(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 106533669 B
(45)授权公告日 2018.07.13

(21)申请号 201611030194.5

(22)申请日 2016.11.15

(65)同一申请的已公布的文献号
申请公布号 CN 106533669 A

(43)申请公布日 2017.03.22

(73)专利权人 百度在线网络技术(北京)有限公司
地址 100085 北京市海淀区上地十街10号百度大厦三层

(72)发明人 丁羽 韦韬 张煜龙

(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 王达佐 马晓亚

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 101873331 A,2010.10.27,说明书第[0007]-[0016]段,第[0020]-[0051]段,图1至图3.
CN 102131188 A,2011.07.20,说明书第[0043]-[0146]段.
CN 102577462 A,2012.07.11,全文.
CN 104283886 A,2015.01.14,全文.
US 2004/0030901 A1,2004.02.12,全文.
CN 104092663 A,2014.10.08,全文.
Antonio Pecchia 等.Identifying Compromised Users in Shared Computing Infrastructures:a Data-Driven Bayesian Network Approach.《IEEE》.2011,全文.
吴俊军 等.一种基于可信计算的NFC认证模型.《计算机工程与科学》.2011,全文.

审查员 薛乐梅

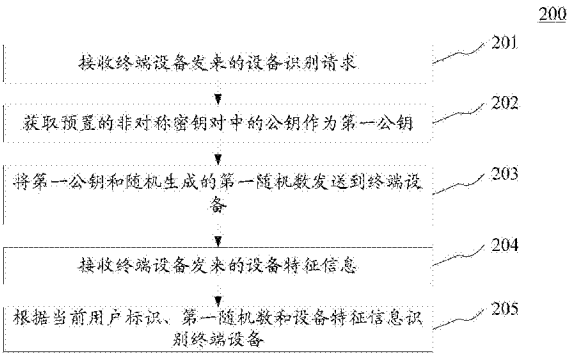
权利要求书3页 说明书15页 附图9页

(54)发明名称

设备识别的方法、装置和系统

(57)摘要

本申请公开了设备识别的方法、装置和系统。该方法的一具体实施方式包括:接收终端设备发来的设备识别请求,设备识别请求包括终端设备的当前用户的当前用户标识;获取预置的非对称密钥对中的公钥作为第一公钥;将第一公钥和随机生成的第一随机数发送到终端设备;接收终端设备发来的设备特征信息,其中,设备特征信息是终端设备根据当前用户标识、第一公钥、第一随机数以及终端设备的设备标识生成的;根据当前用户标识、第一随机数和设备特征信息识别上述终端设备。该实施方式增加了攻击者截取终端设备的设备特征信息的难度,继而提高了终端设备访问服务器的安全性。



CN 106533669 B

1.一种用于服务器的设备识别方法,其特征在于,所述方法包括:

接收终端设备发来的设备识别请求,所述设备识别请求包括所述终端设备的当前用户的当前用户标识;

获取预置的非对称密钥对中的公钥作为第一公钥;

将所述第一公钥和随机生成的第一随机数发送到所述终端设备;

接收所述终端设备发来的设备特征信息,其中,所述设备特征信息是所述终端设备根据所述当前用户标识、所述第一公钥、所述第一随机数以及所述终端设备的设备标识生成的;

根据所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备。

2.根据权利要求1所述的方法,其特征在于,所述设备识别请求还包括识别类型标识符,所述识别类型标识符用于指示所述终端设备在所述服务器中的设备识别类型;以及

所述根据所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备,包括:

根据所述终端设备的设备识别类型、所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备。

3.根据权利要求1所述的方法,其特征在于,所述根据所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备,包括:

解析所述设备特征信息以得到用户标识和随机数;

确定解析所得到的用户标识是否与所述当前用户标识相同以及解析所得到的随机数是否与所述第一随机数相同;

响应于确定解析所得到的用户标识与所述当前用户标识不相同和/或解析所得到的随机数与所述第一随机数不相同,生成用于指示所述设备识别请求识别失败的识别结果。

4.根据权利要求3所述的方法,其特征在于,所述解析所述设备特征信息以得到用户标识和随机数,包括:

使用预设非对称解密算法和所述预置的非对称密钥对中的私钥,解析所述设备特征信息,以得到用户标识、随机数和设备标识。

5.根据权利要求3或4所述的方法,其特征在于,所述根据所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备,还包括:

响应于确定解析所得到的用户标识与所述当前用户标识相同且解析所得到的随机数与所述第一随机数相同,根据所述当前用户标识、所述第一随机数和解析所得到的设备标识识别所述终端设备。

6.一种用于终端设备的设备识别方法,其特征在于,所述方法包括:

向服务器发送设备识别请求,所述设备识别请求包括所述终端设备的当前用户的当前用户标识;

接收所述服务器发来的第一公钥和第一随机数,其中,所述第一公钥是所述服务器从预置的非对称密钥对中获取的公钥,所述第一随机数是由所述服务器随机生成的;

获取所述终端设备的设备标识;

根据所述当前用户标识、所述第一公钥、所述第一随机数以及所述设备标识生成设备特征信息;

将所述设备特征信息发送给所述服务器，以使所述服务器根据所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备。

7.根据权利要求6所述的方法，其特征在于，所述设备识别请求还包括识别类型标识符，所述识别类型标识符用于指示所述终端设备在所述服务器中的设备识别类型；以及

所述根据所述当前用户标识、所述第一公钥、所述第一随机数以及所述设备标识生成设备特征信息，包括：

根据所述终端设备的设备识别类型、所述当前用户标识、所述第一公钥、所述第一随机数以及所述设备标识生成设备特征信息。

8.根据权利要求7所述的方法，其特征在于，所述根据所述终端设备的设备识别类型、所述当前用户标识、所述第一公钥、所述第一随机数以及所述设备标识生成设备特征信息，包括：

根据所述终端设备的设备识别类型、所述第一公钥和所述设备标识，利用预设消息摘要算法计算得到第一摘要值；

利用所述预设消息摘要算法计算所述第一摘要值与所述第一随机数的第二摘要值；

利用预设非对称加密算法，使用所述第一公钥对所述第一摘要值、所述当前用户标识和所述第一随机数进行加密以得到加密信息；

组合所述当前用户标识、所述第二摘要值和所述加密信息以生成设备特征信息。

9.一种用于服务器的设备识别装置，其特征在于，所述装置包括：

请求接收单元，配置用于接收终端设备发来的设备识别请求，所述设备识别请求包括所述终端设备的当前用户的当前用户标识；

获取单元，配置用于获取预置的非对称密钥对中的公钥作为第一公钥；

发送单元，配置用于将所述第一公钥和随机生成的第一随机数发送到所述终端设备；

信息接收单元，配置用于接收所述终端设备发来的设备特征信息，其中，所述设备特征信息是所述终端设备根据所述当前用户标识、所述第一公钥、所述第一随机数以及所述终端设备的设备标识生成的；

识别单元，配置用于根据所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备。

10.根据权利要求9所述的装置，其特征在于，所述设备识别请求还包括识别类型标识符，所述识别类型标识符用于指示所述终端设备在所述服务器中的设备识别类型；以及

所述识别单元进一步配置用于：

根据所述终端设备的设备识别类型、所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备。

11.根据权利要求9所述的装置，其特征在于，所述识别单元包括：

解析模块，配置用于解析所述设备特征信息以得到用户标识和随机数；

确定模块，配置用于确定解析所得到的用户标识是否与所述当前用户标识相同以及解析所得到的随机数是否与所述第一随机数相同；

生成模块，配置用于响应于确定解析所得到的用户标识与所述当前用户标识不相同和/或解析所得到的随机数与所述第一随机数不相同，生成用于指示所述设备识别请求识别失败的识别结果。

12.根据权利要求11所述的装置，其特征在于，所述解析模块进一步配置用于：

使用预设非对称解密算法和所述预置的非对称密钥对中的私钥，解析所述设备特征信息，以得到用户标识、随机数和设备标识。

13.根据权利要求11或12所述的装置，其特征在于，所述识别单元还包括：

识别模块，配置用于响应于确定解析所得到的用户标识与所述当前用户标识相同且解析所得到的随机数与所述第一随机数相同，根据所述当前用户标识、所述第一随机数和解析所得到的设备标识识别所述终端设备。

14.一种用于终端设备的设备识别装置，其特征在于，所述装置包括：

请求发送单元，配置用于向服务器发送设备识别请求，所述设备识别请求包括所述终端设备的当前用户的当前用户标识；

接收单元，配置用于接收所述服务器发来的第一公钥和第一随机数，其中，所述第一公钥是所述服务器从预置的非对称密钥对中获取的公钥，所述第一随机数是由所述服务器随机生成的；

获取单元，配置用于获取所述终端设备的设备标识；

信息生成单元，配置用于根据所述当前用户标识、所述第一公钥、所述第一随机数以及所述设备标识生成设备特征信息；

信息发送单元，配置用于将所述设备特征信息发送给所述服务器，以使所述服务器根据所述当前用户标识、所述第一随机数和所述设备特征信息识别所述终端设备。

15.根据权利要求14所述的装置，其特征在于，所述设备识别请求还包括识别类型标识符，所述识别类型标识符用于指示所述终端设备在所述服务器中的设备识别类型；以及

所述信息生成单元进一步配置用于：

根据所述终端设备的设备识别类型、所述当前用户标识、所述第一公钥、所述第一随机数以及所述设备标识生成设备特征信息。

16.根据权利要求15所述的装置，其特征在于，所述信息生成单元包括：

第一计算模块，配置用于根据所述终端设备的设备识别类型、所述第一公钥和所述设备标识，利用预设消息摘要算法计算得到第一摘要值；

第二计算模块，配置用于利用所述预设消息摘要算法计算所述第一摘要值与所述第一随机数的第二摘要值；

加密模块，配置用于利用预设非对称加密算法，使用所述第一公钥对所述第一摘要值、所述当前用户标识和所述第一随机数进行加密以得到加密信息；

组合模块，配置用于组合所述当前用户标识、所述第二摘要值和所述加密信息以生成设备特征信息。

17.一种设备识别系统，其特征在于，所述系统包括终端设备和服务器，所述服务器包括如权利要求9-13中任一所述的装置和所述终端设备包括如权利要求14-16中任一所述的装置。

设备识别的方法、装置和系统

技术领域

[0001] 本申请涉及计算机技术领域，具体涉及互联网技术领域，尤其涉及设备识别的方法、装置和系统。

背景技术

[0002] 设备生成设备特征发送给服务器，服务器使用接收到的设备特征和相关用户信息进行设备识别。目前，主流的设备识别方法大多基于简单的硬件/软件环境特征在设备端生成设备标识，然后通过在服务器端记录这些设备标识来对设备进行识别。

