(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)

WIPO | PCT

(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

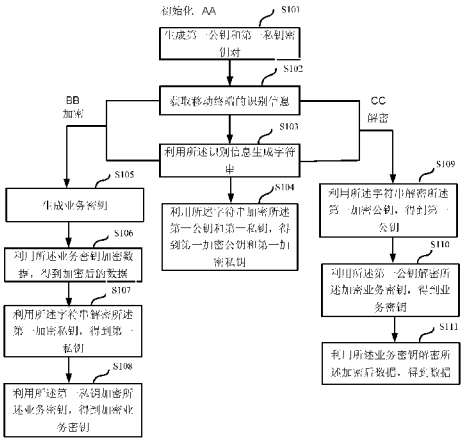

图 1 / FIG. 1

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，在离线的情况下即能保护数据的安全，使其不被窃取和篡改。

WO 2016/086788 A1

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))。

移动终端上数据加/解密方法及装置

技术领域

本申请涉及数据处理领域，尤其涉及一种移动终端上数据加/解密方法及装置。

背景技术

随着移动通信和网络技术的发展，人们逐渐养成了利用移动终端（手机、平板电脑等）访问网络的习惯。因此，在移动终端上需要保存很多隐私数据，包括手机设备的唯一标识及一些关键的业务数据。这些数据需要被安全的存储在移动终端上，因此需要一种安全的数据加密方法来保证这些隐私数据不被窃取和篡改。

现有技术中，移动终端的数据保护采取硬件保护或者公私钥保护的方式。硬件保护一般是利用加密卡或者手机盾作为保护移动终端隐私数据的载体，直接明文存储的方式。例如，使用银行的证书盾，在中央处理器中集成密钥种子进行数据的加密、解密。利用公私密钥对移动终端数据进行保护则需要通过网络交互的密钥进行加密。

采用硬件保护移动终端数据的方式，成本较高，不适合在大众中推广和普及。采用公私密钥对移动终端数据进行保护，使用时需要到服务器解密，需要网络连接才能实现，不能够在离线状态下使用。

发明内容

本申请的目的是提供一种移动终端上数据加/解密方法及装置，无需硬件保护，在离线的情况下即能保护数据的安全，使其不被窃取和篡改。

第一方面，本申请提供了一种移动终端上数据加/解密方法，所述方法包括：生成业务密钥，并对所述业务密钥进行加/解密，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，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加密私钥进行解密，得到所述第一私钥;

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，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加密公钥进行解密，得到所述第一公钥;

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。

第二方面，本申请提供了一种移动终端上数据加/解密装置，所述装置包括:

第一生成单元，用于生成业务密钥;

第二生成单元，用于预先生成第一公钥和第一私钥密钥对;

第一获取单元，用于获取所述移动终端的识别信息;

第一加密单元，用于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;

第一解密单元，用于利用所述识别信息对所述第一加密私钥进行解密，得到所述第一私钥;

第二加密单元，用于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;

第二解密单元，用于利用所述识别信息对所述第一加密公钥进行解密，得到所述第一公钥;

第三解密单元，用于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;

第二获取单元，用于获取所述移动终端需要加/解密的数据;

第三加密单元，用于利用所述业务密钥对所述数据进行加密;

第四解密单元，用于利用所述业务密钥对所述数据进行解密。

本申请实施例提供的移动终端上数据加/解密方法及装置，通过初始化、加密、解密的过程，实现了对移动终端隐私数据的保护。而且，无需硬件参与，数据保护成本低，在离线的情况下即能保护数据的安全，使其不被窃取和篡改。

附图说明

图 1 为本申请实施例一提供的移动终端上数据加/解密方法流程图;

图 2 为本申请实施例二提供的移动终端上数据加/解密装置示意图。

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

为便于对本申请实施例的理解，下面将结合附图以具体实施例做进一步的解释说明，实施例并不构成对本申请实施例的限定。

本申请实施例提供的移动终端上数据加/解密方法及装置，适用于移动终端，如手机、平板电脑等。

图 1 为本申请实施例一提供的移动终端上数据加/解密方法流程图。所述方法各步骤执行主体为移动终端。如图 1 所示，所述方法具体包括:

S101，生成第一公钥和第一私钥密钥对。

具体地，移动终端生成第一公钥和第一私钥密钥对，生成方式为现有技术，此处不做详细描述。所述第一公钥和第一私钥同时生成，第一公钥加密的信息只有第一私钥才能解密，第一私钥加密的信息只有第一公钥才能解密。

