

(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
2017年10月19日 (19.10.2017)



(10) 国际公布号
WO 2017/177435 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2016/079397
- (22) 国际申请日: 2016年4月15日 (15.04.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 深圳前海达闼云端智能科技有限公司 (CLOUDMINDS (SHENZHEN) ROBOTICS SYSTEMS CO., LTD.) [CN/CN]; 中国北京市北京市朝阳区望京 SOHO 塔 3A 区 23 层, Beijing 100102 (CN)。
- (72) 发明人: 张站朝 (ZHANG, Zhanchao); 中国北京市北京市朝阳区望京 SOHO 塔 3A 区 23 层, Beijing 100102 (CN)。
- (74) 代理人: 北京新知远方知识产权代理事务所 (普通合伙) (IPFUTURE INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市北京市海淀区花园东路 10 号高德大厦 905 姚稳稳, Beijing 100191 (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, 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))。

(54) Title: IDENTITY AUTHENTICATION METHOD, TERMINAL AND SERVER

(54) 发明名称: 一种身份认证方法、终端及服务器

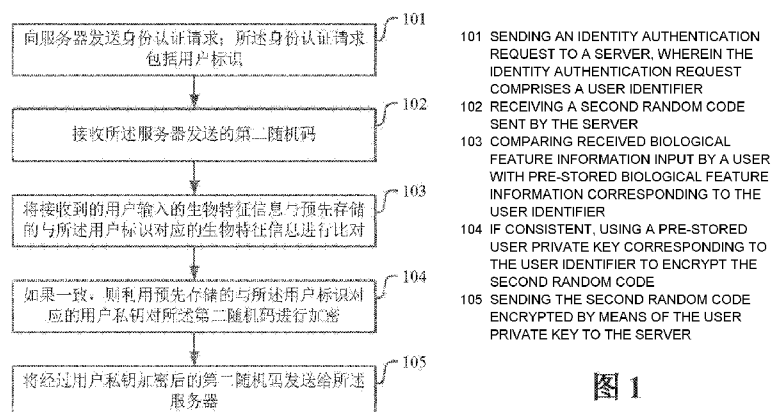


图 1

(57) Abstract: Provided are an identity authentication method, a terminal and a server. The method comprises: a terminal sending an identity authentication request to a server; the server sending a random code to the terminal; the terminal comparing biological feature information input by a user with pre-stored biological feature information corresponding to a user identifier, and if a comparison result is that the two are consistent, using a pre-stored user private key corresponding to the user identifier to encrypt a second random code and sending same to the server; and the server using a pre-stored user public key corresponding to the user identifier to decrypt the second random code after being encrypted by means of the user private key, verifying whether the decrypted second random code is consistent with the sent second random code, and if so, passing identity authentication. The present invention does not require a terminal to upload biological feature information about a user, and the verification of the biological feature information about the user is completed by the terminal itself, thereby ensuring that the biological feature information about the user is not revealed.

(57) 摘要:

[见续页]



WO 2017/177435 A1



本发明提供了一种身份认证方法、终端及服务器，终端向服务器发送身份认证请求，服务器向终端发送随机码，终端将用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对，如果比对一致，利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密并发给服务器，服务器利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密，验证解密得到的第二随机码与发送的第二随机码是否一致，如果一致，则身份认证通过。本发明不需要终端上传用户的生物特征信息，对用户的生物特征信息的验证由终端自身完成，从而确保了用户的生物特征信息不被泄露。

一种身份认证方法、终端及服务器

技术领域

本发明涉及身份识别技术领域，特别涉及一种身份认证方法、终端及服务器。

5

背景技术

云端机器人是将认知系统放在云里，身体、驱动、传感器放在机器人本体上，通过移动通信将二者连接起来的智能机器人；云端机器人是智能仿人机器人发展的方向。

10

身份认证也可以称为身份验证或身份鉴别，是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，保证系统和数据的安全。

15

目前，较为常见的身份认证方式主要有基于口令的认证方式和基于生物特征的认证方式。其中，基于生物特征的认证方式是以人体唯一、可靠、稳定的生物特征（例如：虹膜、指纹、脸部、掌纹等）为依据，具有很好的安全性。

然而，现有基于生物特征的认证方式通常是终端与服务器连接，终端采集用户的生物特征信息后将这些生物特征信息上传至服务器，与服务器预存的生物特征信息进行对比匹配，如果匹配成功，则认证通过。

20

现有技术不足在于：

现有基于生物特征的认证方式在实施时需要将用户的生物特征信息上传至服务器，用户的生物特征信息容易泄露。

发明内容

25

本发明实施例提出了一种身份认证方法、终端及服务器，以解决现有

技术中基于生物特征的认证方式在实施时需要将用户的生物特征信息上传至服务器，用户的生物特征信息容易泄露，导致用户信息不安全的技术问题。

第一个方面，本发明实施例提供了一种身份认证方法，包括如下步骤：

5 向服务器发送身份认证请求；所述身份认证请求包括用户标识；

接收所述服务器发送的第二随机码；

将接收到的用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对；

10 如果一致，则利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；

将经过用户私钥加密后的第二随机码发送给所述服务器。

可选的，在所述向服务器发送身份认证请求之前，进一步包括：

接收服务器发送的第一随机码；

将终端标识、用户标识和所述第一随机码发送至所述服务器；

15 在接收到服务器发送的验证通过消息后，接收用户录入的生物特征信息；

为所述用户生成公私钥对，建立所述生物特征信息、终端标识、用户私钥与用户标识之间的对应关系，并将用户公钥与所述用户标识发送至所述服务器。

20 可选的，所述将经过用户私钥加密后的第二随机码发送给所述服务器，具体为：将经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识发送给所述服务器。

可选的，在所述向服务器发送身份认证请求之前，进一步包括：利用预先存储的服务器生成的证书与所述服务器建立安全传输层协议 TLS 双向
25 认证连接；与所述服务器的通信具体为利用所述 TLS 双向认证连接进行的。

可选的，所述利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密，具体为：利用预先存储的私钥密码与安全装置的密码进行验证，验证成功后获取存储于安全区域的用户私钥，根据所述用户私钥对所述第二随机码进行加密。

- 5 可选的，在所述根据用户私钥对所述第二随机码进行加密之后，进一步包括：接收服务器发送的随机私钥密码，根据所述随机私钥密码修改所述安全装置的密码。

第二个方面，本发明实施例提供了一种身份认证方法，包括如下步骤：

接收终端发送的身份认证请求；所述身份认证请求包括用户标识；

- 10 向所述终端发送第二随机码；

接收所述终端发送的经过用户私钥加密后的第二随机码；

利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密；

验证解密得到的第二随机码与发送的第二随机码是否一致，如果一致，

- 15 则身份认证通过。

可选的，在所述接收终端发送的身份认证请求之前，进一步包括：

确定终端标识与用户标识的对应关系；

向终端发送第一随机码；

在收到终端发送的终端标识、用户标识和第一随机码之后进行验证，

- 20 并在验证通过后向所述终端发送验证通过消息；

接收所述终端发送的用户标识和用户公钥，建立所述用户标识、用户公钥与所述终端标识之间的对应关系。

可选的，所述接收所述终端发送的经过用户私钥加密后的第二随机码，具体为：接收所述终端发送的经过用户私钥加密后的第二随机码和所述用

- 25 户标识、以及终端标识；所述利用预先存储的与所述用户标识对应的用户

公钥对所述经过用户私钥加密后的第二随机码进行解密，具体为：利用与
所述终端标识对应的用户公钥对所述经过用户私钥加密后的第二随机码和
用户标识进行解密；所述验证解密得到的第二随机码与发送的第二随机码
是否一致，如果一致则身份认证通过，具体为：验证解密得到的第二随机
5 码与发送的第二随机码是否一致，以及，验证所述用户标识与所述终端标
识之间的对应关系；如果解密得到的第二随机码与发送的第二随机码一致
且所述终端标识与所述用户标识对应，则身份认证通过。

可选的，在所述接收终端发送的身份认证请求之前，进一步包括：利
用预先存储的证书与所述终端建立安全传输层协议 TLS 双向认证连接；与
10 所述终端的通信具体为利用所述 TLS 双向认证连接进行的。

可选的，在所述接收终端发送的经过用户私钥加密后的第二随机码之
后，进一步包括：向所述终端发送随机私钥密码。

第三个方面，本发明实施例提供了一种终端，包括：

第一发送模块，用于向服务器发送身份认证请求；所述身份认证请求
15 包括用户标识；

第一接收模块，用于接收所述服务器发送的第二随机码；

比对模块，用于将接收到的用户输入的生物特征信息与预先存储的与
所述用户标识对应的生物特征信息进行比对；

加密模块，用于如果一致，则利用预先存储的与所述用户标识对应的
20 用户私钥对所述第二随机码进行加密；

第二发送模块，用于将经过用户私钥加密后的第二随机码发送给所述
服务器。

可选的，进一步包括：

第二接收模块，用于在所述向服务器发送身份认证请求之前，接收服
25 务器发送的第一随机码；

第三发送模块，用于将终端标识、用户标识和所述第一随机码发送至所述服务器；

第三接收模块，用于在接收到服务器发送的验证通过消息后，接收用户录入的生物特征信息；

- 5 密钥处理模块，用于为所述用户生成公私钥对，建立所述生物特征信息、终端标识、用户私钥与用户标识之间的对应关系，并将用户公钥与所述用户标识发送至所述服务器。

可选的，所述第二发送模块具体用于将经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识发送给所述服务器。

- 10 可选的，进一步包括：

连接建立模块，用于在所述向服务器发送身份认证请求之前，利用预先存储的服务器生成的证书与所述服务器建立安全传输层协议 TLS 双向认证连接；与所述服务器的通信具体为利用所述 TLS 双向认证连接进行的。

- 15 可选的，所述加密模块具体用于如果一致，利用预先存储的私钥密码与安全装置的密码进行验证，验证成功后获取存储于安全区域的用户私钥，根据所述用户私钥对所述第二随机码进行加密。

可选的，进一步包括：

- 20 第四接收模块，用于在所述根据用户私钥对所述第二随机码进行加密之后，接收服务器发送的随机私钥密码，根据所述随机私钥密码修改所述安全装置的密码。

第四个方面，本发明实施例提供了一种服务器，包括：

第一接收单元，用于接收终端发送的身份认证请求；所述身份认证请求包括用户标识；

第一发送单元，用于向所述终端发送第二随机码；

- 25 第二接收单元，用于接收所述终端发送的经过用户私钥加密后的第二

随机码；

解密单元，用于利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密；

第一认证单元，用于验证解密得到的第二随机码与发送的第二随机码
5 是否一致，如果一致，则身份认证通过。

可选的，进一步包括：

确定单元，用于在所述接收终端发送的身份认证请求之前，确定终端标识与用户标识的对应关系；

第二发送单元，用于向终端发送第一随机码；

10 第二认证单元，用于在收到终端发送的终端标识、用户标识和第一随机码之后进行验证，并在验证通过后向所述终端发送验证通过消息；

关系建立单元，用于接收所述终端发送的用户标识和用户公钥，建立所述用户标识、用户公钥与所述终端标识之间的对应关系。

可选的，所述第二接收单元具体用于接收所述终端发送的经过用户私
15 钥加密后的第二随机码和所述用户标识、以及终端标识；所述解密单元具体用于利用与所述终端标识对应的用户公钥对所述经过用户私钥加密后的第二随机码和用户标识进行解密；所述第一认证单元具体用于验证解密得到的第二随机码与发送的第二随机码是否一致，以及，验证所述用户标识与
所述终端标识之间的对应关系；如果解密得到的第二随机码与发送的第二
20 随机码一致且所述终端标识与所述用户标识对应，则身份认证通过。

可选的，进一步包括：

连接建立单元，用于在所述接收终端发送的身份认证请求之前，利用预先存储的证书与所述终端建立安全传输层协议 TLS 双向认证连接；与所述终端的通信具体为利用所述 TLS 双向认证连接进行的。

25 可选的，进一步包括：

第三发送单元，用于在所述接收终端发送的经过用户私钥加密后的第二随机码之后，向所述终端发送随机私钥密码。

有益效果如下：

当前身份认证技术需要将用户的生物特征信息上传至服务器，存在个人信息泄露、不安全的问题，由于本发明实施例所提供的身份认证方案，用户的生物特征信息保存在终端侧，不需要上传服务器，由终端完成用户生物特征的验证，在终端验证通过后将利用预先存储的用户私钥加密后的随机码和用户标识上传服务器，服务器利用预先存储的用户公钥解密后对用户标识和随机码等信息进行验证即可，无需存储用户的生物特征信息，从而确保了用户的个人信息安全、不被泄露。

