

(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 3 月 5 日 (05.03.2020)



(10) 国际公布号
WO 2020/042798 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2019/096309

(22) 国际申请日: 2019 年 7 月 17 日 (17.07.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811010286.6 2018 年 8 月 31 日 (31.08.2018) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 肖淑婷 (XIAO, Shuting); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴

巴集团法务部, Zhejiang 311121 (CN)。林孝旦 (LIN, Xiaodan); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。方海峰 (FANG, Haifeng); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。谷胜才 (GU, Shengcai); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (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,

(54) Title: CRYPTOGRAPHIC OPERATION AND WORKING KEY CREATION METHOD AND CRYPTOGRAPHIC SERVICE PLATFORM AND DEVICE

(54) 发明名称: 密码运算、创建工作密钥的方法、密码服务平台及设备

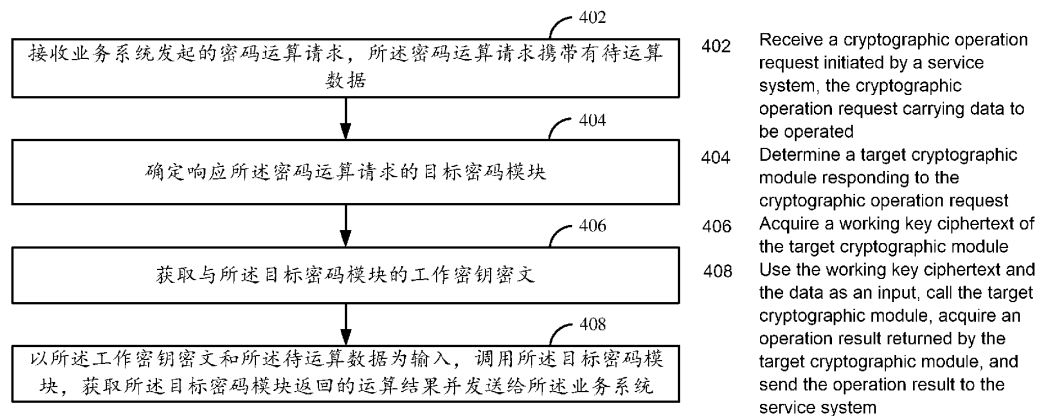


图 4

(57) Abstract: The description provides a cryptographic operation and working key creation method and a cryptographic service platform and device. In a cryptographic module connected to the cryptographic service platform, a key management function is provided by a primary cryptographic module. The primary cryptographic module is for generating a key. Both the primary cryptographic module and secondary cryptographic modules provide a cryptographic operation function required by the cryptographic service platform. Each cryptographic module independently generates a master key thereof. A working key of a service system is generated by the primary cryptographic module. The cryptographic service platform stores a working key ciphertext encrypted by the master key of the primary cryptographic module and a working key ciphertext encrypted by the master key of each secondary cryptographic module. Neither the master key nor a working key plaintext, which function as sensitive security parameters, exceed a boundary of the cryptographic module, such that the security of the key is not put at risk, thereby meeting key security requirements. The cryptographic service platform calls any one of the cryptographic modules to respond to a cryptographic operation request of the service system, and the cryptographic service platform is compatible with various cryptographic modules.

[见续页]

WO 2020/042798 A1

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, 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: 本说明书提供一种密码运算、创建工作密钥的方法、密码服务平台及设备, 密码服务平台所连接的密码模块中, 密钥管理功能由主密码模块提供, 主密码模块用于生成密钥, 主密码模块和次密码模块都可提供密码服务平台所需要的密码运算功能。各个密码模块各自独立生成自身的主密钥, 业务系统的工作密钥则由主密码模块生成, 密码服务平台保存有主密码模块的主密钥加密的工作密钥密文, 以及各个次密码模块的主密钥分别加密的工作密钥密文。作为敏感安全参数的主密钥、工作密钥明文均不会超出密码模块的边界, 不会损失密钥的安全性, 满足密钥的安全性要求。密码服务平台可调用任一密码模块响应业务系统的密码运算请求, 密码服务平台能够兼容多种密码模块。