[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610115076.4

[43] 公开日 2008 年 2 月 27 日

[11] 公开号 CN 101131720A

[22] 申请日 2006.8.23
[21] 申请号 200610115076.4
[71] 申请人 联想（北京）有限公司
地址 100085 北京市海淀区上地信息产业基地创业路 6 号
[72] 发明人 于辰涛

[74] 专利代理机构 北京银龙知识产权代理有限公司
代理人 陈 振

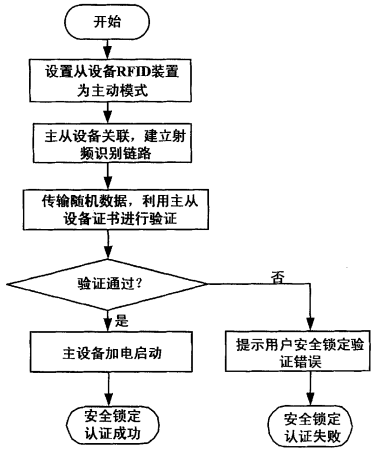
权利要求书 4 页 说明书 14 页 附图 3 页

[54] 发明名称

一种射频识别的计算机安全锁定认证系统和方法

[57] 摘要

本发明公开了一种射频识别的计算机安全锁定认证系统和方法。 该系统包括主设备计算机和从设备移动终端，其中主设备计算机包括安全锁定控制器和第一射频识别装置；从设备移动终端包括第二射频识别装置，所述第一射频识别装置包括第一射频识别安全锁定认证单元，其与安全锁定控制器相连，用于与从设备移动终端在射频识别链路上交互，利用主设备证书与从设备移动终端进行安全锁定认证；所述第二射频识别装置包括第二射频识别安全锁定认证单元，用于与主设备计算机在射频识别链路上交互，通过从设备证书与主设备计算机进行安全锁定认证，控制计算机电源开关休眠状态的安全锁定。 其能够方便地进行计算机的安全锁定认证。



1．一种射频识别的计算机安全锁定认证系统，包括主设备计算机和从设备移动终端，其中：

主设备计算机包括计算机主板，计算机电源，安全锁定控制器和第一射频识别装置；从设备移动终端包括移动终端主板，移动终端电源和第二射频识别装置，其特征在于：

所述第一射频识别装置包括第一射频识别安全锁定认证单元，其与安全锁定控制器相连，用于与从设备移动终端在射频识别链路上交互，利用主设备证书与从设备移动终端进行安全锁定认证；

所述第二射频识别装置包括第二射频识别安全锁定认证单元，用于与主设备计算机在射频识别链路上交互，通过从设备证书与主设备计算机进行安全锁定认证，控制计算机电源开关休眠状态的安全锁定。

2．根据权利要求1所述的射频识别的计算机安全锁定认证系统，其特征在于，所述安全锁定控制器是嵌入式控制器，集成到主设备计算机的主板及电源间的计算机电源控制电路上，对计算机的电源开关休眠状态进行控制。

3．根据权利要求2所述的射频识别的计算机安全锁定认证系统，其特征在于，所述开关休眠状态包括计算机的加电启动，待机启动，进入休眠状态，从休眠状态中唤醒中的一种或者一种以上的组合。

4．根据权利要求2所述的射频识别的计算机安全锁定认证系统，其特征在于，所述安全锁定控制器还包括安全锁定模式控制单元，用于设定主设备计算机的安全锁定控制模式。

5．根据权利要求4所述的射频识别的计算机安全锁定认证系统，其特征在于，所述的安全锁定启动模式，包括正常启动模式，密码分发模式，射频识别安全锁定模式。

6．根据权利要求1或2或4所述的射频识别的计算机安全锁定认证系统，其特征在于，所述主设备证书包括证书有效期，证书唯一性标识，主设备唯一性标识，从设备验证密钥；所述从设备证书包括证书有效期，证书唯一性标识，从设备唯一性标识，主设备验证密钥。

7. 根据权利要求1或2或4所述的射频识别的计算机安全锁定认证系统，其特征在于，所述第一射频识别装置和第二射频识别装置还包括工作模式设定单元，用于控制设定主设备计算机第一射频识别装置和从设备移动终端的第二射频识别装置的工作模式为主动模式或者被动模式。