附图说明

下面将参照附图描述本发明的具体实施例，其中：

图1示出了本发明实施例一中身份认证方法实施的流程示意图；

图2示出了本发明实施例二中身份认证方法实施的流程示意图；

图3示出了本发明实施例三中终端的结构示意图一；

图4示出了本发明实施例三中终端的结构示意图二；

图5示出了本发明实施例三中终端的结构示意图三；

图6示出了本发明实施例三中终端的结构示意图四；

图7示出了本发明实施例四中服务器的结构示意图一；

图8示出了本发明实施例四中服务器的结构示意图二；

图9示出了本发明实施例四中服务器的结构示意图三；

图10示出了本发明实施例四中服务器的结构示意图四；

图11示出了本发明实施例五中用户生物特征信息注册过程的示意图；

图12示出了本发明实施例五中用户身份认证过程的示意图；

图13示出了本发明实施例六中移动支付场景的身份认证过程示意图；

图14示出了本发明实施例七中云机器人场景的身份认证过程示意图；

图15示出了本发明实施例八中门禁系统的身份认证过程示意图。

具体实施方式

5 为了使本发明的技术方案及优点更加清楚明白，以下结合附图对本发明的示例性实施例进行进一步详细的说明，显然，所描述的实施例仅是本发明的一部分实施例，而不是所有实施例的穷举。并且在不冲突的情况下，本说明中的实施例及实施例中的特征可以互相结合。

发明人在发明过程中注意到：

10 现有基于生物特征的认证方式（例如：人脸识别、指纹识别等）的实现过程通常包括以下步骤：

- 1、终端采集用户的生物特征信息；
 - 2、终端将这些生物特征信息上传至服务器；
 - 3、服务器将终端上传的生物特征信息与预存的生物特征信息进行对比
- 15 匹配，如果匹配成功，则认证通过。

采用上述认证方式，由于在实施时需要将用户的生物特征信息上传至服务器，导致用户的生物特征信息容易泄露，具有一定的安全风险。

针对上述不足，本发明实施例提出了一种身份认证方法、终端及服务器，由于本发明实施例中用户个人的生物特征信息（例如：人脸、指纹、虹膜等个人隐私信息）仅存在于终端侧，从而确保了生物特征信息不会泄

20 露，保障用户隐私的安全性。

为了便于本发明的实施，下面结合具体实施例对本发明所提供的身份认证方法、终端及服务器进行说明。

实施例一、

25 图 1 示出了本发明实施例一中身份认证方法实施的流程示意图，如图所示，所述身份认证方法可以包括如下步骤：

步骤 101、向服务器发送身份认证请求；所述身份认证请求包括用户标识；

步骤 102、接收所述服务器发送的第二随机码；

步骤 103、将接收到的用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对；

步骤 104、如果一致，则利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；

步骤 105、将经过用户私钥加密后的第二随机码发送给所述服务器。

本发明实施例所提供的身份认证方法可以在终端侧实施，具体可以在手机、pad、平板电脑、智能机器人等移动终端上实施。

所述向服务器发送身份认证请求可以由用户触发（例如：用户点击/启动身份认证服务），也可以根据用户的操作自行触发（例如：用户想要访问终端或终端上的应用程序时，终端自行发起认证请求），所述身份认证请求可以包括用户标识、终端标识等信息，所述用户标识具体可以为用户的账号、用户 ID、用户二维码等，所述终端标识具体可以为国际移动设备标识码（IMEI, International Mobile Equipment Identity）等。

需要说明的是，本发明实施例对上述步骤之间的顺序不作限制。例如，可以有以下几种情况：

第一种情况，可以先向服务器发送身份认证请求，接收所述服务器发送的第二随机码，然后接收用户输入的生物特征信息，将所述用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对；如果一致，则利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；将经过用户私钥加密后的第二随机码发送给所述服务器。

第二种情况，可以向服务器发送身份认证请求的同时接收用户输入的

生物特征信息，接收所述服务器发送的第二随机码，并将所述用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对；如果一致，则利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；将经过用户私钥加密后的第二随机码发送给所述服务器。

第三种情况是，可以先接收用户输入的生物特征信息，然后将所述用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对，如果一致，向服务器发送身份认证请求，接收所述服务器发送的第二随机码，利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；将经过用户私钥加密后的第二随机码发送给所述服务器。

第四种情况，可以先接收用户输入的生物特征信息，然后将所述用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对，并向服务器发送身份认证请求，接收所述服务器发送的第二随机码，如果生物特征比对一致，则利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；将经过用户私钥加密后的第二随机码发送给所述服务器。

所述接收到的所述服务器发送的第二随机码具体可以为数字、字母或二者结合的一串字符串。

本发明实施例中可以预先存储用户标识、用户生物特征信息、用户私钥的绑定关系，在接收到用户输入的生物特征信息之后，可以将所述用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对，如果一致，则认为该用户标识与生物特征信息匹配，然后利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密，将加密后的第二随机码发送给所述服务器。

其中，所述用户私钥可以为利用现有的密钥生成算法生成的公私钥对中的私钥，所述现有的密钥生成算法可以包括 RAS 算法、3DES 算法等。

本发明实施例所提供的身份认证方法，在向服务器发送身份认证请求后，将用户输入的生物特征信息与预先存储的所述用户的生物特征信息进
5 行比对，完成生物特征信息的验证，在验证通过后利用所述用户的用户私钥对第二随机码进行加密发送给服务器，由于本发明实施例在本地完成了用户生物特征信息的验证，无需将用户的生物特征信息发送至服务器由服务器验证，从而确保了用户信息的安全性，且降低了传输的数据量。

实施中，在所述向服务器发送身份认证请求之前，所述方法可以进一步包括：
10

接收服务器发送的第一随机码；

将终端标识、用户输入的用户标识和所述第一随机码发送至所述服务器；

在接收到服务器发送的验证通过消息后，接收用户录入的生物特征信息；
15

为所述用户生成公私钥对，存储用户私钥并将用户公钥与所述用户标识发送至所述服务器。

本发明实施例中在向服务器发送身份验证请求之前，可以先进行用户注册过程，具体可以为：接收服务器发送的第一随机码，将终端标识、用户标识和所述第一随机码发送至所述服务器，以便服务器进行验证；在接
20 收到服务器发送的验证通过消息后，接收用户录入的生物特征信息，为所述用户生成公私钥对，存储用户私钥并将用户公钥与所述用户标识发送至所述服务器。

具体实施时，可以由用户提出注册申请，本发明实施例先将用户注册
25 请求发送给服务器，服务器在接收到所述注册请求之后为所述用户建立用

户标识与终端标识的对应关系，本发明实施例接收服务器发送的第一随机码；也可以由服务器主动创建用户标识并建立所述用户标识与终端标识的对应关系，然后，本发明实施例接收服务器发送的第一随机码。

其中，所述终端标识与所述用户标识可以为一对一的关系，也可以为一对多的关系，所述用户标识与用户私钥、生物特征信息之间可以为一对一的关系。

经过上述过程后，本地可以成功存储所述用户标识、用户私钥、终端标识、用户生物特征信息之间的对应关系，服务器侧可以成功存储所述用户标识、用户公钥、终端标识之间的对应关系，为后续身份认证提供数据支撑。

实施中，所述将经过用户私钥加密后的第二随机码发送给所述服务器，具体可以为：将经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识发送给所述服务器。

具体实施时，在利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密之后，可以将终端标识与经过用户私钥加密后的第二随机码发送给所述服务器，以便服务器对终端标识进行验证。

实施中，所述接收用户输入的生物特征信息具体可以为：接收用户输入的指纹、掌纹、虹膜、人脸和/或声音。

具体实施时，所述生物特征信息可以包括指纹、掌纹、虹膜、人脸、声音等，所述接收用户输入的生物特征信息具体可以为：接收用户输入的指纹、掌纹、虹膜、人脸、声音等。其中，接收用户输入的指纹、掌纹、虹膜、人脸、声音等，均可以采用现有的传感器或采集器实现，本发明在此不做赘述。

由于指纹、掌纹、虹膜、人脸、声音等信息均为用户的隐私信息，为了确保用户的隐私信息安全，本发明实施例提出了在本地完成生物特征验

证的方式，无需将生物特征信息上传至服务器。

为了进一步增强本申请实施例的数据安全性，本申请还可以采用如下方式实施。

实施中，在所述向服务器发送身份认证请求之前，所述方法可以进一步包括：

利用预先存储的服务器生成的证书与所述服务器建立安全传输层协议（TLS，Transport Layer Security Protocol）双向认证连接；与所述服务器的通信具体为利用所述 TLS 双向认证连接进行的。

具体实施时，可以在终端侧预置一个服务器端生成的证书，这个证书可以用于终端与服务器建立 TLS 双向认证的连接，后续的所有通信均可以基于所述 TLS 连接进行。

本申请实施例通过采用这种方式实施，可以防止终端在向服务器发送终端生成的公私钥对的用户公钥时被非法截取，进一步提高安全性。

实施中，所述利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密，具体可以为：

利用预先存储的私钥密码与安全装置的密码进行验证，验证成功后获取存储于安全区域的用户私钥，根据所述用户私钥对所述第二随机码进行加密。

具体实施时，所述终端生成的公私钥对可以使用一个安全装置并存储在终端的安全区域内。在使用私钥时，可以先利用私钥密码在安全装置进行验证，如果密码验证成功，则可以获取存储于安全区域的用户私钥，进一步提高了用户私钥使用时的安全性。

实施中，在所述根据用户私钥对所述第二随机码进行加密之后，所述方法可以进一步包括：

接收服务器发送的随机私钥密码，根据所述随机私钥密码修改所述安

全装置的密码。

具体实施时，可以在每次使用完私钥密码之后，从服务器获取一个随机私钥密码，来修改所述安全装置的密码，即所述安全装置的密码是一次性的，使用完一次就更新一次，从而保证安全装置中在安全区域存储的用户私钥的安全性。

实施例二、

图 2 示出了本发明实施例二中身份认证方法实施的流程示意图，如图所示，所述身份认证方法可以包括如下步骤：

步骤 201、接收终端发送的身份认证请求；所述身份认证请求包括用户标识；

步骤 202、向所述终端发送第二随机码；

步骤 203、接收所述终端发送的经过用户私钥加密后的第二随机码；

步骤 204、利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密；

步骤 205、验证解密得到的第二随机码与发送的第二随机码是否一致，如果一致，则身份认证通过。

本发明实施例所提供的身份认证方法可以在网络侧、服务器端实施。

所述终端发送的身份认证请求中可以包括用户标识、终端标识等信息，所述用户标识可以为用户的账号、ID 等信息，所述终端标识可以为终端的 IMEI 等信息。

本发明实施例中可以预先存储所述用户标识、用户公钥、终端标识之间的对应关系，在接收到终端发送的经过用户私钥加密后的第二随机码后，可以利用所述用户的公钥对所述第二随机码进行解密，如果解密得到的第二随机码与之前发送的第二随机码一致，则身份认证通过。

采用本发明实施例所提供的身份认证方法，由于服务器侧只需要利用

与所述用户标识对应的公钥对所述终端发送的第二随机码进行解密验证，即可实现身份认证的目的，无需终端上传用户的生物特征信息，从而确保了用户的个人信息的安全性。

实施中，在所述接收终端发送的身份认证请求之前，所述方法可以进一步包括：

确定终端标识与用户标识的对应关系；

向终端发送第一随机码；

在收到终端发送的终端标识、用户标识和第一随机码之后进行验证，并在验证通过后向所述终端发送验证通过消息；

10 接收所述终端发送的用户标识和用户公钥，建立所述用户标识、用户公钥与所述终端标识之间的对应关系。

具体实施时，所述确定终端标识和用户标识的对应关系，具体可以为：接收终端发送的用户注册请求，所述注册请求中可以包括用户标识和终端标识，建立所述用户标识和所述终端标识之间的对应关系；也可以为：为用户生成用户标识，将所述用户标识与终端标识建立对应关系。

15 在接收到终端发送的终端标识、用户标识和第一随机码之后，对所述终端标识和用户标识的对应关系进行验证，并验证所述第一随机码与之前发送的第一随机码是否一致，在验证通过后可以向终端发送验证通过消息，接收所述终端发送的用户标识和用户公钥，建立所述用户标识、用户公钥与
20 与所述终端标识之间的对应关系。

其中，所述终端标识与所述用户标识之间的对应关系可以是一对一的关系，也可以是一对多的关系；所述用户标识与用户公钥之间的对应关系可以为一对一的关系。

所述用户公钥与用户私钥为一对公私钥对，具体实施时，可以采用现有的加密算法生成，公私钥对的具体生成过程本发明不再赘述。

经过上述过程，服务器侧可以存储了所述用户标识、终端标识以及用户公钥之间的对应关系，为后续的身份认证提供了支撑。

实施中，所述接收所述终端发送的经过用户私钥加密后的第二随机码，具体可以为：接收所述终端发送的经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识；

所述利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密，具体可以为：利用与所述终端标识对应的用户公钥对所述经过用户私钥加密后的第二随机码和用户标识进行解密；

所述验证解密得到的第二随机码与发送的第二随机码是否一致，如果一致则身份认证通过，具体可以为：验证解密得到的第二随机码与发送的第二随机码是否一致，以及，验证所述用户标识与所述终端标识之间的对应关系；如果解密得到的第二随机码与发送的第二随机码一致且所述终端标识与所述用户标识对应，则身份认证通过。

