个指示信息，例如参数请求指示信息（para\_request\_indicator）。从而，参  
25 数请求指示信息用于请求 IAB donor 的 IP 地址和 IAB node 的 IP 地址。

示例性的，第二接入网设备发送的第二 IP 地址可以承载于新增的信令中。或者，第二接入网设备发送的第二 IP 地址可以承载于现有的信令中，例如 SN addition/modification request ACK 消息。

- 30 S105、第一接入网设备根据第一密钥输入参数和主基站密钥，生成第一 IAB 密钥  $K_{IAB1}$ 。

其中， $K_{IAB1}$  用于建立第二接入网设备与第一设备之间的安全隧道。

S106、第一接入网设备向第二接入网设备发送  $K_{IAB1}$ 。

- 一种可能的设计中， $K_{IAB1}$  可以承载于一条新增的消息中。示例性的，结合图 1 所示的双连接配置流程进行举例说明，新增的用于承载  $K_{IAB1}$  的消息的发送时机可以位于  
35 于 SN additional/modification Request ACK 消息之后，或者位于 SN reconfiguration complete 消息之后。

另一种可能的设计中， $K_{IAB1}$  可以承载于现有的消息中。示例性的，结合图 1 所示的双连接配置流程进行举例说明，第一接入网设备可以向第二接入网设备发送 SN reconfiguration complete 消息，该 SN reconfiguration complete 消息包括  $K_{IAB1}$ 。

应理解, 第二接入网设备在接收到  $K_{IAB1}$  之后, 会保存  $K_{IAB1}$ 。

基于上述步骤 S103-S106, 在辅基站 (也即第二接入网设备) 作为 IAB donor 的情况下, 主基站 (也即第一接入网设备) 能够主动地以主基站密钥生成  $K_{IAB}$ , 并将该  $K_{IAB}$  发送给辅基站, 以保证 IAB donor 和 IAB node 维护相同的  $K_{IAB}$ 。

- 5 S107、在第一接入网设备具备 IAB donor 功能的情况下, 第一接入网设备选择第三接入网设备作为第一设备的辅基站。

作为一种可能的实现方式中, 第一接入网设备根据第一设备的位置、第一设备的测量报告等因素, 从周围的接入网设备中选择合适的接入网设备 (也即第三接入网设备) 作为第一设备的辅基站。

- 10 应理解, 本申请实施例对第三接入网设备是否具备 IAB donor 功能不进行限定。

也即, 第三接入网设备可以具备 IAB donor 功能, 也可以不具备 IAB donor 功能。

这种情况下, 具备 IAB donor 功能的第一接入网设备即作为第一设备的 IAB donor。

S108、第一接入网设备获取与第一接入网设备关联的第二密钥输入参数。

其中, 第二密钥输入参数包括第一 IP 地址和第三 IP 地址。

- 15 第三 IP 地址为第一接入网设备用于与 IAB node 通信的 IP 地址。

应理解, 第一接入网设备可以从本地 (也即第一接入网设备的数据库) 获取第三 IP 地址。

一种可能的设计中, 作为 IAB donor 的第一接入网设备为第一设备分配第一 IP 地址。基于该设计, 第一接入网设备还需要向第一设备发送第一 IP 地址。

- 20 另外一种可能的设计中, 在第二设备为第一设备分配第一 IP 地址的情况下, 第一接入网设备可以从第二设备或者第一设备获取第一 IP 地址。

示例性的, 第一接入网设备向第一设备发送 IP 地址请求消息。之后, 第一接入网设备接收第一设备发送的 IP 地址通知消息, IP 地址通知消息包括第一 IP 地址。

- 25 S109、第一接入网设备根据第二密钥输入参数和主基站密钥, 生成第二 IAB 密钥  $K_{IAB2}$ 。

其中,  $K_{IAB2}$  用于建立第一接入网设备与第一设备之间的安全隧道。

应理解, 第一接入网设备在生成  $K_{IAB2}$  之后, 会保存该  $K_{IAB2}$ 。

- 30 基于上述步骤 107-S109, 在主基站 (也即第一接入网设备) 作为 IAB donor 的情况下, 主基站主动地以主基站密钥生成  $K_{IAB}$ , 以保证 IAB donor 和 IAB node 维护相同的  $K_{IAB}$ 。

如图 11 所示, 为本申请实施例提供的一种密钥生成方法, 该方法应用于第一设备 (IAB node) 连接主基站和辅基站的场景下。该方法包括以下步骤:

S201、IAB node 根据主基站支持的通信制式、辅基站支持的通信制式以及核心网支持的通信制式, 确定双连接的类型。

- 35 可选的, IAB node 确定主基站支持的通信制式, 可以具体实现为: 支持的通信制式。其中, 广播消息中的配置参数包括以下一项或者多项: 基站标识、逻辑小区标识、物理小区标识、上行频段或者下行频段。应理解, 当广播消息中的配置参数属于 5G 通信系统的配置参数时, IAB node 可以确定主基站支持 5G 通信制式。或者, 当广播消息中的配置参数属于 4G 通信系统的配置参数时, IAB node 可以确定主基站支持 4G

通信制式。

举例来说,假设 4G 频点为 A1、A2、A3,5G 频点为 B1、B2、B3。当主基站发送的广播消息中频点为 B1,IAB node 可以确定主基站支持 5G 通信制式。

可选的,IAB node 确定辅基站支持的通信制式,可以具体实现为:IAB node 接收主基站发送的 RRC 重配置消息,该 RRC 重配置消息用于配置 IAB node 和辅基站之间的无线承载,RRC 重配置消息包括辅小区组配置信息。IAB node 根据辅小区组配置信息,确定辅基站支持的通信制式。应理解,当辅小区组配置信息属于 5G 通信制式时,IAB node 可以确定辅基站支持 5G 通信制式。或者,当辅小区组配置信息属于 4G 通信制式时,IAB node 可以确定辅基站支持 4G 通信制式。

示例性的,属于 5G 通信制式的辅小区组配置信息可以记为 nr-SecondaryCellGroupConfig 或者 sourceSCG-NR-Config。属于 4G 通信制式的辅小区组配置信息可以记为 sourceSCG-EUTRA-Config。

可选的,IAB node 确定核心网支持的通信制式,可以具体实现为:IAB node 接收主基站发送的广播消息。IAB node 根据广播消息中的小区配置信息,确定核心网支持的通信制式。应理解,若广播消息中的小区配置信息属于 5G 通信制式,则 IAB node 确定核心网支持 5G 通信制式。若广播消息中的小区配置信息属于 4G 通信制式,则 IAB node 确定核心网支持 4G 通信制式。

示例性的,小区配置信息可以包括小区接入相关信息 (cellAccessRelatedInfo)。属于 5G 通信制式的小区接入相关信息可以记为 cellAccessRelatedInfo-5GC。属于 4G 通信制式的小区接入相关信息可以记为 cellAccessRelatedInfo-EUTRA-EPC。

可选的,IAB node 确定双连接的类型,包括以下情况之一:

情况 1、当主基站支持 5G 通信制式,辅基站支持 4G 通信制式,核心网支持 5G 通信制式时,IAB node 确定双连接的类型为 NE-DC。

情况 2、当主基站支持 4G 通信制式,辅基站支持 5G 通信制式,核心网支持 5G 通信制式时,IAB node 确定双连接的类型为 NGEN-DC。

情况 3、当主基站支持 5G 通信制式,辅基站支持 5G 通信制式,核心网支持 5G 通信制式时,IAB node 确定双连接的类型为 NR-DC。

情况 4、当主基站支持 4G 通信制式,辅基站支持 5G 通信制式,核心网支持 4G 通信制式时,IAB node 确定双连接的类型为 EN-DC。

S202、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时,IAB node 根据主基站密钥,生成  $K_{IAB}$ 。