S102，获取移动终端的识别信息。

具体地，通过代码获取移动终端的识别信息。

所述识别信息包括以下一种或多种:

移动终端的 IMEI(International Mobile Equipment Identity,移动终端国际身份码)、IMSI(International Mobile Subscriber Identification Number,国际移动用户识别码)、MAC(Media Access Control,介质访问控制地址)和 UUID(Universally Unique Identifier,通用唯一识别)。

S103，利用所述识别信息生成字符串。

具体地，将所述识别信息进行哈希算法处理，得到字符串。

哈希算法将任意长度的二进制值映射为较短的固定长度的二进制值，这个较短的二进制值称为哈希值。哈希值是一段数据唯一且极其紧凑的数值表示形式。如果散列一段明文只更改该段落的一个字母，随后的哈希都将产生不同的值。要找到散列为同一个值的两个不同的输入，在计算上是不可能的，所以数据的哈希值可以检验数据的完整性。一般用于快速查找和加密算法。

S104，利用所述字符串加密所述第一公钥和第一私钥，得到第一加密公钥和第一加密私钥。

具体地，利用所述字符串和对称加密算法加密所述第一公钥和第一私钥，得到第一加密公钥和第一加密私钥。

所述加密算法可以为：高级加密标准算法（Advanced Encryption Standard，AES）、数据加密标准算法（Data Encryption Standard，DES）、三重数据加密算法等。

需要说明的是，所述字符串即为根密钥，生成以后即用来加密所述第一公钥和第一私钥，根密钥不保存，需要时利用所述移动终端的识别信息生成。

以上过程为初始化过程，每台移动终端都需要初始化，只需要初始化一次，初始化是加密、解密的前提条件。初始化过程的目的是得到第一加密公钥和第一加密私钥。

S105，生成业务密钥。

具体地，业务密钥是由移动终端随机生成业务密钥，每一种业务使用一种业务密钥。生成业务密钥和生成第一公钥和第一私钥密钥对的方式相同，此处不做详细描述。

S106，利用所述业务密钥加密数据，得到加密后的数据。

具体地，获取所述移动终端的加密数据，利用所述业务密钥和对称加密算法加密数据，得到加密后的数据，保证了数据的安全性。所述数据包括隐私数据，比如用户的生物特征等。

S107，利用所述字符串解密所述第一加密私钥，得到第一私钥。

在步骤 S107 之前，由于根密钥未保存，所以需要重复执行步骤 S102 和 S103，得到所述字符串。

利用所述字符串和对称解密算法解密所述第一加密私钥，得到第一私钥。

S108，利用所述第一私钥加密所述业务密钥，得到加密业务密钥。

具体地，利用所述第一私钥和非对称算法加密所述业务密钥，得到加密业务密钥。

所述非对称算法可以为：公钥加密算法（RSA）、数字签名算法（Digital Signature Algorithm，DSA）等。

需要说明的是，步骤 S105- S108 为加密过程，实现了对隐私数据进行加密，保护隐私数据不被窃取和篡改。并且步骤 S108 得到的加密后的业务密钥可用于使用隐私数据时，解密所述加密后的隐私数据。

S109，利用所述字符串解密所述第一加密公钥，得到第一公钥。

在步骤 S109 之前，由于根密钥未保存，所以需要重复执行步骤 S102 和 S103，得到所述字符串。

利用所述字符串和对称解密算法解密所述第一加密公钥，得到第一公钥。

S110，利用所述第一公钥解密所述加密业务密钥，得到业务密钥。

具体地，利用所述第一公钥和非对称解密算法解密所述加密业务密钥，得到业务密钥。

S111，利用所述业务密钥解密所述加密后的数据，得到数据。

具体地，利用所述业务密钥和对称解密算法解密所述加密后隐私数据，得到隐私数据。

需要说明的是，步骤 S109-S111 为对加密后的数据进行解密的过程。由于字符串是根据设备本身标识生成的，解密时可以根据手机设备随时生成字符串进行解密，因此无需访问服务器，离线情况下即能对加密后的隐私数据进行解密。同时由于是根据本机设备生成字符串用于加解密，即使数据泄露，当其他人使用其他设备时无法完成解密，因此，可以有效的保护用户隐私不被泄露。