[0003] 然而，目前的设备识别方法存在以下缺陷：首先，攻击者可以劫持网络报文或是系统调用，窃取网络上或操作系统中的设备标识，从而可以伪造用户身份，给设备的用户带来损失；其次，这些方法没有加入设备中安装的应用的特征，每个应用采集到的设备标识均一致，有信息泄露的风险。

发明内容

[0004] 本申请的目的在于提出一种改进的设备识别的方法、装置和系统，来解决以上背景技术部分提到的技术问题。

[0005] 第一方面，本申请提供了一种用于服务器的设备识别方法，上述方法包括：接收终端设备发来的设备识别请求，上述设备识别请求包括上述终端设备的当前用户的当前用户标识；获取预置的非对称密钥对中的公钥作为第一公钥；将上述第一公钥和随机生成的第一随机数发送到上述终端设备；接收上述终端设备发来的设备特征信息，其中，上述设备特征信息是上述终端设备根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述终端设备的设备标识生成的；根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0006] 在一些实施例中，上述设备识别请求还包括识别类型标识符，上述识别类型标识符用于指示上述终端设备在上述服务器中的设备识别类型；以及上述根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备，包括：根据上述终端设备的设备识别类型、上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0007] 在一些实施例中，上述根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备，包括：解析上述设备特征信息以得到用户标识和随机数；确定解析所得到的用户标识是否与上述当前用户标识相同以及解析所得到的随机数是否与上述第一随机数相同；响应于确定解析所得到的用户标识与上述当前用户标识不相同和/或解析所得到的随机数与上述第一随机数不相同，生成用于指示上述设备识别请求识别失败的识别结果。

[0008] 在一些实施例中，上述解析上述设备特征信息以得到用户标识和随机数，包括：使用预设非对称解密算法和上述预置的非对称密钥对中的私钥，解析上述设备特征信息，以得到用户标识、随机数和设备标识。

[0009] 在一些实施例中，上述根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备，还包括：响应于确定解析所得到的用户标识与上述当前用户标识相同且解析所得到的随机数与上述第一随机数相同，根据上述当前用户标识、上述第一随机数和解析所得到的设备标识识别上述终端设备。

[0010] 第二方面，本申请提供了一种用于终端设备的设备识别方法，上述方法包括：向服务器发送设备识别请求，上述设备识别请求包括上述终端设备的当前用户的当前用户标识；接收上述服务器发来的第一公钥和第一随机数，其中，上述第一公钥是上述服务器从预置的非对称密钥对中获取的公钥，上述第一随机数是由上述服务器随机生成的；获取上述终端设备的设备标识；根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息；将上述设备特征信息发送给上述服务器，以使上述服务器根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0011] 在一些实施例中，上述设备识别请求还包括识别类型标识符，上述识别类型标识符用于指示上述终端设备在上述服务器中的设备识别类型；以及上述根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息，包括：根据上述终端设备的设备识别类型、上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息。

[0012] 在一些实施例中，上述根据上述终端设备的设备识别类型、上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息，包括：根据上述终端设备的设备识别类型、上述第一公钥和上述设备标识，利用预设消息摘要算法计算得到第一摘要值；利用上述预设消息摘要算法计算上述第一摘要值与上述第一随机数的第二摘要值；利用预设非对称加密算法，使用上述第一公钥对上述第一摘要值、上述当前用户标识和上述第一随机数进行加密以得到加密信息；组合上述当前用户标识、上述第二摘要值和上述加密信息以生成设备特征信息。

[0013] 第三方面，本申请提供了一种用于服务器的设备识别装置，上述装置包括：请求接收单元，配置用于接收终端设备发来的设备识别请求，上述设备识别请求包括上述终端设备的当前用户的当前用户标识；第一获取单元，配置用于获取预置的非对称密钥对中的公钥作为第一公钥；第一发送单元，配置用于将上述第一公钥和随机生成的第一随机数发送到上述终端设备；信息接收单元，配置用于接收上述终端设备发来的设备特征信息，其中，上述设备特征信息是上述终端设备根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述终端设备的设备标识生成的；识别单元，配置用于根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0014] 在一些实施例中，上述设备识别请求还包括识别类型标识符，上述识别类型标识符用于指示上述终端设备在上述服务器中的设备识别类型；以及上述识别单元进一步配置用于：根据上述终端设备的设备识别类型、上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0015] 在一些实施例中，上述识别单元包括：解析模块，配置用于解析上述设备特征信息以得到用户标识和随机数；确定模块，配置用于确定解析所得到的用户标识是否与上述当前用户标识相同以及解析所得到的随机数是否与上述第一随机数相同；生成模块，配置用于响应于确定解析所得到的用户标识与上述当前用户标识不相同和/或解析所得到的随机

数与上述第一随机数不相同，生成用于指示上述设备识别请求识别失败的识别结果。

[0016] 在一些实施例中，上述解析模块进一步配置用于：使用预设非对称解密算法和上述预置的非对称密钥对中的私钥，解析上述设备特征信息，以得到用户标识、随机数和设备标识。

[0017] 在一些实施例中，上述识别单元还包括：识别模块，配置用于响应于确定解析所得到的用户标识与上述当前用户标识相同且解析所得到的随机数与上述第一随机数相同，根据上述当前用户标识、上述第一随机数和解析所得到的设备标识识别上述终端设备。

[0018] 第四方面，本申请提供了一种用于终端设备的设备识别装置，上述装置包括：第二发送单元，配置用于向服务器发送设备识别请求，上述设备识别请求包括上述终端设备的当前用户的当前用户标识；接收单元，配置用于接收上述服务器发来的第一公钥和第一随机数，其中，上述第一公钥是上述服务器从预置的非对称密钥对中获取的公钥，上述第一随机数是由上述服务器随机生成的；第二获取单元，配置用于获取上述终端设备的设备标识；信息生成单元，配置用于根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息；信息发送单元，配置用于将上述设备特征信息发送给上述服务器，以使上述服务器根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0019] 在一些实施例中，上述设备识别请求还包括识别类型标识符，上述识别类型标识符用于指示上述终端设备在上述服务器中的设备识别类型；以及上述信息生成单元进一步配置用于：根据上述终端设备的设备识别类型、上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息。

[0020] 在一些实施例中，上述信息生成单元包括：第一计算单元，配置用于根据上述终端设备的设备识别类型、上述第一公钥和上述设备标识，利用预设消息摘要算法计算得到第一摘要值；第二计算单元，配置用于利用上述预设消息摘要算法计算上述第一摘要值与上述第一随机数的第二摘要值；加密单元，配置用于利用预设非对称加密算法，使用上述第一公钥对上述第一摘要值、上述当前用户标识和上述第一随机数进行加密以得到加密信息；组合单元，配置用于组合上述当前用户标识、上述第二摘要值和上述加密信息以生成设备特征信息。

[0021] 第五方面，本申请提供了一种设备识别系统，上述系统包括终端设备和服务器，所述服务器包括如上述第三方面任一实现方式描述的用于服务器的设备识别装置，所述终端设备包括如上述第四方面任一实现方式描述的用于终端设备的设备识别装置。

[0022] 本申请提供的用于服务器的设备识别方法和装置通过接收终端设备发来的包括上述终端设备的当前用户的用户标识的设备识别请求；然后，获取预置的非对称密钥对中的公钥作为第一公钥；再，将第一公钥和随机生成的随机数发送到上述终端设备；接着，接收终端设备发来的设备特征信息，其中，上述设备特征信息是终端设备根据上述用户标识、上述随机数、上述第一公钥以及上述终端设备的设备标识而生成的；最后，根据上述设备特征信息识别上述终端设备。在设备识别的过程中使用了当前用户标识、预置非对称密钥对中的公钥、服务器生成的随机数以及终端设备的设备标识，从而增加了攻击者截取终端设备设备特征信息的难度，继而提高了终端设备访问服务器的安全性。

附图说明

[0023] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0024] 图1是本申请可以应用于其中的示例性系统架构图；

[0025] 图2a、图2b、图2c和图2d是根据本申请的用于服务器的设备识别方法的一个实施例的流程图；

[0026] 图3是根据本申请的用于服务器的设备识别方法的又一个实施例的流程图；

[0027] 图4是根据本申请的用于终端设备的设备识别方法的一个实施例的流程图；

[0028] 图5是根据本申请的用于服务器的设备识别装置的一个实施例的结构示意图；

[0029] 图6是根据本申请的用于终端设备的设备识别装置的又一个实施例的结构示意图；

[0030] 图7是根据本申请的设备识别系统的一个实施例的时序图；

[0031] 图8是适于用来实现本申请实施例的终端设备或服务器的计算机系统的结构示意图。

具体实施方式

[0032] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。

[0033] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0034] 图1示出了可以应用本申请的用于服务器的终端设备识别方法或用于服务器的终端设备识别装置以及用于识别终端设备的方法或用于识别终端设备的装置的实施例的示例性系统架构100。

[0035] 如图1所示，系统架构100可以包括终端设备101、102、103，网络104和服务器105。网络104用以在终端设备101、102、103和服务器105之间提供通信链路的介质。网络104可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0036] 用户可以使用终端设备101、102、103通过网络104与服务器105交互，以接收或发送消息等。终端设备101、102、103上可以安装有各种客户端应用，例如用于识别终端设备的应用、网页浏览器应用、购物类应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件等。终端设备可以向服务器发起设备识别请求，并在接收到服务器发来的第一公钥和第一随机数后生成设备识别信息，再将设备识别信息发送给服务器。

[0037] 终端设备101、102、103可以是具有显示屏的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

[0038] 服务器105可以是提供各种服务的服务器，例如对终端设备101、102、103上安装的用于服务器的终端设备识别的应用提供支持的后台服务器。后台服务器可以对接收到的设备识别请求等数据进行分析等处理，并将处理结果(例如第一公钥和第一随机数)反馈给终端设备。

[0039] 需要说明的是，本申请实施例所提供的用于服务器的设备识别方法一般由服务器105执行，相应地，用于服务器的设备识别装置一般设置服务器105中。本申请实施例所提供的用于终端设备的设备识别方法一般由终端设备101、102、103执行，相应地，用于终端设备的设备识别装置一般设置于终端设备101、102、103中。

[0040] 应该理解，图1中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0041] 继续参考图2a，其示出了根据本申请的用于服务器的终端设备识别方法的一个实施例的流程200。本实施例的用于服务器的终端设备识别方法，包括以下步骤：

[0042] 步骤201，接收终端设备发来的设备识别请求。

[0043] 在本实施例中，用于服务器的终端设备识别方法运行于其上的电子设备(例如图1所示的服务器)可以通过有线连接方式或者无线连接方式从终端设备接收设备识别请求，其中，上述设备识别请求包括上述终端设备的当前用户的当前用户标识。这里，终端设备的当前用户标识可以是已登录用户的用户标识，也可以是输入了用户名但还未登录的用户的用户标识。

