(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105722067 B
(45)授权公告日 2019.08.13

(21)申请号 201410721298.5

(22)申请日 2014.12.02

(65)同一申请的已公布的文献号
申请公布号 CN 105722067 A

(43)申请公布日 2016.06.29

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 宋宜涛

(74)专利代理机构 北京亿腾知识产权代理事务所(普通合伙) 11309
代理人 戴燕

(51)Int.Cl.
H04W 12/02(2009.01)

(56)对比文件
CN 1607511 A,2005.04.20,
CN 101778381 A,2010.07.14,
CN 101711028 A,2010.05.19,
CN 101478595 A,2009.07.08,

审查员 雷蕾

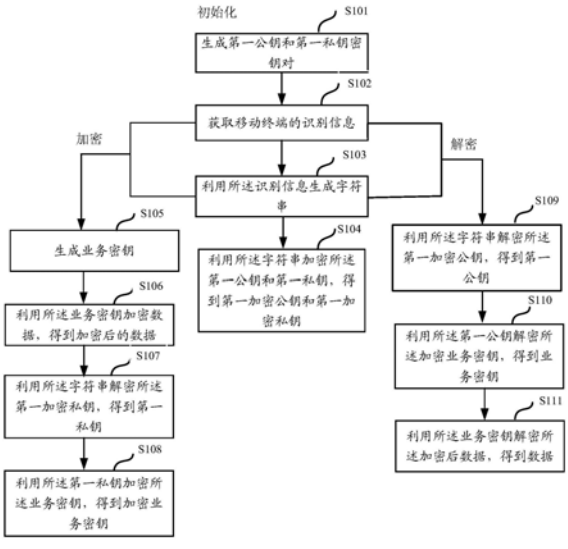
权利要求书2页 说明书5页 附图2页

(54)发明名称

移动终端上数据加/解密方法及装置

(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。



CN 105722067 B

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:

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;

数据加密阶段包括:

生成业务密钥;

获取所述移动终端需要加密的数据;

利用所述业务密钥对所述数据进行加密得到加密后的数据;

加密业务密钥,包括,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;

数据解密阶段包括:

解密业务密钥,包括,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;

获取所述加密后的数据;

利用所述业务密钥对所述加密后的数据进行解密得到所述数据。

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，用于在数据加密阶段获取所述移动终端需要加密的数据，或者在数据解密阶段获取加密后的数据；

第三加密单元，用于在数据加密阶段利用所述业务密钥对所述数据进行加密；

第四解密单元，用于在数据解密阶段利用所述业务密钥对所述加密后的数据进行解密。

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。

移动终端上数据加/解密方法及装置

技术领域

[0001] 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

[0002] 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。

[0003] 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。

[0004] 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

[0005] 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。

[0006] 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：

[0007] 预先生成第一公钥和第一私钥密钥对；

[0008] 获取所述移动终端的识别信息；

[0009] 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；

[0010] 加密业务密钥时，获取所述移动终端的识别信息；

[0011] 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；

[0012] 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；

[0013] 解密业务密钥时，获取所述移动终端的识别信息；

[0014] 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；

[0015] 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；

[0016] 获取所述移动终端需要加/解密的数据；

[0017] 利用所述业务密钥对所述数据进行加/解密。

[0018] 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：

[0019] 第一生成单元，用于生成业务密钥；

[0020] 第二生成单元，用于预先生成第一公钥和第一私钥密钥对；

[0021] 第一获取单元，用于获取所述移动终端的识别信息；

[0022] 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；

[0023] 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；

[0024] 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；

[0025] 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；

[0026] 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；

[0027] 第二获取单元，用于获取所述移动终端需要加/解密的数据；

[0028] 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；

[0029] 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。

[0030] 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

[0031] 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；

[0032] 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

[0033] 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。

[0034] 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。

[0035] 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。

[0036] 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：

[0037] S101，生成第一公钥和第一私钥密钥对。

[0038] 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。

[0039] S102，获取移动终端的识别信息。

[0040] 具体地，通过代码获取移动终端的识别信息。

[0041] 所述识别信息包括以下一种或多种：

[0042] 移动终端的IMEI(International Mobile Equipment Identity,移动终端国际身份码)、IMSI(Internat ional 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)。

[0043] S103,利用所述识别信息生成字符串。

[0044] 具体地,将所述识别信息进行哈希算法处理,得到字符串。

[0045] 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。

[0046] 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。

[0047] 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。

[0048] 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。

[0049] 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。

[0050] 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

[0051] 公钥和第一加密私钥。

[0052] S105,生成业务密钥。

[0053] 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。

[0054] S106,利用所述业务密钥加密数据,得到加密后的数据。

[0055] 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。

[0056] 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。

[0057] 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。

[0058] 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。

[0059] 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。

[0060] 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。

[0061] 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。

[0062] S109,利用所述字符串解密所述第一加密公钥,得到第一公钥。

[0063] 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。

[0064] 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。

[0065] 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。

[0066] 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。

[0067] S111,利用所述业务密钥解密所述加密后的数据,得到数据。

[0068] 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。

[0069] 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。

[0070] 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。

[0071] 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。

[0072] 所述第一生成单元201,用于生成业务密钥;

