

(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 4 月 7 日 (07.04.2022)



(10) 国际公布号
WO 2022/067827 A1

(51) 国际专利分类号:
H04W 12/04 (2021.01)

(21) 国际申请号: PCT/CN2020/119760

(22) 国际申请日: 2020 年 9 月 30 日 (30.09.2020)

(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: 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)。

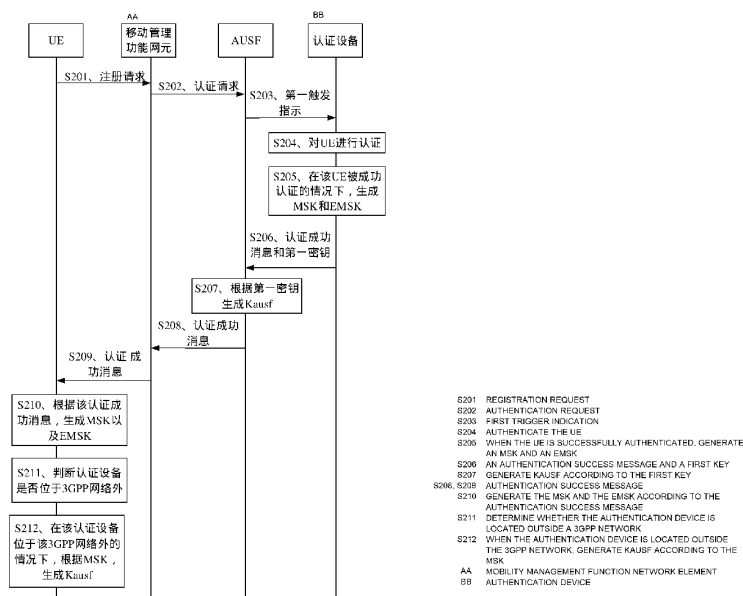
吴荣 (WU, Rong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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 DERIVATION METHOD AND APPARATUS, AND SYSTEM

(54) 发明名称: 一种密钥推衍方法及其装置、系统



(57) Abstract: Disclosed are a key derivation method and apparatus, and a system. The method comprises: a user equipment (UE) receiving an authentication success message from a mobility management function network element, and then generating, according to the authentication success message, a master session key (MSK) and an extended master session key (EMSK); and determining whether an authentication device is located outside a 3rd generation partnership project (3GPP) network, so as to determine whether Kausf is obtained according to the EMSK or the MSK. Therefore, the UE can be compatible with a key derivation mode used by the

[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))。

authentication device when the authentication device is located outside the 3GPP network, and a key derivation mode used by the authentication device when the authentication device is located within the 3GPP network.

(57) 摘要: 本申请实施例公开了一种密钥推衍方法及其装置、系统, 该方法包括: 用户设备UE接收来自移动管理功能网元的认证成功消息, 然后根据该认证成功消息, 生成主会话密钥MSK和扩展主会话密钥EMSK; 并判断认证设备是否位于第三代合作伙伴计划3GPP网络外, 以确定根据EMSK还是MSK获得Kausf, 使得UE可以兼容认证设备位于3GPP网络外所采用的密钥推衍方式, 和认证设备位于3GPP网络内所采用的密钥推衍方式。