

(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
2016 年 6 月 9 日 (09.06.2016)



(10) 国际公布号
WO 2016/086788 A1

(51) 国际专利分类号:

H04W 12/04 (2009.01)

(21) 国际申请号:

PCT/CN2015/095588

(22) 国际申请日:

2015 年 11 月 26 日 (26.11.2015)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201410721298.5 2014 年 12 月 2 日 (02.12.2014) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [GB/CN]; 英国开曼群岛大开曼乔治城资本大厦一座四层 847 号邮箱, Cayman Islands (GB)。

(72) 发明人: 及

(71) 申请人 (仅对美国): 宋宜涛 (SONG, Yitao) [CN/CN]; 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: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区西坝河西里 28 号英特公寓 C 座 104, Beijing 100028 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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,

[见续页]

(54) Title: METHOD AND APPARATUS FOR ENCRYPTING/DECRYPTING DATA ON MOBILE TERMINAL

(54) 发明名称: 移动终端上数据加/解密方法及装置

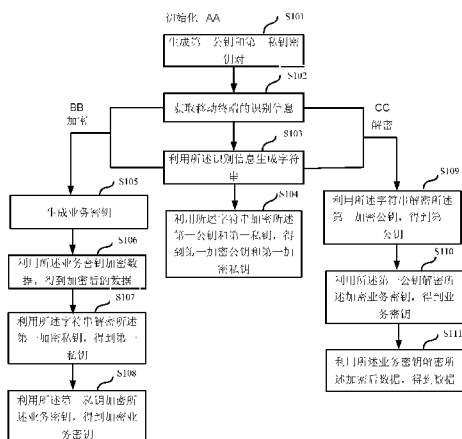


图 1 / FIG. 1

S101 GENERATING A KEY PAIR CONSISTING OF A FIRST PUBLIC KEY AND A FIRST PRIVATE KEY
S102 ACQUIRING IDENTIFICATION INFORMATION ABOUT A MOBILE TERMINAL
S103 GENERATING A CHARACTER STRING USING THE IDENTIFICATION INFORMATION
S104 ENCRYPTING THE FIRST PUBLIC KEY AND THE FIRST PRIVATE KEY USING THE CHARACTER STRING TO OBTAIN A FIRST ENCRYPTED PUBLIC KEY AND A FIRST ENCRYPTED PRIVATE KEY
S105 GENERATING A SERVICE KEY
S106 ENCRYPTING DATA USING THE SERVICE KEY TO OBTAIN ENCRYPTED DATA
S107 DECRYPTING THE FIRST ENCRYPTED PRIVATE KEY USING THE CHARACTER STRING TO OBTAIN A FIRST PRIVATE KEY
S108 ENCRYPTING THE SERVICE KEY USING THE FIRST PRIVATE KEY TO OBTAIN AN ENCRYPTED SERVICE KEY
S109 DECRYPTING THE FIRST ENCRYPTED PUBLIC KEY USING THE CHARACTER STRING TO OBTAIN A FIRST PUBLIC KEY
S110 DECRYPTING THE ENCRYPTED SERVICE KEY USING THE FIRST PUBLIC KEY TO OBTAIN A SERVICE KEY
S111 DECRYPTING THE ENCRYPTED DATA USING THE SERVICE KEY TO OBTAIN DATA
AA INITIALIZATION
BB ENCRYPTION
CC DECRYPTION

(57) Abstract: The present invention relates to a method and apparatus for encrypting/decrypting data on a mobile terminal. The method comprises: pre-generating a key pair consisting of a first public key and a first private key; acquiring identification information about a mobile terminal; encrypting the key pair consisting of the first public key and the first private key using the identification information to obtain a first encrypted public key and a first encrypted private key and saving same; when a service key is encrypted, encrypting the service key using the first private key to obtain an encrypted service key; when the service key is decrypted, decrypting the encrypted service key using the first public key to obtain the service key; acquiring data needing to be encrypted/decrypted of the mobile terminal; and encrypting/decrypting the data using the service key. According to the method and apparatus for encrypting/decrypting data involved in the present invention, hardware protection is not required, and the data protection cost is low. In addition, the security of the data can be protected in an off-line case, so that the data cannot be intercepted and tampered with.

(57) 摘要: 本发明涉及一种移动终端上数据加/解密方法及装置, 所述方法包括: 预先生成第一公钥和第一私钥密钥对; 获取所述移动终端的识别信息; 利用所述识别信息对所述第一公钥和第一私钥密钥对进行加密, 得到第一加密公钥和第一加密私钥并保存; 加密业务密钥时, 利用所述第一私钥对所述业务密钥进行加密, 得到加密业务密钥; 解密业务密钥时, 利用所述第一公钥对所述加密业务密钥进行解密, 得到所述业务密钥; 获取所述移动终端需要加/解密的数据; 利用所述业务密钥对所述数据进行加/解密。本发明涉及的数据加/解密方法及装置, 无需硬件保护, 数据保护成本低, 而且, 在离线的环境下即能保护数据的安全, 使其不被窃取和篡改。



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))。