

(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
2023 年 3 月 16 日 (16.03.2023)



(10) 国际公布号
WO 2023/036348 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) **H04L 61/103** (2022.01)

(21) 国际申请号: PCT/CN2022/130453

(22) 国际申请日: 2022 年 11 月 8 日 (08.11.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:

202111050009.X	2021 年 9 月 8 日 (08.09.2021)	CN
202111051342.2	2021 年 9 月 8 日 (08.09.2021)	CN
202111049948.2	2021 年 9 月 8 日 (08.09.2021)	CN
202111051275.4	2021 年 9 月 8 日 (08.09.2021)	CN

(71) 申请人: 北京世纪互联宽带数据有限公司 (BEIJING VNET BROADBAND DATA CENTER CO., LTD.) [CN/CN]; 中国北京市朝阳区酒仙桥东路 10 号冠捷办公楼, Beijing 100016 (CN)。

(72) 发明人: 陈升 (CHEN, Sheng); 中国北京市朝阳区酒仙桥东路 10 号冠捷办公楼, Beijing 100016 (CN)。李信满 (LI, Xinman); 中国北京市朝阳区酒仙桥东路 10 号冠捷办公楼, Beijing 100016 (CN)。蔡焜 (CAI, Kun); 中国北京市朝阳区酒仙桥东路 10 号冠捷办公楼, Beijing 100016 (CN)。佟磊 (TONG, Lei); 中国北京市朝阳区酒仙桥东路 10 号冠捷办公楼, Beijing 100016 (CN)。马炬 (MA, Ju); 中国北京市朝阳区酒仙桥东路 10 号冠捷办公楼, Beijing 100016 (CN)。

(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)。

(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,

(54) Title: ENCRYPTED COMMUNICATION METHOD AND APPARATUS, DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 一种加密通信方法、装置、设备及介质

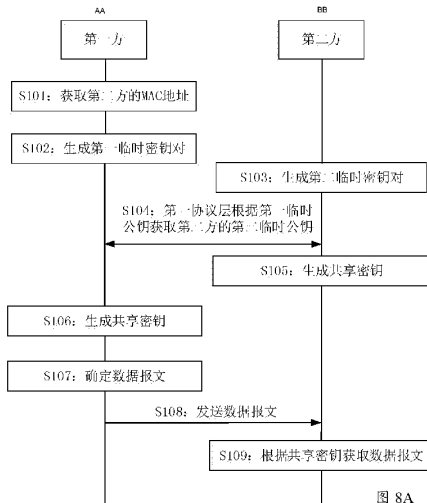


图 8A

S101 Obtain a MAC address of a second party
S102 Generate a first temporary key pair
S103 Generate a second temporary key pair
S104 The first protocol layer obtains a second temporary public key of the second party according to the first temporary public key
S105 Generate a shared key
S106 Generate a shared key
S107 Determine a data message
S108 Send the data message
S109 Obtain the data message according to the shared key
AA The first party
BB The second party

(57) Abstract: The present application provides an encrypted communication method and apparatus, a device, and a medium. The method comprises: a first protocol layer of a first party obtains a MAC address of a second party according to a data transmission request from an application layer, the data transmission request comprising an NLP address of the second party; the first protocol layer generates a first temporary key pair, the first temporary key pair comprising a first temporary public key and a first temporary private key; the first protocol layer obtains a second temporary public key of the second party according to the first temporary public key; the first protocol layer generates a shared key according to the second temporary public key and the first temporary private key; the first protocol layer determines a data message, the data message carrying encrypted data obtained by encrypting the shared key, and the receiver of the data message being the second party. The present method can prevent the shared key from being illegally stolen, and improve the communication security of both communication parties.

(57) 摘要: 本申请提供一种加密通信方法、装置、设备及介质, 其中, 方法包括: 第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的 MAC 地址, 数据传输请求中包括第二方的 NLP 地址; 第一协议层生成第一临时密钥对, 第一临时密钥对包括第一临时公钥以及第一临时私钥; 第一协议层根据第一临时公钥获取第二方的第二临时公钥; 第一协议层根据第二临时公钥和第一临时私钥生成共享密钥; 第一协议层确定数据报文, 数据报文中携带通过共享密钥加密获得的加密数据, 数据报文的接收方为第二方。通过该方法, 可以防止共享密钥被非法盗用, 提高通信双方的通信安全。

[见续页]

WO 2023/036348 A1

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, 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, 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, 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))。
- 在修改权利要求的期限届满之前进行, 在收到该修改后将重新公布 (细则48.2(h))。
- 包括关于请求恢复一项或多项优先权要求的信息 (细则26之二.3和48.2(b)(vii))。