具体实施时，可以接收终端发送的终端标识和所述经过用户私钥加密后的第二随机码，在进行身份认证时，可以验证解密得到的第二随机码与发送的第二随机码是否一致，以及，验证所述终端标识与所述用户标识之间的对应关系。如果解密得到的第二随机码与发送的第二随机码一致且所述终端标识与所述用户标识对应，则身份认证通过。其中，所述终端标识与所述用户标识之间的对应关系可以为一对一的关系。

如果所述终端标识与所述用户标识之间的对应关系为一对一关系，那么，本发明实施例还可以采用如下方式实施。

终端在进行生物特征信息验证之后，利用所述用户的用户私钥对所述第二随机码和所述用户标识进行加密签名，将加密签名后的第二随机码和所述用户标识、以及终端标识发送给服务器，服务器根据所述终端标识确

定所述终端标识确定所述用户公钥，利用所述用户公钥对所述第二随机码和所述用户标识进行解密验签，验证解密得到的第二随机码与之前发送的随机码是否一致，对解密得到的用户标识与所述终端标识的对应关系进行验证。

- 5 本发明实施例不需要终端上传用户的生物特征信息，只需要对用户标识、用户公钥以及终端标识进行验证即可，对用户的生物特征信息的验证由终端自身完成，从而确保了用户的生物特征信息不被泄露，提高了个人信息的安全性，同时降低了传输过程的数据量。

10 实施中，在所述接收终端发送的身份认证请求之前，所述方法可以进一步包括：

利用预先存储的证书与所述终端建立安全传输层协议 TLS 双向认证连接；与所述终端的通信具体为利用所述 TLS 双向认证连接进行的。

15 具体实施时，为了确保终端与服务器的通信安全，本申请实施例在与终端进行通信之前，可以先建立安全连接，服务器预先存储有证书，终端也预先存储所述服务器所生成的证书，双方通过证书建立 TLS 双向认证连接，从而确保后续通信的安全性，防止通信过程中的数据被非法截获。

实施中，在所述接收终端发送的经过用户私钥加密后的第二随机码之后，所述方法可以进一步包括：

向所述终端发送随机私钥密码。

- 20 具体实施时，在每次使用完一次私钥密码后，服务器可以为终端生成一个随机私钥密码，并将所述随机私钥密码发送给所述终端，以便终端更新自身安全装置的密码，使得安全装置的密码的使用为一次性的，确保用户私钥的安全。

实施例三、

- 25 基于同一发明构思，本发明实施例中还提供了一种终端，由于这些设

备解决问题的原理与上述一种身份认证方法（终端侧）相似，因此这些设备的实施可以参见方法的实施，重复之处不再赘述。

图 3 示出了本发明实施例三中终端的结构示意图一，如图所示，所述终端可以包括：

5 第一发送模块 301，用于向服务器发送身份认证请求；所述身份认证请求包括用户标识；

 第一接收模块 302，用于接收所述服务器发送的第二随机码；

 比对模块 303，用于将接收到的用户输入的生物特征信息与预先存储的与
 与所述用户标识对应的生物特征信息进行比对；

10 加密模块 304，用于如果一致，则利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；

 第二发送模块 305，用于将经过用户私钥加密后的第二随机码发送给所述服务器。

 图 4 示出了本发明实施例三中终端的结构示意图二，如图所示，所述
15 终端可以进一步包括：

 第二接收模块 306，用于在所述向服务器发送身份认证请求之前，接收服务器发送的第一随机码；

 第三发送模块 307，用于将终端标识、用户输入的用户标识和所述第一随机码发送至所述服务器；

20 第三接收模块 308，用于在接收到服务器发送的验证通过消息后，接收用户录入的生物特征信息；

 密钥处理模块 309，用于为所述用户生成公私钥对，建立所述生物特征信息、终端标识、用户私钥与用户标识之间的对应关系，并将用户公钥与
 所述用户标识发送至所述服务器。

25 本发明实施例所述的终端具体可以为手机、pad、平板电脑等移动终端，

这些移动终端可以为触摸屏、也可以为按键形式，本发明对此不作限制。

由于本发明实施例所提供的终端，第一发送模块发送身份认证请求，第一接收模块接收服务器发送的第二随机码，在所述第二接收模块接收到用户输入的生物特征信息之后，只需要比对模块将所述用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对，在终端侧即可完成生物特征信息的验证，无需将生物特征信息发送给服务器由服务器验证，避免在上传过程中导致的生物特征信息泄露，从而确保了生物特征信息的安全性，同时也降低了传输过程的数据量。

实施中，所述第二发送模块具体可以用于将经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识发送给所述服务器。

实施中，所述生物特征信息具体可以为：指纹、掌纹、虹膜、人脸和/或声音。

具体实施时，所述生物特征信息具体可以为：指纹、掌纹、虹膜、人脸、声音等生物特征信息。本发明实施例中可以掌纹采集仪、虹膜采集装置、人脸采集装置、声音录入装置等设备进行采集，这些设备在具体实现时可以采用现有技术中的元器件，也可以由本领域技术人员根据实际需要进行开发设计，本发明对此不作限制。

图 5 示出了本发明实施例三中终端的结构示意图三，如图所示，所述终端可以进一步包括：

连接建立模块 310，用于在所述向服务器发送身份认证请求之前，利用预先存储的服务器生成的证书与所述服务器建立安全传输层协议 TLS 双向认证连接；与所述服务器的通信具体为利用所述 TLS 双向认证连接进行的。

实施中，所述加密模块具体用于如果一致，利用预先存储的私钥密码与安全装置的密码进行验证，验证成功后获取存储于安全区域的用户私钥，根据所述用户私钥对所述第二随机码进行加密。

图 6 示出了本发明实施例三中终端的结构示意图四，如图所示，所述终端可以进一步包括：

第四接收模块 311，用于在所述根据用户私钥对所述第二随机码进行加密之后，接收服务器发送的随机私钥密码，根据所述随机私钥密码修改所述安全装置的密码。

实施例四、

基于同一发明构思，本发明实施例中还提供了一种服务器，由于这些设备解决问题的原理与一种身份认证方法（网络侧）相似，因此这些设备的实施可以参见方法的实施，重复之处不再赘述。

图 7 示出了本发明实施例四中服务器的结构示意图一，如图所示，所述服务器可以包括：

第一接收单元 701，用于接收终端发送的身份认证请求；所述身份认证请求包括用户标识；

第一发送单元 702，用于向所述终端发送第二随机码；

第二接收单元 703，用于接收所述终端发送的经过用户私钥加密后的第二随机码；

解密单元 704，用于利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密；

第一认证单元 705，用于验证解密得到的第二随机码与发送的第二随机码是否一致，如果一致，则身份认证通过。

具体实施时，服务器接收终端发送的身份认证请求，所述身份认证请求中可以包括用户标识、终端标识、其他信息等。本发明实施例所提供的服务器可以预先存储所述用户标识、用户公钥和终端标识的对应关系，在接收到所述终端发送的经过用户私钥加密后的第二随机码之后，利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二

随机码进行解密，验证解密得到的第二随机码与发送的第二随机码是否一致，即可完成身份认证。

本发明实施例所提供的服务器，对用户标识进行验证、利用所述用户标识对应的用户公钥对第二随机码进行解密，即可验证用户公钥、用户标识的对应关系，无需终端上传生物特征信息进行验证，确保了生物特征信息不会被泄露，提高安全性的同时降低了传输的数据量。

图 8 示出了本发明实施例四中服务器的结构示意图二，如图所示，所述服务器可以进一步包括：

确定单元 706，用于在所述接收终端发送的身份认证请求之前，确定终端标识与用户标识的对应关系；

第二发送单元 707，用于向终端发送第一随机码；

第二认证单元 708，用于在收到终端发送的终端标识、用户标识和第一随机码之后进行验证，并在验证通过后向所述终端发送验证通过消息；

关系建立单元 709，用于接收所述终端发送的用户标识和用户公钥，建立所述用户标识、用户公钥与所述终端标识之间的对应关系。

实施中，所述第二接收单元具体可以用于接收所述终端发送的经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识；

所述解密单元具体可以用于利用与所述终端标识对应的用户公钥对所述经过用户私钥加密后的第二随机码和用户标识进行解密；

所述第一认证单元具体可以用于验证解密得到的第二随机码与发送的第二随机码是否一致，以及，验证所述用户标识与所述终端标识之间的对应关系；如果解密得到的第二随机码与发送的第二随机码一致且所述终端标识与所述用户标识对应，则身份认证通过。

图 9 示出了本发明实施例四中服务器的结构示意图三，如图所示，所述服务器可以进一步包括：

连接建立单元 710, 用于在所述接收终端发送的身份认证请求之前, 利用预先存储的证书与所述终端建立安全传输层协议 TLS 双向认证连接; 与所述终端的通信具体为利用所述 TLS 双向认证连接进行的。

图 10 示出了本发明实施例四中服务器的结构示意图四, 如图所示, 所述服务器可以进一步包括:

第三发送单元 711, 用于在所述接收终端发送的经过用户私钥加密后的第二随机码之后, 向所述终端发送随机私钥密码。

在明了运用的环境后, 在终端侧、网络侧分别可以按如下方式实施。在说明过程中, 将分别从终端与网络侧服务器的实施进行说明, 但这并不意味着二者必须配合实施, 实际上, 当终端与服务器分开实施时, 其也各自解决终端侧、网络侧的问题, 只是二者结合使用时, 会获得更好的技术效果。

实施例五、

本发明实施例以移动终端和身份认证服务器的交互过程为例, 进行说明。

身份认证过程可以包括两个步骤: 第一步, 移动终端用户身份信息注册; 第二步, 通过移动终端进行指纹、虹膜或人脸生物特征识别以及在身份认证服务器进行二次认证。

图 11 示出了本发明实施例五中用户生物特征信息注册过程的示意图, 如图所示, 用户生物特征信息注册过程可以包括如下步骤:

步骤 1101、用户申请注册账号;

用户使用所述移动终端进行终端设备注册, 输入用户账号信息, 终端向服务器发送注册请求。

步骤 1102、为所述移动终端用户在身份认证服务器中建立用户账号;

步骤 1103、在身份认证服务器中建立用户账号与移动终端标识之间一

对一的绑定关系；

步骤 1104、身份认证服务器向所述移动终端发送随机码；

步骤 1105、用户使用所述移动终端输入所述身份认证服务器下发的随机码，发送到身份认证服务器进行验证；

5 步骤 1106、所述身份认证服务器验证所述用户账号、所述移动终端标识以及所述随机码，如果验证成功，执行步骤 1107；

步骤 1107、所述身份认证服务器向所述移动终端发送提示信息，提示所述用户输入生物特征信息；

10 步骤 1108、所述用户在所述移动终端上录入指纹、虹膜或人脸等生物特征信息；

步骤 1109、所述移动终端生成公私钥对；

将生成的私钥存储在所述移动终端的安全区域内，以保证其他设备无法访问获取；

15 将生成的公钥以及用户标识信息（例如：用户账号等）通过安全网络发送至所述身份认证服务器；

步骤 1110、所述身份认证服务器存储所述用户公钥和所述用户标识信息。

在完成用户注册后，当用户下次再对所述移动终端进行操作时，则需要进行身份认证。

20 图 12 示出了本发明实施例五中用户身份认证过程的示意图，如图所示，所述用户身份认证过程可以包括如下步骤：

步骤 1201、所述用户启动身份认证服务，所述移动终端向所述身份认证服务器发送身份认证请求；

25 步骤 1202、所述身份认证服务器根据当前用户信息生成随机码，并将所述随机码发送至所述用户；

步骤 1203、所述用户根据所述移动终端的提示录入需要验证的指纹、虹膜或人脸等生物特征，以及所述身份认证服务器下发的随机码；

步骤 1204、所述移动终端对录入的指纹、虹膜或人脸等生物特征进行验证，在验证成功后，执行步骤 1205；

5 步骤 1205、利用所述移动终端内存储的私钥对所述用户信息以及所述随机码进行加密签名，将加密签名后的信息发送至所述身份认证服务器；

步骤 1206、所述身份认证服务器利用存储在所述身份认证服务器端的用户公钥进行解密验签，并验证所述随机码是否正确，完成用户身份的二次验证，如果验证成功，则执行步骤 1207；

10 步骤 1207、通知其他控制系统，允许所述用户访问、操作。

由于本发明实施例所提供的身份认证方式，用户的人脸、指纹或虹膜等个人隐私信息仅存在于所述移动终端内，并不会发送给所述身份认证服务器，因此，确保了用户的生物特征信息不被泄露，提高了数据安全性。

实施例六、

15 本发明实施例所提供的身份认证方案可以应用于移动支付场景，下面以移动支付为例进行说明。

在用户 A 在手机 A-mobile 下载了移动支付软件之后，用户 A 可以在所述移动支付软件的界面内点击注册，输入用户名、密码等信息，手机 A-mobile 可以将这些信息以及手机自身的 IMEI 号码发送给服务器。

20 假设所述手机 A-mobile 的 IMEI 号码为 123456，服务器为用户 A 创建账号 A，建立所述账号 A 与 123456 的绑定关系，然后向所述手机 A-mobile 下发随机码。

