

(43) 国际公布日
2022 年 11 月 17 日 (17.11.2022)

(51) 国际专利分类号:
H04W 12/04 (2021.01) H04W 12/06 (2021.01)

(72) 发明人:李飞(LI, Fei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(21) 国际申请号: PCT/CN2022/089936

(74) 代理人: 北京同达信恒知识产权代理有限公司
(TDIP & PARTNERS); 中国北京市西城区裕民路
18号北环中心A座2002, Beijing 100029 (CN)。

(22) 国际申请日: 2022 年 4 月 28 日 (28.04.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:

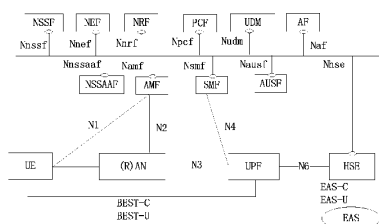
202110504785.6 2021年5月10日 (10.05.2021) CN

(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)。

(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, JM, 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,

(54) **Title:** COMMUNICATION METHOD AND APPARATUS

(54) 发明名称：一种通信方法及装置



S101	First request
S102	Second request
S103	Generate a first key according to a second identifier of the UE
S104	First key
S105	Generate a second key according to the first key
S106	Receive a random number
S107	Generate a cipher key and an integrity key according to the random number and a root key of the UE
S108	Generate the first key according to the cipher key, the integrity key and first information
S109	Generate the second key according to the first key
AA	First network function

图 4

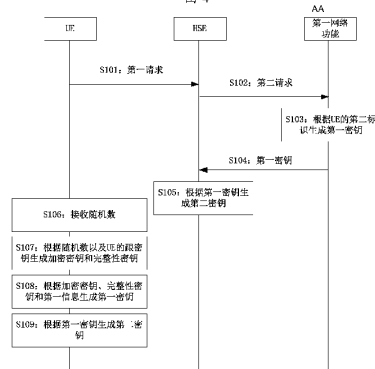


图 5

(57) **Abstract:** A communication method and apparatus, the method comprising: a home network security endpoint being capable of receiving a first request from a user equipment, wherein the first request comprises a first identifier of the user equipment; the home network security endpoint being further capable of sending a second request to a first network function, wherein the second request comprises a second identifier of the user equipment, and receiving a first key from the first network function, wherein the first key is generated according to a cipher key, an integrity key and first information; and the home network security endpoint being capable of

[见续页]

WO 2022/237561 A1

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))。

generating a second key according to the first key, wherein the second key comprises a confidentiality protection key and/or an integrity protection key. The first information comprises at least one of a service network name of the user equipment, an identifier of the home network security endpoint, a SUPI of the user equipment, and a BEST service identifier. In the process, a security key acquisition mode applicable to a 5G network architecture is provided, and data security risk of the user equipment can be reduced.

(57) 摘要: 一种通信方法及装置, 其中方法包括: 归属网络安全节点可接收来自用户设备的第一请求, 第一请求包括用户设备的第一标识。归属网络安全节点还可向第一网络功能发送第二请求, 第二请求包括用户设备的第二标识, 并接收来自于第一网络功能的第一密钥, 第一密钥根据加密密钥、完整性密钥和第一信息生成。归属网络安全节点可根据第一密钥生成第二密钥, 第二密钥包括机密性保护密钥和/或完整性保护密钥。其中, 第一信息包括用户设备的服务网络名称、归属网络安全节点的标识、用户设备的SUPI, 以及BEST服务标识中的至少一个。该过程提供了适用于5G网络架构的安全密钥获取方式, 能够降低用户设备的数据安全风险。