(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106341817 A
(43)申请公布日 2017.01.18

(21)申请号 201610804140.3

(22)申请日 2016.09.05

(71)申请人 努比亚技术有限公司
地址 518000 广东省深圳市南山区高新区北环大道9018号大族创新大厦A区6-8层、10-11层、B区6层、C区6-10层

(72)发明人 符兴富

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 韩辉峰 李丹

(51)Int.Cl.
H04W 12/06(2009.01)
H04L 9/30(2006.01)
H04L 29/06(2006.01)
G07C 9/00(2006.01)

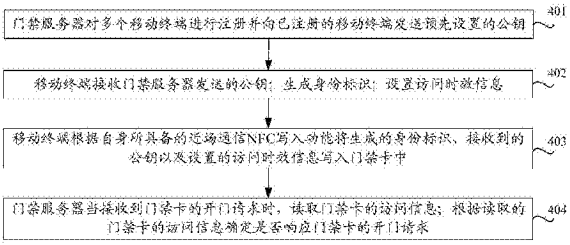
权利要求书2页 说明书15页 附图4页

(54)发明名称

一种门禁控制系统、方法、移动终端和门禁服务器

(57)摘要

本文公布一种门禁控制系统、方法、移动终端和门禁服务器，该门禁控制方法包括：门禁服务器对多个移动终端进行注册并向已注册的移动终端发送预先设置的公钥；移动终端接收门禁服务器发送的公钥；生成身份标识；设置访问时效信息；移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中；门禁服务器当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。本发明实施例提高了授权操作的效率以及提高了访问效率，增强了用户体验。



CN 106341817 A

1.一种门禁控制系统，其特征在于，包括：一个门禁服务器、多个移动终端和多个门禁卡；其中，

门禁服务器，用于对多个移动终端进注册并向已注册的移动终端发送预先设置的公钥；当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求；

移动终端，用于生成身份标识；接收门禁服务器发送的公钥；设置访问时效信息；根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中；

门禁卡，用于向门禁服务器发送开门请求。

2.根据权利要求1所述的门禁控制系统，其特征在于，所述访问信息包括：所述移动终端生成的身份标识、所述公钥、所述访问时效信息以及所述门禁卡的身份标识。

3.根据权利要求2所述的门禁控制系统，其特征在于，所述门禁服务器中用于根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求包括：

判断所述门禁卡的身份标识是否包含在自身存储的多个门禁卡的效身份标识中；判断读取的公钥是否是自身预先设置的公钥；判断所述移动终端生成的身份标识是否是已注册的移动终端的身份标识；判断所述访问时效信息是否在有效期内；

当判断出所述门禁卡的身份标识包含在自身存储的多个门禁卡的效身份标识中，并且当判断出读取的公钥是自身预先设置的公钥，并且当判断出所述移动终端生成的身份标识是已注册的移动终端的身份标识，并且当判断出所述访问时效信息在有效期内时，响应所述门禁卡的开门请求；

当判断出所述门禁卡的身份标识未包含在自身存储的多个门禁卡的效身份标识中，或者当判断出的公钥不是自身预先设置的公钥，或者当判断出所述移动终端生成的身份标识不是已注册的移动终端的身份标识，或者当判断出所述访问时效信息不在有效期内时，拒绝响应所述门禁卡的开门请求。

4.根据权利要求3所述的门禁控制系统，其特征在于，所述门禁服务器中用于对多个移动终端进行注册包括：

获取多个移动终端的移动设备国际身份码IMEI并存储。

5.根据权利要求4所述的门禁控制系统，其特征在于，所述移动终端中用于生成身份标识包括：

获取自身的IMEI；

按照第一预设加密算法对所述IMEI进行加密以生成身份标识。

6.根据权利要求5所述的门禁控制系统，其特征在于，所述门禁服务器中用于判断所述移动终端生成的身份标识是否是已注册的移动终端的身份标识包括：

按照与所述第一预设加密算法对应的第一预设解密算法对所述移动终端生成的身份标识进行解密以获取所述移动终端的IMEI；

判断获得的所述移动终端的IMEI是否包含在自身预先存储的多个移动终端的IMEI中；

当判断出获得的所述移动终端的IMEI包含在自身存储的多个移动终端的IMEI中时，判断出所述移动终端生成的身份标识是已注册的移动终端的身份标识；

当判断出获得的所述移动终端的IMEI未包含在自身存储的多个移动终端的IMEI中时，

判断出所述移动终端生成的身份标识不是已注册的移动终端的身份标识。

7.根据权利要求3所述的门禁控制系统，其特征在于，所述访问时效信息包括：访问次数阈值和/或可访问时间段；相应地，

所述门禁服务器中用于判断所述访问时效信息是否在有效期内包括：

获取所述门禁卡的访问次数，和/或获取当前时刻；

判断获得的所述门禁卡的访问次数是否达到所述访问次数阈值，和/或判断获得的当前时刻是否在所述可访问时间段内；

当判断出获得的所述门禁卡的访问次数未达到所述访问次数阈值，并且当判断出获得的当前时刻在所述可访问时间段内时，判断出所述访问时效信息在有效期内；

当判断出获得的所述门禁卡的访问次数达到所述访问次数阈值，或者当判断出获得的当前时刻不在所述可访问时间段内时，判断出所述访问时效信息不在有效期内。

8.一种门禁控制方法，其特征在于，包括：

门禁服务器对多个移动终端进行注册并向已注册的移动终端发送预先设置的公钥；

移动终端接收门禁服务器发送的公钥；生成身份标识；设置访问时效信息；

移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中；

门禁服务器当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。

9.一种移动终端，其特征在于，包括：接收模块、生成模块、设置模块和写入模块；其中，

接收模块，用于接收门禁服务器发送的公钥；

生成模块，用于生成身份标识；

设置模块，用于设置访问时效信息；

写入模块，用于根据自身所属的移动终端所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中。

10.一种门禁服务器，其特征在于，包括：注册模块、发送模块、读取模块和处理模块；其中，

注册模块，用于对多个移动终端进注册；

发送模块，用于向已注册的移动终端发送预先设置的公钥；

读取模块，用于当接收到门禁卡的开门请求时，读取门禁卡的访问信息；

处理模块，用于根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。

一种门禁控制系统、方法、移动终端和门禁服务器

技术领域

[0001] 本发明实施例涉及但不限于通信领域，尤指一种门禁控制系统、方法、移动终端和门禁服务器。

背景技术

[0002] 目前，生态社区的门禁系统，还处于人为授权的阶段，如通过个人电脑(PC，Personal Computer)携带的门禁卡读取和写入装置进行门禁数据的写入以及注销操作，这样造成了授权操作不规范，授权操作的效率低下，访问操作效率低下，用户体验不好。

发明内容

[0003] 本申请提供了一种门禁控制系统、方法、移动终端和门禁服务器，能够提高授权操作的效率以及提高访问效率，增强用户体验。

[0004] 为了达到本申请目的，本发明实施例提供了一种门禁控制系统，包括：一个门禁服务器、多个移动终端和多个门禁卡；其中，

[0005] 门禁服务器，用于对多个移动终端进注册并向已注册的移动终端发送预先设置的公钥；当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求；

[0006] 移动终端，用于生成身份标识；接收门禁服务器发送的公钥；设置访问时效信息；根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中；

[0007] 门禁卡，用于向门禁服务器发送开门请求。

[0008] 可选地，所述访问信息包括：所述移动终端生成的身份标识、所述公钥、所述访问时效信息以及所述门禁卡的身份标识。

[0009] 可选地，所述门禁服务器中用于根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求包括：

[0010] 判断所述门禁卡的身份标识是否包含在自身存储的多个门禁卡的效身份标识中；判断读取的公钥是否是自身预先设置的公钥；判断所述移动终端生成的身份标识是否是已注册的移动终端的身份标识；判断所述访问时效信息是否在有效期内；

[0011] 当判断出所述门禁卡的身份标识包含在自身存储的多个门禁卡的效身份标识中，并且当判断出读取的公钥是自身预先设置的公钥，并且当判断出所述移动终端生成的身份标识是已注册的移动终端的身份标识，并且当判断出所述访问时效信息在有效期内时，响应所述门禁卡的开门请求；