用户在所述手机 A-mobile 的移动支付软件界面输入所述随机码，所述手机 A-mobile 将账号 A 和所述随机码发送至所述服务器。

25 服务器验证成功后，提示用户 A 在手机上录入指纹；用户在手机上录

入指纹之后，手机可以通过内部装置为用户 A 生成公私钥对，将生成的私钥存储在手机的安全区域内，将生成的公钥以及账号 A 发送给服务器。

所述服务器接收到账号 A 和 A 的公钥之后，将这些一对一的信息存储在服务器的指定区域。

5 以上，完成了用户注册过程，所述手机侧存储了账号 A、手机 IMEI、用户 A 的私钥、用户 A 的指纹的对应关系，所述服务器侧存储了账号 A、手机 IMEI、用户 A 的公钥的对应关系。

图 13 示出了本发明实施例六中移动支付场景的身份认证过程示意图，如图所示，身份验证过程可以包括：

10 当用户 A 进行了消费、需要进行支付时，用户 A 可以点击身份认证按钮触发手机 A-mobile 向服务器发送认证请求，也可以在用户 A 点击支付按钮时手机 A-mobile 自行发起向服务器发送认证请求，所述认证请求中可以包括手机 IMEI、用户账号 A 等信息。

服务器在接收到手机 A-mobile 发送的认证请求后，可以生成一个随机
15 码发送给所述手机 A-mobile。

所述手机 A-mobile 收到随机码之后，可以提示用户 A 录入指纹和随机码，并在用户 A 录入指纹和随机码之后对所述用户 A 的指纹进行验证，确定所述录入的指纹与所述手机 A-mobile 中存储的指纹是否匹配，如果匹配（具体实施时可以设定阈值，小于一定误差即可认为是匹配的）则认为生
20 物特征验证成功。

所述手机 A-mobile 利用预先存储的用户 A 的私钥对账号 A 和随机码进行加密签名，发送给服务器。

所述服务器接收到经加密签名后的信息时，可以对用户的身份进行二次验证，即，用预先存储的用户 A 的公钥对所述信息进行解密验签，验证
25 所述解密得到的随机码是否与服务器之前发送的随机码一致，验证所述终

端标识与所述账号 A 是否对应等。

如果验证通过，所述服务器可以通知支付系统进行支付操作。

至此，完成了移动支付过程。

在移动支付之前进行了手机端的指纹验证以及服务器端的终端-用户验证，不需要手机上传用户 A 的指纹，确保了用户 A 的隐私信息的安全性。

实施例七、

本发明实施例所提供的身份认证方案可以应用于云机器人场景，下面以云机器人为例进行说明。

所述云机器人可以包括机器人本体和云端机器人，所述云端机器人具体可以为云服务器。

用户 B 购买了机器人 Joan，假设机器人 Joan 的编号为 JQR1，用户 B 可以提出注册请求，所述云端机器人为用户 B 建立账号 b 并建立账号 b 与 JQR1 之间的一对一的绑定关系，并向所述机器人 Joan 发送随机码，用户 B 在机器人 Joan 上输入所述随机码之后，机器人 Joan 将账号 b 与编码 JQR1、随机码一并发送至云端机器人。

所述云端机器人对账号 b 与编码 JQR1 的对应关系进行验证，并验证随机码是否与之前发送的随机码一致，如果验证通过，则通知机器人 Joan 验证通过。

用户 B 可以在机器人 Joan 上录入声音，例如：“我是用户 B，我是你的主人。” 机器人 Joan 可以存储这段声音，也可以对这段声音进行识别、提取声音特征等，如音调、音色等。

机器人 Joan 为所述用户 B 生成公私钥对，将私钥存储在机器人本体内，将账号 b、编号 JQR1 以及公钥发送至所述云端机器人。

所述云端机器人将收到的账号 b、编号 JQR1 以及公钥一对一的存储起来。

以上，完成了机器人注册过程，所述机器人本体存储了账号 b、编号 JQR1、B 的私钥及 B 的语音特征的对应关系；所述云端机器人存储了账号 b、编号 JQR1 及 B 的公钥的对应关系。

图 14 示出了本发明实施例七中云机器人场景的身份认证过程示意图，

5 如图所示，所述云机器人场景的身份认证过程可以包括：

当用户 B 需要所述机器人 Joan 为他提供服务时，例如：用户 B 通过语音发出“请扫地。”

机器人 Joan 可以将账号 b 发送给云端机器人，在收到云端机器人下发的随机码之后，用户 B 可以根据提示输入所述随机码，具体实施时可以为
10 手动键盘输入、触摸屏输入或者语音输入等。

机器人 Joan 对用户 B 的语音信息（“请扫地”）进行语音识别、提取语音特征，并将所述语音特征与预先存储的语音特征进行比较，如果音调、音色等特征一致或在一定误差范围内，则认为该用户是用户 B。

此时，机器人 Joan 可以用私钥对随机码进行加密签名，将加密签名后的随机码和用户信息发送至云端机器人。
15

所述云端机器人利用预先存储的所述用户 B 的公钥进行解密验签，验证账号 b、编号 JQR1 以及公钥之间的对应关系，验证随机码是否与之前下发的随机码一致。

如果验证成功，则可以通知机器人的扫地控制模块可以执行扫地操作，
20 所述机器人 Joan 即可对房间地面进行打扫。

采用上述方案，避免用户 B 的语音信息泄露，确保了用户 B 的个人信息安全性。

假设用户 C 来到用户 B 的家中，用户 C 对所述机器人 Joan 发出语音指令，例如“你家主人叫什么名字？”

25 机器人 Joan 将所述用户 C 的语音信息进行识别后与预先存储的用户 B

的语音特征进行比较，发现二者的音调、音色等信息有较大区别（大于误差范围），则可以确定所述用户不是用户 B，拒绝为其提供服务。

采用上述方案，在机器人本地即可完成生物特征的验证，如果验证不通过可以直接、快速的给出验证结果，无需将用户的生物特征信息发送至云端机器人，一方面确保了用户个人信息不会被传输、泄露，另一方面也提高了验证的效率。

实施例八、

本发明实施例所提供的身份认证方案可以应用于门禁场景，下面以门禁为例进行说明。

假设公司 D 购买了门禁系统（可以包括门禁设备和网络侧服务器）并在公司门口安装了门禁设备，每位员工可以通过注册账号录入了自己的人脸信息，所述门禁设备为每位员工生成了公私钥对，所述门禁设备端保存了员工编号、相对的人脸信息、相应的私钥、门禁设备号，所述门禁系统的网络侧存储了员工编号、相应的公钥以及门禁设备号。

图 15 示出了本发明实施例八中门禁系统的身份认证过程示意图，如图所示，所述门禁系统的身份认证过程可以包括：

当员工进出公司时，发起身份认证服务。

所述网络侧向所述门禁设备发送随机码。

员工根据提示输入随机码并将自己的面部朝向门禁设备的采集装置，所述门禁设备获取到员工的人脸信息后将其与预先存储的人脸信息进行比对，如果比对一致，即可根据所述人脸信息确定所述员工的编号。

利用所述员工的私钥对所述随机码进行加密签名，将所述随机码与员工编号、门禁设备号发送至网络侧。

网络侧通过所述员工编号确定所述员工的公钥，对所述随机码进行解密验签。

如果解密后的随机码与之前下发的随机码一致，则认为身份验证成功，通知开关控制模块，所述开关控制模块收到验证通过通知后对公司的门执行解锁。

本发明实施例所提供的身份认证方案还可以应用于智能家居等其他场景，本发明在此不做一一说明。

本发明实施例所提供的身份认证方案，移动终端可以预先存储用户标识、生物特征信息、用户私钥和终端标识的绑定关系，服务器侧可以预先存储用户标识、用户公钥和终端标识的绑定关系，认证流程可以包括移动终端本地生物特征信息的一次认证和服务器侧设备信息的二次认证，从而在确保用户个人隐私信息不被泄露的前提下实现身份认证。

为了描述的方便，以上所述装置的各部分以功能分为各种模块或单元分别描述。当然，在实施本发明时可以把各模块或单元的功能在同一个或多个软件或硬件中实现。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产

生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

5 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程 and / 或方框图一个方框或多个方框中指定的功能。

10 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程 and / 或方框图一个方框或多个方框中指定的功能的步骤。

15 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

权利要求书

1. 一种身份认证方法，其特征在于，包括如下步骤：

向服务器发送身份认证请求；所述身份认证请求包括用户标识；

接收所述服务器发送的第二随机码；

5 将接收到的用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比较；

如果一致，则利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；

将经过用户私钥加密后的第二随机码发送给所述服务器。

10 2. 如权利要求 1 所述的方法，其特征在于，在所述向服务器发送身份认证请求之前，进一步包括：

接收服务器发送的第一随机码；

将终端标识、用户标识和第一随机码发送至所述服务器；

15 在接收到服务器发送的验证通过消息后，接收用户录入的生物特征信息；

为所述用户生成公私钥对，建立所述生物特征信息、终端标识、用户私钥与用户标识之间的对应关系，并将用户公钥与所述用户标识发送至所述服务器。

20 3. 如权利要求 1 所述的方法，其特征在于，所述将经过用户私钥加密后的第二随机码发送给所述服务器，具体为：将经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识发送给所述服务器。

4. 如权利要求 1 所述的方法，其特征在于，在所述向服务器发送身份认证请求之前，进一步包括：利用预先存储的服务器生成的证书与所述服务器建立安全传输层协议 TLS 双向认证连接；与所述服务器的通信具体为
25 利用所述 TLS 双向认证连接进行的。

5. 如权利要求 1 所述的方法, 其特征在于, 所述利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密, 具体为: 利用预先存储的私钥密码与安全装置的密码进行验证, 验证成功后获取存储于安全区域的用户私钥, 根据所述用户私钥对所述第二随机码进行加密。

6. 如权利要求 6 所述的方法, 其特征在于, 在所述根据用户私钥对所述第二随机码进行加密之后, 进一步包括: 接收服务器发送的随机私钥密码, 根据所述随机私钥密码修改所述安全装置的密码。

7. 一种身份认证方法, 其特征在于, 包括如下步骤:

接收终端发送的身份认证请求; 所述身份认证请求包括用户标识;

向所述终端发送第二随机码;

接收所述终端发送的经过用户私钥加密后的第二随机码;

利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密;

验证解密得到的第二随机码与发送的第二随机码是否一致, 如果一致,

则身份认证通过。

8. 如权利要求 7 所述的方法, 其特征在于, 在所述接收终端发送的身份认证请求之前, 进一步包括:

确定终端标识与用户标识的对应关系;

向终端发送第一随机码;

在收到终端发送的终端标识、用户标识和第一随机码之后进行验证, 并在验证通过后向所述终端发送验证通过消息;

接收所述终端发送的用户标识和用户公钥, 建立所述用户标识、用户公钥与所述终端标识之间的对应关系。

9. 如权利要求 7 所述的方法, 其特征在于, 所述接收所述终端发送的经过用户私钥加密后的第二随机码, 具体为: 接收所述终端发送的经过用

户私钥加密后的第二随机码和所述用户标识、以及终端标识；所述利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密，具体为：利用与所述终端标识对应的用户公钥对所述经过用户私钥加密后的第二随机码和用户标识进行解密；所述验证解密得到的第二随机码与发送的第二随机码是否一致，如果一致则身份认证通过，具体为：验证解密得到的第二随机码与发送的第二随机码是否一致，以及，验证所述用户标识与所述终端标识之间的对应关系；如果解密得到的第二随机码与发送的第二随机码一致且所述终端标识与所述用户标识对应，则身份认证通过。

10. 如权利要求 7 所述的方法，其特征在于，在所述接收终端发送的身份认证请求之前，进一步包括：利用预先存储的证书与所述终端建立安全传输层协议 TLS 双向认证连接；与所述终端的通信具体为利用所述 TLS 双向认证连接进行的。

11. 如权利要求 7 所述的方法，其特征在于，在所述接收终端发送的经过用户私钥加密后的第二随机码之后，进一步包括：向所述终端发送随机私钥密码。

12. 一种终端，其特征在于，包括：

第一发送模块，用于向服务器发送身份认证请求；所述身份认证请求包括用户标识；

第一接收模块，用于接收所述服务器发送的第二随机码；

比对模块，用于将接收到的用户输入的生物特征信息与预先存储的与所述用户标识对应的生物特征信息进行比对；

加密模块，用于如果一致，则利用预先存储的与所述用户标识对应的用户私钥对所述第二随机码进行加密；

第二发送模块，用于将经过用户私钥加密后的第二随机码发送给所述

服务器。

13. 如权利要求 12 所述的终端，其特征在于，进一步包括：

第二接收模块，用于在所述向服务器发送身份认证请求之前，接收服务器发送的第一随机码；

5 第三发送模块，用于将终端标识、用户标识和所述第一随机码发送至所述服务器；

第三接收模块，用于在接收到服务器发送的验证通过消息后，接收用户录入的生物特征信息；

10 密钥处理模块，用于为所述用户生成公私钥对，建立所述生物特征信息、终端标识、用户私钥与用户标识之间的对应关系，并将用户公钥与所述用户标识发送至所述服务器。

14. 如权利要求 12 所述的终端，其特征在于，所述第二发送模块具体用于将经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识发送给所述服务器。

