

(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
2020 年 7 月 2 日 (02.07.2020)



(10) 国际公布号
WO 2020/135853 A1

- (51) 国际专利分类号:
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
- (21) 国际申请号: PCT/CN2019/129769
- (22) 国际申请日: 2019 年 12 月 30 日 (30.12.2019)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201811633995.X 2018 年 12 月 29 日 (29.12.2018) CN
- (71) 申请人: 上海唯链信息科技有限公司 (SHANGHAI WEILIAN INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国上海市长宁区镇宁路 465 弄 161 号 3 号楼 229 室, Shanghai 200050 (CN)。
- (72) 发明人: 顾建良 (GU, Jianliang); 中国上海市虹口区海伦路 555 弄 C 楼 2301 室, Shanghai 200080 (CN)。
马帮亚 (MA, Bangya); 中国上海市浦东新区秀沿路 1028 号 101 号楼 303 室, Shanghai 201315 (CN)。
- (74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路 8 号 B 座 1601A, Beijing 100192 (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, 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,

(54) Title: KEY SECURITY MANAGEMENT SYSTEM AND METHOD, MEDIUM, AND COMPUTER PROGRAM

(54) 发明名称: 密钥安全管理系统和方法、介质和计算机程序

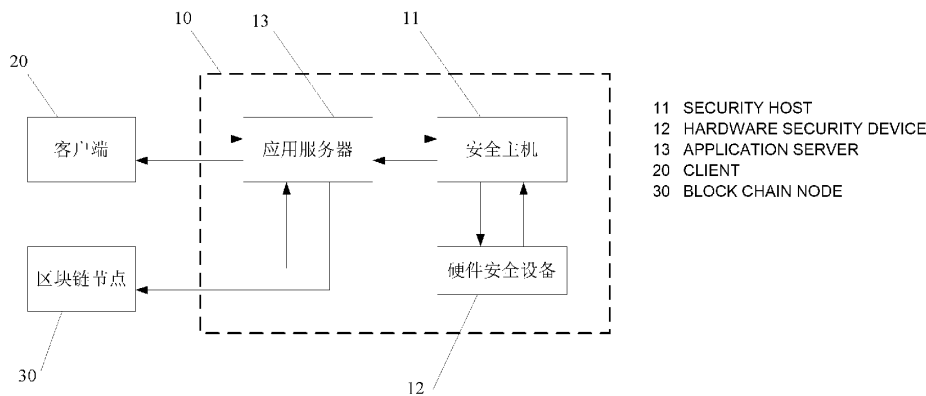


图 1

(57) Abstract: Disclosed in the present application are a key security management system and method, a computer readable storage medium, and a computer program. The key security management system comprises a security host and a hardware security device; the security host is configured to receive a first operation request, verify the first operation request, and generate a second operation request on the basis of the first operation request when the verification succeeds, the first operation request and the second operation request each comprising an identification; the hardware security device is configured to receive the second operation request from the security host, verify the second operation request, parse the type of the second operation request when the verification succeeds, and execute, on the basis of the type of the second operation request, an operation related to a key pair associated with the identification, the key pair comprising a public key and a private key which are specific to the identification.

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, 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))。

(57) 摘要: 本申请公开了一种密钥安全管理系统、方法、计算机可读存储介质和计算机程序。密钥安全管理系统包括安全主机和硬件安全设备, 安全主机被配置为接收第一操作请求, 对第一操作请求进行验证, 并在验证通过时基于第一操作请求生成第二操作请求, 所述第一操作请求和所述第二操作请求都包括身份标识, 硬件安全设备被配置为从安全主机接收第二操作请求, 对第二操作请求进行验证, 并且在验证通过时解析第二操作请求的类型, 以及基于第二操作请求的类型执行和关联于身份标识的密钥对有关的操作, 其中密钥对包括特定于该身份标识的一个公钥和一个私钥。