

(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

(43) 国际公布日
2022 年 5 月 5 日 (05.05.2022)



(10) 国际公布号
WO 2022/088029 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01)

(21) 国际申请号: PCT/CN2020/125224

(22) 国际申请日: 2020 年 10 月 30 日 (30.10.2020)

(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: 吴义壮 (WU, Yizhuang); 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, 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。

(54) Title: KEY ACQUISITION METHOD AND COMMUNICATION APPARATUS

(54) 发明名称: 密钥获取方法和通信装置

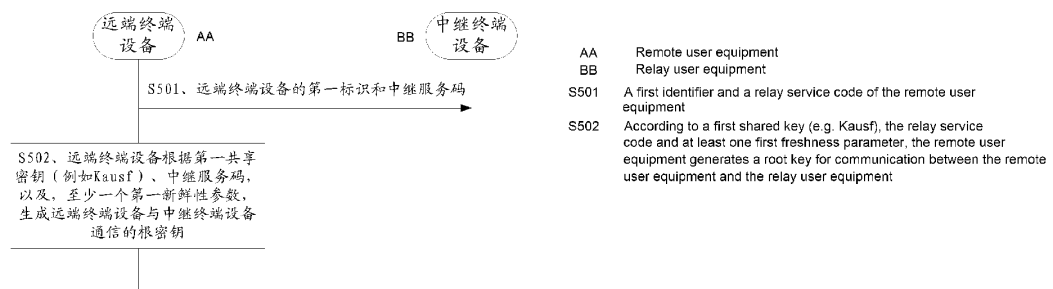


图 5

(57) Abstract: Disclosed are a key acquisition method and a communication apparatus, which relate to the field of communications, and are used for sharing a key between a remote user equipment and a relay user equipment. The key acquisition method comprises: a remote user equipment sending a first identifier and a relay service code to a relay user equipment, wherein the first identifier is an identifier, corresponding to the relay service code, of the remote user equipment, or the first identifier is an anonymous identifier of the remote user equipment; and according to a first shared key, the relay service code and at least one first freshness parameter, the remote user equipment generating a root key for communication between the remote user equipment and the relay user equipment, wherein a remote authentication service function network element is an authentication service function network element that serves the remote user equipment, and the first shared key is a key shared between the remote user equipment and the remote authentication service function network element.

(57) 摘要: 本申请公开了一种密钥获取方法和通信装置, 涉及通信领域, 用于在远端终端设备与中继终端设备之间共享密钥。密钥获取方法包括: 远端终端设备向中继终端设备发送第一标识和中继服务码, 第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识; 远端终端设备根据第一共享密钥、中继服务码, 以及, 至少一个第一新鲜性参数, 生成远端终端设备与中继终端设备通信的根密钥, 远端认证服务功能网元为服务远端终端设备的认证服务功能网元, 第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥。

[见续页]

(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))。