15 15. 如权利要求 12 所述的终端，其特征在于，进一步包括：

连接建立模块，用于在所述向服务器发送身份认证请求之前，利用预先存储的服务器生成的证书与所述服务器建立安全传输层协议 TLS 双向认证连接；与所述服务器的通信具体为利用所述 TLS 双向认证连接进行的。

20 16. 如权利要求 12 所述的终端，其特征在于，所述加密模块具体用于如果一致，利用预先存储的私钥密码与安全装置的密码进行验证，验证成功后获取存储于安全区域的用户私钥，根据所述用户私钥对所述第二随机码进行加密。

17. 如权利要求 16 所述的终端，其特征在于，进一步包括：

25 第四接收模块，用于在所述根据用户私钥对所述第二随机码进行加密之后，接收服务器发送的随机私钥密码，根据所述随机私钥密码修改所述

安全装置的密码。

18. 一种服务器，其特征在于，包括：

第一接收单元，用于接收终端发送的身份认证请求；所述身份认证请求包括用户标识；

5 第一发送单元，用于向所述终端发送第二随机码；

第二接收单元，用于接收所述终端发送的经过用户私钥加密后的第二随机码；

解密单元，用于利用预先存储的与所述用户标识对应的用户公钥对所述经过用户私钥加密后的第二随机码进行解密；

10 第一认证单元，用于验证解密得到的第二随机码与发送的第二随机码是否一致，如果一致，则身份认证通过。

19. 如权利要求 18 所述的服务器，其特征在于，进一步包括：

确定单元，用于在所述接收终端发送的身份认证请求之前，确定终端标识与用户标识的对应关系；

15 第二发送单元，用于向终端发送第一随机码；

第二认证单元，用于在收到终端发送的终端标识、用户标识和第一随机码之后进行验证，并在验证通过后向所述终端发送验证通过消息；

关系建立单元，用于接收所述终端发送的用户标识和用户公钥，建立所述用户标识、用户公钥与所述终端标识之间的对应关系。

20 20. 如权利要求 18 所述的服务器，其特征在于，所述第二接收单元具体用于接收所述终端发送的经过用户私钥加密后的第二随机码和所述用户标识、以及终端标识；所述解密单元具体用于利用与所述终端标识对应的用户公钥对所述经过用户私钥加密后的第二随机码和用户标识进行解密；所述
25 第一认证单元具体用于验证解密得到的第二随机码与发送的第二随机码是否一致，以及，验证所述用户标识与所述终端标识之间的对应关系；如

果解密得到的第二随机码与发送的第二随机码一致且所述终端标识与所述用户标识对应，则身份认证通过。

21. 如权利要求 18 所述的服务器，其特征在于，进一步包括：

连接建立单元，用于在所述接收终端发送的身份认证请求之前，利用
5 预先存储的证书与所述终端建立安全传输层协议 TLS 双向认证连接；与所述终端的通信具体为利用所述 TLS 双向认证连接进行的。