作为一种可能的实现方式,IAB node 根据主基站密钥和密钥输入参数,生成  $K_{IAB}$ 。

其中,密钥输入参数包括 IAB donor 的 IP 地址和 IAB node 的 IP 地址。

可选的,IAB node 可以从第二设备获取到 IAB donor 的 IP 地址。示例性的,第二设备可以为 OAM 系统或者核心网网元。

可选的,在 IAB node 的 IP 地址由第二设备分配的情况下,IAB node 可以从第二设备获取到 IAB node 的 IP 地址。这种情况下,第二设备可以将 IAB node 的 IP 地址和 IAB donor 的 IP 地址封装到一条消息中,并将该消息发送给 IAB node。

可选的,在 IAB node 的 IP 地址由 IAB donor 分配的情况下,IAB node 可以从主

基站或者辅基站获取到 IAB node 的 IP 地址。

例如,主基站作为 IAB donor,并且主基站为 IAB node 分配 IP 地址。从而,IAB node 向主基站发送 IP 地址请求消息;之后,IAB node 接收主基站发送的 IP 地址通知消息,该 IP 地址通知消息包括 IAB node 的 IP 地址。

- 5 又例如,主基站作为 IAB donor,并且主基站为 IAB node 分配 IP 地址。从而,IAB node 接收主基站发送的 RRC 重配置消息,该 RRC 重配置消息包括 IAB node 的 IP 地址。

- 10 又例如,辅基站作为 IAB donor,并且辅基站为 IAB node 分配 IP 地址。从而,IAB node 可以向辅基站发送 IP 地址请求消息;之后,IAB node 接收辅基站发送的 IP 地址通知消息,该 IP 地址通知消息包括 IAB node 的 IP 地址。

应理解,IAB node 在生成  $K_{IAB}$  之后,会保存  $K_{IAB}$ 。

- 15 基于图 11 所示的实施例,IAB node 可以根据主基站支持的通信制式、辅基站支持的通信制式以及核心网支持的通信制式,准确确定 IAB node 使用的双连接的类型。进而,当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时,IAB node 可以根据主基站密钥生成  $K_{IAB}$ ,以保证 IAB donor 和 IAB node 维护相同的  $K_{IAB}$ 。

应理解,当双连接的类型为 EN-DC 时,IAB node 根据辅基站密钥和密钥输入参数,生成  $K_{IAB}$ 。

下面结合具体应用场景以举例的方式来对技术方案一进行详细说明。

- 20 场景 1、第一设备(也即 IAB node)通过不具备 IAB donor 功能的第一接入网设备注册到网络。之后,第一接入网设备为第一设备选择具备 IAB donor 功能的第二接入网设备作为辅基站,并且第二接入网设备负责为第一设备分配 IAB node 的 IP 地址。

基于场景 1,如图 12 所示,为本申请实施例提供的一种密钥生成方法,该方法包括以下步骤:

- 25 S301、第一设备通过第一接入网设备注册到网络。  
在注册到网络的过程中,第一设备可以执行鉴权、安全上下文协商等流程。  
在第一设备的注册过程中,第一设备和第一接入网设备获取到相同的 AS 层密钥。第一设备与第一接入网设备之间的 AS 层密钥用于对第一设备与第一接入网设备之间的 AS 层通信进行安全保护。在双连接场景下,由于第一接入网设备作为第一设备的主基站,因此第一设备和第一接入网设备之间的 AS 层密钥可以被称为主基站密钥。  
30 S302、第一接入网设备确定第一设备为 IAB node。  
S303、在需要为第一设备选择辅基站的情况下,第一接入网设备判断自身是否具备 IAB node 功能。  
S304、在第一接入网设备不具备 IAB node 功能的情况下,第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站。  
35 S305、第一接入网设备向第二接入网设备发送 SN addition/modification request 消息。

其中,SN addition/modification request 消息包括第三指示信息。第三指示信息用于指示第一设备为 IAB node。

这样一来,第二接入网设备能够基于第三指示信息,获知第一设备为 IAB node。

进而，由于第二接入网设备具有 IAB donor 功能，因此第二接入网设备可以作为第一设备的 IAB donor，并为第一设备分配 IAB node 的 IP 地址。应理解，这里的 IAB node 的 IP 地址即为图 10 所示实施例中的第一 IP 地址。

5 可选的，SN addition/modification request 消息除了包括现有技术中的相关信元之外，还可以包括第一指示信息和第二指示信息。

S306、第一接入网设备接收第二接入网设备发送的 SN addition/modification request ACK 消息。

10 可选的，在 SN addition/modification request 消息包括第一指示信息和第二指示信息的情况下，SN addition/modification request ACK 消息包括 IAB donor 的 IP 地址和 IAB node 的 IP 地址。

S307、第一接入网设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

S308、第一接入网设备向第一设备发送 RRC 重配置消息。

其中，RRC 重配置消息包括 IAB node 的 IP 地址。

15 S309、第一接入网设备接收第一设备发送的 RRC 重配置完成消息。

S310、第一接入网设备向第二接入网设备发送 SN reconfiguration complete 消息。

其中，SN reconfiguration complete 消息包括  $K_{IAB}$ 。

应理解，第二接入网设备从 SN reconfiguration complete 消息获取到  $K_{IAB}$ 。之后，第二接入网设备会保存  $K_{IAB}$ 。

20 S311、第一设备接收第二设备发送的 IP 地址通知（IP address notification）消息。

其中，IP 地址通知消息包括 IAB donor 的 IP 地址。

应理解，步骤 S311 的执行时机仅在步骤 S304 之后，不对步骤 S312 的具体执行时机进行限定。例如，步骤 S311 的执行时机可以位于步骤 S310 之前。

S312、第一设备确定双连接的类型。

25 S313、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

其中，步骤 S312-S313 的具体实现细节可以参考图 11 所示的实施例，在此不再赘述。另外，步骤 S312-S313 可以在步骤 S308 之后的任意时刻执行，本申请实施例对此不作限定。

30 S314、第一设备和第二接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 12 所示的实施例，在辅基站作为 IAB donor 的情况下，主基站以主基站密钥生成  $K_{IAB}$ ，并将  $K_{IAB}$  发送给辅基站。IAB node 以主基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

35 场景 2、第一设备（也即 IAB node）通过不具备 IAB donor 功能的第一接入网设备注册到网络。之后，第一接入网设备为第一设备选择具备 IAB donor 功能的第二接入网设备作为辅基站。第二设备负责为第一设备分配 IAB node 的 IP 地址。

基于场景 2、如图 13 所示，为本申请实施例提供的一种密钥生成方法，该方法包括以下步骤：

S401-S404、与步骤 S301-S304 相同，其具体描述可以参考图 12 所示的实施例，在此不再赘述。

S405、第一设备接收第二设备发送的第一 IP 地址通知消息。

其中，第一 IP 地址通知消息包括 IAB donor 的 IP 地址和 IAB node 的 IP 地址。

- 5 应理解，本申请实施例不限制步骤 S405 与步骤 S406-S410 之间的执行顺序。也即，步骤 S405 可以在步骤 S406-S410 中的任意一个步骤之前或者之后执行。

S406、第一接入网设备向第二接入网设备发送 SN addition/modification request 消息。

- 10 其中，SN addition/modification request 消息包括第三指示信息。第三指示信息用于指示第一设备为 IAB node。

可选的，SN addition/modification request 消息除了包括现有技术中的相关信元之外，还可以包括第一指示信息和第二指示信息。

S407、第一接入网设备接收第二接入网设备发送的 SN addition/modification request ACK 消息。

- 15 S408、第一接入网设备向第一设备发送 RRC 重配置消息。

S409、第一接入网设备接收第一设备发送的 RRC 重配置完成消息。

S410、第一接入网设备向第二接入网设备发送 SN reconfiguration complete 消息。

S411、第一设备向第二接入网设备发送第二 IP 地址通知消息。

其中，第二 IP 地址通知消息包括 IAB node 的 IP 地址。

- 20 S412、第二接入网设备向第一接入网设备发送 SN key request 消息。

其中，SN key request 消息用于请求  $K_{IAB}$ 。

SN key request 消息包括 IAB donor 的 IP 地址和 IAB node 的 IP 地址。

S413、第一接入网设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

- 25 S414、第一接入网设备向第二接入网设备发送 SN key response 消息。

其中，SN key response 消息包括  $K_{IAB}$ 。

S415、第一设备确定双连接的类型。

S416、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

- 30 S417、第一设备和第二接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 13 所示的实施例，在辅基站作为 IAB donor 的情况下，主基站以主基站密钥生成  $K_{IAB}$ ，并将  $K_{IAB}$  发送给辅基站。IAB node 以主基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