[0012] 当判断出所述门禁卡的身份标识未包含在自身存储的多个门禁卡的效身份标识中，或者当判断出的公钥不是自身预先设置的公钥，或者当判断出所述移动终端生成的身份标识不是已注册的移动终端的身份标识，或者当判断出所述访问时效信息不在有效期内时，拒绝响应所述门禁卡的开门请求。

[0013] 可选地，所述门禁服务器中用于对多个移动终端进行注册包括：

[0014] 获取多个移动终端的移动设备国际身份码IMEI并存储。

[0015] 可选地，所述移动终端中用于生成身份标识包括：

[0016] 获取自身的IMEI；

[0017] 按照第一预设加密算法对所述IMEI进行加密以生成身份标识。

[0018] 可选地，所述门禁服务器中用于判断所述移动终端生成的身份标识是否是已注册的移动终端的身份标识包括：

[0019] 按照与所述第一预设加密算法对应的第一预设解密算法对所述移动终端生成的身份标识进行解密以获取所述移动终端的IMEI；

[0020] 判断获得的所述移动终端的IMEI是否包含在自身预先存储的多个移动终端的IMEI中；

[0021] 当判断出获得的所述移动终端的IMEI包含在自身存储的多个移动终端的IMEI中时，判断出所述移动终端生成的身份标识是已注册的移动终端的身份标识；

[0022] 当判断出获得的所述移动终端的IMEI未包含在自身存储的多个移动终端的IMEI中时，判断出所述移动终端生成的身份标识不是已注册的移动终端的身份标识。

[0023] 可选地，所述访问时效信息包括：访问次数阈值和/或可访问时间段；相应地，

[0024] 所述门禁服务器中用于判断所述访问时效信息是否在有效期内包括：

[0025] 获取所述门禁卡的访问次数，和/或获取当前时刻；

[0026] 判断获得的所述门禁卡的访问次数是否达到所述访问次数阈值，和/或判断获得的当前时刻是否在所述可访问时间段内；

[0027] 当判断出获得的所述门禁卡的访问次数未达到所述访问次数阈值，并且当判断出获得的当前时刻在所述可访问时间段内时，判断出所述访问时效信息在有效期内；

[0028] 当判断出获得的所述门禁卡的访问次数达到所述访问次数阈值，或者当判断出获得的当前时刻不在所述可访问时间段内时，判断出所述访问时效信息不在有效期内。

[0029] 本发明实施例还提供了一种门禁控制方法，包括：

[0030] 门禁服务器对多个移动终端进行注册并向已注册的移动终端发送预先设置的公钥；

[0031] 移动终端接收门禁服务器发送的公钥；生成身份标识；设置访问时效信息；

[0032] 移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中；

[0033] 门禁服务器当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。

[0034] 本发明实施例还提供了一种移动终端，包括：接收模块、生成模块、设置模块和写入模块；其中，

[0035] 接收模块，用于接收门禁服务器发送的公钥；

[0036] 生成模块，用于生成身份标识；

[0037] 设置模块，用于设置访问时效信息；

[0038] 写入模块，用于根据自身所属的移动终端所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中。

[0039] 本发明实施例还提供了一种门禁服务器，包括：注册模块、发送模块、读取模块和处理模块；其中，

[0040] 注册模块，用于对多个移动终端进注册；

[0041] 发送模块，用于向已注册的移动终端发送预先设置的公钥；

[0042] 读取模块，用于当接收到门禁卡的开门请求时，读取门禁卡的访问信息；

[0043] 处理模块，用于根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。

[0044] 本发明实施例包括：门禁服务器对多个移动终端进行注册并向已注册的移动终端发送预先设置的公钥；移动终端接收门禁服务器发送的公钥；生成身份标识；设置访问时效信息；移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中；门禁服务器当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。本发明实施例提高了授权操作的效率以及提高了访问效率，增强了用户体验。

附图说明

[0045] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0046] 图1为实现本申请各个实施例一个可选的移动终端的硬件结构示意图；

[0047] 图2为支持本申请移动终端之间进行通信的通信系统的示意图；

[0048] 图3为本申请门禁控制系统的架构图；

[0049] 图4为本申请门禁控制方法的流程图；

[0050] 图5为本申请门禁控制方法的实施例的流程图；

[0051] 图6为本申请移动终端的结构示意图；

[0052] 图7为本申请门禁服务器的结构示意图。

具体实施方式

[0053] 下面将结合附图及实施例对本发明的技术方案进行更详细的说明。

[0054] 现在将参考附图描述实现本申请各个实施例的移动终端。在后续的描述中，使用用于表示元件的诸如“模块”、“部件”或“单元”的后缀仅为了有利于本发明的说明，其本身并没有特定的意义。因此，"模块"与"部件"可以混合地使用。

[0055] 移动终端可以以各种形式来实施。例如，本发明中描述的终端可以包括诸如移动电话、智能电话、笔记本电脑、数字广播接收器、PDA(个人数字助理)、PAD(平板电脑)、PMP(便携式多媒体播放器)、导航装置等等的移动终端以及诸如数字TV、台式计算机等等的固定终端。下面，假设终端是移动终端。然而，本领域技术人员将理解的是，除了特别用于移动目的的元件之外，根据本发明的实施方式的构造也能够应用于固定类型的终端。

[0056] 图1为实现本申请各个实施例一个可选的移动终端的硬件结构示意图。

[0057] 移动终端100可以包括无线通信单元110、A/V(音频/视频)输入单元120、用户输入单元130、感测单元140、输出单元150、存储器160、接口单元170、控制器180和电源单元190等等。图1示出了具有各种组件的移动终端，但是应理解的是，并不要求实施所有示出的组件。可以替代地实施更多或更少的组件。将在下面详细描述移动终端的元件。

[0058] 无线通信单元110通常包括一个或多个组件，其允许移动终端100与无线通信系统或网络之间的无线电通信。例如，无线通信单元可以包括广播接收模块111、移动通信模块112、无线互联网模块113、短程通信模块114和位置信息模块115中的至少一个。

[0059] 广播接收模块111经由广播信道从外部广播管理服务器接收广播信号和/或广播相关信息。广播信道可以包括卫星信道和/或地面信道。广播管理服务器可以是生成并发送广播信号和/或广播相关信息的服务器或者接收之前生成的广播信号和/或广播相关信息并且将其发送给终端的服务器。广播信号可以包括TV广播信号、无线电广播信号、数据广播信号等等。而且，广播信号可以进一步包括与TV或无线电广播信号组合的广播信号。广播相关信息也可以经由移动通信网络提供，并且在该情况下，广播相关信息可以由移动通信模块112来接收。广播信号可以以各种形式存在，例如，其可以以数字多媒体广播(DMB)的电子节目指南(EPG)、数字视频广播手持(DVB-H)的电子服务指南(ESG)等等的形式而存在。广播接收模块111可以通过使用各种类型的广播系统接收信号广播。特别地，广播接收模块111可以通过使用诸如多媒体广播-地面(DMB-T)、数字多媒体广播-卫星(DMB-S)、数字视频广播-手持(DVB-H)，前向链路媒体(MediaFLO®)的数据广播系统、地面数字广播综合服务(ISDB-T)等等的数字广播系统接收数字广播。广播接收模块111可以被构造为适合提供广播信号的各种广播系统以及上述数字广播系统。经由广播接收模块111接收的广播信号和/或广播相关信息可以存储在存储器160(或者其它类型的存储介质)中。

[0060] 移动通信模块112将无线电信号发送到基站(例如，接入点、节点B等等)、外部终端以及服务器中的至少一个和/或从其接收无线电信号。这样的无线电信号可以包括语音通话信号、视频通话信号、或者根据文本和/或多媒体消息发送和/或接收的各种类型的数据。

[0061] 无线互联网模块113支持移动终端的无线互联网接入。该模块可以内部或外部地耦接到终端。该模块所涉及的无线互联网接入技术可以包括WLAN(无线LAN)(Wi-Fi)、Wibro(无线宽带)、Wimax(全球微波互联接入)、HSDPA(高速下行链路分组接入)等等。

[0062] 短程通信模块114是用于支持短程通信的模块。短程通信技术的一些示例包括蓝牙™、射频识别(RFID)、红外数据协会(IrDA)、超宽带(UWB)、紫蜂™等等。