8. 根据权利要求7所述的射频识别的计算机安全锁定认证系统，其特征在于，所述第一射频识别装置和第二射频识别装置还包括保存单元，用于保存主设备证书和从设备证书，并在射频识别认证过程中，将主设备证书提供给第一射频识别安全锁定认证单元，将从设备证书提供给第二射频识别安全锁定认证单元进行安全锁定认证。

9. 根据权利要求8所述的射频识别的计算机安全锁定认证系统，其特征在于，所述第一射频识别安全锁定认证单元包含多个对应一个或多个从设备移动终端的一个或多个主设备证书；第二射频识别安全锁定认证单元包含多个对应一个或多个主设备计算机的一个或多个从设备证书。

10. 根据权利要求8所述的射频识别的计算机安全锁定认证系统，其特征在于，所述的第一射频识别装置和第二射频识别装置还包括的射频识别访问单元，用于射频识别装置进行通讯，完成数据传输通信工作。

11. 一种射频识别的计算机安全锁定认证方法，其特征在于，包括下列步骤：

步骤 A）主设备计算机第一射频识别装置与从设备移动终端的第二射频识别装置关联，建立射频识别通信链路时，利用主设备证书和从设备证书进行安全锁定验证并确认后，安全锁定控制器控制计算机电源开关休眠状态。

12. 根据权利要求11所述的计算机安全锁定认证方法，其特征在于，所述步骤A）之前还包括下列步骤：

步骤A1′）安全锁定控制器设定主设备计算机在正常启动模式下启动，第一射频识别装置生成主设备证书和从设备证书，安全锁定控制器设定主设备计算机为密码分发模式；

步骤A2′）当主设备计算机的第一射频识别装置与从设备移动终端第二射频识别装置关联，建立射频识别通信链路时，第一射频识别装置和第二射频识别装置之间交互，交换从设备证书给从设备移动终端，并获取和保存从

设备移动终端信息，安全锁定控制器设置主设备计算机的启动模式为射频识别安全锁定模式。

13．根据权利要求 12 所述的计算机安全锁定认证方法，其特征在于，所述步骤 A）包括下列步骤：

步骤 A1）在主设备计算机设置了射频识别安全锁定模式后，启动主设备计算机时，在从设备移动终端移动到离主设备计算机足够近的距离时，主设备计算机的第一射频识别装置与从设备移动终端的第二射频识别装置关联，建立射频识别通信链路；

步骤 A2）主从设备之间在无线射频识别链路上，利用主设备证书和从设备证书进行安全锁定验证，进行主设备安全锁定认证确认，然后安全锁定控制器控制计算机电源开关休眠状态。

14．根据权利要求 13 所述的计算机安全锁定认证方法，其特征在于，所述步骤 A2）包括下列步骤：

步骤 A21）由从设备移动终端的第二射频识别装置生成第一随机数据，并将第一随机数据在射频识别通信链路上发送给主设备计算机；

步骤 A22）主设备计算机中的第一射频识别装置收到第一随机数据后，使用主设备证书中的从设备验证密钥通过对第一随机数据加密并签名，将加密签名的第一随机数据传回从设备移动终端；

步骤 A23）从设备移动终端的第二射频识别装置收到主设备计算机传来的加密签名第一随机数据后，使用从设备证书中的主设备验证密钥验证签名并解密，比较确认主设备计算机验证通过。

15．根据权利要求 14 所述的计算机安全锁定认证方法，其特征在于，所述步骤 A22）还包括下列步骤：

主设备计算机中的第一射频识别装置生成向从设备移动终端发送的第二随机数据；

所述步骤 A23）之后还包括下列步骤：

步骤 A24）从设备移动终端的第二射频识别装置使用从设备证书中的主设备验证密钥对所述第二随机数加密并签名，并将加密签名的第二随机数据传回主设备计算机；

步骤 A25）主设备计算机的第一射频识别装置使用主设备证书中的从设备验证密钥所述加密签名的第二随机数据验证签名并解密，比较确认；并在比较主设备计算机发出加密签名的第一随机数据和从设备发传送回来的加密签名的第一随机数据后确认从设备验证通过。

16．根据权利要求 15 所述的计算机安全锁定认证方法，其特征在于，所述步骤 A25）后还包括下列步骤：

步骤 A26）主从设备的双端验证完成，主设备计算机启动后，主设备计算机进行计算机平台进行完整性检验，主设备计算机和第一射频识别装置建立的通信传输链路相互访问数据，主设备计算机的主板 BIOS 能够确认主设备计算机的安全锁定认证加电复位动作由第一射频识别装置发出。

