

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2022/094976 A1

(43) 国际公布日
2022 年 5 月 12 日 (12.05.2022)

(51) 国际专利分类号:
H04W 48/20 (2009.01)

(21) 国际申请号: PCT/CN2020/127300

(22) 国际申请日: 2020 年 11 月 6 日 (06.11.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 郭龙华(GUO, Longhua); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 朱元萍(ZHU, Yuanping); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(CN)。 胡力(HU, Li); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 吴荣(WU, Rong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京中博世达专利商标代理有限公司 (BEIJING ZBSD PATENT & TRADEMARK AGENT LTD.); 中国北京市海淀区交大东路 31 号 11 号楼 8 层, Beijing 100044 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) Title: KEY GENERATION METHOD AND APPARATUS

(54) 发明名称: 密钥生成方法及装置

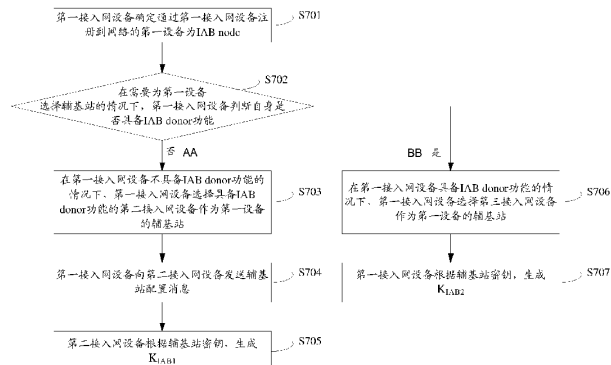


图 16

S701 A first access network device determines that a first device registered with a network by means of the first access network device is an IAB node
S702 When a secondary base station needs to be selected for the first device, the first access network device determines whether the first access network device itself has an IAB donor function
S703 When the first access network device does not have an IAB donor function, the first access network device selects a second access network device having an IAB donor function to serve as a secondary base station for the first device
S704 The first access network device sends a secondary base station configuration message to the second access network device
S705 The second access network device generates K_{IAB1} according to a key of the secondary base station
S706 When the first access network device has an IAB donor function, the first access network device selects a third access network device to serve as a secondary base station for the first device
S707 The first access network device generates K_{IAB2} according to a key of the secondary base station
AA No
BB Yes

(57) Abstract: A key generation method and apparatus, which relate to the technical field of communications, and are used for making an IAB donor and an IAB node use the same K_{IAB} in a dual-connectivity scenario. The key generation method comprises the following steps: a first access network device determining that a first device registered with a 5G core network by means of the first access network device is an IAB node; when a secondary base station needs to be selected for the first device, the first access network device determining whether the first

[见续页]

WO 2022/094976 A1

MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

access network device itself has an IAB donor function; if the first access network device has an IAB donor function, the first access network device selecting a third access network device to serve as a secondary base station for the first device; and the first access network device generating a second IAB key K_{IAB2} according to a key of the secondary base station, with K_{IAB2} being used to establish a secure tunnel between the first access network device and the first device.

(57) 摘要: 一种密钥生成方法及装置, 涉及通信技术领域, 用于在双连接场景下, 使得IABdonor和IAB node使用相同的 K_{IAB} 。密钥生成方法包括以下步骤: 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。