[0044] 在本实施例的一些可选的实现方式中，如果终端设备的当前用户标识是已登录用户的用户标识，则上述设备识别请求中可以包括终端设备与上述电子设备之间交互的会话(Session)标识，而上述会话标识中包括了当前用户标识。

[0045] 在本实施例的一些可选的实现方式中，如果终端设备的当前用户标识是未登录用户的用户标识，则上述设备识别请求中可以直接包括上述当前用户标识。

[0046] 需要指出的是，上述无线连接方式可以包括但不限于3G/4G连接、WiFi连接、蓝牙连接、WiMAX连接、Zigbee连接、UWB(ultra wideband)连接、以及其他现在已知或将来开发的无线连接方式。

[0047] 步骤202，获取预置的非对称密钥对中的公钥作为第一公钥。

[0048] 在本实施例中，上述电子设备(例如图1所示的服务器)可以预置有非对称密钥对，这样，上述电子设备可以本地获取上述预置非对称密钥对中的公钥作为第一公钥。

[0049] 在本实施例的一些可选的实现方式中，上述电子设备(例如图1所示的服务器)可以是对终端设备上安装的应用中的指定功能部分(例如，AA支付工具)进行支持的服务器，这样，上述电子设备上预置的非对称密钥对就是针对上述指定功能部分而预设的用于执行非对称加密/解密时用的非对称密钥对。

[0050] 在本实施例的一些可选的实现方式中，上述电子设备(例如图1所示的服务器)也可以是对终端设备上安装的不同应用中的多个功能部分进行支持的服务器，这样，上述电子设备上会预置针对各个功能部分的非对称密钥对，从而上述设备识别请求中也会包括用于区分不同功能部分的标识，以供上述电子设备用于获取与上述用于区分不同功能部分的标识对应的非对称密钥对中的公钥作为第一公钥。

[0051] 步骤203，将第一公钥和随机生成的第一随机数发送到终端设备。

[0052] 在本实施例中，上述电子设备可以在步骤202中获取到第一公钥后，首先采用各种方法随机生成随机数作为第一随机数，然后将上述第一公钥和上述随机数发送到上述终端设备，以供上述终端设备生成设备特征信息。

[0053] 作为示例，随机生成随机数的方法可以采用线性同余法。上述线性同余法生成随

机数的方法是目前广泛研究和应用的公知技术，在此不再赘述。

[0054] 在本实施例的一些可选的实现方式中，上述第一随机数可以是密码学中的Nonce(Number used once或Number once)，即上述随机数可以是一个只被使用一次的任意或非重复的随机数值。Nonce在加密技术中的初始向量和加密散列函数都发挥着重要作用，在各类验证协议的通信应用中确保验证信息不被重复使用以对抗重放攻击(ReplayAttack)。需要说明的是，上述密码学中生成Nonce随机数的方法是目前广泛研究和应用的公知技术，在此不再赘述。

[0055] 步骤204，接收终端设备发来的设备特征信息。

[0056] 在本实施例中，上述电子设备可以接收终端设备发来的设备特征信息，以供后续识别终端设备使用。其中，上述设备特征信息是终端设备根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述终端设备的设备标识生成的。

[0057] 步骤205，根据当前用户标识、第一随机数和设备特征信息识别终端设备。

[0058] 在本实施例中，上述电子设备可以在接收到终端设备发来的设备特征信息后，根据当前用户标识、第一随机数和设备特征信息识别终端设备。

[0059] 在本实施例的一些可选的实现方式中，上述设备识别请求还包括识别类型标识符，其中，识别类型标识符用于指示上述终端设备在上述电子设备(例如图1所示的服务器)中的设备识别类型，这样，上述电子设备就可以根据上述终端设备的设备识别类型、上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0060] 在本实施例的一些可选的实现方式中，识别类型标识符可以是数字形式，例如可以采用数字1表示第一种设备识别类型，采用数字2表示第二种设备识别类型，采用数字3表示第三种设备识别类型；识别类型标识符也可以是字符串，例如采用字符串“FisrtType”表示第一种设备识别类型，采用字符串“SecondType”表示第二种设备识别类型，采用字符串“ThirdType”表示第三种设备识别类型。

[0061] 在本实施例的一些可选的实现方式中，步骤205可以包括如图2b所示的如下子步骤：

[0062] 步骤2051，解析设备特征信息以得到用户标识、随机设备特征值和加密信息，将解析所得到的用户标识作为第一用户标识。

[0063] 在本实施例中，上述电子设备可以解析步骤204中接收到的设备特征信息以得到用户标识、随机设备特征值和加密信息，并将解析所得到的用户标识作为第一用户标识。这里，可以按照上述电子设备与终端设备之间约定的生成设备特征信息的方法设置解析设备特征信息的方法。例如，当生成设备特征信息时是按照用户标识、随机设备特征值和加密信息的从前到后的顺序生成的，则解析设备特征信息的时候也是按照用户标识、随机设备特征值和加密信息的从前到后的顺序进行解析。

[0064] 步骤2052，根据终端设备的设备识别类型，确定与第一用户标识对应的历史设备特征值列表。

[0065] 在本实施例中，上述电子设备可以根据设备识别类型，确定与第一用户标识对应的历史设备特征值列表。

[0066] 在本实施例的一些可选的实现方式中，终端设备的设备识别类型可以是以下任意一项：第一类型、第二类型和第三类型，这样步骤2052可以包括如图2c所示的如下子步骤：

[0067] 步骤20521，判断设备识别类型是否是第一类型或第三类型，如果是，转到步骤20522。

[0068] 步骤20522，检测预设的用户标识列表中是否包括第一用户标识，如果是，转到步骤20523，如果否，转到步骤20524。

[0069] 步骤20523，确定与第一用户标识对应的第一历史设备特征值列表作为与第一用户标识对应的历史设备特征值列表。

[0070] 步骤20524，建立与第一用户标识对应的第一历史设备特征值列表，将所建立的第一历史设备特征值列表作为与第一用户标识对应的历史设备特征值列表。

[0071] 在本实施例的一些可选的实现方式中，还可以在步骤20521中判断终端设备的设备识别类型不是第一类型或第三类型的情况下转到如下子步骤20525：

[0072] 步骤20525，进一步判断上述终端设备的设备识别类型是否是第二类型，如果是，转到步骤20526。

[0073] 步骤20526，检测预设的用户标识列表中是否包括第一用户标识，如果是，转到步骤20527，如果否，转到步骤20528。

[0074] 步骤20527，确定与第一用户标识对应的第二历史设备特征值列表作为与第一用户标识对应的历史设备特征值列表。

[0075] 步骤20528，建立与第一用户标识对应的第二历史设备特征值列表，将所建立的第二历史设备特征值列表作为与第一用户标识对应的历史设备特征值列表。

[0076] 步骤2053，根据设备识别类型、历史设备特征值列表中的各历史设备特征值、当前用户标识、第一随机数以及随机设备特征值，识别终端设备。

[0077] 在本实施例中，上述电子设备可以根据设备识别类型、历史设备特征值列表中的各历史设备特征值、当前用户标识、第一随机数以及随机设备特征值，识别终端设备。

[0078] 在本实施例的一些可选的实现方式中，步骤2053还可以包括如图2d所示的如下子步骤：

[0079] 步骤20531，判断设备识别类型是否是第一类型或第二类型，如果是，转到步骤20532。

[0080] 步骤20532，利用预设消息摘要算法，计算各历史设备特征值与第一随机数的各摘要值。

[0081] 步骤20533，检测随机设备特征值是否与各摘要值中的一个相等，如果是，转到步骤20534。

[0082] 步骤20534，生成用于指示设备识别请求识别成功的识别结果。

[0083] 在本实施例的一些可选的实现方式中，还可以在步骤20533中检测随机设备特征值与各摘要值均不相等的情况下转到如下描述的步骤20535：

[0084] 步骤20535，利用预设的非对称解密算法，使用预置的非对称密钥对中的私钥对加密信息进行解密以得到用户标识、随机数和当前设备特征值，并将解密所得到的用户标识作为第二用户标识，将解密所得到的随机数作为第二随机数。

[0085] 步骤20536，分别检测当前用户标识与第二用户标识是否相等以及第一随机数与上述第二随机数是否相等，如果均相等，则转到步骤20537。

[0086] 步骤20537，将解密所得到的当前设备特征值加入历史设备特征值列表，并生成用

于指示设备识别请求识别成功的识别结果。

[0087] 在本实施例的一些可选的实现方式中，还可以在步骤20536中检测到当前用户标识与第二用户标识不相等或者第一随机数与第二随机数不相等的情况下，生成用于指示设备识别请求识别失败的识别结果。

[0088] 进一步参见图3，其示出了根据本申请的用于服务器的终端设备识别方法的又一个实施例的流程300。本实施例的用于服务器的终端设备识别方法，包括以下步骤：

[0089] 步骤301，接收终端设备发来的设备识别请求。

[0090] 步骤302，获取预置的非对称密钥对中的公钥作为第一公钥。

[0091] 步骤303，将第一公钥和随机生成的第一随机数发送到终端设备。

[0092] 步骤304，接收终端设备发来的设备特征信息。

[0093] 上述步骤301、步骤302、步骤303和步骤304的具体处理与图2a所示的流程200中的步骤201、步骤202、步骤203和步骤204的具体处理基本相同，在此不再赘述。

[0094] 步骤305，解析设备特征信息以得到用户标识和随机数。

[0095] 在本实施例中，上述电子设备可以解析设备特征信息以得到用户标识和随机数。这里，可以按照上述电子设备与终端设备之间约定的生成设备特征信息的方法设置解析设备特征信息的方法。

[0096] 在本实施例的一些可选的实现方式中，上述电子设备可以采用预设非对称解密算法和预置的非对称密钥对中的私钥，解析设备特征信息，以得到用户标识、随机数。

[0097] 步骤306，确定解析所得到的用户标识是否与当前用户标识相同以及解析所得到的随机数是否与第一随机数相同，如果是，转到步骤307，如果否，转到步骤308。

[0098] 在本实施例中，上述电子设备可以在步骤305中解析得到用户标识和随机数后，确定解析所得到的用户标识是否与当前用户标识相同以及解析所得到的随机数是否与第一随机数相同。如果确定解析所得到的用户标识与当前用户标识相同而且解析所得到的随机数与第一随机数也相同，则可以继续后续的识别步骤307。如果确定解析所得到的用户标识与当前用户标识不相同和/或解析所得到的随机数与第一随机数不相同，则转到后续的生成识别失败结果的步骤308。