[0063] 位置信息模块115是用于检查或获取移动终端的位置信息的模块。位置信息模块的典型示例是GPS(全球定位系统)。根据当前的技术，GPS模块115计算来自三个或更多卫星的距离信息和准确的时间信息并且对于计算的信息应用三角测量法，从而根据经度、纬度和高度准确地计算三维当前位置信息。当前，用于计算位置和时间信息的方法使用三颗卫星并且通过使用另外的一颗卫星校正计算出的位置和时间信息的误差。此外，GPS模块115能够通过实时地连续计算当前位置信息来计算速度信息。

[0064] A/V输入单元120用于接收音频或视频信号。A/V输入单元120可以包括相机121和麦克风122，相机121对在视频捕获模式或图像捕获模式中由图像捕获装置获得的静态图片或视频的图像数据进行处理。处理后的图像帧可以显示在显示单元151上。经相机121处理后的图像帧可以存储在存储器160(或其它存储介质)中或者经由无线通信单元110进行发送，可以根据移动终端的构造提供两个或更多相机121。麦克风122可以在电话通话模式、记录模式、语音识别模式等等运行模式中经由麦克风接收声音(音频数据)，并且能够将这样的声音处理为音频数据。处理后的音频(语音)数据可以在电话通话模式的情况下转换为可经由移动通信模块112发送到移动通信基站的格式输出。麦克风122可以实施各种类型的噪

声消除(或抑制)算法以消除(或抑制)在接收和发送音频信号的过程中产生的噪声或者干扰。

[0065] 用户输入单元130可以根据用户输入的命令生成键输入数据以控制移动终端的各种操作。用户输入单元130允许用户输入各种类型的信息,并且可以包括键盘、锅仔片、触摸板(例如,检测由于被接触而导致的电阻、压力、电容等等的变化的触敏组件)、滚轮、摇杆等等。特别地,当触摸板以层的形式叠加在显示单元151上时,可以形成触摸屏。

[0066] 感测单元140检测移动终端100的当前状态,(例如,移动终端100的打开或关闭状态)、移动终端100的位置、用户对于移动终端100的接触(即,触摸输入)的有无、移动终端100的取向、移动终端100的加速或减速移动和方向等等,并且生成用于控制移动终端100的操作的命令或信号。例如,当移动终端100实施为滑动型移动电话时,感测单元140可以感测该滑动型电话是打开还是关闭。另外,感测单元140能够检测电源单元190是否提供电力或者接口单元170是否与外部装置耦接。

[0067] 接口单元170用作至少一个外部装置与移动终端100连接可以通过的接口。例如,外部装置可以包括有线或无线头戴式耳机端口、外部电源(或电池充电器)端口、有线或无线数据端口、存储卡端口、用于连接具有识别模块的装置的端口、音频输入/输出(I/O)端口、视频I/O端口、耳机端口等等。识别模块可以是存储用于验证用户使用移动终端100的各种信息并且可以包括用户识别模块(UIM)、客户识别模块(SIM)、通用客户识别模块(USIM)等等。另外,具有识别模块的装置(下面称为"识别装置")可以采取智能卡的形式,因此,识别装置可以经由端口或其它连接装置与移动终端100连接。接口单元170可以用于接收来自外部装置的输入(例如,数据信息、电力等等)并且将接收到的输入传输到移动终端100内的一个或多个元件或者可以用于在移动终端和外部装置之间传输数据。

[0068] 另外,当移动终端100与外部底座连接时,接口单元170可以用作允许通过其将电力从底座提供到移动终端100的路径或者可以用作允许从底座输入的各种命令信号通过其传输到移动终端的路径。从底座输入的各种命令信号或电力可以用作用于识别移动终端是否准确地安装在底座上的信号。输出单元150被构造为以视觉、音频和/或触觉方式提供输出信号(例如,音频信号、视频信号、警报信号、振动信号等等)。输出单元150可以包括显示单元151、音频输出模块152、警报单元153等等。

[0069] 显示单元151可以显示在移动终端100中处理的信息。例如,当移动终端100处于电话通话模式时,显示单元151可以显示与通话或其它通信(例如,文本消息收发、多媒体文件下载等等)相关的用户界面(UI)或图形用户界面(GUI)。当移动终端100处于视频通话模式或者图像捕获模式时,显示单元151可以显示捕获的图像和/或接收的图像、示出视频或图像以及相关功能的UI或GUI等等。

[0070] 同时,当显示单元151和触摸板以层的形式彼此叠加以形成触摸屏时,显示单元151可以用作输入装置和输出装置。显示单元151可以包括液晶显示器(LCD)、薄膜晶体管LCD(TFT-LCD)、有机发光二极管(OLED)显示器、柔性显示器、三维(3D)显示器等等中的至少一种。这些显示器中的一些可以被构造为透明状以允许用户从外部观看,这可以称为透明显示器,典型的透明显示器可以例如为TOLED(透明有机发光二极管)显示器等等。根据特定想要的实施方式,移动终端100可以包括两个或更多显示单元(或其它显示装置),例如,移动终端可以包括外部显示单元(未示出)和内部显示单元(未示出)。触摸屏可用于检测触摸

输入压力以及触摸输入位置和触摸输入面积。

[0071] 音频输出模块152可以在移动终端处于呼叫信号接收模式、通话模式、记录模式、语音识别模式、广播接收模式等等模式下时，将无线通信单元110接收的或者在存储器160中存储的音频数据转换音频信号并且输出为声音。而且，音频输出模块152可以提供与移动终端100执行的特定功能相关的音频输出(例如，呼叫信号接收声音、消息接收声音等等)。音频输出模块152可以包括扬声器、蜂鸣器等等。

[0072] 警报单元153可以提供输出以将事件的发生通知给移动终端100。典型的事件可以包括呼叫接收、消息接收、键信号输入、触摸输入等等。除了音频或视频输出之外，警报单元153可以以不同的方式提供输出以通知事件的发生。例如，警报单元153可以以振动的形式提供输出，当接收到呼叫、消息或一些其它进入通信(incoming communication)时，警报单元153可以提供触觉输出(即，振动)以将其通知给用户。通过提供这样的触觉输出，即使在用户的移动电话处于用户的口袋中时，用户也能够识别出各种事件的发生。警报单元153也可以经由显示单元151或音频输出模块152提供通知事件的发生的输出。

[0073] 存储器160可以存储由控制器180执行的处理和控制操作的软件程序等等，或者可以暂时地存储已经输出或将要输出的数据(例如，电话簿、消息、静态图像、视频等等)。而且，存储器160可以存储关于当触摸施加到触摸屏时输出的各种方式的振动和音频信号的数据。

[0074] 存储器160可以包括至少一种类型的存储介质，所述存储介质包括闪存、硬盘、多媒体卡、卡型存储器(例如，SD或DX存储器等等)、随机访问存储器(RAM)、静态随机访问存储器(SRAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、可编程只读存储器(PROM)、磁性存储器、磁盘、光盘等等。而且，移动终端100可以与通过网络连接执行存储器160的存储功能的网络存储装置协作。

[0075] 控制器180通常控制移动终端的总体操作。例如，控制器180执行与语音通话、数据通信、视频通话等等相关的控制和处理。另外，控制器180可以包括用于再现(或回放)多媒体数据的多媒体模块181，多媒体模块181可以构造在控制器180内，或者可以构造为与控制器180分离。控制器180可以执行模式识别处理，以将在触摸屏上执行的手写输入或者图片绘制输入识别为字符或图像。

[0076] 电源单元190在控制器180的控制下接收外部电力或内部电力并且提供操作各元件和组件所需的适当的电力。

[0077] 这里描述的各种实施方式可以以使用例如计算机软件、硬件或其任何组合的计算机可读介质来实施。对于硬件实施，这里描述的实施方式可以通过使用特定用途集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理装置(DSPD)、可编程逻辑装置(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器、被设计为执行这里描述的功能的电子单元中的至少一种来实施，在一些情况下，这样的实施方式可以在控制器180中实施。对于软件实施，诸如过程或功能的实施方式可以与允许执行至少一种功能或操作的单独的软件模块来实施。软件代码可以由以任何适当的编程语言编写的软件应用程序(或程序)来实施，软件代码可以存储在存储器160中并且由控制器180执行。

[0078] 至此，已经按照其功能描述了移动终端。下面，为了简要起见，将描述诸如折叠型、直板型、摆动型、滑动型移动终端等等的各种类型的移动终端中的滑动型移动终端作为示