- 35 场景 3、第一设备（也即 IAB node）通过具备 IAB donor 功能的第一接入网设备注册到网络。从而，第一接入网设备作为第一设备的 IAB donor，并且第一接入网设备为第一设备分配 IAB node 的 IP 地址。第一接入网设备为第一设备选择第三接入网设备作为辅基站。

基于场景 3，如图 14 所示，为本申请实施例提供的一种密钥生成方法，该方法包

括以下步骤：

S501、第一设备通过第一接入网设备注册到网络。

S502、第一接入网设备确定第一设备为 IAB node。

5 S503、在第一接入网设备具备 IAB node 功能的请下，第一接入网设备向第二设备发送通知消息。

其中，通知消息用于表示第一设备通过具备 IAB donor 功能的第一接入网设备注册到网络中。或者说，通知消息用于表示第一接入网设备作为第一设备的 IAB donor。

可选的，通知消息可以包含第一设备的标识和第一接入网设备的标识。

S504、第二设备向第一设备发送 IP 地址通知消息。

10 其中，IP 地址通知信息包括 IAB donor 的 IP 地址。

应理解，步骤 S504 可以在步骤 S513 之前的任意时刻执行，本申请实施例对此不作限定。

S505、第一接入网设备选择第三接入网设备作为第一设备的辅基站。

15 S506、第一接入网设备向第三接入网设备发送 SN addition/modification request 消息。

S507、第一接入网设备接收第三接入网设备发送的 SN addition/modification request ACK 消息。

S508、第一接入网设备向第一设备发送 RRC 重配置消息。

20 由于第一接入网设备作为 IAB donor 负责为第一设备分配 IAB node 的 IP 地址，因此 RRC 重配置消息可以包括 IAB node 的 IP 地址。

S509、第一接入网设备接收第一设备发送的 RRC 重配置完成消息。

S510、第一接入网设备向第三接入网设备发送 SN reconfiguration complete 消息。

S511、第一接入网设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

25 应理解，本申请实施例不限制步骤 S511 与步骤 S504-S510 之间的执行顺序。也即，步骤 S511 可以在步骤 S504-S510 中的任意一个步骤之前或者之后执行。

S512、第一设备确定双连接的类型。

S513、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

30 S514、第一设备和第一接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 14 所示的实施例，在主基站作为 IAB donor 的情况下，主基站和 IAB node 均以主基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

35 场景 4、第一设备（也即 IAB node）通过具备 IAB donor 功能的第一接入网设备注册到网络。从而，第一接入网设备作为第一设备的 IAB donor。第一接入网设备为第一设备选择第三接入网设备作为辅基站。第二设备负责为第一设备分配 IAB node 的 IP 地址。

基于场景 4，如图 15 所示，为本申请实施例提供的一种密钥生成方法，该方法包

括以下步骤：

S601、第一设备通过第一接入网设备注册到网络。

S602、第一接入网设备确定第一设备为 IAB node。

- 5 发送通知消息。

其中，通知消息用于表示第一设备通过具备 IAB donor 功能的第一接入网设备注册到网络中。或者说，通知消息用于表示第一接入网设备作为第一设备的 IAB donor。

S604、第二设备向第一设备发送第一 IP 地址通知消息。

其中，第一 IP 地址通知消息包括 IAB node 的 IP 地址和 IAB donor 的 IP 地址。

- 10 应理解，本申请实施例不限制步骤 S603-S604 与步骤 S605-S610 之间的执行顺序。

也即，步骤 S603-S604 可以在步骤 S606-S610 中的任意一个步骤之前或者之后执行。

S605、第一接入网设备选择第三接入网设备作为第一设备的辅基站。

S606、第一接入网设备向第三接入网设备发送 SN addition/modification request 消息。

- 15 S607、第一接入网设备接收第三接入网设备发送的 SN addition/modification request ACK 消息。

S608、第一接入网设备向第一设备发送 RRC 重配置消息。

S609、第一接入网设备接收第一设备发送的 RRC 重配置完成消息。

S610、第一接入网设备向第三接入网设备发送 SN reconfiguration complete 消息。

- 20 S611、第一接入网设备接收第一设备发送的第二 IP 地址通知消息。

其中，第二 IP 地址通知消息包括 IAB node 的 IP 地址。

S612、第一接入网设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

- 25 应理解，步骤 S611-S612 可以在步骤 S604 之后的任意时刻执行，本申请实施例对此不作限定。

S613、第一设备确定双连接的类型。

S614、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

S615、第一设备和第一接入网设备使用  $K_{IAB}$  建立安全隧道。

- 30 基于图 15 所示的实施例，在主基站作为 IAB donor 的情况下，主基站和 IAB node 均以主基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

技术方案二

- 35 在双连接场景（例如 NE-DC、NR-DC 或者 NGEN-DC 等场景）下，网络侧可以按照图 16 所示的实施例来获取 IAB 密钥，IAB node 可以按照图 17 所示的实施例来获取 IAB 密钥。

如图 16 所示，为本申请实施例提供的一种密钥生成方法，该方法包括以下步骤：

S701、第一接入网设备确定通过第一接入网设备注册到网络的第一设备为 IAB

node。

S702、在需要为第一设备选择辅基站的情况下，第一接入网设备判断自身是否具备 IAB node 功能。

其中，步骤 S701-S702 与图 10 中的步骤 S101-S102 相似，其具体实现方式可以参考图 10 所示实施例中的描述。

应理解，第一接入网设备可以根据主基站密钥和 SN 计数值，生成辅基站密钥。

可选的，当第一接入网设备不具备 IAB donor 功能时，执行下述步骤 S703-S705；当第一接入网设备具备 IAB donor 功能时，执行下述步骤 S706-S707。

S703、在第一接入网设备不具备 IAB donor 功能的情况下，第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站。

S704、第一接入网设备向第二接入网设备发送辅基站配置消息。

其中，辅基站配置消息用于将第二接入网设备配置为第一设备的辅基站。

在本申请实施例中，辅基站配置消息包括第三指示信息和辅基站密钥。第三指示信息用于指示第一设备为 IAB node。

应理解，在辅基站配置消息包括第三指示信息的情况下，第二接入网设备能够根据第三指示信息获知第一设备为 IAB node。进而，第二接入网设备确定自身是否具备 IAB donor 功能。在第二接入网设备具备 IAB donor 功能的情况下，第二接入网设备可以认为自身是第一设备的 IAB donor，从而第二接入网设备可以执行下述步骤 S705。

S705、第二接入网设备根据辅基站密钥，生成  $K_{IAB1}$ 。

作为一种可能的实现方式，第二接入网设备根据辅基站密钥和第一密钥输入参数，生成  $K_{IAB1}$ 。其中，第一密钥输入参数包括第一 IP 地址和第二 IP 地址。第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址。第二 IP 地址为第二接入网设备用于与 IAB node 通信的 IP 地址。

在本申请实施例中，第二接入网设备可以从自身的数据库中获取到第二 IP 地址。

在本申请实施例中，第二接入网设备可以确定第一 IP 地址。或者，第二接入网设备从第一设备或者第二设备获取到第一 IP 地址。

基于上述步骤 S703-S705，在辅基站（也即第二接入网设备）作为 IAB donor 的情况下，辅基站主动地以辅基站密钥生成  $K_{IAB}$ ，以保证 IAB donor 和 IAB node 维护相同的  $K_{IAB}$ 。

S706、在第一接入网设备具备 IAB donor 功能的情况下，第一接入网设备选择第三接入网设备作为第一设备的辅基站。

S707、第一接入网设备根据辅基站密钥，生成  $K_{IAB2}$ 。

作为一种可能的实现方式，第一接入网设备根据辅基站密钥和第二密钥输入参数，生成  $K_{IAB2}$ 。其中，第二密钥输入参数包括第一 IP 地址和第三 IP 地址。第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址。第三 IP 地址为第一接入网设备用于与 IAB node 通信的 IP 地址。