22. 如权利要求 18 所述的服务器，其特征在于，进一步包括：

第三发送单元，用于在所述接收终端发送的经过用户私钥加密后的第二随机码之后，向所述终端发送随机私钥密码。

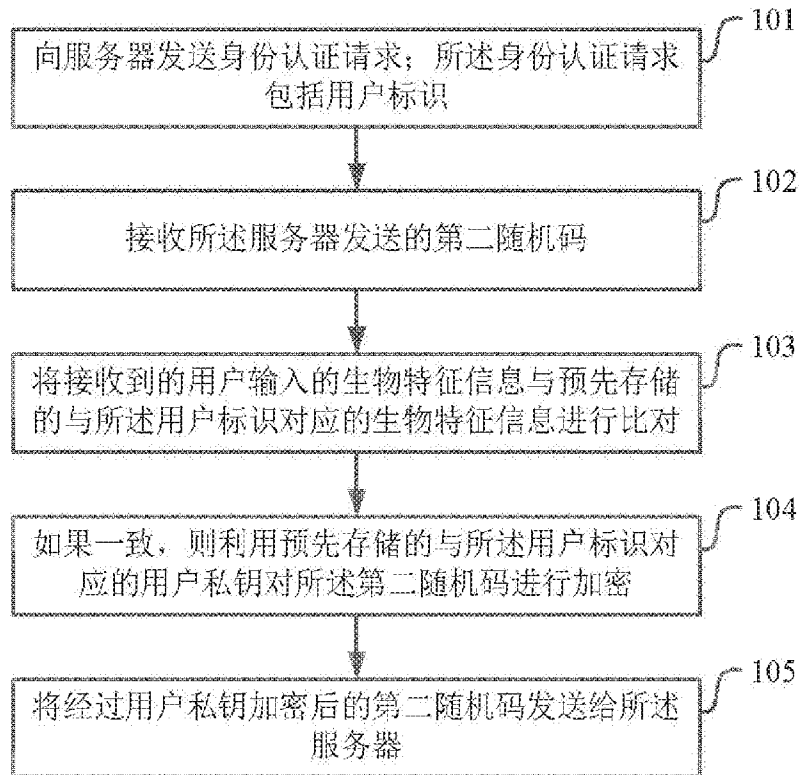


图 1

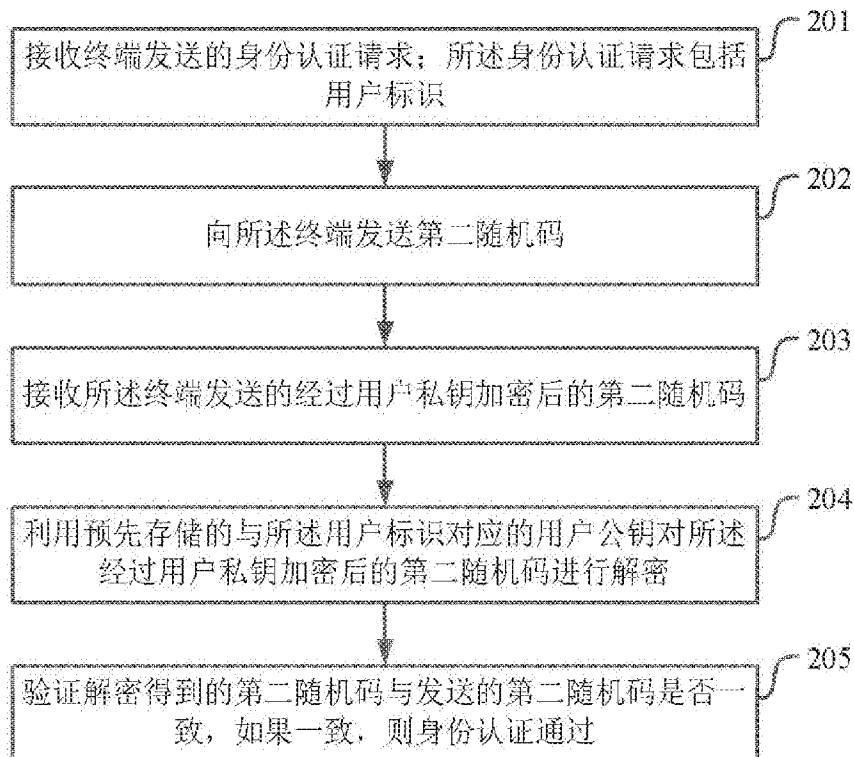


图 2

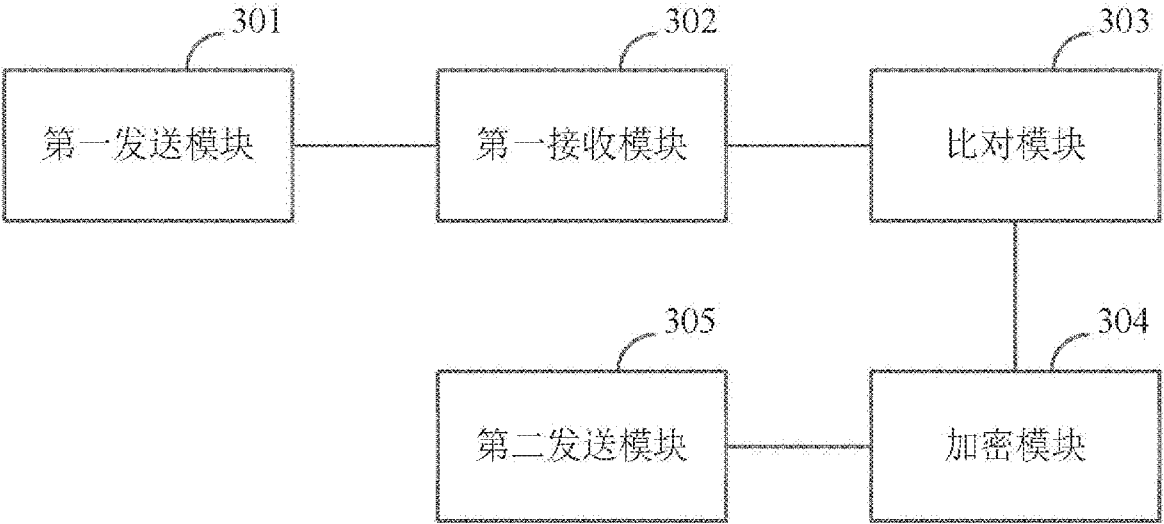


图 3

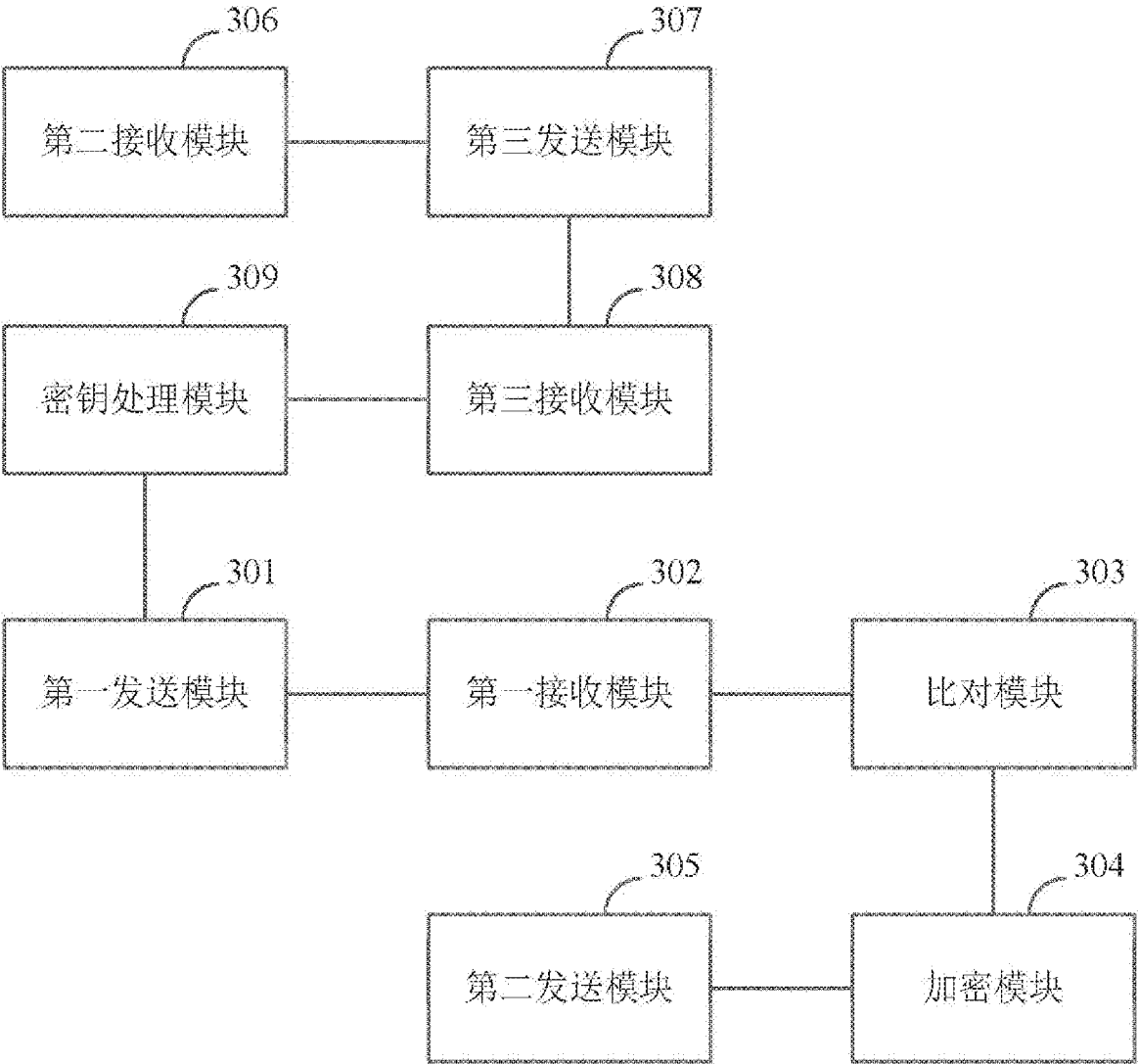


图 4

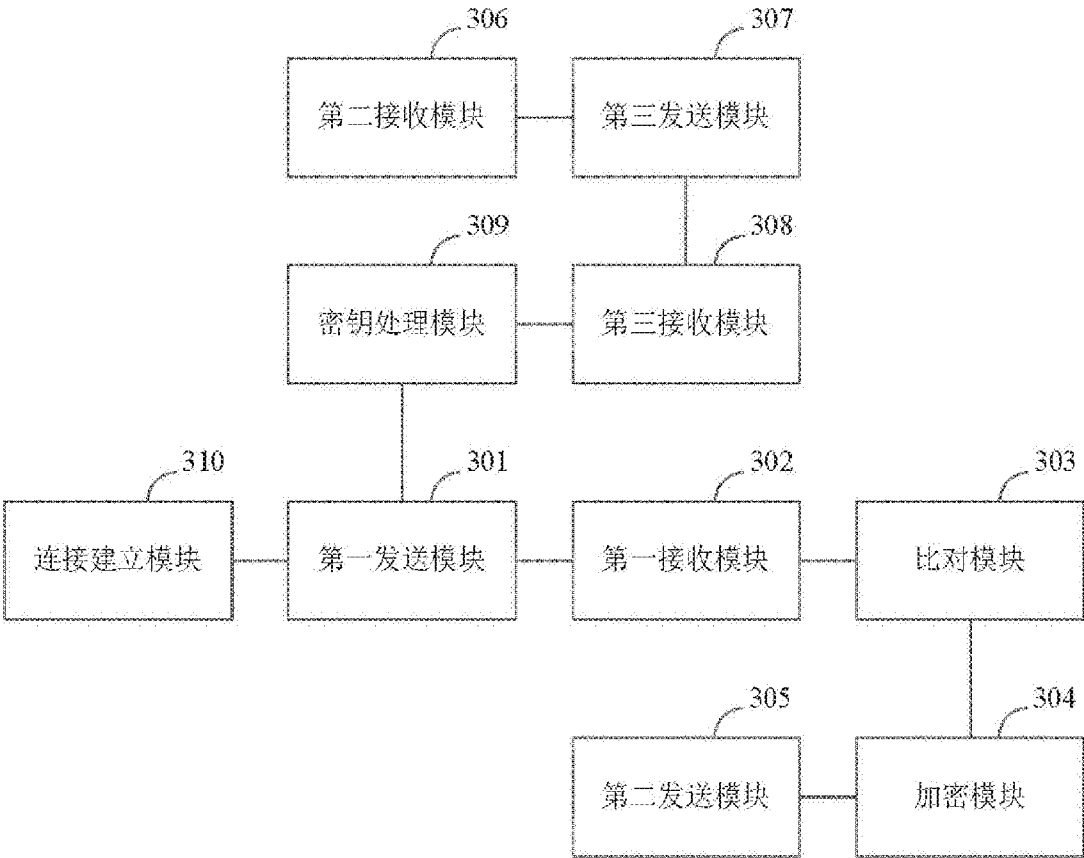


图 5

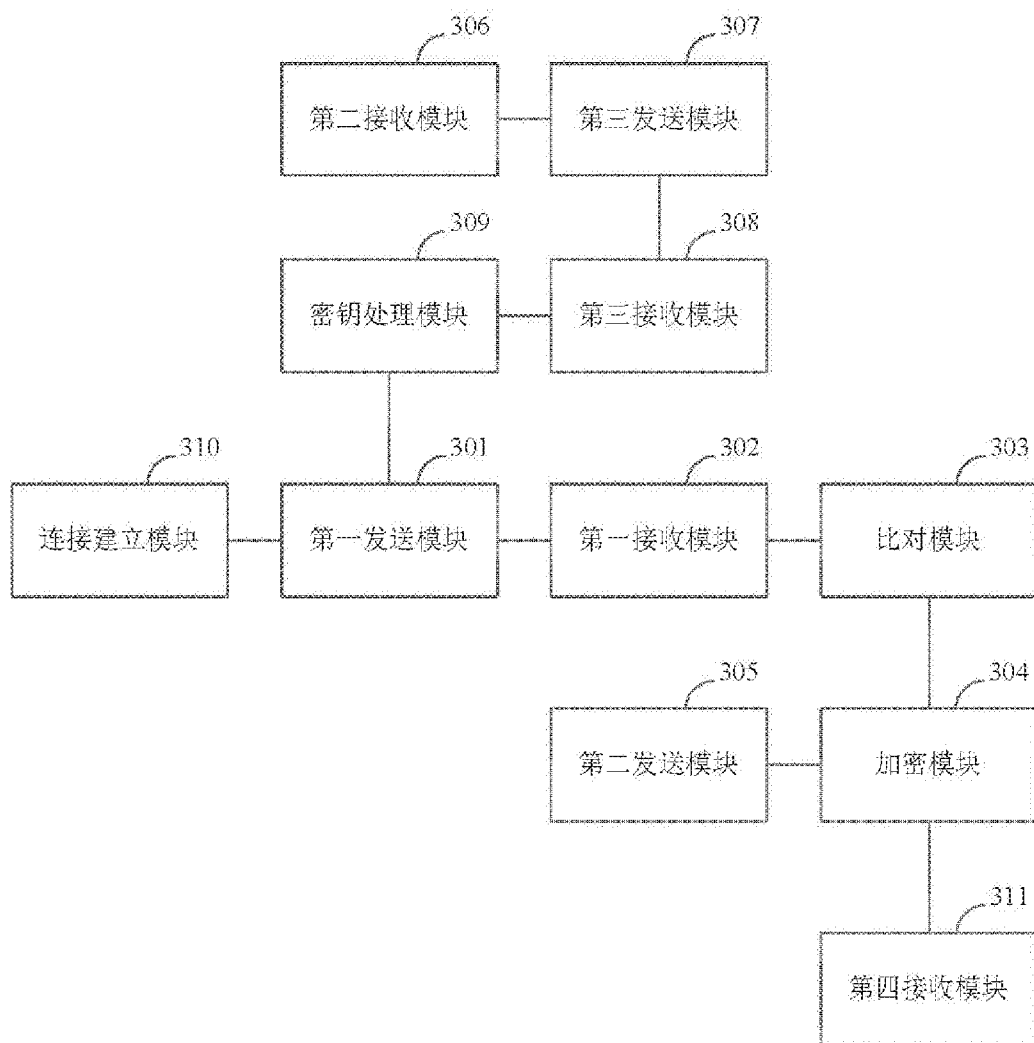


图 6

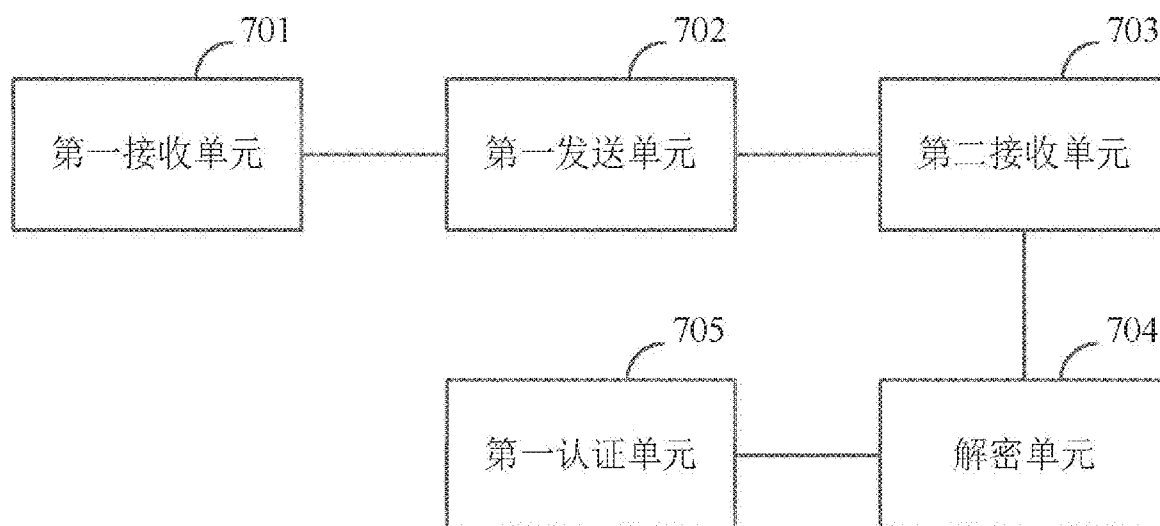
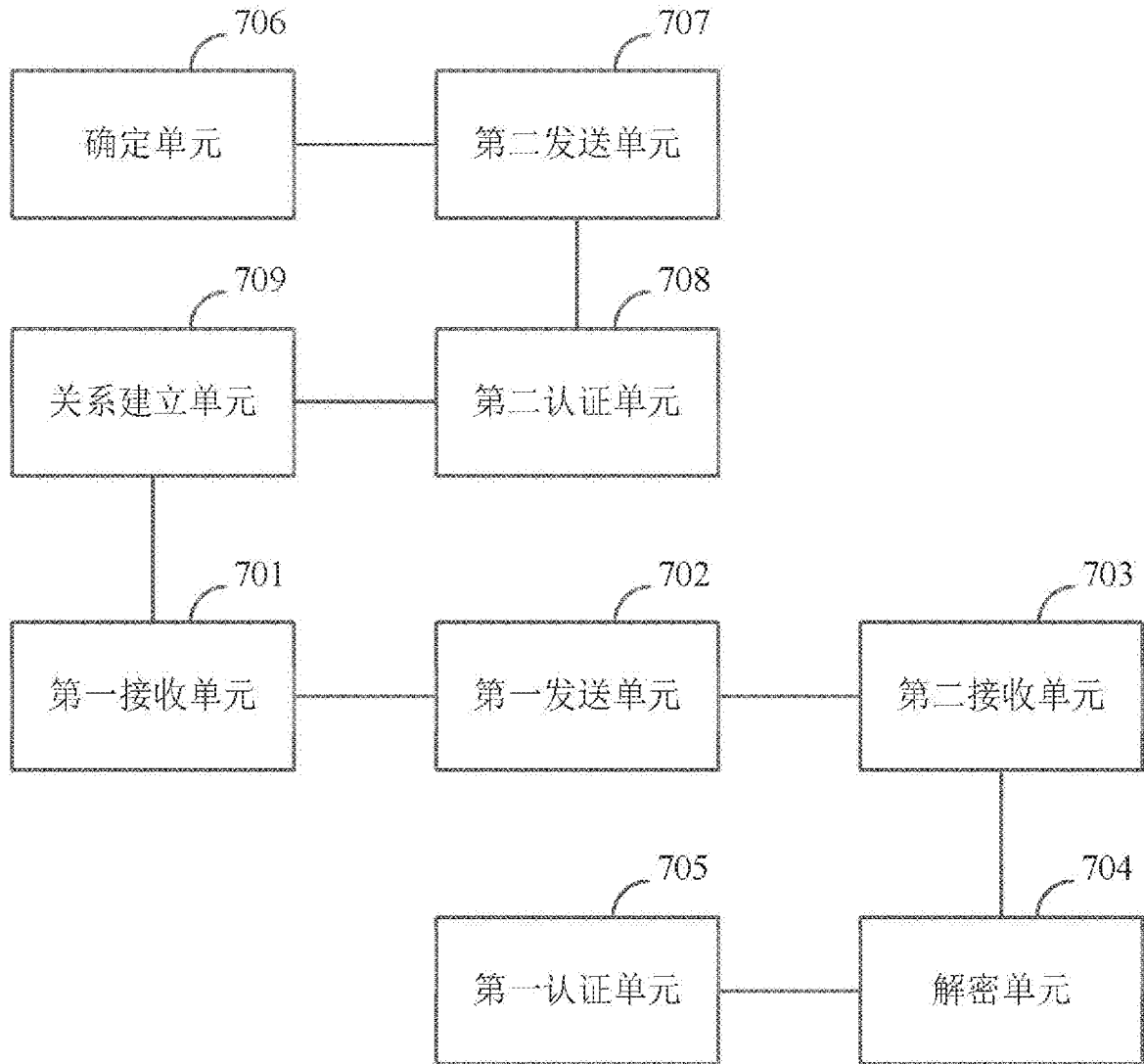