例。因此，本申请能够应用于任何类型的移动终端，并且不限于滑动型移动终端。

[0079] 如图1中所示的移动终端100可以被构造为利用经由帧或分组发送数据的诸如有线和无线通信系统以及基于卫星的通信系统来操作。

[0080] 现在将参考图2描述其中根据本申请的移动终端能够操作的通信系统。

[0081] 这样的通信系统可以使用不同的空中接口和/或物理层。例如，由通信系统使用的空中接口包括例如频分多址(FDMA)、时分多址(TDMA)、码分多址(CDMA)和通用移动通信系统(UMTS)(特别地，长期演进(LTE))、全球移动通信系统(GSM)等等。作为非限制性示例，下面的描述涉及CDMA通信系统，但是这样的教导同样适用于其它类型的系统。

[0082] 参考图2，CDMA无线通信系统可以包括多个移动终端100、多个基站(BS)270、基站控制器(BSC)275和移动交换中心(MSC)280。MSC280被构造为与公共电话交换网络(PSTN)290形成接口。MSC280还被构造为与可以经由回程线路耦接到基站270的BSC275形成接口。回程线路可以根据若干已知的接口中的任一种来构造，所述接口包括例如E1/T1、ATM，IP、PPP、帧中继、HDSL、ADSL或xDSL。将理解的是，如图2中所示的系统可以包括多个BSC275。

[0083] 每个BS270可以服务一个或多个分区(或区域)，由多向天线或指向特定方向的天线覆盖的每个分区放射状地远离BS270。或者，每个分区可以由用于分集接收的两个或更多天线覆盖。每个BS270可以被构造为支持多个频率分配，并且每个频率分配具有特定频谱(例如，1.25MHz，5MHz等等)。

[0084] 分区与频率分配的交叉可以被称为CDMA信道。BS270也可以被称为基站收发器子系统(BTS)或者其它等效术语。在这样的情况下，术语"基站"可以用于笼统地表示单个BSC275和至少一个BS270。基站也可以被称为"蜂窝站"。或者，特定BS270的各分区可以被称为多个蜂窝站。

[0085] 如图2中所示，广播发射器(BT)295将广播信号发送给在系统内操作的移动终端100。如图1中所示的广播接收模块111被设置在移动终端100处以接收由BT295发送的广播信号。在图2中，示出了几个全球定位系统(GPS)卫星300。卫星300帮助定位多个移动终端100中的至少一个。

[0086] 在图2中，描绘了多个卫星300，但是理解的是，可以利用任何数目的卫星获得有用的定位信息。如图1中所示的GPS模块115通常被构造为与卫星300配合以获得想要的定位信息。替代GPS跟踪技术或者在GPS跟踪技术之外，可以使用可以跟踪移动终端的位置的其它技术。另外，至少一个GPS卫星300可以选择性地或者额外地处理卫星DMB传输。

[0087] 作为无线通信系统的一个典型操作，BS270接收来自各种移动终端100的反向链路信号。移动终端100通常参与通话、消息收发和其它类型的通信。特定基站270接收的每个反向链路信号被在特定BS270内进行处理。获得的数据被转发给相关的BSC275。BSC提供通话资源分配和包括BS270之间的软切换过程的协调的移动管理功能。BSC275还将接收到的数据路由到MSC280，其提供用于与PSTN290形成接口的额外的路由服务。类似地，PSTN290与MSC280形成接口，MSC与BSC275形成接口，并且BSC275相应地控制BS270以将正向链路信号发送到移动终端100。

[0088] 基于上述移动终端硬件结构以及通信系统，提出本申请方法各个实施例。

[0089] 图3为本申请门禁控制系统的架构图，如图3所示，包括：一个门禁服务器、多个移动终端和多个门禁卡。其中，

[0090] 门禁服务器，用于对多个移动终端进注册并向已注册的移动终端发送预先设置的公钥；当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。

[0091] 其中，门禁服务器中用于对多个移动终端进行注册包括：

[0092] 获取多个移动终端的移动设备国际身份码(IMEI，International Mobile Equipment Identity)并存储。

[0093] 其中，预先设置的公钥是门禁服务器采用第二预设加密算法对自身存储的某一文件进行加密从而获取的。

[0094] 其中，访问信息包括：移动终端生成的身份标识、公钥、访问时效信息以及门禁卡的身份标识。

[0095] 其中，门禁服务器中用于根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求包括：

[0096] 判断门禁卡的身份标识是否包含在自身存储的多个门禁卡的效身份标识中；判断读取的公钥是否是自身预先设置的公钥；判断移动终端生成的身份标识是否是已注册的移动终端的身份标识；判断访问时效信息是否在有效期内；

[0097] 当判断出门禁卡的身份标识包含在自身存储的多个门禁卡的效身份标识中，并且当判断出读取的公钥是自身预先设置的公钥，并且当判断出移动终端生成的身份标识是已注册的移动终端的身份标识，并且当判断出访问时效信息在有效期内时，响应门禁卡的开门请求；

[0098] 当判断出门禁卡的身份标识未包含在自身存储的多个门禁卡的效身份标识中，或者当判断出的公钥不是自身预先设置的公钥，或者当判断出移动终端生成的身份标识不是已注册的移动终端的身份标识，或者当判断出访问时效信息不在有效期内时，拒绝响应门禁卡的开门请求。

[0099] 移动终端，用于生成身份标识；接收门禁服务器发送的公钥；设置访问时效信息；根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中。

[0100] 其中，访问时效信息包括：访问次数阈值和/或可访问时间段。其中，访问次数阈值可以是移动终端的系统设置的默认值，也可以提供一人机交互界面由用户根据自身的需求进行设置，如可以设置访问次数阈值为2，也可以设置为5，还可以设置为10。

[0101] 其中，移动终端中用于生成身份标识包括：

[0102] 获取自身的IMEI；

[0103] 按照第一预设加密算法对IMEI进行加密以生成身份标识。

[0104] 门禁卡，用于向门禁服务器发送开门请求。

[0105] 其中，门禁服务器中用于判断移动终端生成的身份标识是否是已注册的移动终端的身份标识包括：

[0106] 按照与第一预设加密算法对应的第一预设解密算法对移动终端生成的身份标识进行解密以获取移动终端的IMEI；

[0107] 判断获得的移动终端的IMEI是否包含在自身预先存储的多个移动终端的IMEI中；

[0108] 当判断出获得的移动终端的IMEI包含在自身存储的多个移动终端的IMEI中时，判

断出移动终端生成的身份标识是已注册的移动终端的身份标识；

[0109] 当判断出获得的移动终端的IMEI未包含在自身存储的多个移动终端的IMEI中时，判断出移动终端生成的身份标识不是已注册的移动终端的身份标识。

[0110] 其中，门禁服务器中用于判断访问时效信息是否在有效期内包括：

[0111] 获取门禁卡的访问次数，和/或获取当前时刻；

[0112] 判断获得的门禁卡的访问次数是否达到访问次数阈值，和/或判断获得的当前时刻是否在可访问时间段内；

[0113] 当判断出获得的门禁卡的访问次数未达到访问次数阈值，并且当判断出获得的当前时刻在可访问时间段内时，判断出访问时效信息在有效期内；

[0114] 当判断出获得的门禁卡的访问次数达到访问次数阈值，或者当判断出获得的当前时刻不在可访问时间段内时，判断出访问时效信息不在有效期内。

[0115] 其中，门禁服务器中用于判断读取的公钥是否是自身预先设置的公钥包括：

[0116] 按照与第二预设加密算法对应的第二预设解密算法对读取的公钥进行解密以获取解密后的某一文件；

[0117] 判断获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件是否相同；

[0118] 当判断出获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件相同时，断出读取的公钥是自身预先设置的公钥；

[0119] 当判断出获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件不同时，断出读取的公钥不是自身预先设置的公钥。