[0099] 步骤307，根据当前用户标识、第一随机数和解析所得到的设备标识识别终端设备。

[0100] 在本实施例中，上述电子设备可以步骤306确定得出解析所得到的用户标识与当前用户标识相同而且解析所得到的随机数与第一随机数也相同的情况下，根据当前用户标识、第一随机数和解析所得到的设备标识识别终端设备。

[0101] 步骤308，生成用于指示设备识别请求识别失败的识别结果。

[0102] 在本实施例中，上述电子设备可以步骤306确定得出解析所得到的用户标识与当前用户标识不相同和/或解析所得到的随机数与第一随机数不相同的情况下，生成用于指示上述设备识别请求识别失败的识别结果。

[0103] 本申请的上述实施例提供的方法通过解析终端设备发出的设备特征信息以得到用户标识和随机数，并基于解析出的用户标识和随机数与当前用户标识和第一随机数的比较结果，识别上述终端设备，提高了服务器设备识别的效率。

[0104] 进一步参考图4，其示出了用于终端设备设备识别方法的一个实施例的流程400。

该用于终端设备的设备识别方法的流程400，包括以下步骤：

[0105] 步骤401，向服务器发送设备识别请求。

[0106] 在本实施例中，用于终端设备的设备识别方法运行于其上的电子设备(如图1中的终端设备101、102、103)可通过有线连接或无线连接的方式向服务器(如图1中的服务器105)发送设备识别请求。其中，设备识别请求包括上述终端设备的当前用户的当前用户标识。

[0107] 需要指出的是，上述无线连接方式可以包括但不限于3G/4G连接、WiFi连接、蓝牙连接、WiMAX连接、Zigbee连接、UWB(ultra wideband)连接、以及其他现在已知或将来开发的无线连接方式。

[0108] 在本实施例的一些可选的实现方式中，可以在检测到用户执行了预设操作集合中的某个操作(例如，用户打开指定应用或者用户使用电子购物应用执行支付操作)时，由终端设备通过后台自动向服务器发出设备识别请求。

[0109] 在本实施例的一些可选的实现方式中，也可以是在服务器向终端设备推送信息时，服务器向设备发出指令，该指令指示终端设备向服务器发送设备识别请求。

[0110] 步骤402，接收服务器发来的第一公钥和第一随机数。

[0111] 在本实施例中，上述电子设备可以接收服务器发来的第一公钥和第一随机数。其中，第一公钥是上述服务器从预置的非对称密钥对中获取的公钥，上述第一随机数是由上述服务器随机生成的。

[0112] 步骤403，获取终端设备的设备标识。

[0113] 在本实施例中，上述电子设备可以在接收到第一公钥和第一随机数后，获取终端设备(即上述电子设备)的设备标识。

[0114] 在本实施例的一些可选的实现方式中，可以使用终端设备的IMEI(International Mobile Equipment Identity，国际移动设备身份码)作为该终端设备的设备标识。

[0115] 在本实施例的一些可选的实现方式中，还可以使用终端设备的硬件参数的组合作为该终端设备的设备标识。

[0116] 在本实施例的一些可选的实现方式中，还可以在终端设备中配置有可以产生唯一设备标识码的硬件设备，并以该可以产生唯一设备标识码的硬件设备生成的唯一设备标识码作为终端设备的设备标识。

[0117] 在本实施例的一些可选的实现方式中，终端设备还可以配置有可信计算环境(例如，采用了TrustZone技术的计算环境)，并在终端设备内设置可以产生唯一设备标识码的硬件设备，并将终端设备的可信计算环境与上述可以产生唯一设备标识码的硬件设备电性连接。这样可以通过终端设备的可信计算环境获取上述可以产生唯一设备标识码的硬件设备生成的设备标识。上述获取的设备标识的方式可以保证设备标识不会被攻击者截取，从而可以提高设备识别的安全性。

[0118] 在本实施例的一些可选的实现方式中，上述设备识别请求还可以包括识别类型标识符，上述识别类型标识符用于指示上述终端设备在上述服务器中的设备识别类型，这样，上述电子设备就可以根据上述终端设备的设备识别类型、上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息。

[0119] 在本实施例的一些可选的实现方式中，上述终端设备的设备识别类型可以是以下

中的任意一项：第一类型、第二类型、第三类型。这样，上述电子设备就可以按照如下步骤获取终端设备的设备标识：

[0120] 首先，上述电子设备可以判断上述终端设备的设备识别类型是否为第三类型；

[0121] 然后，响应于上述终端设备的设备识别类型是第三类型，则重置上述终端设备的设备标识，并获取重置后的设备标识。

[0122] 如果终端设备中配置有可以产生唯一设备标识码的硬件设备，就可以通过向该可以产生唯一设备标识码的硬件设备发送重置指令，以供该可以产生唯一设备标识码的硬件设备生成新的唯一设备标识码作为终端设备重置后的设备标识。

[0123] 步骤404，根据当前用户标识、第一公钥、第一随机数以及设备标识生成设备特征信息。

[0124] 在本实施例中，上述电子设备可以在获取到设备标识后，根据当前用户标识、第一公钥、第一随机数以及设备标识生成设备特征信息。

[0125] 在本实施例的一些可选的实现方式中，上述设备识别请求还可以包括识别类型标识符，上述识别类型标识符用于指示上述终端设备在上述服务器中的设备识别类型，这样，上述电子设备就可以根据上述终端设备的设备识别类型、上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息。

[0126] 在本实施例的一些可选的实现方式中，上述电子设备根据上述终端设备的设备识别类型、上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息，可以包括如下步骤：

[0127] 首先，根据上述终端设备的设备识别类型、上述第一公钥和上述设备标识，利用预设消息摘要算法计算得到第一摘要值；

[0128] 然后，利用上述预设消息摘要算法计算上述第一摘要值与上述第一随机数的第二摘要值；

[0129] 为了区分第一摘要值和第二摘要值，在本申请中将第一摘要值也称为设备特征值，将第二摘要值也称为随机设备特征值。

[0130] 接着，利用预设非对称加密算法，使用上述第一公钥对上述第一摘要值、上述当前用户标识和上述第一随机数进行加密以得到加密信息；

[0131] 最后，组合上述当前用户标识、上述第二摘要值和上述加密信息以生成设备特征信息。

[0132] 在本实施例的一些可选的实现方式中，上述电子设备根据上述终端设备的设备识别类型、上述第一公钥和上述设备标识，利用预设消息摘要算法计算得到第一摘要值，可以包括如下步骤：

[0133] 首先，判断上述终端设备的设备识别类型是否为第一类型或第三类型。

[0134] 接着，响应于上述终端设备的设备识别类型是第一类型或第三类型，则利用上述预设消息摘要算法计算上述设备标识与上述第一公钥的第一摘要值，并将计算所得的第一摘要值作为设备特征值。

[0135] 然后，响应于上述终端设备的设备识别类型不是第一类型或第三类型，进一步判断上述终端设备的设备识别类型是否为第二类型。

[0136] 最后，响应于上述终端设备的设备识别类型是第二类型，则：获取预设的第二公

钥;利用上述预设消息摘要算法计算上述设备标识、上述第一公钥和上述第二公钥的摘要值,并将计算所得的摘要值作为设备特征值。

[0137] 在本实施例的一些可选的实现方式中,上述预设的第一公钥可以是上述服务器针对其所支持的服务的不同而设置的不同的公钥。上述预设的第二公钥可以是上述电子设备中针对上述电子设备上安装的不同应用而设置的不同的公钥。这样,当设备识别请求中的识别类型标识符所指示的终端设备的设备识别是第一类型时,使用设备标识和第一公钥而生成设备特征值可以针对同一个终端设备上安装的不同应用中的相同服务生成相同的设备特征值,针对同一个终端设备上安装的相同应用中的不同服务生成不同的设备特征值;当设备识别请求中的识别类型标识符所指示的终端设备的设备识别是第二类型时,使用设备标识、第一公钥和第二公钥而生成的设备特征值可以针对同一个终端设备上安装的不同应用上的相同服务生成不同的设备特征值,针对同一个终端设备上安装的相同应用上的不同服务也生成不同的设备特征值,以适合不同的设备特征识别的需求。

[0138] 步骤405,将设备特征信息发送给服务器。

[0139] 在本实施例中,上述电子设备可以在生成设备特征信息后,将设备特征信息发送给服务器,以使服务器根据当前用户标识、第一随机数和设备特征信息识别终端设备。

[0140] 本申请的上述实施例提供的方法通过向服务器发送设备识别请求,并根据当前用户标识、从服务器接收的第一公钥和第一随机数以及设备标识生成设备特征信息,再将所生成的设备特征信息发送给服务器,从而可以服务器根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备,实现了基于当前用户标识、第一公钥、第一随机数以及设备标识生成设备特征信息,提高了终端设备访问服务器的安全性。

[0141] 进一步参考图5,作为对上述各图所示方法的实现,本申请提供了一种用于服务器的设备识别装置的一个实施例,该装置实施例与图2所示的方法实施例相对应,该装置具体可以应用于各种电子设备中。

[0142] 如图5所示,本实施例上述的用于服务器的设备识别装置500包括:请求接收单元501、获取单元502、发送单元503、信息接收单元504和识别单元505。其中,请求接收单元501,配置用于接收终端设备发来的设备识别请求,上述设备识别请求包括上述终端设备的当前用户的当前用户标识;获取单元502,配置用于获取预置的非对称密钥对中的公钥作为第一公钥;发送单元503,配置用于将上述第一公钥和随机生成的第一随机数发送到上述终端设备;信息接收单元504,配置用于接收上述终端设备发来的设备特征信息,其中,上述设备特征信息是上述终端设备根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述终端设备的设备标识生成的;识别单元505,配置用于根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0143] 在本实施例中,用于服务器的设备识别装置500的请求接收单元501、获取单元502、发送单元503、信息接收单元504和识别单元505的具体处理可分别参考图2对应实施例中步骤201、步骤202、步骤203、步骤204和步骤205的相关说明,在此不再赘述。

[0144] 在本实施例的一些可选的实现方式中,上述设备识别请求还可以包括识别类型标识符,上述识别类型标识符用于指示上述终端设备在上述服务器中的设备识别类型;以及上述识别单元505可以进一步配置用于:根据上述终端设备的设备识别类型、上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0145] 在本实施例的一些可选的实现方式中，上述识别单元505可以包括：解析模块(未示出)，配置用于解析上述设备特征信息以得到用户标识和随机数；确定模块，配置用于确定解析所得到的用户标识是否与上述当前用户标识相同以及解析所得到的随机数是否与上述第一随机数相同；生成模块(未示出)，配置用于响应于确定解析所得到的用户标识与上述当前用户标识不相同和/或解析所得到的随机数与上述第一随机数不相同，生成用于指示上述设备识别请求识别失败的识别结果。

[0146] 在本实施例的一些可选的实现方式中，上述解析模块可以进一步配置用于：使用预设非对称解密算法和上述预置的非对称密钥对中的私钥，解析上述设备特征信息，以得到用户标识、随机数和设备标识。