[0073] 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;

[0074] 所述第一获取单元203,用于获取所述移动终端的识别信息;

[0075] 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;

[0076] 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;

[0077] 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;

[0078] 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;

[0079] 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;

[0080] 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;

[0081] 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;

[0082] 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。

[0083] 可选地,所述第一加密单元204具体用于:

[0084] 根据所述识别信息生成字符串;

[0085] 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。

[0086] 可选地,所述第一解密单元205具体用于:

[0087] 根据所述识别信息生成字符串;

[0088] 利用所述字符串对所述第一加密私钥进行解密处理。

[0089] 可选地,所述第二解密单元207具体用于:

[0090] 根据所述识别信息生成字符串;

[0091] 利用所述字符串对所述第一加密公钥进行解密处理。

[0092] 可选地,所述根据所述识别信息生成字符串,具体为:

[0093] 将所述识别信息进行哈希算法处理,得到所述字符串。

[0094] 可选地,所述识别信息包括以下一种或多种:

[0095] 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)。

[0096] 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。

[0097] 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。

[0098] 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。

[0099] 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。

[0100] 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。

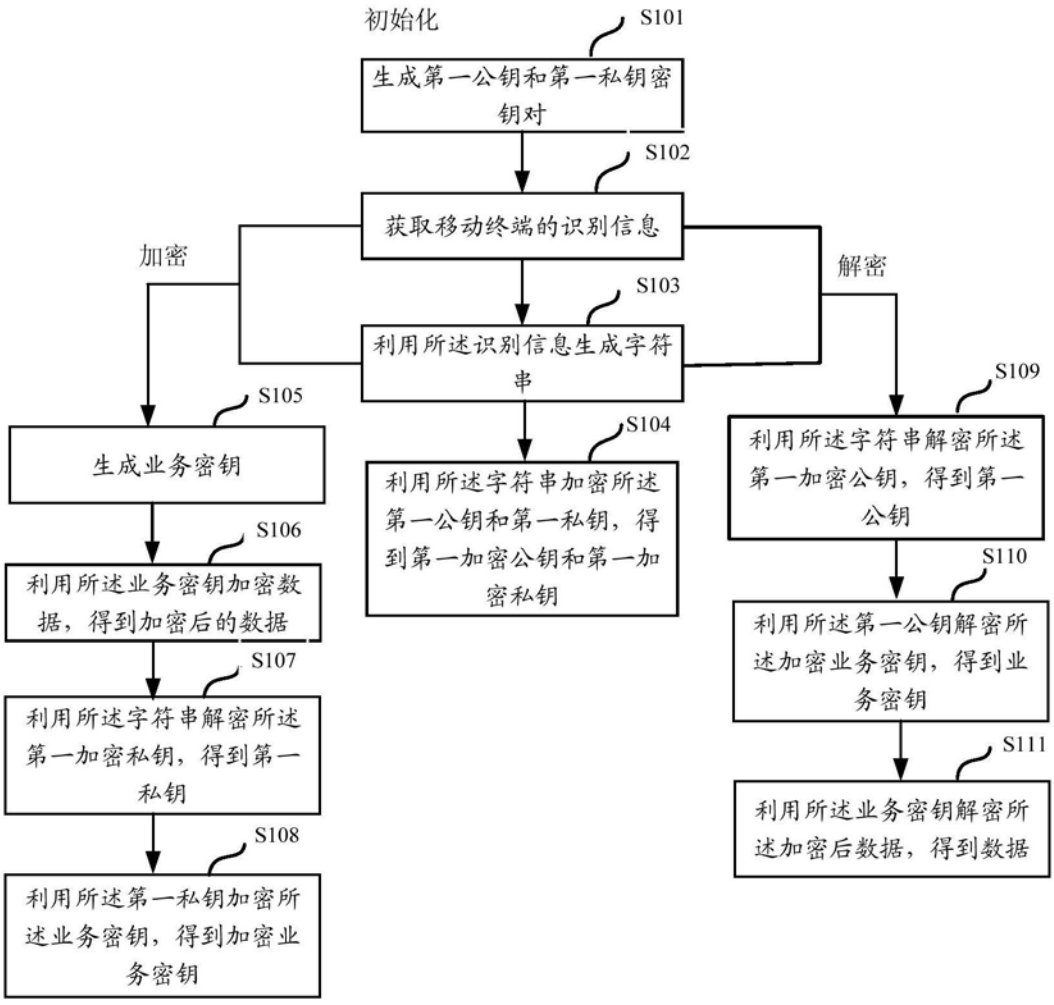

初始化
S101
生成第一公钥和第一私钥密钥对
S102
获取移动终端的识别信息
加密
解密
S103
利用所述识别信息生成字符串
S105
生成业务密钥
S104
利用所述字符串加密所述第一公钥和第一私钥，得到第一加密公钥和第一加密私钥
S109
利用所述字符串解密所述第一加密公钥，得到第一公钥
S106
利用所述业务密钥加密数据，得到加密后的数据
S110
利用所述第一公钥解密所述加密业务密钥，得到业务密钥
S107
利用所述字符串解密所述第一加密私钥，得到第一私钥
S111
利用所述业务密钥解密所述加密后数据，得到数据
S108
利用所述第一私钥加密所述业务密钥，得到加密业务密钥

图1

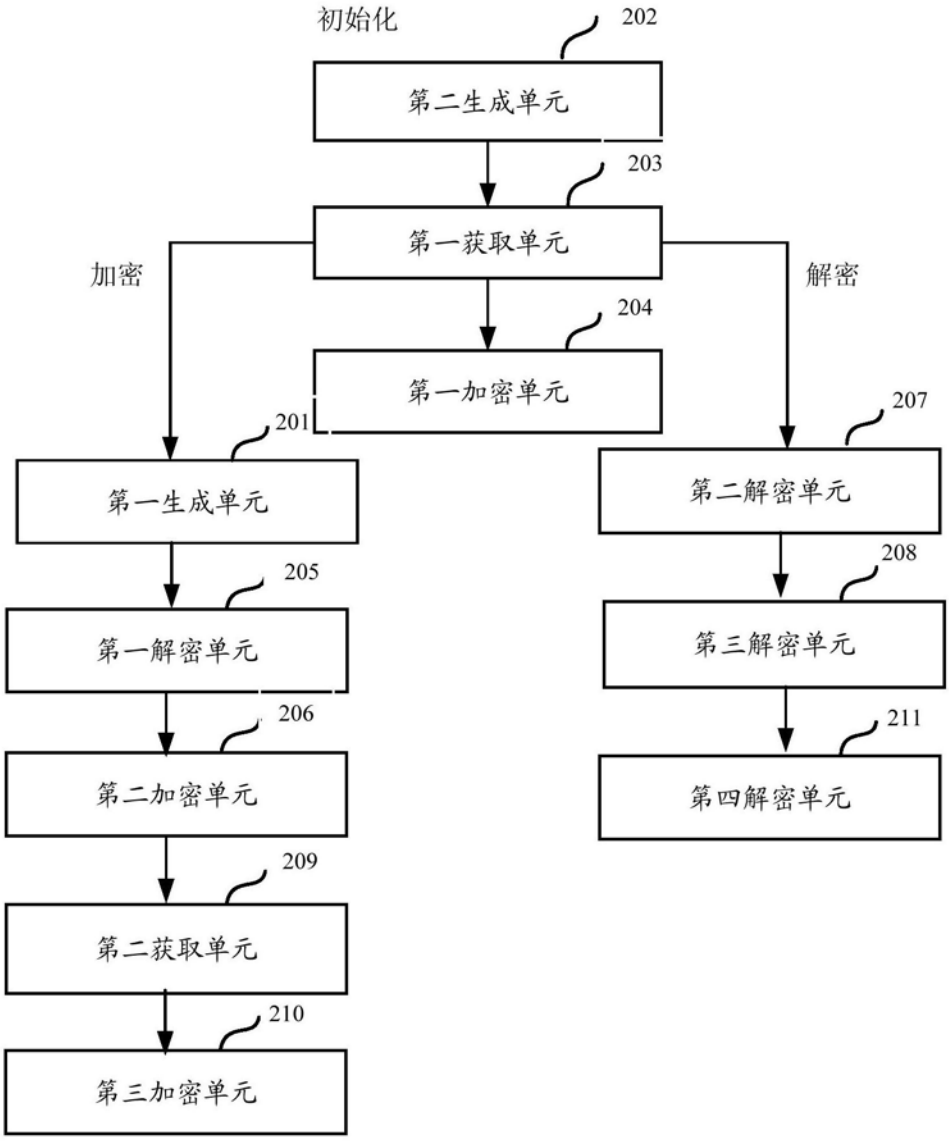

初始化
202
第二生成单元
203
第一获取单元
加密
解密
204
第一加密单元
201
第一生成单元
207
第二解密单元
205
第一解密单元
208
第三解密单元
206
第二加密单元
211
第四解密单元
209
第二获取单元
210
第三加密单元

图2