17．根据权利要求 11 至 16 中任一项所述的计算机安全锁定认证方法，其特征在于，所述开关休眠状态包括计算机的加电启动，待机启动，进入休眠状态，从休眠状态中唤醒中的一种或者一种以上的组合。

18．根据权利要求 17 所述的计算机安全锁定认证方法，其特征在于，所述的安全锁定启动模式，包括正常启动模式，密码分发模式，射频识别安全锁定模式。

19．根据权利要求 18 所述的计算机安全锁定认证方法，其特征在于，所述主设备证书包括证书有效期，证书唯一性标识，主设备唯一性标识，从设备验证密钥；所述从设备证书包括证书有效期，证书唯一性标识，从设备唯一性标识，主设备验证密钥。

20．根据权利要求 19 所述的计算机安全锁定认证方法，其特征在于，所述密钥为 RSA、Diffie-Hellman、ECC 算法中的公私钥对。

21．根据权利要求 19 所述的计算机安全锁定认证方法，其特征在于，所述密钥为 DES、3DES、IDEA、RC4、RC5、AES 算法中的共享对称密钥。

一种射频识别的计算机安全锁定认证系统和方法

技术领域

本发明涉及安全认证技术，特别是涉及一种射频识别的非接触式计算机安全锁定认证系统和方法。

背景技术

随着 RFID（Radio Frequency Identification，射频识别）和 NFC（Near Field Communication，近距离射频通讯）等非接触式射频识别技术的发展，越来越多的移动设备开始增加非接触式芯片的功能，以完成购物、电子购票、小额电子支付、移动终端间数据交换和门禁等功能。

非接触式射频识别终端使得无需用户任何设置的移动终端间数据交换成为可能，此时，用户只需将两个移动终端靠近，由终端自动进行双端的认证和协商，然后就可以完成设备间数据交换的复杂任务。

NFC 属于下一代射频识别技术，它遵循现有的 ISO14443 和 ISO18092 技术标准，它可在具备 NFC 功能的任意两个设备间实现信息交互、读取内容和获得服务。NFC 技术支持三种主要应用，包括移动支付与交易、对等式通信及移动中信息访问等。

欧洲专利局专利公开号：EP1501038 公开了一种手持终端，包括一个 NFC 设备，一个写按钮和一个读按钮。为了将存储到手持终端中的信息写入一个信息提供设备，用户可以将手持终端靠近信息提供设备。为了将存储在信息存储设备中的信息读入到手持设备中，用户可以将手持终端靠近信息提供设备。

现有移动终端的射频识别设备既可以工作在主动模式下，也可以工作在被动模式下。当工作在主动模式下时，其需要一个电源对移动终端设备进行供电，由此产生非接触式设备的射频能量场，其相当于一个射频识别读卡器；当工作在被动模式下时，射频识别设备仿真成为射频标签（如 IC 卡），此时不需要任何外部供电或较低的外部电流，其接受主设备的射频识别信号，由

外部设备感应电压进行工作，并通过感应完成主从设备间的应用功能交换，其相当于一个射频识别标签。

随着世界各地各厂商的推动，在日本已经有超过 10%的移动终端（如手机）带有非接触射频识别功能。

目前，在笔记本计算机或者台式个人计算机（PC）存在很多安全开机和计算机锁定方法，比如用 USB key，智能卡，专有的计算机钥匙等，这些安全锁定方法增加了计算机的安全性。然而，这些方法需要特殊的设备支持，用户携带非常不方便，而且设备遗失之后，重新配置非常麻烦。

现有的另一种方法是通过蓝牙手机对笔记本计算机的安全锁定，进行管理的方法，但是，此方法只能在计算机开机状态下解决计算机安全锁定的问题，使用不方便，受到很多的限制，很难在市场上得到推广应用。

发明内容

本发明的目的在于提供一种射频识别的计算机安全锁定认证系统和方法，其解决了计算机安全锁定过程中锁定设备不方便携带，使用不便而受到限制等问题。

为实现本发明目的而提供的一种射频识别的计算机安全锁定认证系统，包括主设备计算机和从设备移动终端，其中：

主设备计算机包括计算机主板，计算机电源，安全锁定控制器和第一射频识别装置；从设备移动终端包括移动终端主板，移动终端电源和第二射频识别装置：

所述第一射频识别装置包括第一射频识别安全锁定认证单元，其与安全锁定控制器相连，用于与从设备移动终端在射频识别链路上交互，利用主设备证书与从设备移动终端进行安全锁定认证；