[0147] 在本实施例的一些可选的实现方式中，上述识别单元505还可以包括：识别模块(未示出)，配置用于响应于确定解析所得到的用户标识与上述当前用户标识相同且解析所得到的随机数与上述第一随机数相同，根据上述当前用户标识、上述第一随机数和解析所得到的设备标识识别上述终端设备。

[0148] 进一步参考图6，作为对上述各图所示方法的实现，本申请提供了一种用于终端设备的设备识别装置的一个实施例，该装置实施例与图4所示的方法实施例相对应，该装置具体可以应用于各种电子设备中。

[0149] 如图6所示，本实施例描述的用于终端设备的设备识别装置600包括：请求发送单元601、接收单元602、获取单元603、信息生成单元604和信息发送单元605。其中，请求发送单元601，配置用于向服务器发送设备识别请求，上述设备识别请求包括上述终端设备的当前用户的当前用户标识；接收单元602，配置用于接收上述服务器发来的第一公钥和第一随机数，其中，上述第一公钥是上述服务器从预置的非对称密钥对中获取的公钥，上述第一随机数是由上述服务器随机生成的；获取单元603，配置用于获取上述终端设备的设备标识；信息生成单元604，配置用于根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息；信息发送单元605，配置用于将上述设备特征信息发送给上述服务器，以使上述服务器根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0150] 本实施例的一些可选的实现方式中，上述设备识别请求还包括识别类型标识符，上述识别类型标识符用于指示上述终端设备在上述服务器中的设备识别类型；以及上述信息生成单元604可以进一步配置用于：根据上述终端设备的设备识别类型、上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息。

[0151] 本实施例的一些可选的实现方式中，上述信息生成单元604可以包括：第一计算模块(未示出)，配置用于根据上述终端设备的设备识别类型、上述第一公钥和上述设备标识，利用预设消息摘要算法计算得到第一摘要值；第二计算模块(未示出)，配置用于利用上述预设消息摘要算法计算上述第一摘要值与上述第一随机数的第二摘要值；加密模块(未示出)，配置用于利用预设非对称加密算法，使用上述第一公钥对上述第一摘要值、上述当前用户标识和上述第一随机数进行加密以得到加密信息；组合模块(未示出)，配置用于组合上述当前用户标识、上述第二摘要值和上述加密信息以生成设备特征信息。

[0152] 下面参考图7，其示出了根据本申请的设备识别系统的一个实施例的时序700。如图7所示，本实施例的设备识别系统，包括：终端设备和服务器。其中，服务器中可以包括如

图5所示的用于服务器的设备识别装置500，终端设备中可以包括如图6所示的用于终端设备的设备识别装置600。

[0153] 本实施例的终端设备和服务器之间时序的主要过程是：上述终端设备向服务器发送设备识别请求；服务器响应于接收到上述终端设备发来的设备识别请求，获取预置的非对称密钥对中的公钥作为第一公钥，然后将上述第一公钥和随机生成的第一随机数发送到上述终端设备；终端设备响应于接收到上述服务器发来的第一公钥和第一随机数，首先获取上述终端设备的设备标识，然后根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息，将上述设备特征信息发送给上述服务器；上述服务器，首先接收上述终端设备发来的设备特征信息，然后根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。具体地：

[0154] 在步骤701中，终端设备向服务器发送设备识别请求。

[0155] 在本实施例中，步骤701的具体操作可以参看图4所示的实施例中的相关说明，在此不再赘述。

[0156] 在步骤702中，服务器响应于接收到上述终端设备发来的设备识别请求，获取预置的非对称密钥对中的公钥作为第一公钥。

[0157] 在本实施例中，步骤702的具体操作可以参看图2所示的实施例的相关说明，在此不再赘述。

[0158] 在步骤703中，服务器将上述第一公钥和随机生成的第一随机数发送到上述终端设备。

[0159] 在本实施例中，步骤703的具体操作可以参看图2所示的实施例中的相关说明，在此不再赘述。

[0160] 在步骤704中，终端设备根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息，将上述设备特征信息发送给上述服务器。

[0161] 在本实施例中，步骤704的具体操作可以参看图4所示的实施例的相关说明，在此不再赘述。

[0162] 在步骤705中，终端设备将设备特征信息发送给上述服务器。

[0163] 在本实施例中，步骤705的具体操作可以参看图4所示的实施例的相关说明，在此不再赘述。

[0164] 在步骤706中，服务器根据当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0165] 在本实施例中，步骤706的具体操作可以参看图2所示的实施例和图3所示的实施例中的相关说明，在此不再赘述。

[0166] 本实施例提供的设备识别系统通过由服务器响应于接收到终端设备发来的设备识别请求，预置的非对称密钥对中的公钥和随机生成的随机数发送到上述终端设备，再由终端设备生成用于识别终端设备的设备识别信息并发送给服务器，以供服务器对终端设备进行识别，从而提高了终端设备访问服务器的安全性。

[0167] 下面参考图8，其示出了适于用来实现本申请实施例的终端设备或服务器的计算机系统800的结构示意图。

[0168] 如图8所示，计算机系统800包括中央处理单元(CPU，Central Processing Unit)

801，其可以根据存储在只读存储器(ROM，Read Only Memory)802中的程序或者从存储部分808加载到随机访问存储器(RAM，Random Access Memory)803中的程序而执行各种适当的动作和处理。在RAM 803中，还存储有系统800操作所需的各种程序和数据。CPU 801、ROM802以及RAM 803通过总线804彼此相连。输入/输出(I/O)接口805也连接至总线804。

[0169] 以下部件连接至I/O接口805：包括键盘、鼠标、触摸屏等的输入部分806；包括诸如阴极射线管(CRT)、液晶显示器(LCD)、触摸屏等以及扬声器等的输出部分807；包括硬盘等的存储部分808；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分809。通信部分809经由诸如因特网的网络执行通信处理。驱动器810也根据需要连接至I/O接口805。可拆卸介质811，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器810上，以便于从其上读出的计算机程序根据需要被安装入存储部分808。

[0170] 特别地，根据本公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括有形地包含在机器可读介质上的计算机程序，上述计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分809从网络上被下载和安装，和/或从可拆卸介质811被安装。在该计算机程序被中央处理单元(CPU)801执行时，执行本申请的方法中限定的上述功能。

[0171] 附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0172] 描述于本申请实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中，例如，可以描述为：一种处理器包括请求接收单元、获取单元、发送单元、信息接收单元和识别单元。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定，例如，识别单元还可以被描述为“识别设备的单元”。

[0173] 作为另一方面，本申请还提供了一种非易失性计算机存储介质，该非易失性计算机存储介质可以是上述实施例中上述装置中所包含的非易失性计算机存储介质；也可以是单独存在，未装配入终端中的非易失性计算机存储介质。上述非易失性计算机存储介质存储有一个或者多个程序，当上述一个或者多个程序被一个设备执行时，使得上述设备：接收终端设备发来的设备识别请求，上述设备识别请求包括上述终端设备的当前用户的当前用户标识；获取预置的非对称密钥对中的公钥作为第一公钥；将上述第一公钥和随机生成的第一随机数发送到上述终端设备；接收上述终端设备发来的设备特征信息，其中，上述设备特征信息是上述终端设备根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述终端设备的设备标识生成的；根据上述当前用户标识、上述第一随机数和上述设备特征

信息识别上述终端设备。

[0174] 作为又一方面，本申请还提供了一种非易失性计算机存储介质，该非易失性计算机存储介质可以是上述实施例中上述装置中所包含的非易失性计算机存储介质；也可以是单独存在，未装配入终端中的非易失性计算机存储介质。上述非易失性计算机存储介质存储有一个或者多个程序，当上述一个或者多个程序被一个设备执行时，使得上述设备：向服务器发送设备识别请求，上述设备识别请求包括上述终端设备的当前用户的当前用户标识；接收上述服务器发来的第一公钥和第一随机数，其中，上述第一公钥是上述服务器从预置的非对称密钥对中获取的公钥，上述第一随机数是由上述服务器随机生成的；获取上述终端设备的设备标识；根据上述当前用户标识、上述第一公钥、上述第一随机数以及上述设备标识生成设备特征信息；将上述设备特征信息发送给上述服务器，以使上述服务器根据上述当前用户标识、上述第一随机数和上述设备特征信息识别上述终端设备。

[0175] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本申请中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离上述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

