

(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 2022/027476 A1

(43) 国际公布日
2022 年 2 月 10 日 (10.02.2022)

- (51) 国际专利分类号:
H04L 9/32 (2006.01) **H04W 12/04 (2021.01)**
- (21) 国际申请号: PCT/CN2020/107498
- (22) 国际申请日: 2020 年 8 月 6 日 (06.08.2020)
- (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)。 李赫(LI, He); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

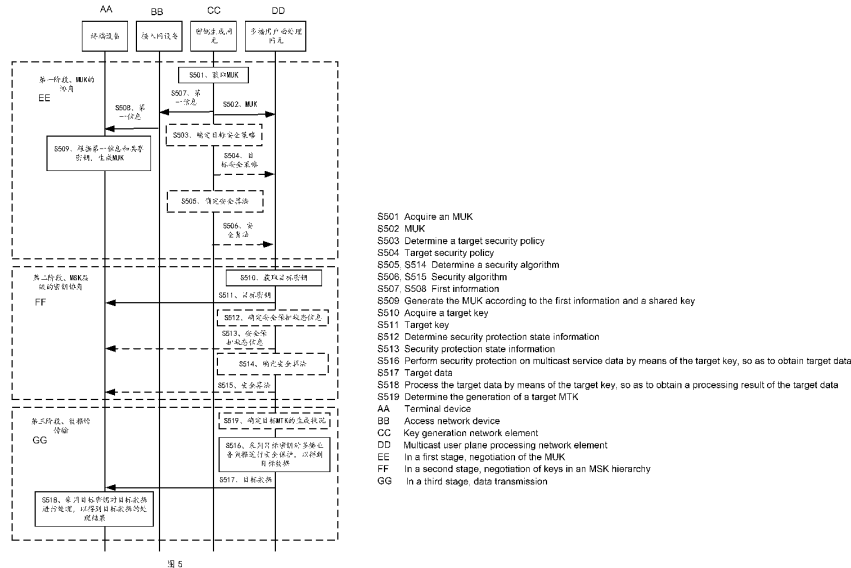
吴荣(WU, Rong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(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, 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,

(54) Title: KEY MANAGEMENT METHOD AND COMMUNICATION APPARATUS

(54) 发明名称: 密钥管理方法及通信装置



(57) Abstract: Provided are a key management method and a communication apparatus, which relate to the technical field of communications, and can enable multicast service data to be securely transmitted, thereby preventing an unauthorized terminal device from acquiring the multicast service data. The method comprises: a terminal device acquiring a target key, wherein the target key comprises at least one of the following keys: a target multimedia broadcast/multicast service service key (MSK), a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK, the first sub-key being used for confidentiality protection

[见续页]

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))。

calculation, and the second sub-key being used for integrity protection calculation; the terminal device receiving target data from a multicast user plane processing network element, wherein the target data is securely protected data; and then, the terminal device processing the target data by using the target key.

(57) 摘要: 本申请实施例提供了密钥管理方法及通信装置, 涉及通信技术领域, 能够使得多播业务数据安全传输, 防止非授权的终端设备获取到多播业务数据。该方法包括: 终端设备获取目标密钥, 其中, 目标密钥包括以下密钥中的至少一个: 目标多媒体广播多播业务业务密钥MSK, 目标MSK对应的第一子密钥, 或目标MSK对应的第二子密钥, 第一子密钥用于机密性保护计算, 第二子密钥用于完整性保护计算。终端设备接收来自多播用户面处理网元的目标数据, 其中, 目标数据是经过安全保护后的数据。然后, 终端设备采用目标密钥对目标数据进行处理。