在本申请实施例中，第一接入网设备可以从自身的数据库中获取到第三 IP 地址。

在本申请实施例中，第一接入网设备可以确定第一 IP 地址。或者，第一接入网设备从第一设备或者第二设备获取到第一 IP 地址。

基于上述步骤 S706-S707, 在主基站 (也即第一接入网设备) 作为 IAB donor 的情况下, 主基站主动地以辅基站密钥生成  $K_{IAB}$ , 以保证 IAB donor 和 IAB node 维护相同的  $K_{IAB}$ 。

如图 17 所示, 为本申请实施例提供的一种密钥生成方法, 该方法应用于 IAB node 连接主基站和辅基站的场景下。该方法包括以下步骤:

S801、与步骤 S20 相同, 其具体描述可以参考图 11 所示的实施例, 在此不再赘述。

S802、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时, IAB node 根据辅基站密钥, 生成  $K_{IAB}$ 。

其中, IAB node 可以根据主基站密钥, 推演出辅基站密钥。

作为一种可能的实现方式, IAB node 根据辅基站密钥和密钥输入参数, 生成  $K_{IAB}$ 。

应理解, 密钥输入参数的具体介绍以及获取方式可以参考图 11 所示实施例中步骤 S202 的相关描述, 在此不再赘述。

基于图 17 所示的实施例, 在 NE-DC、NR-DC 或者 NGEN-DC 场景下, 保证 IAB node 以辅基站密钥生成  $K_{IAB}$ , 进而保证 IAB donor 和 IAB node 维护相同的  $K_{IAB}$ 。

下面结合具体应用场景以举例的方式来对技术方案二进行详细说明。

场景 1、第一设备 (也即 IAB node) 通过不具备 IAB donor 功能的第一接入网设备注册到网络。之后, 第一接入网设备为第一设备选择具备 IAB donor 功能的第二接入网设备作为辅基站, 并且第二接入网设备负责为第一设备分配 IAB node 的 IP 地址。

基于场景 1, 如图 18 所示, 为本申请实施例提供的一种密钥生成方法, 该方法包括以下步骤:

S901、第一设备通过第一接入网设备注册到网络。

S902、第一接入网设备确定第一设备为 IAB node。

S903、在需要为第一设备选择辅基站的情况下, 第一接入网设备判断自身是否具备 IAB node 功能。

S904、在第一接入网设备不具备 IAB node 功能的情况下, 第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站。

在选择辅基站之后, 第一接入网设备可以根据主基站密钥和 SN 计数值, 推演出辅基站密钥。

S905、第一接入网设备向第二接入网设备发送 SN addition/modification request 消息。

其中, SN addition/modification request 消息包括辅基站密钥和第三指示信息。第三指示信息用于指示第一设备为 IAB node。

在 SN addition/modification request 消息包括第三指示信息的情况下, 第二接入网设备可以确定自身是否具备 IAB donor 功能。在第二接入网设备具备 IAB donor 功能的情况下, 第二接入网设备可以认为是第一设备的 IAB donor, 从而第二接入网设备需要执行下述步骤 S910。

S906、第一接入网设备接收第二接入网设备发送的 SN addition/modification request ACK 消息。

S907、第一接入网设备向第一设备发送 RRC 重配置消息。

其中，RRC 重配置消息用于配置第二接入网设备与第一设备之间的无线承载。从而，基于 RRC 重配置消息，第一设备能够获知第二接入网设备作为辅基站。

另外，RRC 重配置消息还包括 SN 计数值。从而，第一设备能够根据主基站密钥和 SN 计数值，推演出辅基站密钥。

5 S908、第一接入网设备接收第一设备发送的 RRC 重配置完成消息。

S909、第一接入网设备向第二接入网设备发送 SN reconfiguration complete 消息。

应理解，第二接入网设备在接收到 SN reconfiguration complete 消息之后，第二接入网设备可以与第一设备建立 RRC 连接，从而第二接入网设备与第一设备之间可以直接通信。

10 S910、第二接入网设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

应理解，第二接入网设备从本地获取 IAB donor 的 IP 地址。并且，第二接入网设备为第一设备分配 IAB node 的 IP 地址。

15 应理解，步骤 S910 可以在步骤 S905 之后的任意时刻执行，本申请实施例对此不作限定。

S911、第二接入网设备向第一设备发送第一 IP 地址通知消息。

其中，第一 IP 地址通知消息包括 IAB node 的 IP 地址。

S912、第二设备向第一设备发送第二 IP 地址通知消息。

其中，第二 IP 地址通知消息包括 IAB donor 的 IP 地址。

20 应理解，步骤 S912 可以在步骤 S904 之后的任意时刻执行，本申请实施例对此不作限定。

基于步骤 S911 和 S912，第一设备能够获取到 IAB donor 的 IP 地址和 IAB node 的 IP 地址。

S913、第一设备确定双连接的类型。

25 S914、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

S915、第一设备和第二接入网设备使用  $K_{IAB}$  建立安全隧道。

30 基于图 18 所示的实施例，在辅基站作为 IAB donor 的情况下，辅基站以辅基站密钥生成  $K_{IAB}$ ，IAB node 以辅基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

场景 2、第一设备（也即 IAB node）通过不具备 IAB donor 功能的第一接入网设备注册到网络。之后，第一接入网设备为第一设备选择具备 IAB donor 功能的第二接入网设备作为辅基站。第二设备负责为第一设备分配 IAB node 的 IP 地址。

35 基于场景 2，如图 19 所示，为本申请实施例提供的一种密钥生成方法，该方法包括以下步骤：

S1001、第一设备通过第一接入网设备注册到网络。

S1002、第一接入网设备确定第一设备为 IAB node。

S1003、在需要为第一设备选择辅基站的情况下，第一接入网设备判断自身是否具

备 IAB node 功能。

S1004、在第一接入网设备不具备 IAB node 功能的情况下，第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站。

S1005、第二设备向第一设备发送第一 IP 地址通知消息。

5 其中，第一 IP 地址通知消息包括 IAB node 的 IP 地址和 IAB donor 的 IP 地址。

应理解，步骤 S1005 可以在步骤 S1004 之后，步骤 S1011 之前的任意时刻执行，本申请实施例对此不作限定。

S1006、第一接入网设备向第二接入网设备发送 SN addition/modification request 消息。

10 其中，SN addition/modification request 消息包括辅基站密钥和第三指示信息。第三指示信息用于指示第一设备为 IAB node。

在 SN addition/modification request 消息包括第三指示信息的情况下，第二接入网设备可以确定自身是否具备 IAB donor 功能。在第二接入网设备具备 IAB donor 功能的情况下，第二接入网设备可以认为是第一设备的 IAB donor，从而第二接入网设备需要执行下述步骤 S1012。

15 S1007、第一接入网设备接收第二接入网设备发送的 SN addition/modification request ACK 消息。

S1008、第一接入网设备向第一设备发送 RRC 重配置消息。

20 其中，RRC 重配置消息用于配置第二接入网设备与第一设备之间的无线承载。从而，基于 RRC 重配置消息，第一设备能够获知第二接入网设备作为辅基站。

另外，RRC 重配置消息还包括 SN 计数值。从而，第一设备能够根据主基站密钥和 SN 计数值，推演出辅基站密钥。

S1009、第一接入网设备接收第一设备发送的 RRC 重配置完成消息。

S1010、第一接入网设备向第二接入网设备发送 SN reconfiguration complete 消息。

25 应理解，第二接入网设备在接收到 SN reconfiguration complete 消息之后，第二接入网设备可以与第一设备建立 RRC 连接，从而第二接入网设备与第一设备之间可以直接通信。

S1011、第一设备向第二接入网设备发送第二 IP 地址通知消息。

其中，第二 IP 地址通知消息包括 IAB donor 的 IP 地址。

30 S1012、第二接入网设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

应理解，第二接入网设备从本地获取 IAB donor 的 IP 地址。以及，第二接入网设备根据上述第二 IP 地址通知消息，获取 IAB node 的 IP 地址。