[0120] 图4为本申请门禁控制方法的流程图，如图4所示，包括：

[0121] 步骤401：门禁服务器对多个移动终端进行注册并向已注册的移动终端发送预先设置的公钥。

[0122] 其中，门禁服务器对多个移动终端进行注册包括：

[0123] 获取多个移动终端的移动设备国际身份码(IMEI，International Mobile Equipment Identity)并存储。

[0124] 其中，预先设置的公钥是门禁服务器采用第二预设加密算法对自身存储的某一文件进行加密从而获取的。

[0125] 步骤402：移动终端接收门禁服务器发送的公钥；生成身份标识；设置访问时效信息。

[0126] 其中，移动终端生成身份标识包括：

[0127] 移动终端获取自身的IMEI；

[0128] 移动终端按照第一预设加密算法对IMEI进行加密以生成身份标识。

[0129] 例如，可以按照以下方法对IMEI进行加密：根据当前时间距1970(或者是其它年份)年1月1号零时的秒数除以100以内的随机数，同时乘以移动终端的IMEI。移动终端每次生成的身份标识均不相同，这样可以确保生成的身份标识仅一次有效，防止其它设备盗用。

[0130] 其中，访问时效信息包括：访问次数阈值和/或可访问时间段。其中，访问次数阈值可以是移动终端的系统设置的默认值，也可以提供一人机交互界面由用户根据自身的需求进行设置，如可以设置访问次数阈值为2，也可以设置为5，还可以设置为10。

[0131] 步骤403：移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中。

[0132] 需要说明的是，如何利用NFC写入功能将数据进行写入属于本领域技术人员所熟知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0133] 步骤404：门禁服务器当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。

[0134] 其中，访问信息包括：移动终端生成的身份标识、公钥、访问时效信息以及门禁卡的身份标识。

[0135] 其中，门禁服务器根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求包括：

[0136] 门禁服务器判断门禁卡的身份标识是否包含在自身存储的多个门禁卡的效身份标识中；门禁服务器判断读取的公钥是否是自身预先设置的公钥；门禁服务器判断移动终端生成的身份标识是否是已注册的移动终端的身份标识；门禁服务器判断访问时效信息是否在有效期内；

[0137] 当门禁服务器判断出门禁卡的身份标识包含在自身存储的多个门禁卡的效身份标识中，并且当门禁服务器判断出读取的公钥是自身预先设置的公钥，并且当门禁服务器判断出移动终端生成的身份标识是已注册的移动终端的身份标识，并且当门禁服务器判断出访问时效信息在有效期内时，门禁服务器响应门禁卡的开门请求；

[0138] 当门禁服务器判断出门禁卡的身份标识未包含在自身存储的多个门禁卡的效身份标识中，或者当门禁服务器判断出的公钥不是自身预先设置的公钥，或者当门禁服务器判断出移动终端生成的身份标识不是已注册的移动终端的身份标识，或者当门禁服务器判断出访问时效信息不在有效期内时，门禁服务器拒绝响应门禁卡的开门请求。

[0139] 其中，门禁服务器判断移动终端生成的身份标识是否是已注册的移动终端的身份标识包括：

[0140] 门禁服务器按照与第一预设加密算法对应的第一预设解密算法对移动终端生成的身份标识进行解密以获取移动终端的IMEI；

[0141] 门禁服务器判断获得的移动终端的IMEI是否包含在自身预先存储的多个移动终端的IMEI中；

[0142] 当门禁服务器判断出获得的移动终端的IMEI包含在自身存储的多个移动终端的IMEI中时，门禁服务器判断出移动终端生成的身份标识是已注册的移动终端的身份标识；

[0143] 当门禁服务器判断出获得的移动终端的IMEI未包含在自身存储的多个移动终端的IMEI中时，门禁服务器判断出移动终端生成的身份标识不是已注册的移动终端的身份标识。

[0144] 其中，门禁服务器判断访问时效信息是否在有效期内包括：

[0145] 门禁服务器获取门禁卡的访问次数，和/或获取当前时刻；

[0146] 门禁服务器判断获得的门禁卡的访问次数是否达到访问次数阈值，和/或门禁服务器判断获得的当前时刻是否在可访问时间段内；

[0147] 当门禁服务器判断出获得的门禁卡的访问次数未达到访问次数阈值，并且当门禁服务器判断出获得的当前时刻在可访问时间段内时，门禁服务器判断出访问时效信息在有

效期内；

[0148] 当门禁服务器判断出获得的门禁卡的访问次数达到访问次数阈值，或者当门禁服务器判断出获得的当前时刻不在可访问时间段内时，判断出访问时效信息不在有效期内。

[0149] 其中，门禁服务器判断读取的公钥是否是自身预先设置的公钥包括：

[0150] 按照与第二预设加密算法对应的第二预设解密算法对读取的公钥进行解密以获取解密后的某一文件；

[0151] 判断获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件是否相同；

[0152] 当判断出获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件相同时，断出读取的公钥是自身预先设置的公钥；

[0153] 当判断出获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件不同时，断出读取的公钥不是自身预先设置的公钥。

[0154] 本申请实施方式中，通过移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中，以及根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求，从而提高了授权操作的效率以及提高了访问效率，增强了用户体验。

[0155] 图5为本申请门禁控制方法的实施例的流程图，如图5所示，本实施例以访问时效信息是访问次数阈值为例进行阐述，包括：

[0156] 步骤500：门禁服务器采用第二预设加密算法对自身存储的某一文件进行加密以获取的预先设置的公钥。

[0157] 步骤501：门禁服务器对多个移动终端进注册。

[0158] 其中，步骤501具体包括：

[0159] 门禁服务器获取多个移动终端的移动设备国际身份码(IMEI，International Mobile Equipment Identity)并存储。

[0160] 步骤502：门禁服务器向已注册的移动终端发送预先设置的公钥。

[0161] 步骤503：移动终端接收门禁服务器发送的公钥，生成身份标识，以及设置访问次数阈值。

[0162] 其中，移动终端生成身份标识包括：

[0163] 移动终端获取自身的IMEI；

[0164] 移动终端按照第一预设加密算法对IMEI进行加密以生成身份标识。

[0165] 例如，可以按照以下方法对IMEI进行加密：根据当前时间距1970(或者是其它年份)年1月1号零时的秒数除以100以内的随机数，同时乘以移动终端的IMEI。移动终端每次生成的身份标识均不相同，这样可以确保生成的身份标识仅一次有效，防止其它设备盗用。

[0166] 其中，访问次数阈值可以是移动终端的系统设置的默认值，也可以提供一人机交互界面由用户根据自身的需求进行设置，如可以设置访问次数阈值为2，也可以设置为5，还可以设置为10。

[0167] 步骤504：移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问次数阈值写入门禁卡中。

[0168] 需要说明的是，如何利用NFC写入功能将数据进行写入属于本领域技术人员所熟

知的惯用技术手段，此处不再赘述，并不用来限制本申请。

[0169] 步骤505：门禁卡向门禁服务器发送开门请求。

[0170] 步骤506：门禁服务器当接收到门禁卡的开门请求时，读取门禁卡的访问信息。

[0171] 其中，访问信息包括：移动终端生成的身份标识、公钥、访问次数阈值以及门禁卡的身份标识。

[0172] 步骤507：门禁服务器根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。

[0173] 其中，门禁服务器根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求包括：

[0174] 门禁服务器判断门禁卡的身份标识是否包含在自身存储的多个门禁卡的效身份标识中；门禁服务器判断读取的公钥是否是自身预先设置的公钥；门禁服务器判断移动终端生成的身份标识是否是已注册的移动终端的身份标识；门禁服务器判断访问次数阈值是否在有效期内；

[0175] 当门禁服务器判断出门禁卡的身份标识包含在自身存储的多个门禁卡的效身份标识中，并且当门禁服务器判断出读取的公钥是自身预先设置的公钥，并且当门禁服务器判断出移动终端生成的身份标识是已注册的移动终端的身份标识，并且当门禁服务器判断出访问次数阈值在有效期内时，门禁服务器响应门禁卡的开门请求；

[0176] 当门禁服务器判断出门禁卡的身份标识未包含在自身存储的多个门禁卡的效身份标识中，或者当门禁服务器判断出的公钥不是自身预先设置的公钥，或者当门禁服务器判断出移动终端生成的身份标识不是已注册的移动终端的身份标识，或者当门禁服务器判断出访问次数阈值不在有效期内时，门禁服务器拒绝响应门禁卡的开门请求。