图 7

**图 8**

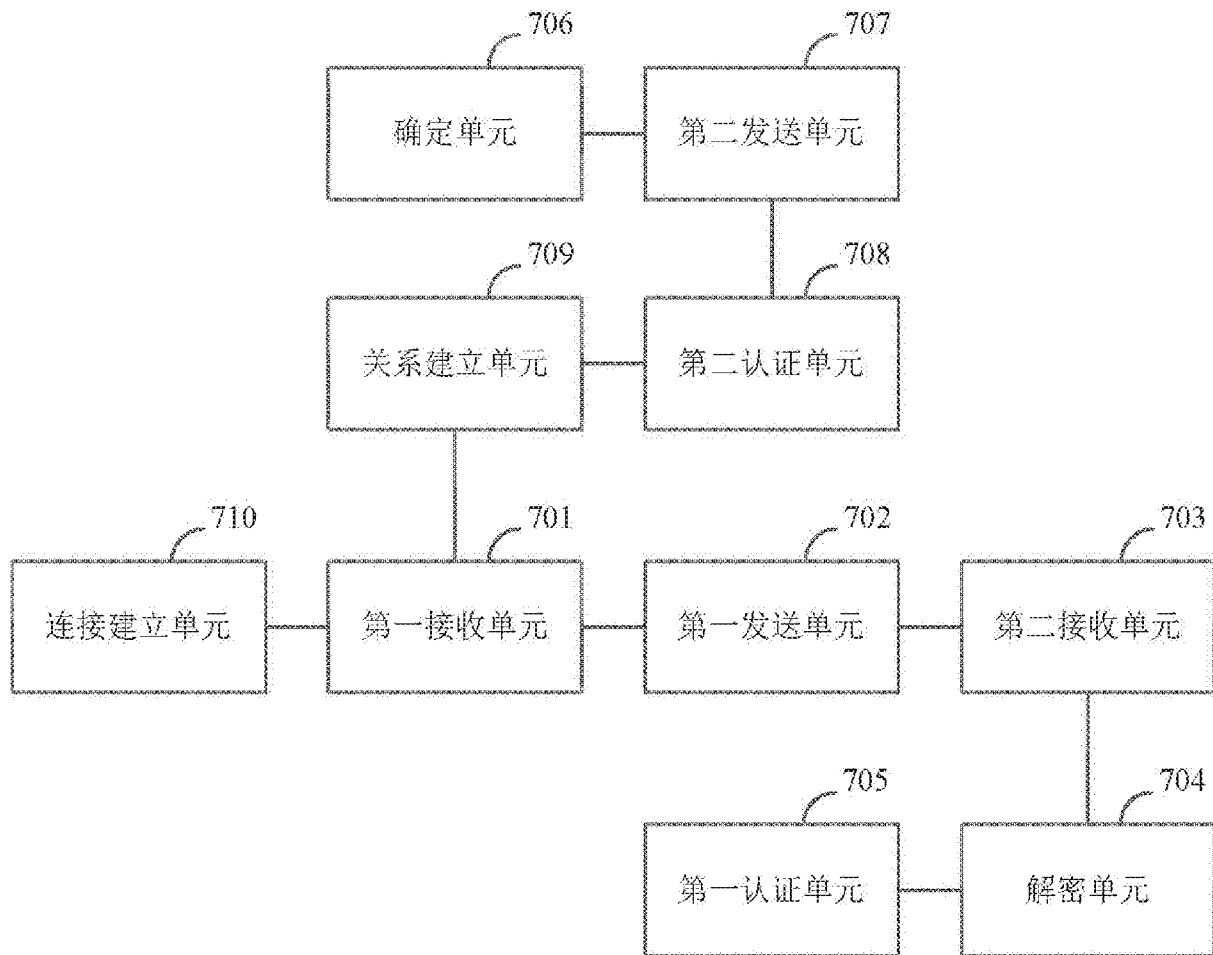


图 9

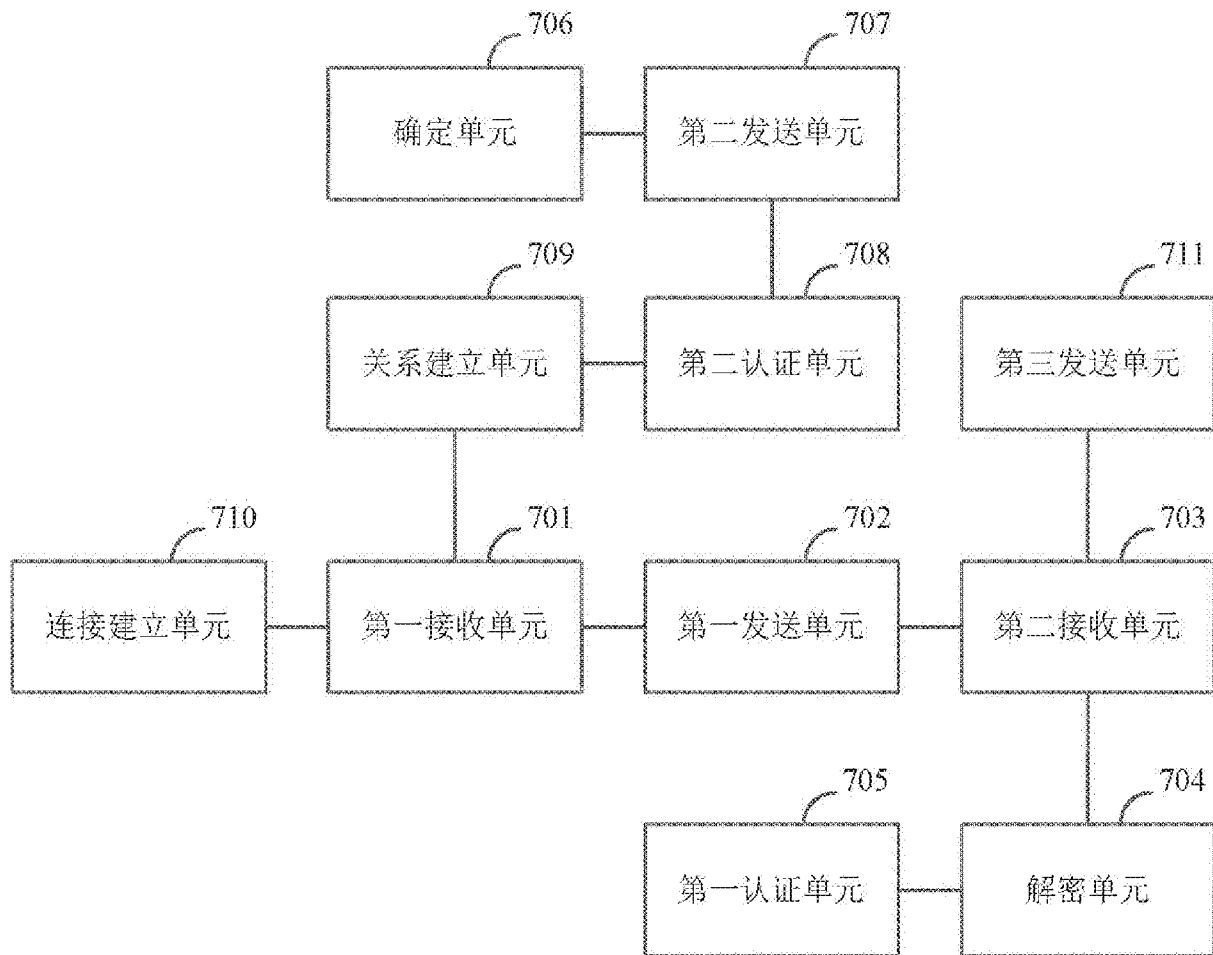


图 10

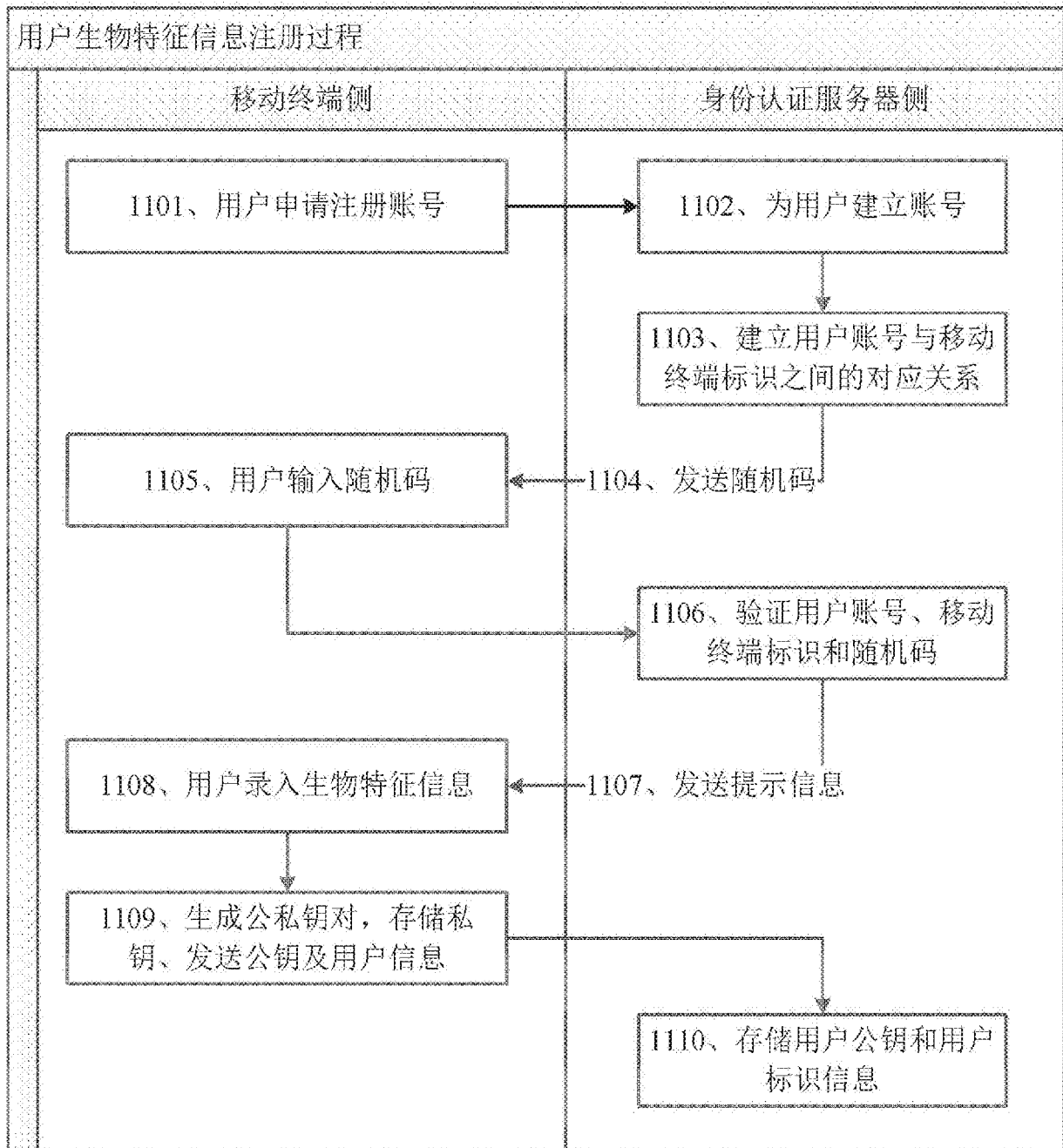


图 11

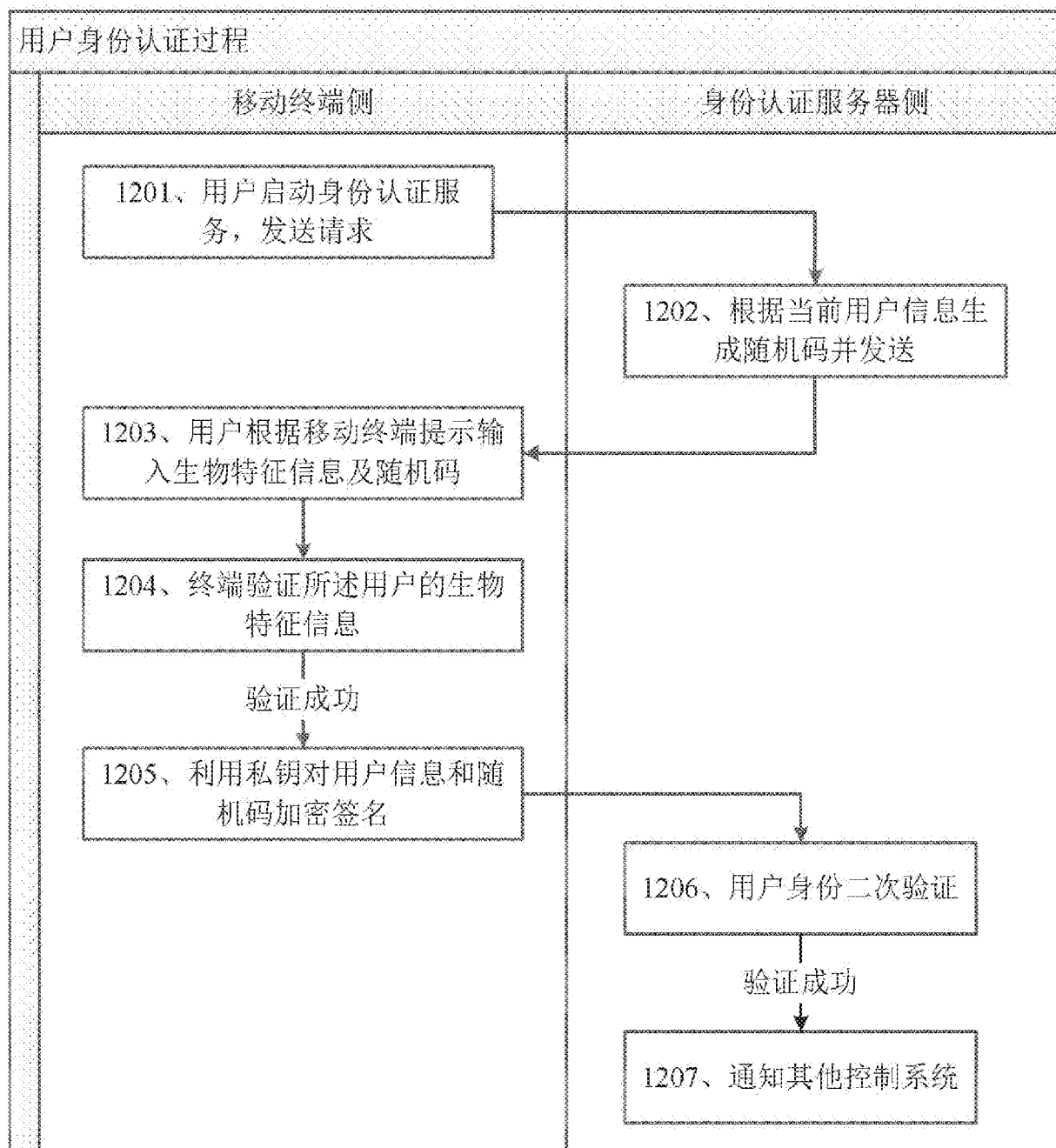


图 12

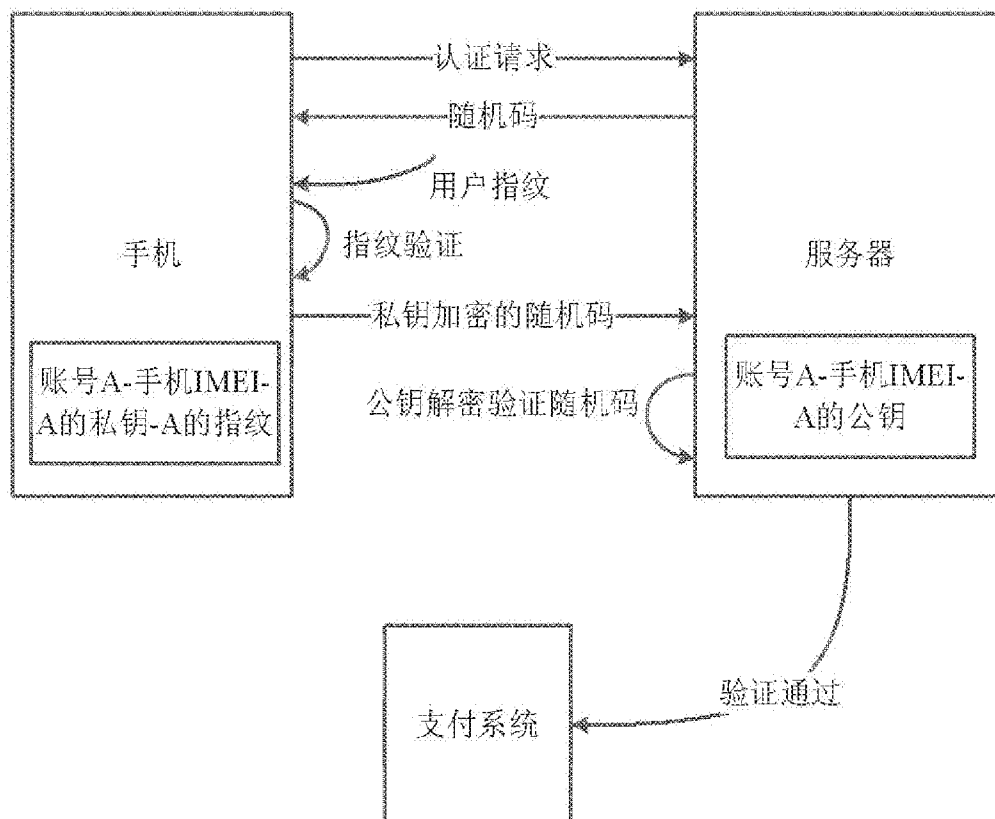


图 13

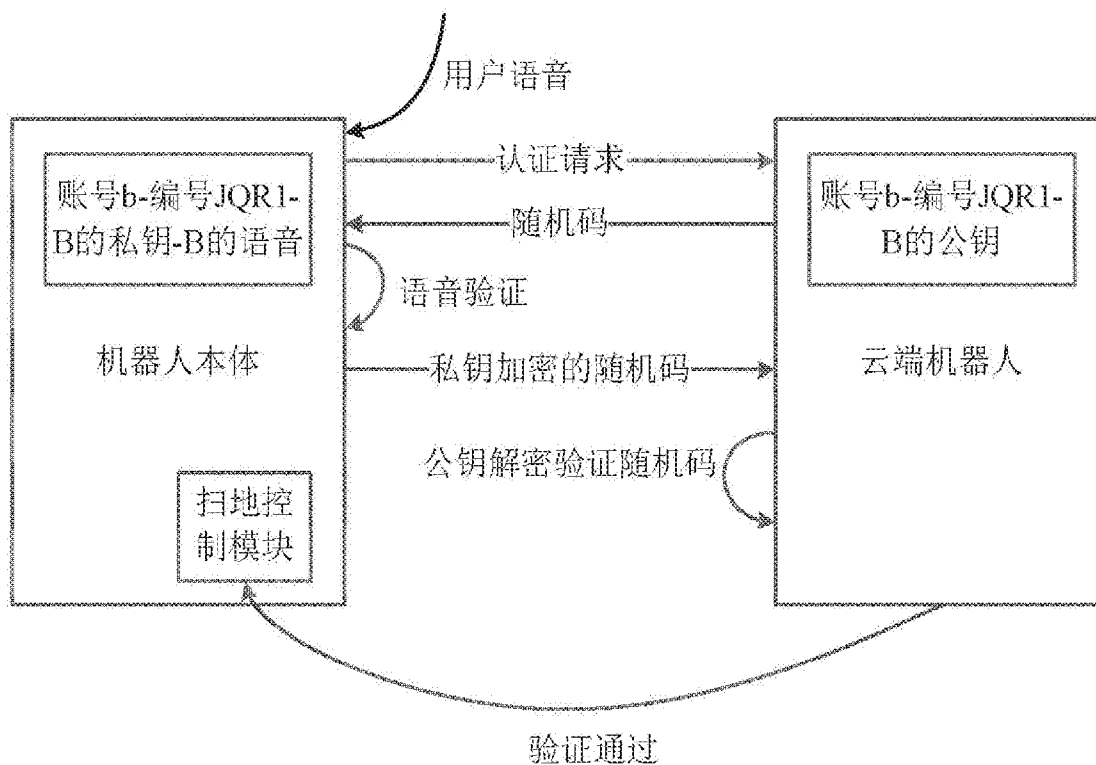


图 14

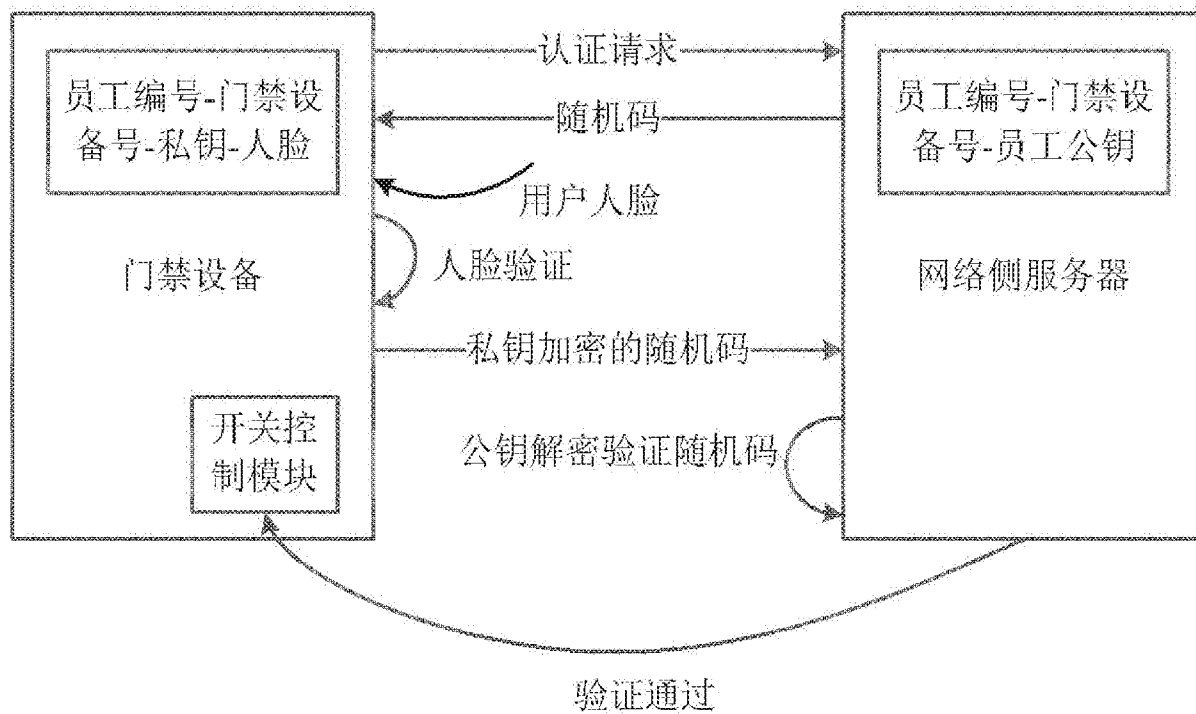


图 15

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/079397

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) 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)

H04L

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)

CNPAT, CNKI, WPI, SIPOABS: biological, fingerprint, iris, face, palmprint, auricle, asymmetric key, key pair, random number, random code, biometric, private key, random, challenge, public key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104660412 A (NANJING ZEBEN INFORMATION TECHNOLOGY CO., LTD.), 27 May 2015 (27.05.2015), description, paragraphs [0014]-[0033]	1-22
Y	CN 101848213 A (NORTHWESTERN POLYTECHNICAL UNIVERSITY et al.), 29 September 2010 (29.09.2010), description, paragraphs [0042]-[0079]	1-22
A	CN 104363099 A (NANJING ZEBEN INFORMATION TECHNOLOGY CO., LTD.), 18 February 2015 (18.02.2015), the whole document	1-22
A	CN 105227537 A (HUAWEI TECHNOLOGIES CO., LTD.), 06 January 2016 (06.01.2016), the whole document	1-22
A	US 2005/0246763 A1 (NATIONAL UNIVERSITY OF IRELAND), 03 November 2005 (03.11.2005), the whole document	1-22

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 29 December 2016 (29.12.2016)	Date of mailing of the international search report 18 January 2017 (18.01.2017)
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 LIAO, Jiajia Telephone No.: (86-10) 62413304

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/079397