S1013、第一设备确定双连接的类型。

35 S1014、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

应理解，步骤 S1013-S1014 可以在步骤 S1008 之后的任意时刻执行，本申请实施例对此不作限定。

S1015、第一设备和第二接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 19 所示的实施例,在辅基站作为 IAB donor 的情况下,辅基站以辅基站密钥生成  $K_{IAB}$ , IAB node 以辅基站密钥生成  $K_{IAB}$ 。从而, IAB node 和 IAB donor 维护相同的  $K_{IAB}$ , 以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道, 有利于 IAB node 采用双连接方式进行组网。

5 场景 3、第一设备(也即 IAB node)通过具备 IAB donor 功能的第一接入网设备注册到网络。从而, 第一接入网设备作为第一设备的 IAB donor, 并且第一接入网设备为第一设备分配 IAB node 的 IP 地址。第一接入网设备为第一设备选择第三接入网设备作为辅基站。

10 基于场景 3, 如图 20 所示, 为本申请实施例提供的一种密钥生成方法, 该方法包括以下步骤:

S1101-S1110、与步骤 S501-S510 相同, 其具体描述可以参考图 14 所示实施例, 在此不再赘述。

其中, 在选择第三接入网设备作为辅基站之后, 第一接入网设备会生成辅基站密钥, 并通过 SN addition/modification request 消息向第三接入网设备发送辅基站密钥。

15 S1111、第一接入网设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址, 生成  $K_{IAB}$ 。

应理解, 步骤 S1111 可以在 S1105 之后的任意时刻执行, 本申请实施例对此不作限定。

20 可选的, 若步骤 S1111 在步骤 S1106 之前执行, 则第一接入网设备在执行完步骤 S1106 之后, 可以删除辅基站密钥。

可选的, 若步骤 S1111 在步骤 S1106 之后执行, 则第一接入网设备在执行完步骤 S1106 之前, 需要保存辅基站密钥, 直至执行完步骤 S1111。

S1112、第一设备确定双连接的类型。

25 S1113、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时, 第一设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址, 生成  $K_{IAB}$ 。

应理解, 步骤 S1112-S1113 可以在步骤 S1108 之后的任意时刻执行, 本申请实施例对此不作限定。

S1114、第一设备和第一接入网设备使用  $K_{IAB}$  建立安全隧道。

30 基于图 20 所示的实施例, 在主基站作为 IAB donor 的情况下, 主基站和 IAB node 均以辅基站密钥生成  $K_{IAB}$ 。从而, IAB node 和 IAB donor 维护相同的  $K_{IAB}$ , 以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道, 有利于 IAB node 采用双连接方式进行组网。

35 场景 4、第一设备(也即 IAB node)通过具备 IAB donor 功能的第一接入网设备注册到网络。从而, 第一接入网设备作为第一设备的 IAB donor。第一接入网设备为第一设备选择第三接入网设备作为辅基站。第二设备负责为第一设备分配 IAB node 的 IP 地址。

基于场景 4, 如图 21 所示, 为本申请实施例提供的一种密钥生成方法, 该方法包括以下步骤:

S1201-S1211、与步骤 S601-S611 相同, 其具体描述可以参考图 15 所示的实施例,

在此不再赘述。

其中，在选择第三接入网设备作为辅基站之后，第一接入网设备会生成辅基站密钥，并通过 SN addition/modification request 消息向第三接入网设备发送辅基站密钥。

5 S1212、第一接入网设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

应理解，步骤 S1211 可以在步骤 S1204 之后的任意时刻执行。步骤 S1212 可以在步骤 S1205 和 S1211 之后的任意时刻执行。

可选的，若步骤 S1212 在步骤 S1206 之前执行，则第一接入网设备在执行完步骤 S1206 之后，可以删除辅基站密钥。

10 可选的，若步骤 S1212 在步骤 S1206 之后执行，则第一接入网设备在执行完步骤 S1206 之前，需要保存辅基站密钥，直至执行完步骤 S1212。

S1213、第一设备确定双连接的类型。

S1214、当双连接的类型为 NE-DC、NR-DC 或者 NGEN-DC 时，第一设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

15 应理解，步骤 S1213-S1214 可以在步骤 S1208 之后的任意时刻执行，本申请实施例对此不作限定。

S1215、第一设备和第一接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 21 所示的实施例，在主基站作为 IAB donor 的情况下，主基站和 IAB node 均以辅基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

### 技术方案三

在一些双连接场景（例如 NE-DC、NR-DC 或者 NGEN-DC 等场景）下，IAB node 可以按照图 22 所示的实施例来获取  $K_{IAB}$ ，网络侧可以按照图 23 所示的实施例来获取  $K_{IAB}$ 。

如图 22 所示，为本申请实施例提供的一种密钥生成方法，应用于第一设备（IAB node）连接主基站和辅基站的场景，该方法包括以下步骤：

S1301、IAB node 获知主基站或者辅基站作为 IAB donor。

可选的，步骤 S1301 可以采用以下实现方式中的任意一种：

30 实现方式一、当 IAB node 接收到第四指示信息时，IAB node 获知主基站为 IAB donor，第四指示信息用于指示主基站为 IAB donor。或者，当 IAB node 接收到第五指示信息时，IAB node 获知辅基站为 IAB donor，第五指示信息用于指示辅基站为 IAB donor。

35 可选的，IAB node 接收第四指示信息，可以具体实现为：IAB node 接收主基站发送的第四指示信息。示例性的，这种情况下，第四指示信息可以承载于主基站发送给 IAB node 的 RRC 重配置消息中。

可选的，IAB node 接收第五指示信息，可以具体实现为：IAB node 接收主基站或者辅基站发送的第五指示信息。示例性的，这种情况下，第五指示信息可以承载于主基站发送给 IAB node 的 RRC 重配置消息中。或者，第五指示信息可以承载于辅基站

发送给 IAB node 的 AS 消息中。

实现方式二、当 IAB node 与主基站之间建立无线回程链路时, IAB node 获知主基站为 IAB donor。或者, 当 IAB node 与辅基站之间建立无线回程链路时, IAB node 获知辅基站为 IAB donor。

- 5 实现方式三、IAB node 获取主基站支持的频段以及辅基站支持的频段。当主基站支持的频段高于辅基站支持的频段时, IAB node 获知主基站为 IAB donor。或者, 当主基站的频段低于辅基站支持的频段时, IAB node 获知辅基站为 IAB donor。

- 10 实现方式四、当 IAB node 接收到主基站广播的第六指示信息时, IAB node 获知主基站为 IAB donor。或者, 当 IAB node 接收到辅基站广播的第六指示信息时, IAB node 获知辅基站为 IAB donor。其中, 第六指示信息用于指示基站具备 IAB donor 功能。

S1302、当主基站作为 IAB donor 时, IAB node 根据主基站密钥生成  $K_{IAB}$ 。

作为一种可能的实现方式, IAB node 根据主基站密钥和密钥输入参数, 生成  $K_{IAB}$ 。

其中, 主基站密钥是 IAB node 在通过主基站注册到网络的过程中生成的。

S1303、当辅基站作为 IAB donor 时, IAB node 根据辅基站密钥, 生成  $K_{IAB}$ 。

- 15 作为一种可能的实现方式, IAB node 根据辅基站密钥和密钥输入参数, 生成  $K_{IAB}$ 。

其中, 辅基站密钥是 IAB node 根据主基站密钥生成的。

基于图 22 所示的实施例, 无论主基站作为 IAB donor 还是辅基站作为 IAB donor, IAB node 均能使用 IAB donor 的本地密钥来生成  $K_{IAB}$ , 以保证 IAB node 和 IAB donor 维护相同的  $K_{IAB}$ 。

- 20 如图 23 所示, 为本申请实施例提供的一种密钥生成方法, 该方法包括以下步骤:

S1401、第一接入网设备确定通过第一接入网设备注册到网络的第一设备为 IAB node。

S1402、在需要为第一设备选择辅基站的情况下, 第一接入网设备判断自身是否具备 IAB node 功能。

- 25 其中, 步骤 S1401-S1402 与图 10 中的步骤 S101-S102 相似, 其具体实现方式可以参考图 10 所示实施例中的描述。

可选的, 当第一接入网设备不具备 IAB donor 功能时, 执行下述步骤 S1403-S1405; 当第一接入网设备具备 IAB donor 功能时, 执行下述步骤 S1406-S1407。