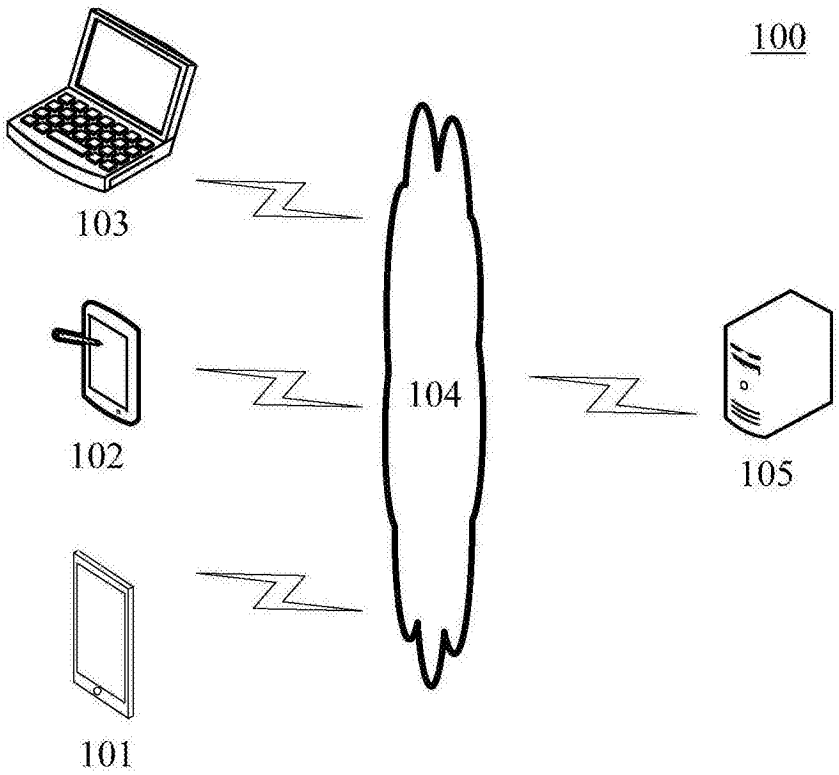

100
103
102
101
104
105

图1

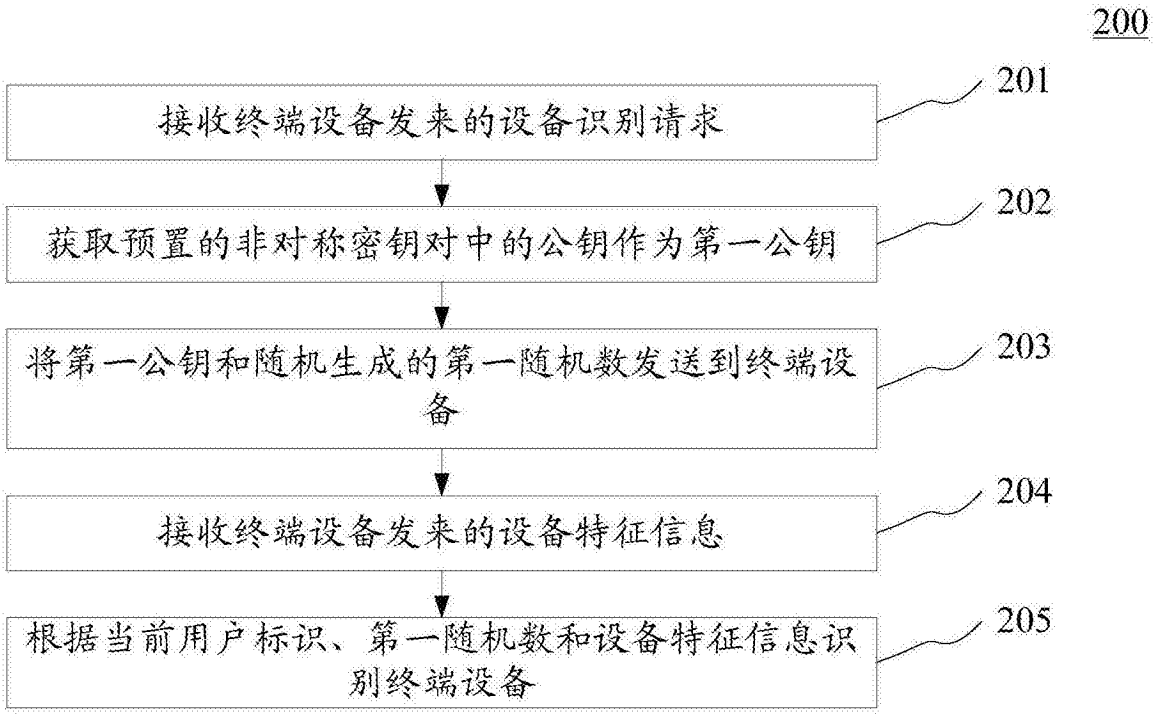

200
接收终端设备发来的设备识别请求
201
获取预置的非对称密钥对中的公钥作为第一公钥
202
将第一公钥和随机生成的第一随机数发送到终端设备
203
接收终端设备发来的设备特征信息
204
根据当前用户标识、第一随机数和设备特征信息识别终端设备
205

图2a

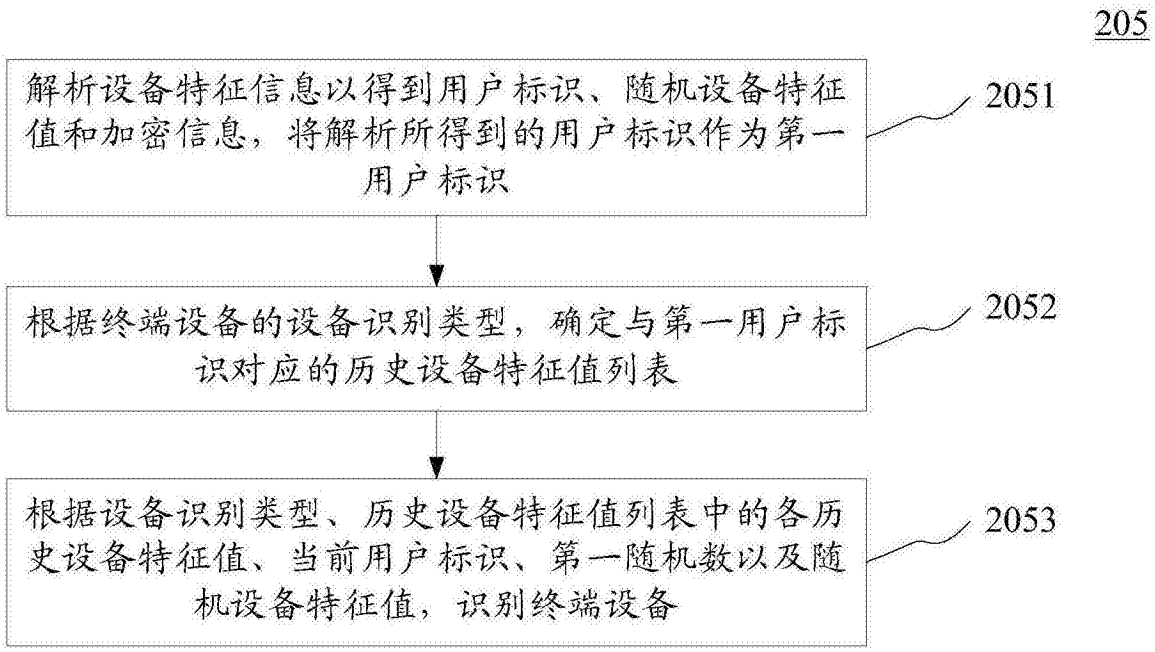

205
解析设备特征信息以得到用户标识、随机设备特征值和加密信息，将解析所得到的用户标识作为第一用户标识
2051
根据终端设备的设备识别类型，确定与第一用户标识对应的历史设备特征值列表
2052
根据设备识别类型、历史设备特征值列表中的各历史设备特征值、当前用户标识、第一随机数以及随机设备特征值，识别终端设备
2053

图2b

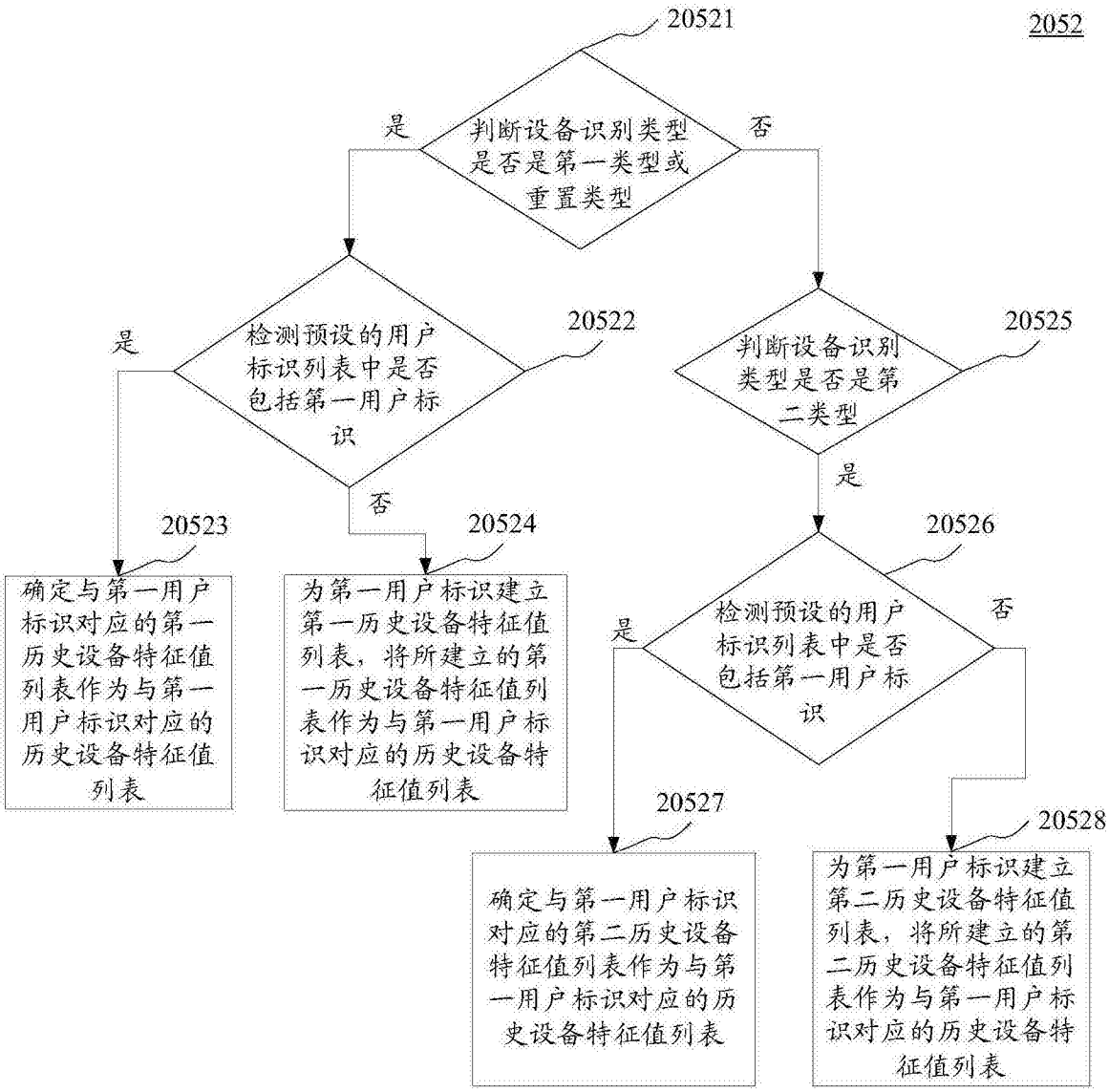

2052
20521
判断设备识别类型是否是第一类型或重置类型
是
否
检测预设的用户标识列表中是否包括第一用户标识
20522
是
否
20523
确定与第一用户标识对应的第一历史设备特征值列表作为与第一用户标识对应的历史设备特征值列表
20524
为第一用户标识建立第一历史设备特征值列表，将所建立的第一历史设备特征值列表作为与第一用户标识对应的历史设备特征值列表
判断设备识别类型是否是第二类型
20525
是
20526
检测预设的用户标识列表中是否包括第一用户标识
是
否
20527
确定与第一用户标识对应的第二历史设备特征值列表作为与第一用户标识对应的历史设备特征值列表
20528
为第一用户标识建立第二历史设备特征值列表，将所建立的第二历史设备特征值列表作为与第一用户标识对应的历史设备特征值列表