[0177] 其中，门禁服务器判断移动终端生成的身份标识是否是已注册的移动终端的身份标识包括：

[0178] 门禁服务器按照与第一预设加密算法对应的第一预设解密算法对移动终端生成的身份标识进行解密以获取移动终端的IMEI；

[0179] 门禁服务器判断获得的移动终端的IMEI是否包含在自身预先存储的多个移动终端的IMEI中；

[0180] 当门禁服务器判断出获得的移动终端的IMEI包含在自身存储的多个移动终端的IMEI中时，门禁服务器判断出移动终端生成的身份标识是已注册的移动终端的身份标识；

[0181] 当门禁服务器判断出获得的移动终端的IMEI未包含在自身存储的多个移动终端的IMEI中时，门禁服务器判断出移动终端生成的身份标识不是已注册的移动终端的身份标识。

[0182] 其中，门禁服务器判断访问次数阈值是否在有效期内包括：

[0183] 门禁服务器获取门禁卡的访问；

[0184] 门禁服务器判断获得的门禁卡的访问次数是否达到访问次数阈值，和/或门禁服务器判断获得的当前时刻是否在可访问时间段；

[0185] 当门禁服务器判断出获得的门禁卡的访问次数未达到访问次数阈值时，门禁服务器判断出访问次数阈值在有效期内；

[0186] 当门禁服务器判断出获得的门禁卡的访问次数达到访问次数阈值时，判断出访问

次数阈值不在有效期内。

[0187] 其中，门禁服务器判断读取的公钥是否是自身预先设置的公钥包括：

[0188] 按照与第二预设加密算法对应的第二预设解密算法对读取的公钥进行解密以获取解密后的某一文件；

[0189] 判断获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件是否相同；

[0190] 当判断出获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件相同时，断出读取的公钥是自身预先设置的公钥；

[0191] 当判断出获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件不同时，断出读取的公钥不是自身预先设置的公钥。

[0192] 图6为本申请移动终端的结构示意图，如图6所示，包括：接收模块60、生成模块61、设置模块62和写入模块63。其中，

[0193] 接收模块60，用于接收门禁服务器发送的公钥。

[0194] 生成模块61，用于生成身份标识。

[0195] 其中，生成模块61，具体用于：

[0196] 获取自身所属的移动终端的移动设备国际身份码(IMEI，International Mobile Equipment Identity)；

[0197] 按照第一预设加密算法对IMEI进行加密以生成身份标识。

[0198] 设置模块62，用于设置访问时效信息。

[0199] 其中，访问时效信息包括：访问次数阈值和/或可访问时间段。其中，访问次数阈值可以是移动终端的系统设置的默认值，也可以提供一人机交互界面由用户根据自身的需求进行设置，如可以设置访问次数阈值为2，也可以设置为5，还可以设置为10。

[0200] 写入模块63，用于根据自身所属的移动终端所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中。

[0201] 图7为本申请门禁服务器的结构示意图，如图7所示，包括：注册模块70、发送模块71、读取模块72和处理模块73。其中，

[0202] 注册模块70，用于对多个移动终端进注册。

[0203] 其中，注册模块70，具体用于：

[0204] 获取多个移动终端的移动设备国际身份码(IMEI，International Mobile Equipment Identity)并存储。

[0205] 发送模块71，用于向已注册的移动终端发送预先设置的公钥。

[0206] 其中，预先设置的公钥是门禁服务器采用第二预设加密算法对自身存储的某一文件进行加密从而获取的。

[0207] 读取模块72，用于当接收到门禁卡的开门请求时，读取门禁卡的访问信息。

[0208] 其中，访问信息包括：移动终端生成的身份标识、公钥、访问时效信息以及门禁卡的身份标识。

[0209] 处理模块73，用于根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求。

[0210] 其中，处理模块73，具体用于：

[0211] 判断门禁卡的身份标识是否包含在自身存储的多个门禁卡的效身份标识中;判断读取的公钥是否是自身预先设置的公钥;判断移动终端生成的身份标识是否是已注册的移动终端的身份标识;判断访问时效信息是否在有效期内;

[0212] 当判断出门禁卡的身份标识包含在自身存储的多个门禁卡的效身份标识中,并且当判断出读取的公钥是自身预先设置的公钥,并且当判断出移动终端生成的身份标识是已注册的移动终端的身份标识,并且当判断出访问时效信息在有效期内时,响应门禁卡的开门请求;

[0213] 当判断出门禁卡的身份标识未包含在自身存储的多个门禁卡的效身份标识中,或者当判断出的公钥不是自身预先设置的公钥,或者当判断出移动终端生成的身份标识不是已注册的移动终端的身份标识,或者当判断出访问时效信息不在有效期内时,拒绝响应门禁卡的开门请求。

[0214] 其中,处理模块73中用于判断移动终端生成的身份标识是否是已注册的移动终端的身份标识包括:

[0215] 按照与第一预设加密算法对应的第一预设解密算法对移动终端生成的身份标识进行解密以获取移动终端的IMEI;

[0216] 判断获得的移动终端的IMEI是否包含在自身预先存储的多个移动终端的IMEI中;

[0217] 当判断出获得的移动终端的IMEI包含在自身存储的多个移动终端的IMEI中时,判断出移动终端生成的身份标识是已注册的移动终端的身份标识;

[0218] 当判断出获得的移动终端的IMEI未包含在自身存储的多个移动终端的IMEI中时,判断出移动终端生成的身份标识不是已注册的移动终端的身份标识。

[0219] 其中,访问时效信息包括:访问次数阈值和/或可访问时间段。此时,

[0220] 处理模块73中用于判断访问时效信息是否在有效期内包括:

[0221] 获取门禁卡的访问次数,和/或获取当前时刻;

[0222] 判断获得的门禁卡的访问次数是否达到访问次数阈值,和/或判断获得的当前时刻是否在可访问时间段内;

[0223] 当判断出获得的门禁卡的访问次数未达到访问次数阈值,并且当判断出获得的当前时刻在可访问时间段内时,判断出访问时效信息在有效期内;

[0224] 当判断出获得的门禁卡的访问次数达到访问次数阈值,或者当判断出获得的当前时刻不在可访问时间段内时,判断出访问时效信息不在有效期内。

[0225] 其中,门禁服务器判断读取的公钥是否是自身预先设置的公钥包括:

[0226] 按照与第二预设加密算法对应的第二预设解密算法对读取的公钥进行解密以获取解密后的某一文件;

[0227] 判断获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件是否相同;

[0228] 当判断出获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件相同时,断出读取的公钥是自身预先设置的公钥;

[0229] 当判断出获得的解密后的某一文件和采用第二预设加密算法加密前的某一文件不同时,断出读取的公钥不是自身预先设置的公钥。

[0230] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其他变体意在涵盖非排

他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0231] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0232] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件(例如处理器)完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，例如通过集成电路来实现其相应功能，也可以采用软件功能模块的形式实现，例如通过处理器执行存储于存储器中的程序/指令来实现其相应功能。本发明不限制于任何特定形式的硬件和软件的结合。