本申请实施例一提供的移动终端上数据加/解密方法，通过初始化、加密、解密的过程，实现了对移动终端隐私数据的保护。其中，根秘钥不保存，通过移动终端的信息计算，公私密钥对保护业务秘钥的安全，业务秘钥保护数据的安全。无需硬件保护，数据保护成本低，在离线的情况下即能保护数据的安全，使其不被窃取和篡改。

与上述移动终端上数据加/解密方法对应地，本申请实施例二提供了一种移动终端上数据加/解密装置，图 2 为本申请实施例二提供的移动终端上数据加/解密装置示意图。如图 2 所示，所述装置具体包括：第一生成单元 201、第二生成单元 202、第一获取单元 203、第一加密单元 204、第一解密单元 205、第二加密单元 206、第二解密单元 207、第三解密单元 208、第二获取单元 209、第三加密单元 210、第四解密单元 211。

所述第一生成单元 201，用于生成业务密钥；

所述第二生成单元 202，用于预先生成第一公钥和第一私钥密钥对；

所述第一获取单元 203，用于获取所述移动终端的识别信息；

所述第一加密单元 204，用于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；

所述第一解密单元 205，用于利用所述识别信息对所述第一加密私钥进行解密，得到所述第一私钥；

所述第二加密单元 206，用于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；

所述第二解密单元 207，用于利用所述识别信息对所述第一加密公钥进行解密，得到所述第一公钥；

所述第三解密单元 208，用于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；

所述第二获取单元 209，用于获取所述移动终端需要加/解密的数据；

所述第三加密单元 210，用于利用所述业务密钥对所述数据进行加密；

所述第四解密单元 211，用于利用所述业务密钥对所述数据进行解密。

可选地，所述第一加密单元 204 具体用于：

根据所述识别信息生成字符串；

利用所述字符串分别对第一公钥和第一私钥对进行加密处理。

可选地，所述第一解密单元 205 具体用于：

根据所述识别信息生成字符串；

利用所述字符串对所述第一加密私钥进行解密处理。

可选地，所述第二解密单元 207 具体用于：

根据所述识别信息生成字符串；

利用所述字符串对所述第一加密公钥进行解密处理。

可选地，所述根据所述识别信息生成字符串，具体为：

将所述识别信息进行哈希算法处理，得到所述字符串。

可选地，所述识别信息包括以下一种或多种：

移动终端的 IMEI(International Mobile Equipment Identity,移动终端国际身份码)、IMSI(International Mobile Subscriber Identification Number,国际移动用户识别码)、MAC(Media Access Control,介质访问控制地址)和 UUID(Universally Unique Identifier,通用唯一识别)。

本申请实施例二提供的装置植入了本申请实施例一提供的方法，因此，本申请提供的装置的具体工作过程，在此不复赘述。

本申请实施例二提供的移动终端上数据加/解密装置，通过初始化、加密、解密的过程，实现了对移动终端隐私数据的保护。其中，根秘钥不保存，通过移动终端的信息计算，公私密钥对保护业务秘钥的安全，业务秘钥保护数据的安全。无需硬件保护，数据保护成本低，在离线的情况下即能保护数据的安全，使其不被窃取和篡改。

专业人员应该还可以进一步意识到，结合本文中所公开的实施例描述的各示例的对象及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

结合本文中所公开的实施例描述的方法或算法的步骤可以用硬件、处理器执行的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

以上所述的具体实施方式，对本申请的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本申请的具体实施方式而已，并不用于限定本申请的保护范围，凡在本申请的精神和原则之内，所做

的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权 利 要 求 书

1. 一种移动终端上数据加/解密方法，其特征在于，所述方法包括:

生成业务密钥，并对所述业务密钥进行加/解密，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，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加密私钥进行解密，得到所述第一私钥，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，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加密公钥进行解密，得到所述第一公钥，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。

2. 根据权利要求 1 所述的数据加/解密方法，其特征在于，所述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，具体为:

根据所述识别信息生成字符串;

利用所述字符串分别对第一公钥和第一私钥对进行加密处理。

3. 根据权利要求 1 所述的数据加/解密方法，其特征在于，所述利用所述识别信息对所述第一加密私钥进行解密，具体为:

根据所述识别信息生成字符串;