图2c

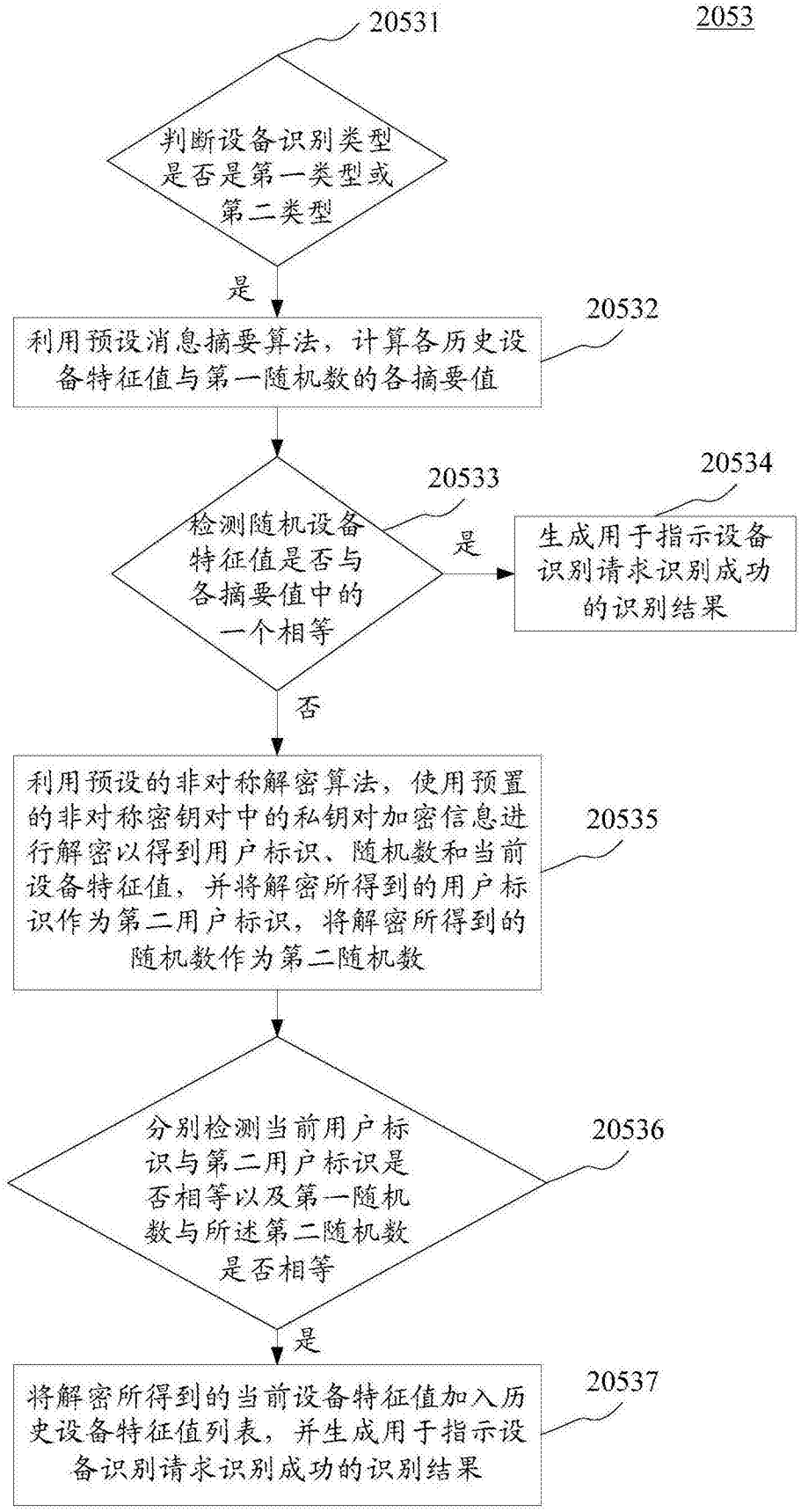

2053
20531
判断设备识别类型是否是第一类型或第二类型
是
20532
利用预设消息摘要算法，计算各历史设备特征值与第一随机数的各摘要值
20533
检测随机设备特征值是否与各摘要值中的一个相等
是
20534
生成用于指示设备识别请求识别成功的识别结果
否
利用预设的非对称解密算法，使用预置的非对称密钥对中的私钥对加密信息进行解密以得到用户标识、随机数和当前设备特征值，并将解密所得到的用户标识作为第二用户标识，将解密所得到的随机数作为第二随机数
20535
分别检测当前用户标识与第二用户标识是否相等以及第一随机数与所述第二随机数是否相等
20536
是
将解密所得到的当前设备特征值加入历史设备特征值列表，并生成用于指示设备识别请求识别成功的识别结果
20537

图2d

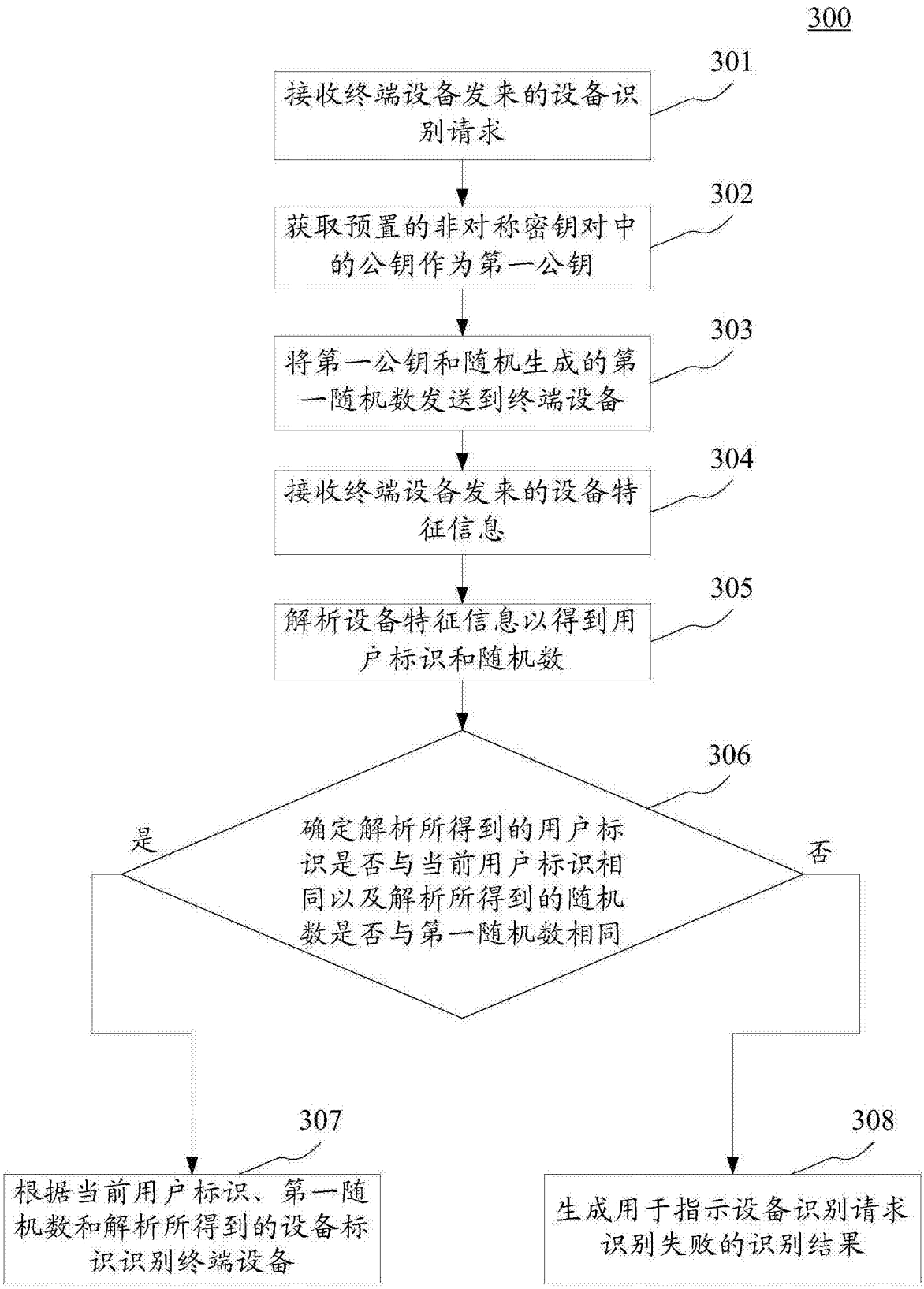

300
301
接收终端设备发来的设备识别请求
302
获取预置的非对称密钥对中的公钥作为第一公钥
303
将第一公钥和随机生成的第一随机数发送到终端设备
304
接收终端设备发来的设备特征信息
305
解析设备特征信息以得到用户标识和随机数
306
确定解析所得到的用户标识是否与当前用户标识相同以及解析所得到的随机数是否与第一随机数相同
是
否
307
根据当前用户标识、第一随机数和解析所得到的设备标识识别终端设备
308
生成用于指示设备识别请求识别失败的识别结果

图3

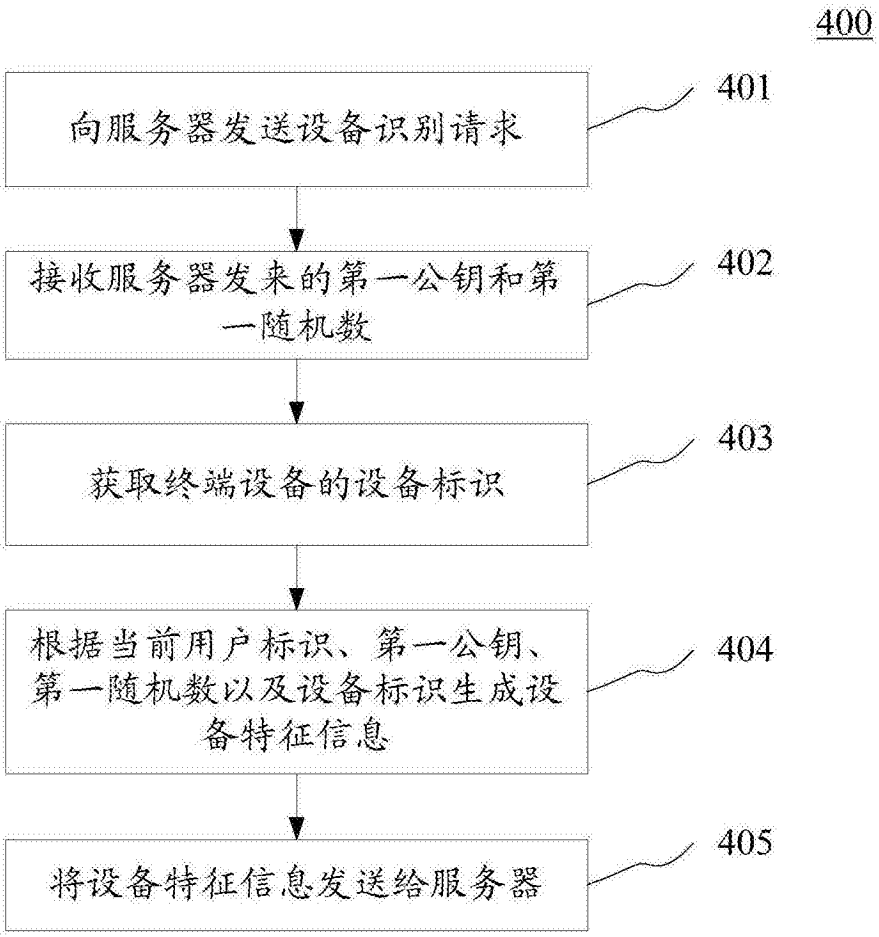

400
向服务器发送设备识别请求
401
接收服务器发来的第一公钥和第一随机数
402
获取终端设备的设备标识
403
根据当前用户标识、第一公钥、第一随机数以及设备标识生成设备特征信息
404
将设备特征信息发送给服务器
405