[0233] 以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

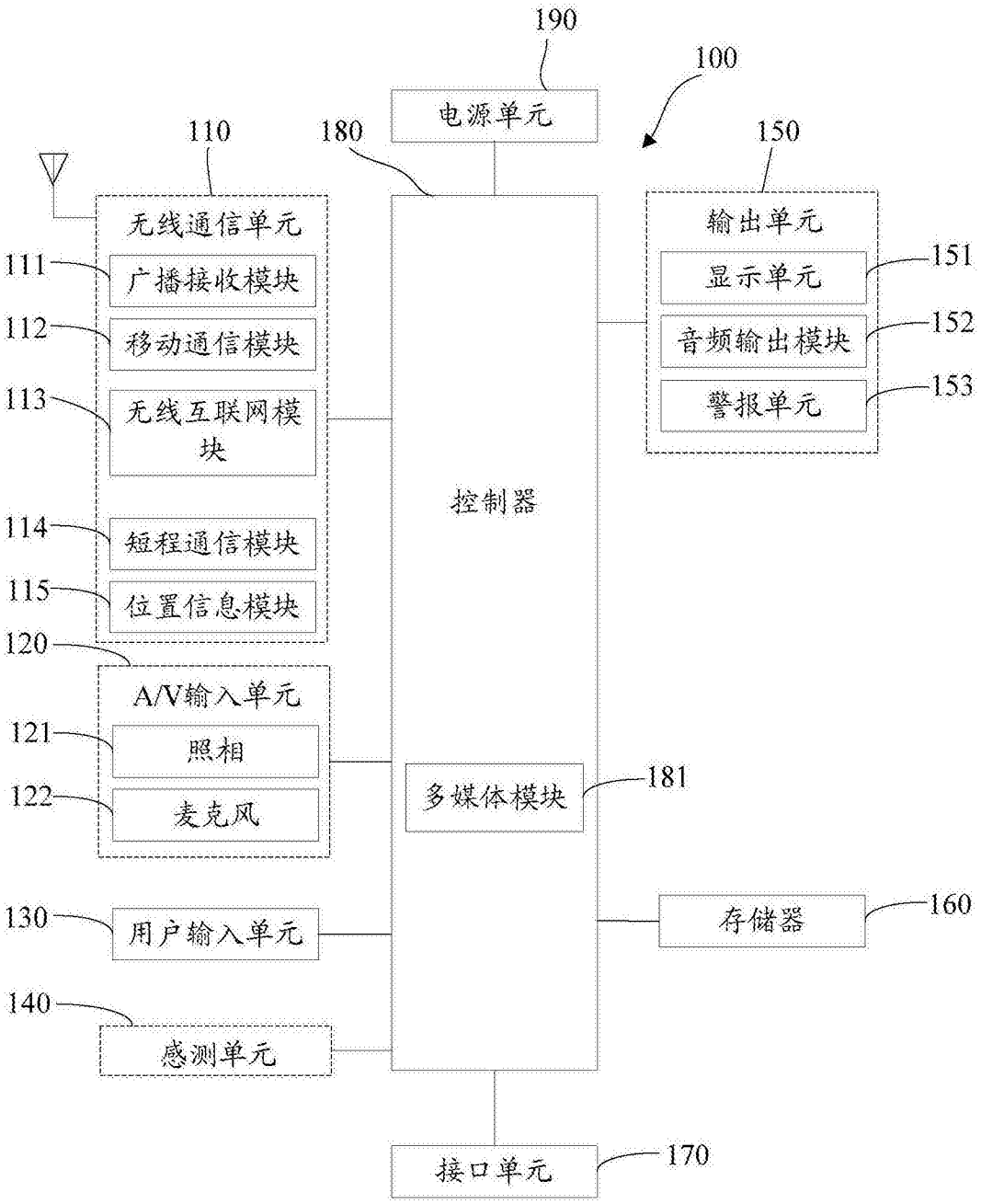

190
100
电源单元
110
180
150
无线通信单元
输出单元
111
广播接收模块
显示单元
151
112
移动通信模块
音频输出模块
152
113
无线互联网模块
警报单元
153
控制器
114
短程通信模块
115
位置信息模块
120
A/V输入单元
121
照相
122
麦克风
多媒体模块
181
130
用户输入单元
存储器
160
140
感测单元
接口单元
170

图1

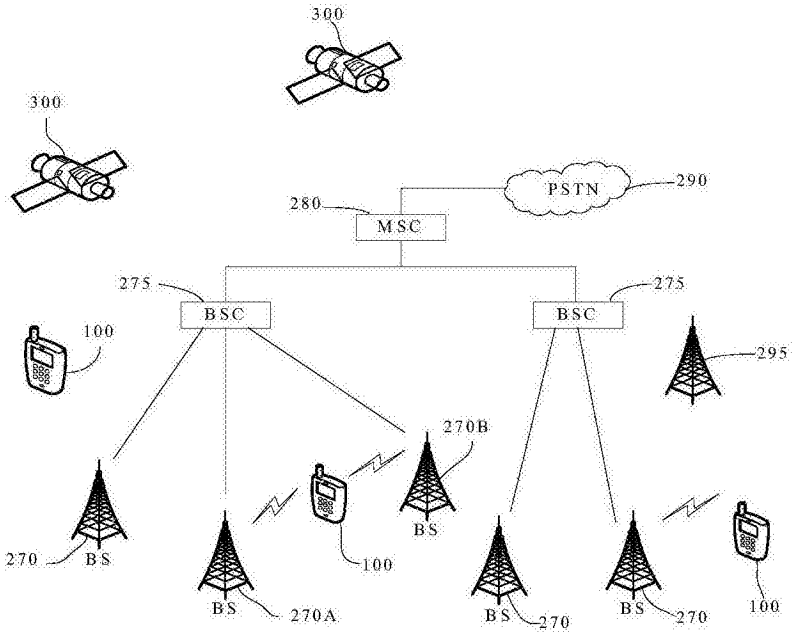

300
300
PSTN
290
280
MSC
275
BSC
BSC
275
100
295
270B
BS
270
BS
100
BS
270A
BS
270
BS
270
100

图2

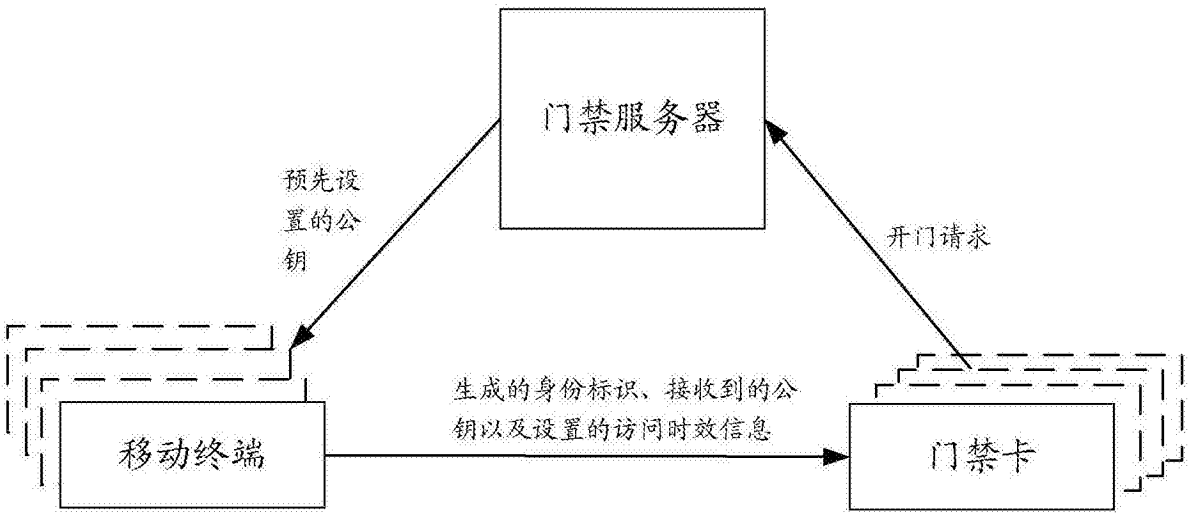

门禁服务器
预先设置的公钥
开门请求
生成的身份标识、接收到的公钥以及设置的访问时效信息
移动终端
门禁卡

图3

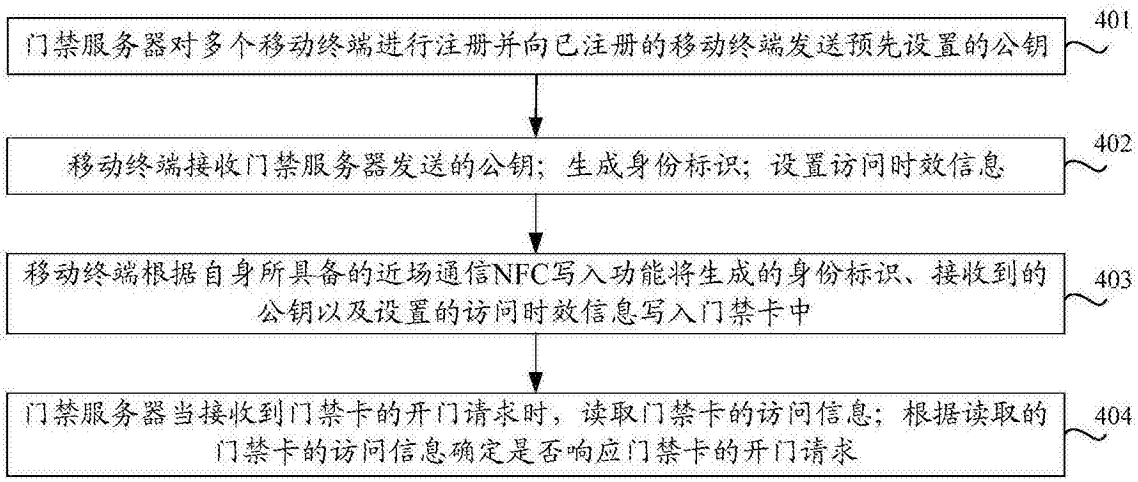

门禁服务器对多个移动终端进行注册并向已注册的移动终端发送预先设置的公钥
401
移动终端接收门禁服务器发送的公钥；生成身份标识；设置访问时效信息
402
移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问时效信息写入门禁卡中
403
门禁服务器当接收到门禁卡的开门请求时，读取门禁卡的访问信息；根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求
404