利用所述字符串对所述第一加密私钥进行解密处理。

4. 根据权利要求 1 所述的数据加/解密方法，其特征在于，所述利用所述识别信息对所述第一加密公钥进行解密，具体为:

根据所述识别信息生成字符串;

利用所述字符串对所述第一加密公钥进行解密处理。

5. 根据权利要求 3 或 4 所述的数据加/解密方法，其特征在于，所述根据所述识别信息生成字符串，具体为：

将所述识别信息进行哈希算法处理，得到所述字符串。

6. 根据权利要求 1 所述的数据加/解密方法，其特征在于，所述识别信息包括以下一种或多种：

移动终端的移动终端国际身份码、国际移动用户识别码、介质访问控制地址和通用唯一识别。

7. 一种移动终端上数据加/解密装置，其特征在于，所述装置包括：

第一生成单元，用于生成业务密钥；

第二生成单元，用于预先生成第一公钥和第一私钥密钥对；

第一获取单元，用于获取所述移动终端的识别信息；

第一加密单元，用于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；

第一解密单元，用于利用所述识别信息对所述第一加密私钥进行解密，得到所述第一私钥；

第二加密单元，用于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；

第二解密单元，用于利用所述识别信息对所述第一加密公钥进行解密，得到所述第一公钥；

第三解密单元，用于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；

第二获取单元，用于获取所述移动终端需要加/解密的数据；

第三加密单元，用于利用所述业务密钥对所述数据进行加密；

第四解密单元，用于利用所述业务密钥对所述数据进行解密。

8. 根据权利要求 7 所述的数据加/解密装置，其特征在于，所述第一加

密单元具体用于:

根据所述识别信息生成字符串;

利用所述字符串分别对第一公钥和第一私钥对进行加密处理。

9. 根据权利要求 7 所述的数据加/解密装置，其特征在于，所述第一解密单元具体用于:

根据所述识别信息生成字符串;

利用所述字符串对所述第一加密私钥进行解密处理。

10. 根据权利要求 7 所述的数据加/解密装置，其特征在于，所述第二解密单元具体用于:

根据所述识别信息生成字符串;

利用所述字符串对所述第一加密公钥进行解密处理。

11. 根据权利要求 9 或 10 所述的数据加/解密装置，其特征在于，所述根据所述识别信息生成字符串，具体为:

将所述识别信息进行哈希算法处理，得到所述字符串。

12. 根据权利要求 7 所述的数据加/解密装置，其特征在于，所述识别信息包括以下一种或多种:

移动终端的移动终端国际身份码、国际移动用户识别码、介质访问控制地址和通用唯一识别。

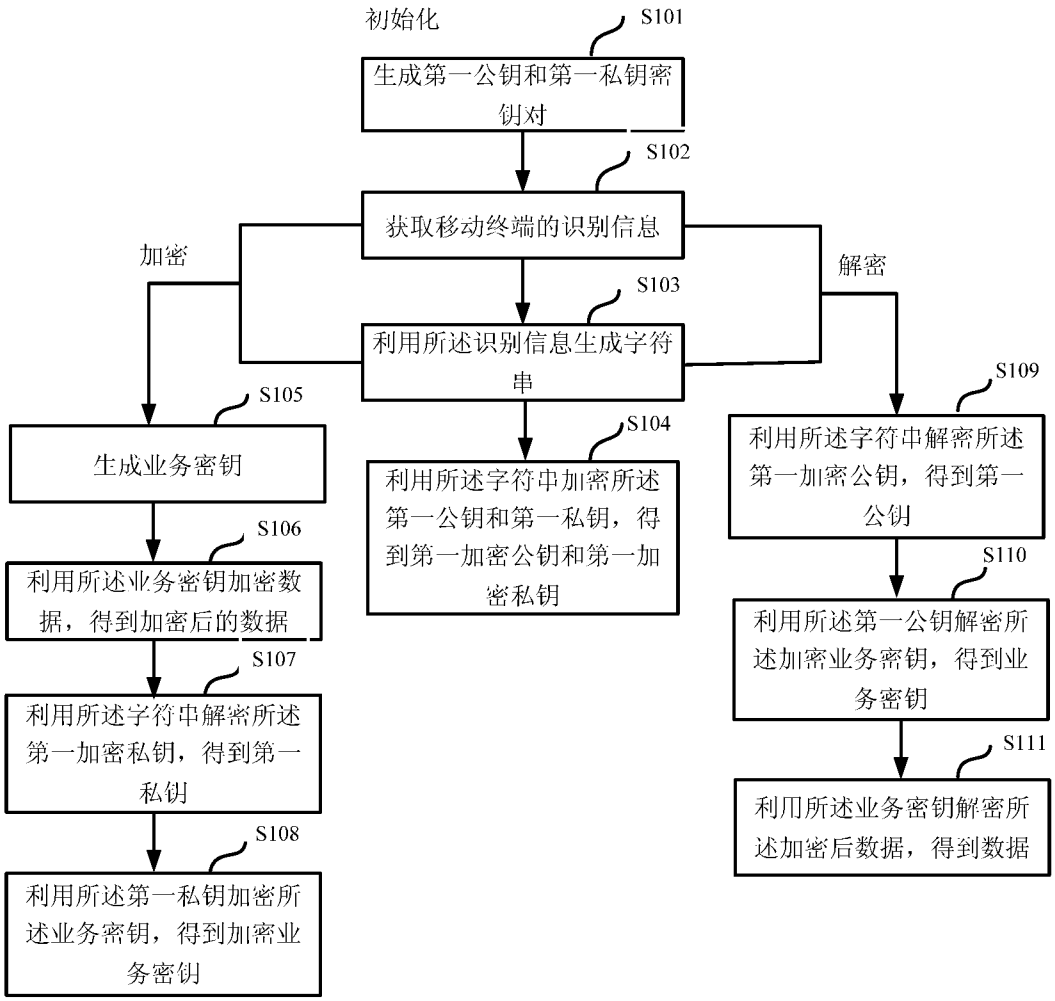
初始化
S101
生成第一公钥和第一私钥密钥对
S102
获取移动终端的识别信息
加密
解密
S103
利用所述识别信息生成字符串
S105
生成业务密钥
S104
利用所述字符中加密所述第一公钥和第一私钥，得到第一加密公钥和第一加密私钥
S109
利用所述字符中解密所述第一加密公钥，得到第一公钥
S106
利用所述业务密钥加密数据，得到加密后的数据
S110
利用所述第一公钥解密所述加密业务密钥，得到业务密钥
S107
利用所述字符中解密所述第一加密私钥，得到第一私钥
S111
利用所述业务密钥解密所述加密后数据，得到数据
S108
利用所述第一私钥加密所述业务密钥，得到加密业务密钥

图 1

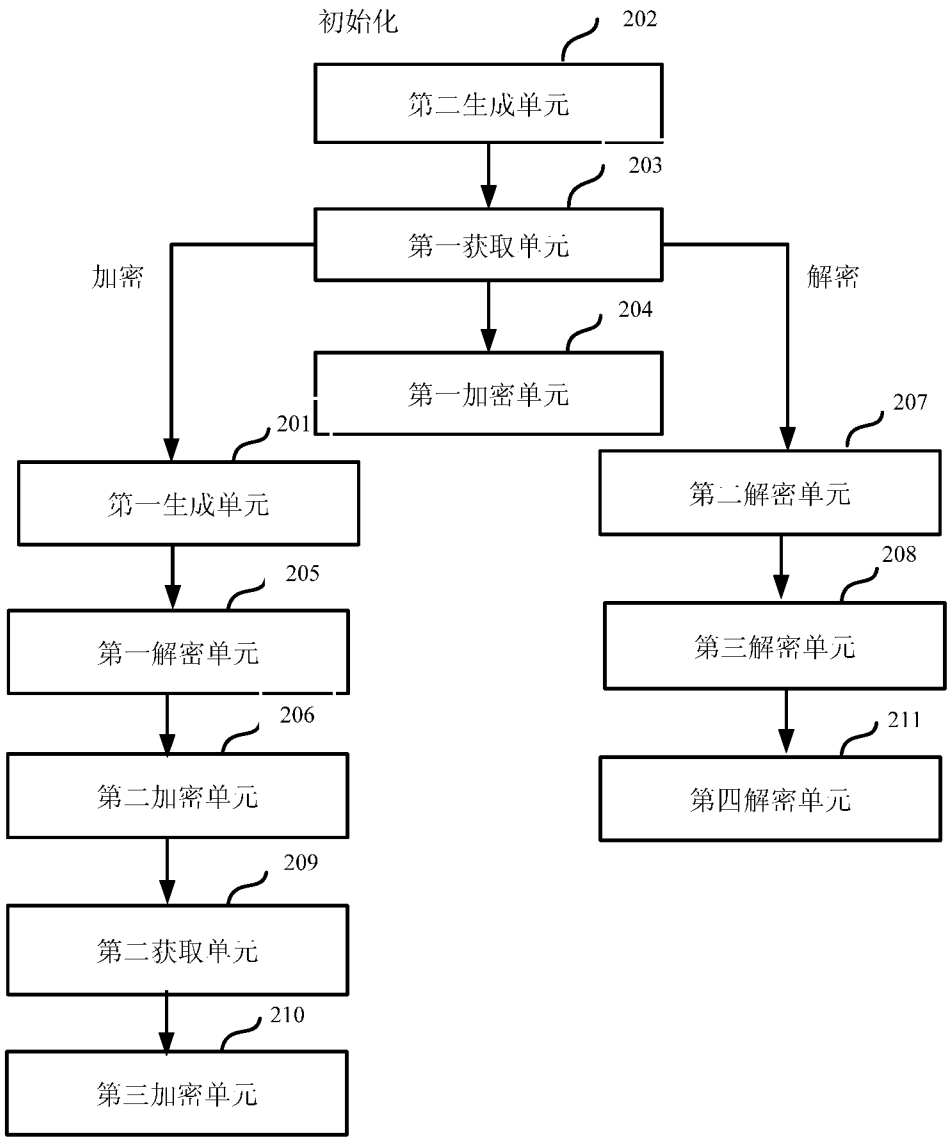
初始化
202
第二生成单元
203
第一获取单元
加密
解密
204
第一加密单元
201
第一生成单元
207
第二解密单元
205
第一解密单元
208
第三解密单元
206
第二加密单元
211
第四解密单元
209
第二获取单元
210
第三加密单元