图4

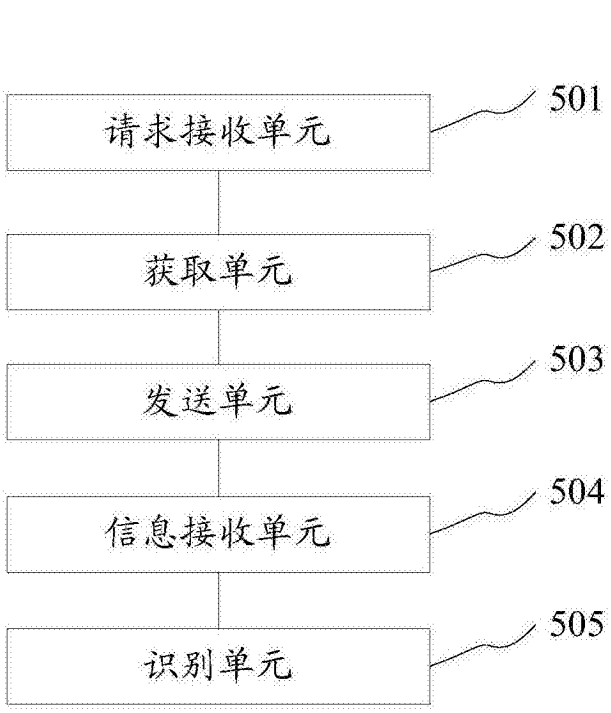

500
请求接收单元
501
获取单元
502
发送单元
503
信息接收单元
504
识别单元
505

图5

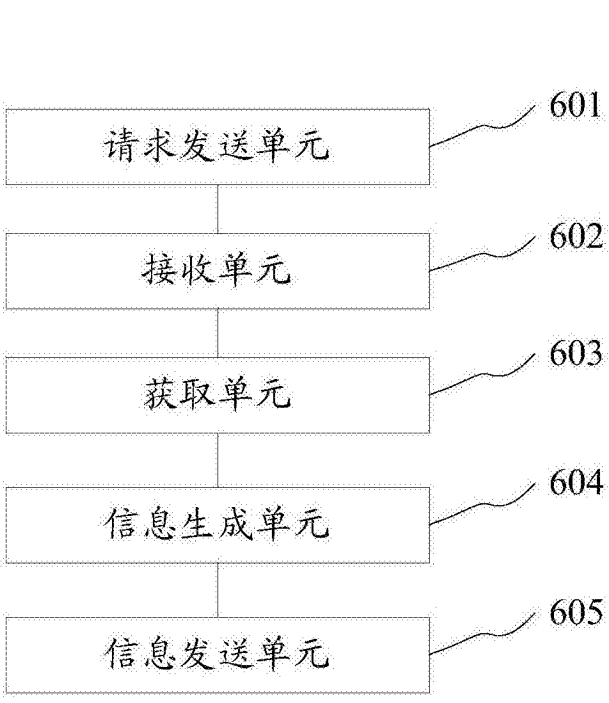

600
请求发送单元
601
接收单元
602
获取单元
603
信息生成单元
604
信息发送单元
605

图6

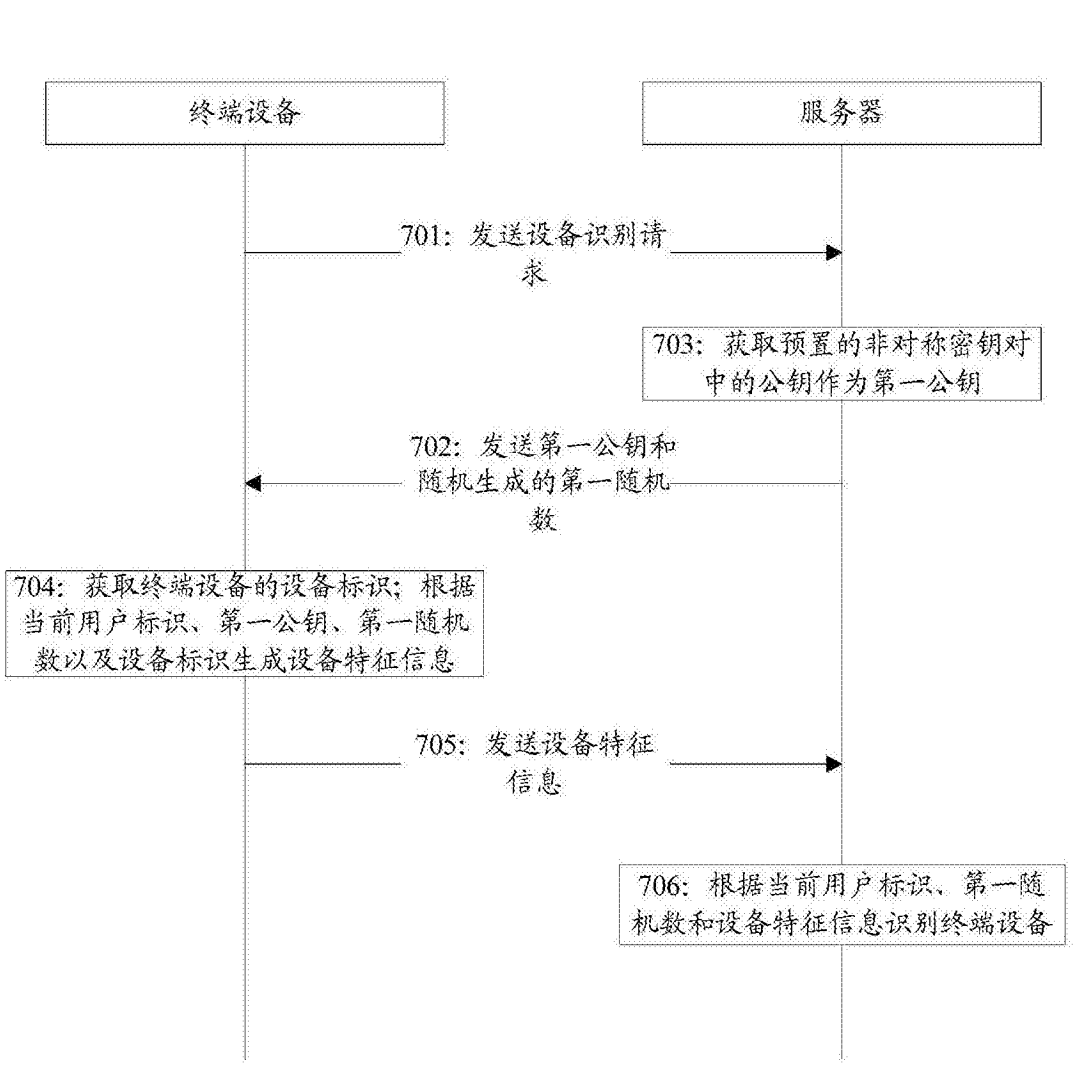

700
终端设备
服务器
701：发送设备识别请求
703：获取预置的非对称密钥对中的公钥作为第一公钥
702：发送第一公钥和随机生成的第一随机数
704：获取终端设备的设备标识；根据当前用户标识、第一公钥、第一随机数以及设备标识生成设备特征信息
705：发送设备特征信息
706：根据当前用户标识、第一随机数和设备特征信息识别终端设备

图7

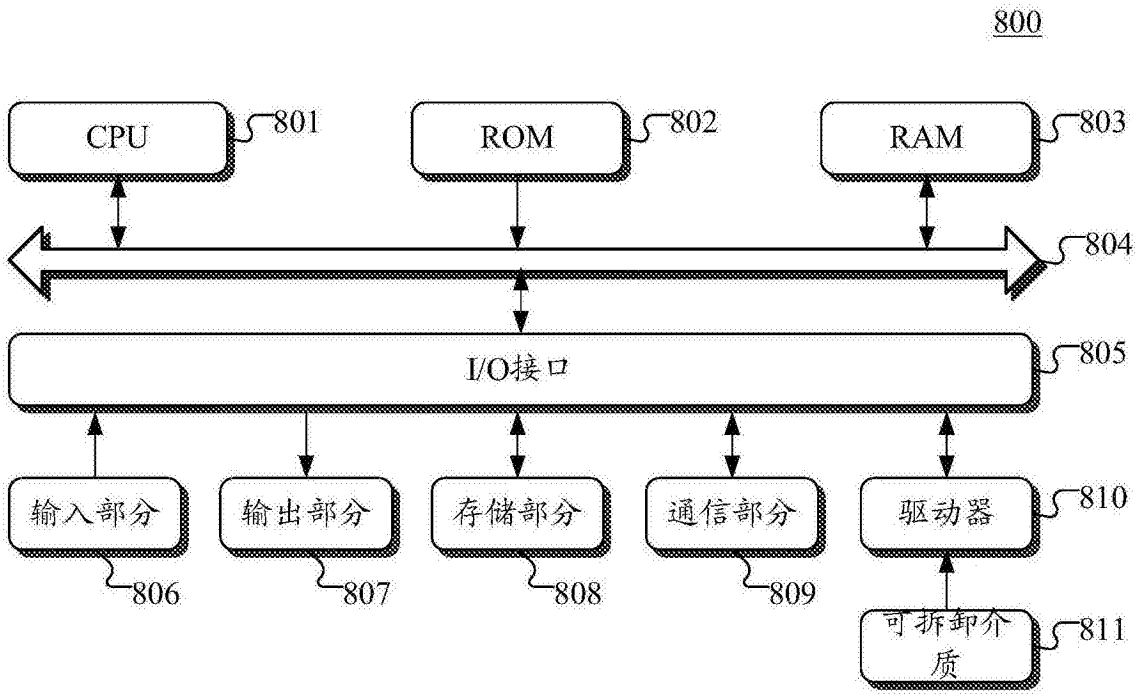

800
CPU
801
ROM
802
RAM
803
804
I/O接口
805
输入部分
806
输出部分
807
存储部分
808
通信部分
809
驱动器
810
可拆卸介质
811

图8