- 30 S1403、在第一接入网设备不具备 IAB donor 功能的情况下, 第一接入网设备选择具备 IAB donor 功能的第二接入网设备作为第一设备的辅基站。

S1404、第一接入网设备向第二接入网设备发送辅基站配置消息。

其中, 辅基站配置消息用于将第二接入网设备配置为第一设备的辅基站。

在本申请实施例中, 辅基站配置消息包括第三指示信息和辅基站密钥。第三指示信息用于指示第一设备为 IAB node。

- 35 应理解, 在辅基站配置消息包括第三指示信息的情况下, 第二接入网设备可以获知第一设备为 IAB node。从而, 第二接入网设备可以判断自身是否具备 IAB donor 功能。在第二接入网设备具备 IAB donor 功能的情况下, 第二接入网设备可以认为自身是第一设备的 IAB donor, 从而第二接入网设备可以执行下述步骤 S1405。

S1405、第二接入网设备根据辅基站密钥, 生成  $K_{IAB1}$ 。

作为一种可能的实现方式,第二接入网设备根据辅基站密钥和第一密钥输入参数,生成  $K_{IAB1}$ 。其中,第一密钥输入参数包括第一 IP 地址和第二 IP 地址。第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址。第二 IP 地址为第二接入网设备用于与 IAB node 通信的 IP 地址。

5 在本申请实施例中,第二接入网设备可以从自身的数据库中获取到第二 IP 地址。

在本申请实施例中,第二接入网设备可以确定第一 IP 地址。或者,第二接入网设备从第一设备或者第二设备获取到第一 IP 地址。

基于上述步骤 S1403-S1405,在辅基站(也即第二接入网设备)作为 IAB donor 的情况下,辅基站主动地以辅基站密钥生成  $K_{IAB}$ ,以保证 IAB donor 和 IAB node 维护  
10 相同的  $K_{IAB}$ 。

S1406、在第一接入网设备具备 IAB donor 功能的情况下,第一接入网设备选择第三接入网设备作为第一设备的辅基站。

S1407、第一接入网设备根据主基站密钥,生成  $K_{IAB2}$ 。

作为一种可能的实现方式,第一接入网设备根据主基站密钥和第二密钥输入参数,  
15 生成  $K_{IAB2}$ 。其中,第二密钥输入参数包括第一 IP 地址和第三 IP 地址。第一 IP 地址为第一设备用于与 IAB donor 通信的 IP 地址。第三 IP 地址为第一接入网设备用于与 IAB node 通信的 IP 地址。

在本申请实施例中,第一接入网设备可以从自身的数据库中获取到第三 IP 地址。

在本申请实施例中,第一接入网设备可以确定第一 IP 地址。或者,第一接入网设备  
20 从第一设备或者第二设备获取到第一 IP 地址。

基于上述步骤 S1406-S1407,在主基站(也即第一接入网设备)作为 IAB donor 的情况下,主基站主动地以主基站密钥生成  $K_{IAB}$ ,以保证 IAB donor 和 IAB node 维护相同的  $K_{IAB}$ 。

下面结合具体应用场景以举例的方式来对技术方案三进行详细说明。

25 场景 1、第一设备(也即 IAB node)通过不具备 IAB donor 功能的第一接入网设备注册到网络。之后,第一接入网设备为第一设备选择具备 IAB donor 功能的第二接入网设备作为辅基站,并且第二接入网设备负责为第一设备分配 IAB node 的 IP 地址。

基于场景 1,如图 24 所示,为本申请实施例提供的一种密钥生成方法,该方法包括以下步骤:

30 S1501-S1512、与步骤 S901-S912 相似,其具体描述可以参考图 18 所示实施例,在此不再赘述。

可选的,区别于步骤 S906,在步骤 S1506 中,第二接入网设备发送的 SN addition/modification request ACK 消息可以包括第五指示信息。

可选的,区别于步骤 S907,在步骤 S1507 中,第一接入网设备发送的 RRC 重配置消息可以包括第五指示信息,以便于第一设备获知辅基站(也即第二接入网设备)为 IAB donor。  
35

S1513、第一设备获知第二接入网设备为 IAB donor。

S1514、第一设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址,生成  $K_{IAB}$ 。

S1515、第一设备和第二接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 24 所示的实施例，在辅基站作为 IAB donor 的情况下，辅基站以辅基站密钥生成  $K_{IAB}$ ，IAB node 以辅基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

场景 2、第一设备（也即 IAB node）通过不具备 IAB donor 功能的第一接入网设备注册到网络。之后，第一接入网设备为第一设备选择具备 IAB donor 功能的第二接入网设备作为辅基站。第二设备负责为第一设备分配 IAB node 的 IP 地址。

基于场景 2，如图 25 所示，为本申请实施例提供的一种密钥生成方法，该方法包括以下步骤：

S1601-S1612、与步骤 S1001-S1012 相似，其具体描述可以参考图 19 所示实施例，在此不再赘述。

可选的，区别于步骤 S1007，在步骤 S1607 中，第二接入网设备发送的 SN addition/modification request ACK 消息可以包括第五指示信息。

可选的，区别于步骤 S1008，在步骤 S1608 中，第一接入网设备发送的 RRC 重配置消息可以包括第五指示信息，以便于第一设备获知辅基站（也即第二接入网设备）为 IAB donor。

S1613、第一设备获知第二接入网设备为 IAB donor。

S1614、第一设备根据辅基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

S1615、第一设备和第二接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 25 所示的实施例，在辅基站作为 IAB donor 的情况下，辅基站以辅基站密钥生成  $K_{IAB}$ ，IAB node 以辅基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

场景 3、第一设备（也即 IAB node）通过具备 IAB donor 功能的第一接入网设备注册到网络。从而，第一接入网设备作为第一设备的 IAB donor，并且第一接入网设备为第一设备分配 IAB node 的 IP 地址。第一接入网设备为第一设备选择第三接入网设备作为辅基站。

基于场景 3，如图 26 所示，为本申请实施例提供的一种密钥生成方法，该方法包括以下步骤：

S1701-S1711、与步骤 S501-S511 相似，其具体描述可以参考图 14 所示实施例，在此不再赘述。

可选的，区别于步骤 S508，在步骤 S1708 中，第一接入网设备发送的 RRC 重配置消息可以包括第四指示信息，以便于第一设备获知主基站（也即第一接入网设备）为 IAB donor。

S1712、第一设备获知第一接入网设备为 IAB donor。

S1713、第一设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

S1714、第一设备和第一接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 26 所示的实施例，在主基站作为 IAB donor 的情况下，主基站和 IAB node 均以主基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

场景 4、第一设备（也即 IAB node）通过具备 IAB donor 功能的第一接入网设备注册到网络。从而，第一接入网设备作为第一设备的 IAB donor。第一接入网设备为第一设备选择第三接入网设备作为辅基站。第二设备负责为第一设备分配 IAB node 的 IP 地址。

10 基于场景 4，如图 27 所示，为本申请实施例提供的一种密钥生成方法，该方法包括以下步骤：

S1801-S1812、与步骤 S601-S612 相似，其具体描述可以参考图 15 所示实施例，在此不再赘述。

15 可选的，区别于步骤 S608，在步骤 S1808 中，第一接入网设备发送的 RRC 重配置消息可以包括第四指示信息，以便于第一设备获知主基站（也即第一接入网设备）为 IAB donor。

S1813、第一设备获知第一接入网设备为 IAB donor。

S1814、第一设备根据主基站密钥、IAB donor 的 IP 地址和 IAB node 的 IP 地址，生成  $K_{IAB}$ 。

20 S1815、第一设备和第一接入网设备使用  $K_{IAB}$  建立安全隧道。

基于图 27 所示的实施例，在主基站作为 IAB donor 的情况下，主基站和 IAB node 均以主基站密钥生成  $K_{IAB}$ 。从而，IAB node 和 IAB donor 维护相同的  $K_{IAB}$ ，以便于 IAB node 和 IAB donor 之间根据  $K_{IAB}$  建立安全隧道，有利于 IAB node 采用双连接方式进行组网。

