

(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 2022/199291 A1

(43) 国际公布日
2022 年 9 月 29 日 (29.09.2022)

(51) 国际专利分类号:
H04W 4/80 (2018.01)

(21) 国际申请号: PCT/CN2022/076773

(22) 国际申请日: 2022 年 2 月 18 日 (18.02.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110317802.5 2021 年 3 月 25 日 (25.03.2021) CN

(71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 黄琳 (HUANG, Lin); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。简云定 (JIAN, Yunding); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。伏伟 (FU, Wei); 中国浙

江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。曹鸿健 (CAO, Hongjian); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。张婉桥 (ZHANG, Wanqiao); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。刘宇佳 (LIU, Yujia); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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,

(54) Title: APPLICATION LAYER KEY GENERATION

(54) 发明名称: 生成应用层密钥

(57) Abstract: Embodiments of the present description provide an application layer key generation method and apparatus. The method of the embodiments comprises: first determining a connecting mode used when a Bluetooth connection is established with an external Bluetooth device; then determining an application layer key generation function according to the determined connecting mode; then obtaining a link layer dynamic parameter used in a link layer; obtaining an application layer key identifier agreed with the external Bluetooth device; and using the application layer key generation function, the link layer dynamic parameter, and the application layer key identifier to generate an application layer key.

(57) 摘要: 本说明书实施例提供了一种生成应用层密钥的方法和装置。根据该实施例的方法, 首先确定该与外部蓝牙设备建立蓝牙连接时使用的连接模式, 然后根据确定的连接模式确定应用层密钥生成函数, 然后获取在链路层使用的链路层动态参数, 以及获取与外部蓝牙设备约定好的应用层密钥标识, 通过利用该应用层密钥生成函数、链路层动态参数和应用层密钥标识, 从而生成应用层密钥。

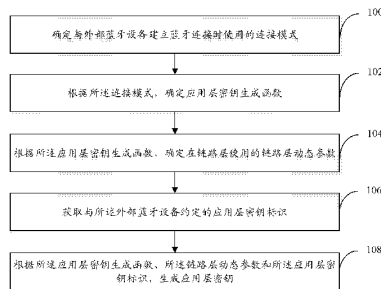


图 2

- 100 Determine a connecting mode used when a Bluetooth connection is established with an external Bluetooth device
102 Determine an application layer key generation function according to the connecting mode
104 Determine, according to the application layer key generation function, a link layer dynamic parameter used in a link layer
106 Obtain an application layer key identifier agreed with the external Bluetooth device
108 Generate an application layer key according to the application layer key generation function, the link layer dynamic parameter, and the application layer key identifier

WO 2022/199291 A1

[见续页]

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。

(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))。