图4

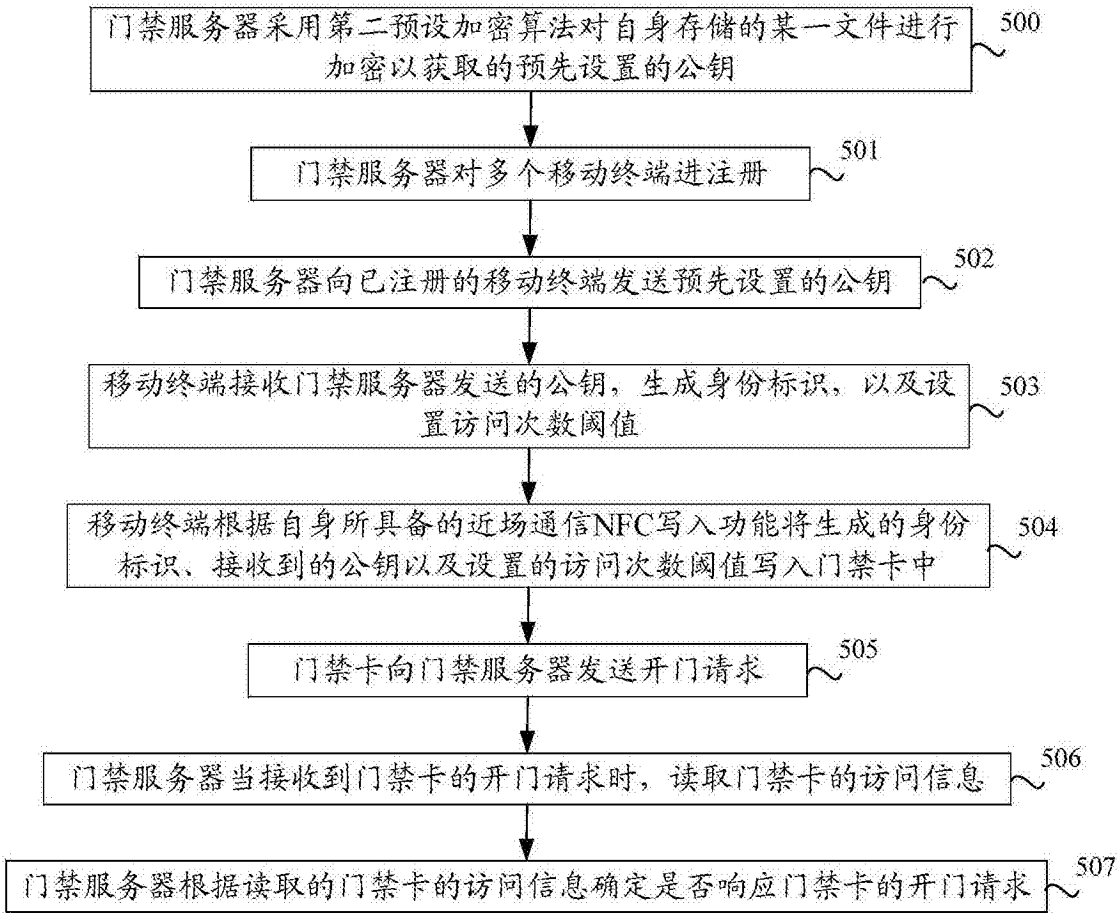

门禁服务器采用第二预设加密算法对自身存储的某一文件进行加密以获取的预先设置的公钥
500
门禁服务器对多个移动终端进注册
501
门禁服务器向已注册的移动终端发送预先设置的公钥
502
移动终端接收门禁服务器发送的公钥，生成身份标识，以及设置访问次数阈值
503
移动终端根据自身所具备的近场通信NFC写入功能将生成的身份标识、接收到的公钥以及设置的访问次数阈值写入门禁卡中
504
门禁卡向门禁服务器发送开门请求
505
门禁服务器当接收到门禁卡的开门请求时，读取门禁卡的访问信息
506
门禁服务器根据读取的门禁卡的访问信息确定是否响应门禁卡的开门请求
507

图5

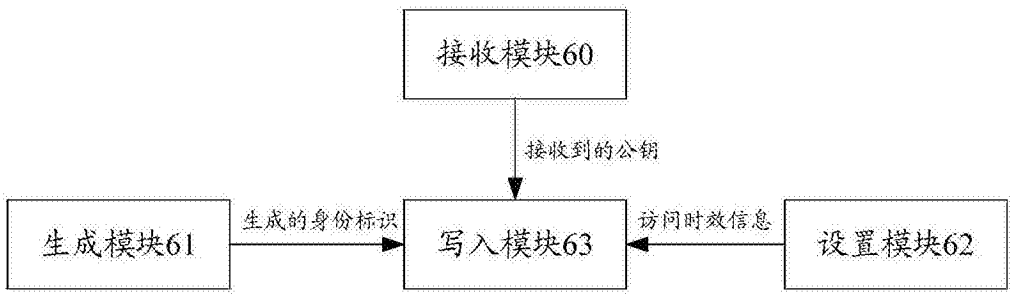

接收模块60
接收到的公钥
生成模块61
生成的身份标识
写入模块63
访问时效信息
设置模块62

图6

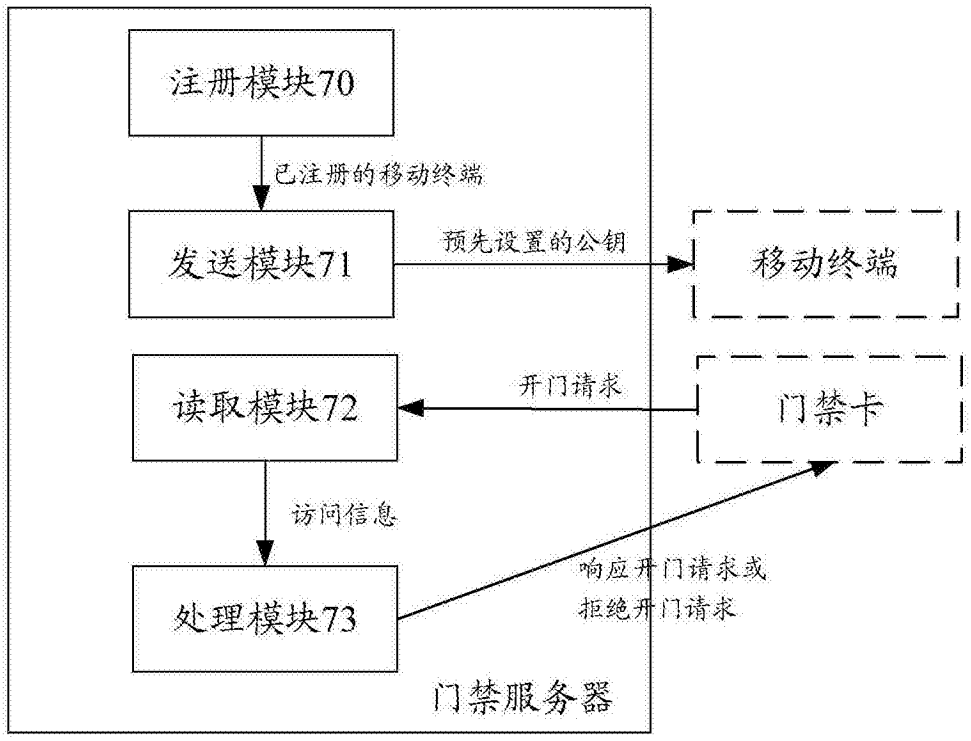

注册模块70
已注册的移动终端
发送模块71
预先设置的公钥
移动终端
读取模块72
开门请求
门禁卡
访问信息
处理模块73
响应开门请求或
拒绝开门请求
门禁服务器

图7