25 上述主要从方法的角度对本申请实施例提供的方案进行了介绍。可以理解的是，通信装置（例如第一设备、第一接入网设备、第二接入网设备）为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。结合本申请中所公开的实施例描述的各示例的单元及算法步骤，本申请实施例能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。本领域技术人员可以对每个特定的应用来使用不同的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实施例的技术方案的范围。

30 本申请实施例可以根据上述方法示例对通信装置进行功能单元的划分，例如，可以对应各个功能划分各个功能单元，也可以将两个或两个以上的功能集成在一个处理单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。需要说明的是，本申请实施例中对单元的划分是示意性的，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。

如图 28 所示，为本申请实施例提供的一种通信装置，该通信装置包括处理模块 101 和通信模块 102。

一种可能的示例中,以通信装置为 IAB node 为例,处理模块 101 用于支持 IAB node 执行图 11 中的步骤 S201-S202,图 17 中的步骤 S801-S805,图 22 中的步骤 S1301-S1303,和/或本申请实施例中 IAB node 需要执行的其他处理操作。通信模块 102 用于支持 IAB node 执行图 12 中的步骤 S308、S309、S311,图 13 中的步骤 S405、S408、S409、S411,和/或本申请实施例中 IAB node 需要执行的其他通信操作。

另一种可能的示例中,以通信装置为第一接入网设备为例,处理模块 101 用于支持第一接入网设备执行图 10 中的步骤 S101-S105、S107-S109,图 16 中的步骤 S701-S703、S706-S707,图 23 中的步骤 S1401-S1403、S1406-S1407,和/或本申请实施例中第一接入网设备需要执行的其他处理操作。通信模块 102 用于支持第一接入网设备执行图 10 中的步骤 S106,图 16 中的步骤 S704,图 23 中的步骤 S1404,和/或本申请实施例中第一接入网设备需要执行的其他通信操作。

另一种可能的示例中,以通信装置为第二接入网设备为例,处理模块 101 用于支持第二接入网设备执行图 16 中的步骤 S705,图 23 中的步骤 S1405,和/或本申请实施例中第二接入网设备需要执行的其他处理操作。通信模块 102 用于支持第二接入网设备执行图 10 中的步骤 S106,图 16 中的步骤 S704,图 23 中的步骤 S1404,和/或本申请实施例中第二接入网设备需要执行的其他通信操作。

可选,该通信装置还可以包括存储模块 103,用于存储通信装置的程序代码和数据,数据可以包括但不限于原始数据或者中间数据等。

其中,处理模块 101 可以是处理器或控制器,例如可以是 CPU,通用处理器,专用集成电路(application specific integrated circuit, ASIC),现场可编程逻辑门阵列(field programmable gate array, FPGA)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框,模块和电路。处理器也可以是实现计算功能的组合,例如包含一个或多个微处理器组合,DSP 和微处理器的组合等等。

通信模块 102 可以是通信接口、收发器或收发电路等,其中,该通信接口是统称,在具体实现中,该通信接口可以包括多个接口,例如可以包括:基站和终端之间的接口和/或其他接口。

存储模块 103 可以是存储器。

当处理模块 101 为处理器,通信模块 102 为通信接口,存储模块 103 为存储器时,本申请实施例所涉及的通信装置可以为图 29 所示。

参阅图 29 所示,该通信装置包括:处理器 201、通信接口 202、存储器 203。可选的,通信装置还可以包括总线 204。其中,通信接口 202、处理器 201 以及存储器 203 可以通过总线 204 相互连接;总线 204 可以是外设部件互连标准(peripheral component interconnect, PCI)总线或扩展工业标准结构(extended industry standard architecture, EISA)总线等。所述总线 204 可以分为地址总线、数据总线、控制总线等。为便于表示,图 29 中仅用一条粗线表示,但并不表示仅有一根总线或一种类型的总线。

可选的,本申请实施例还提供一种携带计算机指令的计算机程序产品,当该计算机指令在计算机上运行时,使得计算机执行上述实施例所介绍的方法。

可选的，本申请实施例还提供一种计算机可读存储介质，所述计算机可读存储介质存储计算机指令，当该计算机指令在计算机上运行时，使得计算机执行上述实施例所介绍的方法。

5 可选的，本申请实施例还提供一种芯片，包括：处理电路和收发管脚，处理电路和收发管脚用于实现上述实施例所介绍的方法。其中，处理电路用于执行相应方法中的处理动作，收发管脚用于执行相应方法中的接收/发送的动作。

本领域普通技术人员可以理解：在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，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。在计算机上  
10 加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、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（例如同轴电缆、光纤、数字用户线（Digital  
15 Subscriber Line, DSL））或无线（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括一个或多个可用介质集成的服务器、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，数字视频光盘（Digital Video Disc, DVD））、或者半导体介质（例如固态硬盘（Solid  
20 State Disk, SSD））等。

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  
25 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，可以是电性或其它的形式。

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设备上。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  
30 的目的。

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，也可以是各个功能单元独立存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现，当然也可以通过硬件，但很多情况下前者是  
35 更佳的实施方式。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可读取的存储介质中，如计算机的软盘、硬盘或光盘等，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的方法。

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，在本申请揭露的技术范围内的变化或替换，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。

## 权 利 要 求 书

1、一种密钥生成方法，其特征在于，所述方法包括：

第一接入网设备确定通过所述第一接入网设备注册到 5G 核心网的第一设备为接入回传一体化 IAB 节点；

5 在需要为所述第一设备选择辅基站的情况下，所述第一接入网设备判断自身是否具备 IAB 宿主功能；

若所述第一接入网设备不具备 IAB 宿主功能，则所述第一接入网设备选择具备 IAB 宿主功能的第二接入网设备作为所述第一设备的辅基站；

所述第一接入网设备获取第一密钥输入参数；

10 所述第一接入网设备根据主基站密钥和所述第一密钥输入参数，生成第一 IAB 密钥  $K_{IAB1}$ ，所述主基站密钥用于对所述第一接入网设备与所述第一设备之间的通信进行安全保护，所述  $K_{IAB1}$  用于建立所述第二接入网设备与所述第一设备之间的安全隧道；

所述第一接入网设备向所述第二接入网设备发送所述  $K_{IAB1}$ 。

2、根据权利要求 1 所述的方法，其特征在于，所述第一接入网设备选择具备 IAB 15 宿主功能的第二接入网设备作为所述第一设备的辅基站，包括：

所述第一接入网设备向第二设备发送第一请求消息，所述第一请求消息包括所述第一设备的标识；

所述第一接入网设备接收所述第二设备发送的第一响应消息，所述第一响应消息包括所述第二接入网设备的标识。

20 3、根据权利要求 1 或 2 所述的方法，其特征在于，所述第一密钥输入参数包括第一 IP 地址和第二 IP 地址，所述第一 IP 地址为所述第一设备用于与 IAB 宿主通信的 IP 地址，所述第二 IP 地址为所述第二接入网设备用于与 IAB 节点通信的 IP 地址。

4、根据权利要求 3 所述的方法，其特征在于，所述第一接入网设备获取第一密钥输入参数，包括：

25 所述第一接入网设备向所述第二接入网设备发送辅基站配置消息，所述辅基站配置消息用于配置所述第二接入网设备为所述第一设备的辅基站，所述辅基站配置消息包括第一指示信息和/或第二指示信息，所述第一指示信息用于请求所述第一 IP 地址，所述第二指示信息用于请求所述第二 IP 地址；

30 所述第一接入网设备接收所述第二接入网设备发送的辅基站配置响应消息，所述辅基站配置响应消息包括所述第一 IP 地址和/或所述第二 IP 地址。

5、根据权利要求 4 所述的方法，其特征在于，所述辅基站配置消息包括由所述主基站密钥推演得到的辅基站密钥，所述辅基站密钥用于对所述辅基站和所述第一设备之间的通信进行安全保护。

