

(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 2023/230929 A1

(43) 国际公布日
2023 年 12 月 7 日 (07.12.2023)

(51) 国际专利分类号:
H04L 9/30 (2006.01)

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/CN2022/096486

(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)。

(22) 国际申请日: 2022 年 5 月 31 日 (31.05.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

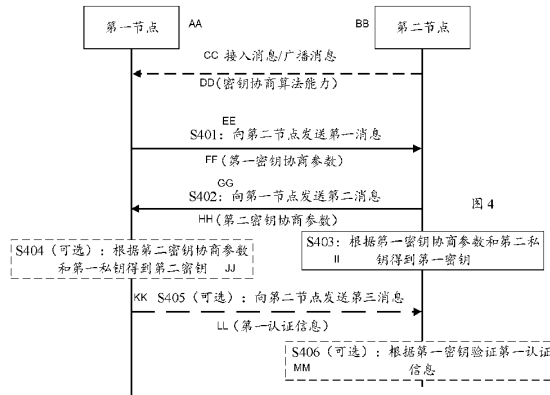
(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(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, IQ, 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,

(72) 发明人: 王勇 (WANG, Yong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 杨艳江 (YANG, Yanjiang); 中国广

(54) Title: COMMUNICATION METHOD AND RELATED APPARATUS

(54) 发明名称: 通信方法及相关装置



AA First node
BB Second node
CC Access message/broadcast message
DD (key negotiation algorithm capability)
EE S401: Send a first message to a second node
FF (first key negotiation parameter)
GG S402: Send a second message to a first node
HH (second key negotiation parameter)
II S403: Obtain a first key according to the first key negotiation parameter and a second private key
JJ S404 (optional): Obtain a second private key according to the second key negotiation parameter and a first private key
KK S405 (optional): Send a third message to the second node
LL (first authentication information)
MM S406 (optional): Verify the first authentication information according to the first key

(57) Abstract: Provided are a communication method and a related apparatus, applicable to the fields of communication technologies and intelligent vehicles. The method comprises: receiving a first message from a first node, wherein the first message comprises a first key negotiation parameter, the first key negotiation parameter is obtained by means of a first private key and an intermediate parameter, the intermediate parameter is obtained from a security parameter and a common parameter, and the security parameter is a first password or a PSK; determining a first key according to the first key negotiation parameter and a second private key; sending a

[见续页]

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, 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, 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))。

second message to the first node, the second message comprising a second key negotiation parameter, and the second key negotiation parameter being obtained by means of the second private key and the intermediate parameter; and obtaining the first key according to the first key negotiation parameter and the second private key. According to embodiments of the present application, the security of a shared key can be improved, thereby avoiding the access of an untrusted attacker and improving the security of a node.

(57) 摘要: 一种提供通信方法及相关装置, 应用于通信技术、智能车领域。该方法包括: 接收来自第一节点的第一消息, 第一消息包含第一密钥协商参数, 第一密钥协商参数通过第一私钥和中间参数得到, 中间参数由安全参数和公共参数得到, 安全参数为第一口令或PSK; 根据第一密钥协商参数和第二私钥确定第一密钥; 向第一节点发送第二消息, 第二消息包含第二密钥协商参数, 第二密钥协商参数通过第二私钥和中间参数得到; 根据所述第一密钥协商参数和所述第二私钥, 得到第一密钥。本申请实施例能够提高共享密钥的安全性, 避免不可信的攻击者接入, 提升节点安全性。