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104660412 A	27 May 2015	None	
CN 101848213 A	29 September 2010	None	
CN 104363099 A	18 February 2015	None	
CN 105227537 A	06 January 2016	WO 2015192670 A1	23 December 2015
		KR 20160021763 A	26 February 2016
		EP 3001351 A1	30 March 2016
		US 2016119143 A1	28 April 2016
US 2005/0246763 A1	03 November 2005	WO 2005101965 A2	03 November 2005

A. 主题的分类 H04L 9/32 (2006.01) 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) H04L 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)) CNPAT, CNKI, WPI, SIPOABS: 生物, 指纹, 虹膜, 脸, 掌纹, 耳廓, 非对称密钥, 私钥, 密钥对, 质询, 挑战, 随机数, 随机码, biometric, private key, random, challenge, public key		
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 104660412 A (南京泽本信息技术有限公司) 2015年 5月 27日 (2015 - 05 - 27) 说明书第[0014]-[0033]段	1-22
Y	CN 101848213 A (西北工业大学等) 2010年 9月 29日 (2010 - 09 - 29) 说明书第[0042]-[0079]段	1-22
A	CN 104363099 A (南京泽本信息技术有限公司) 2015年 2月 18日 (2015 - 02 - 18) 全文	1-22
A	CN 105227537 A (华为技术有限公司) 2016年 1月 6日 (2016 - 01 - 06) 全文	1-22
A	US 2005/0246763 A1 (NATIONAL UNIVERSITY OF IRELAND) 2005年 11月 3日 (2005 - 11 - 03) 全文	1-22
☐ 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 2016年 12月 29日		国际检索报告邮寄日期 2017年 1月 18日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451		受权官员 廖佳佳 电话号码 (86-10)62413304

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/079397

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	104660412	A	2015年 5月 27日	无			
CN	101848213	A	2010年 9月 29日	无			
CN	104363099	A	2015年 2月 18日	无			
CN	105227537	A	2016年 1月 6日	WO	2015192670	A1	2015年 12月 23日
				KR	20160021763	A	2016年 2月 26日
				EP	3001351	A1	2016年 3月 30日
				US	2016119143	A1	2016年 4月 28日
US	2005/0246763	A1	2005年 11月 3日	WO	2005101965	A2	2005年 11月 3日