

(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 2024/235050 A1

(43) 国际公布日
2024 年 11 月 21 日 (21.11.2024)

(51) 国际专利分类号:
H04W 12/04 (2021.01)

(21) 国际申请号: PCT/CN2024/091411

(22) 国际申请日: 2024 年 5 月 7 日 (07.05.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310544449.3 2023年5月15日 (15.05.2023) 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)。

(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

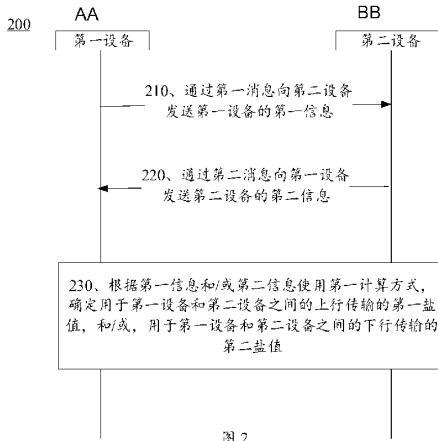
(CN)。亨达诺阿门·本 (HENDA, Noamen Ben); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (LONGSUN LEAD IP LTD.); 中国北京市海淀区北清路 81 号院二区 3 号楼 8 层 801-1 室, Beijing 100094 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,

(54) Title: SECURE COMMUNICATION METHOD AND APPARATUS

(54) 发明名称: 安全通信方法和装置



210 Send first information of a first device to a second device by means of a first message
220 Send second information of the second device to the first device by means of a second message
230 According to the first information and/or the second information, determine a first salt value for uplink transmission between the first device and the second device by using a first calculation mode, and/or determine a second salt value for downlink transmission between the first device and the second device
AA First device
BB Second device

图 2

(57) Abstract: The present application provides a secure communication method and apparatus. The method comprises: a first device sends first information of the first device to a second device by means of a first message, the first message comprising one or more of a first port number, a first security parameter index (SPI), a first Internet protocol (IP) address, a first security algorithm list, and a first random number; the first device receives a second message from the second device, the second message comprising second information, and the second message comprising one or more of a second port number, a second SPI, a second IP address, a second security algorithm list, and a second random number; and according to the first information and/or the second information, the first device determines a first salt value for uplink transmission between the first device and the second device by using a first calculation mode, and/or determines a second salt value for downlink transmission between the first device and the second device by using a second calculation mode. The security of uplink and downlink communication between the first device and the second device can be ensured.

[见续页]

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, CV, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SC, 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, ME, 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))。

(57) 摘要: 本申请提供了一种安全通信方法和装置, 该方法包括: 第一设备通过第一消息向第二设备发送第一设备的第一信息, 第一消息包括第一端口号、第一安全参数索引SPI、第一互联网协议IP地址、第一安全算法列表、第一随机数中的一项或多项; 第一设备接收来自第二设备的包括第二信息的第二消息, 第二消息包括第二端口号、第二SPI、第二IP地址、第二安全算法列表、第二随机数中的一项或多项; 第一设备根据第一信息和/或第二信息, 使用第一计算方式确定用于第一设备与第二设备之间上行传输的第一盐值, 和/或使用第二计算方式确定用于第一设备与第二设备之间下行传输的第二盐值。能够保证第一设备和第二设备之间的上行、下行通信安全。