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/095588

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L/9-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; CNKI: identity, mobile phone, private key, public key, service key, encrypt+, decrypt+, identif+, address+, terminal, termination, phone

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 1780413 A (HUAWEI TECHNOLOGIES CO., LTD.), 31 May 2006 (31.05.2006), description, page 5, line 18 to page 7, line 17	1-12
Y	CN 102170357 A (BEIJING HUFU TECHNOLOGY CO.,LTD.), 31 August 2011 (31.08.2011), claims 1-3 and 6-8	1-12
A	CN 101977299 A (ZTE CORP.), 16 February 2011 (16.02.2011), the whole document	1-12
A	CN 101335579 A (BEIJING INNOFIDEI TECHNOLOGY CO., LTD.), 31 December 2008 (31.12.2008), the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 January 2016 (25.01.2016)	**16 February 2016 (16.02.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **CHAO, Lulin** Telephone No.: (86-10) **62089448**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/095588

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1780413 A	31 May 2006	CN 100403814 C	16 July 2008
CN 102170357 A	31 August 2011	CN 102170357 B	25 September 2013
CN 101977299 A	16 February 2011	None	
CN 101335579 A	31 December 2008	None	

国际检索报告

国际申请号
PCT/CN2015/095588

A. 主题的分类

H04W 12/04(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; H04L/9-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;VEN;CNKI:私钥，公钥，业务密钥，加密，解密，识别，地址，身份，终端，手机，电话，private key，public key，service key，encrypt+，decrypt+，identif+，address+，terminal，termination，phone

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 1780413 A (华为技术有限公司) 2006年 5月 31日 (2006-05-31) 说明书第5页第18行-第7页第17行	1-12
Y	CN 102170357 A (北京虎符科技有限公司) 2011年 8月 31日 (2011-08-31) 权利要求1-3、6-8	1-12
A	CN 101977299 A (中兴通讯股份有限公司) 2011年 2月 16日 (2011-02-16) 全文	1-12
A	CN 101335579 A (北京创毅视讯科技有限公司) 2008年 12月 31日 (2008-12-31) 全文	1-12

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 1月 25日	2016年 2月 16日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	巢露琳
传真号 (86-10)62019451	电话号码 (86-10)62089448

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/095588

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	1780413	A	2006年 5月 31日	CN	100403814	C	2008年 7月 16日
CN	102170357	A	2011年 8月 31日	CN	102170357	B	2013年 9月 25日
CN	101977299	A	2011年 2月 16日		无		
CN	101335579	A	2008年 12月 31日		无		