6、根据权利要求 5 所述的方法，其特征在于，所述方法还包括：

35 所述第一接入网设备向所述第一设备发送所述第一 IP 地址。

7、根据权利要求 3 所述的方法，其特征在于，所述第一接入网设备获取第一密钥输入参数，包括：

所述第一接入网设备接收所述第一设备发送的 IP 地址通知消息，所述 IP 地址通知消息包括所述第一 IP 地址；

所述第一接入网设备向所述第二接入网设备发送辅基站配置消息，所述辅基站配置消息用于配置所述第二接入网设备为所述第一设备的辅基站，所述辅基站配置消息包括第二指示信息，所述第二指示信息用于请求所述第二 IP 地址；

5 所述所述第一接入网设备接收所述第二接入网设备发送的辅基站配置响应消息，所述辅基站配置响应消息包括所述第二 IP 地址。

8、根据权利要求 1 至 7 任一项所述的方法，其特征在于，所述方法还包括：

若所述第一接入网设备具备 IAB 宿主功能，则所述第一接入网设备选择第三接入网设备作为所述第一设备的辅基站；

所述所述第一接入网设备获取第二密钥输入参数；

10 所述所述第一接入网设备根据所述主基站密钥和所述第二密钥输入参数，生成第二 IAB 密钥  $K_{IAB2}$ ，所述  $K_{IAB2}$  用于建立所述第一接入网设备与所述第一设备之间的安全隧道。

9、根据权利要求 8 所述的方法，其特征在于，所述第二密钥输入参数包括：第一 IP 地址和第三 IP 地址，所述第一 IP 地址为所述第一设备用于与 IAB 宿主通信的 IP 地址，所述第三 IP 地址为所述第一接入网设备用于与 IAB 节点通信的 IP 地址。

10、根据权利要求 9 所述的方法，其特征在于，所述第一接入网设备获取第二密钥输入参数，包括：

所述所述第一接入网设备为所述第一设备分配所述第一 IP 地址；

所述所述第一接入网设备从数据库中获取所述第三 IP 地址。

20 11、根据权利要求 9 所述的方法，其特征在于，所述第一接入网设备获取第二密钥输入参数，包括：

所述所述第一接入网设备接收所述第一设备发送的 IP 地址通知消息，所述 IP 地址通知消息包括所述第一 IP 地址；

所述所述第一接入网设备从数据库中获取所述第三 IP 地址。

25 12、一种密钥生成方法，其特征在于，所述方法包括：

第二接入网设备接收第一接入网设备发送的辅基站配置消息，所述辅基站配置消息用于配置所述第二接入网设备作为第一设备的辅基站；

当所述辅基站配置消息包括第三指示信息时，所述第二接入网设备确定自身是否具备 IAB 宿主功能，所述第三指示信息用于指示所述第一设备为 IAB 节点；

30 当所述第二接入网设备具备 IAB 宿主功能时，所述第二接入网设备从所述第一接入网设备获取第一 IAB 密钥  $K_{IAB1}$ ，所述  $K_{IAB1}$  用于建立所述第二接入网设备与所述第一设备之间的安全隧道，所述  $K_{IAB1}$  是根据主基站密钥生成的，所述主基站密钥用于对所述第一接入网设备和所述第一设备之间的通信进行安全保护。

35 13、根据权利要求 12 所述的方法，其特征在于，所述  $K_{IAB1}$  是根据主基站密钥生成的，包括：

所述  $K_{IAB1}$  是根据所述主基站密钥和所述第一密钥输入参数生成的，所述第一密钥输入参数包括第一 IP 地址和第二 IP 地址，所述第一 IP 地址为所述第一设备用于与 IAB 宿主通信的 IP 地址，所述第二 IP 地址为所述第二接入网设备用于与 IAB 节点通信的 IP 地址。

14、根据权利要求 13 所述的方法，其特征在于，所述辅基站配置消息还包括第一指示信息和/或第二指示信息，所述第一指示信息用于请求所述第一 IP 地址，所述第二指示信息用于请求所述第二 IP 地址。

15、根据权利要求 14 所述的方法，其特征在于，所述方法还包括：

- 5 所述第二接入网设备向所述第一接入网设备发送辅基站配置响应消息，所述辅基站配置响应消息包括所述第一 IP 地址和/或所述第二 IP 地址。

16、根据权利要求 15 所述的方法，其特征在于，所述第二接入网设备从所述第一接入网设备获取  $K_{IAB1}$ ，包括：

- 10 所述第二接入网设备接收所述第一接入网设备发送的辅基站重配置完成消息，所述辅基站重配置完成消息包括所述  $K_{IAB1}$ 。

17、根据权利要求 14 所述的方法，其特征在于，所述第二接入网设备从所述第一接入网设备获取  $K_{IAB1}$ ，包括：

所述第二接入网设备向所述第一接入网设备发送密钥请求消息，所述密钥请求消息用于请求所述  $K_{IAB1}$ ；

- 15 所述第二接入网设备接收所述第一接入网设备发送的密钥响应消息，所述密钥响应消息包括所述  $K_{IAB1}$ 。

18、根据权利要求 17 所述的方法，其特征在于，所述密钥请求消息还包括所述第一 IP 地址和/或第二 IP 地址。

19、一种密钥生成方法，其特征在于，所述方法包括：

- 20 第一接入网设备确定通过所述第一接入网设备注册到网络的第一设备为 IAB 节点；  
在需要为所述第一设备选择辅基站的情况下，所述第一接入网设备判断自身是否具备 IAB 宿主功能；

若所述第一接入网设备具备 IAB 宿主功能，则所述第一接入网设备选择第三接入网设备作为所述第一设备的辅基站；

- 25 所述第一接入网设备根据辅基站密钥，生成第二 IAB 密钥  $K_{IAB2}$ ，所述  $K_{IAB2}$  用于建立所述第一接入网设备与所述第一设备之间的安全隧道，所述辅基站密钥用于对所述辅基站和所述第一设备之间的通信进行安全保护。

- 20、根据权利要求 19 所述的方法，其特征在于，所述辅基站密钥是根据主基站密钥推演得到的，所述主基站密钥用于对所述第一接入网设备和所述第一设备之间的通信进行安全保护。

21、根据权利要求 19 或 20 所述的方法，其特征在于，在所述第一接入网设备根据辅基站密钥，生成  $K_{IAB2}$  之后，所述方法还包括：

所述第一接入网设备向所述第二接入网设备发送辅基站配置消息，所述辅基站配置消息包括所述辅基站密钥；

- 35 所述第一接入网设备接收所述第二接入网设备发送的辅基站配置响应消息。

22、根据权利要求 20 或 21 所述的方法，其特征在于，所述第一接入网设备根据辅基站密钥，生成  $K_{IAB2}$ ，包括：

所述第一接入网设备在发送辅基站配置消息之后，根据所述辅基站密钥，生成所述  $K_{IAB2}$ 。

23、根据权利要求 20 或 21 所述的方法，其特征在于，所述第一接入网设备根据辅基站密钥，生成  $K_{IAB2}$ ，包括：

所述第一接入网设备在接收到辅基站配置响应消息之后，根据所述辅基站密钥，生成所述  $K_{IAB2}$ 。

5 24、根据权利要求 19 至 23 任一项所述的方法，其特征在于，所述方法还包括：

若所述第一接入网设备不具备 IAB 宿主功能，则所述第一接入网设备选择具备 IAB 宿主功能的第二接入网设备作为所述第一设备的辅基站；

所述第一接入网设备向所述第二接入网设备发送辅基站配置消息，所述辅基站配置消息包括所述辅基站密钥。

10 25、一种通信装置，其特征在于，所述通信装置包括用于执行权利要求 1 至 24 中任一项所涉及的方法中的各个步骤的模块。

26、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存储计算机指令，当所述计算机指令在计算机上运行时，使得所述计算机执行权利要求 1 至 24 任一项所述的方法。

15 27、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指令，当所述指令在计算机上运行时，使得计算机执行权利要求 1 至 24 任一项所述的方法。

28、一种芯片，其特征在于，所述芯片包括处理单元和收发管脚；所述处理单元用于执行权利要求 1 至 24 中任一项所涉及的方法中的处理操作，所述收发管脚用于执行权利要求 1 至 24 中任一项所涉及的方法中的通信操作。