所述第二射频识别装置包括第二射频识别安全锁定认证单元，用于与主设备计算机在射频识别链路上交互，通过从设备证书与主设备计算机进行安全锁定认证，控制计算机电源开关休眠状态的安全锁定。

所述安全锁定控制器是嵌入式控制器，集成到主设备计算机的主板及电源间的计算机电源控制电路上，对计算机的电源开关休眠状态进行控制。

所述安全锁定控制器还包括安全锁定模式控制单元，用于设定主设备计

算机的安全锁定控制模式。

所述第一射频识别装置和第二射频识别装置还包括工作模式设定单元，用于控制设定主设备计算机第一射频识别装置和从设备移动终端的第二射频识别装置的工作模式为主动模式或者被动模式。

所述第一射频识别装置和第二射频识别装置还包括保存单元，用于保存主设备证书和从设备证书，并在射频识别认证过程中，将主设备证书提供给第一射频识别安全锁定认证单元，将从设备证书提供给第二射频识别安全锁定认证单元进行安全锁定认证。

所述第一射频识别安全锁定认证单元包含多个对应一个或多个从设备移动终端的一个或多个主设备证书；第二射频识别安全锁定认证单元包含多个对应一个或多个主设备计算机的一个或多个从设备证书。

所述的第一射频识别装置和第二射频识别装置还包括的射频识别访问单元，用于射频识别装置进行通讯，完成数据传输通信工作。

为实现本发明目的还提供了一种射频识别的计算机安全锁定认证方法，包括下列步骤：

步骤 A）主设备计算机第一射频识别装置与从设备移动终端的第二射频识别装置关联，建立射频识别通信链路时，利用主设备证书和从设备证书进行安全锁定验证并确认后，安全锁定控制器控制计算机电源开关休眠状态。

所述步骤 A）之前还包括下列步骤：

步骤 A1′）安全锁定控制器设定主设备计算机在正常启动模式下启动，第一射频识别装置生成主设备证书和从设备证书，安全锁定控制器设定主设备计算机为密码分发模式；

步骤 A2′）当主设备计算机的第一射频识别装置与从设备移动终端第二射频识别装置关联，建立射频识别通信链路时，第一射频识别装置和第二射频识别装置之间交互，交换从设备证书给从设备移动终端，并获取和保存从设备移动终端信息，安全锁定控制器设置主设备计算机的启动模式为射频识别安全锁定模式。

所述步骤 A）包括下列步骤：

步骤 A1）在主设备计算机设置了射频识别安全锁定模式后，启动主设备

计算机时，在从设备移动终端移动到离主设备计算机足够近的距离时，主设备计算机的第一射频识别装置与从设备移动终端的第二射频识别装置关联，建立射频识别通信链路；

步骤 A2）主从设备之间在无线射频识别链路上，利用主设备证书和从设备证书进行安全锁定验证，进行主设备安全锁定认证确认，然后安全锁定控制器控制计算机电源开关休眠状态。

所述步骤 A2）包括下列步骤：

步骤 A21）由从设备移动终端的第二射频识别装置生成第一随机数据，并将第一随机数据在射频识别通信链路上发送给主设备计算机；

步骤 A22）主设备计算机中的第一射频识别装置收到第一随机数据后，使用主设备证书中的从设备验证密钥通过对第一随机数据加密并签名，将加密签名的第一随机数据传回从设备移动终端；

步骤 A23）从设备移动终端的第二射频识别装置收到主设备计算机传来的加密签名第一随机数据后，使用从设备证书中的主设备验证密钥验证签名并解密，比较确认主设备计算机验证通过。

所述步骤 A22）还包括下列步骤：

主设备计算机中的第一射频识别装置生成向从设备移动终端发送的第二随机数据；

所述步骤 A23）之后还包括下列步骤：

步骤 A24）从设备移动终端的第二射频识别装置使用从设备证书中的主设备验证密钥对所述第二随机数加密并签名，并将加密签名的第二随机数据传回主设备计算机；

步骤 A25）主设备计算机的第一射频识别装置使用主设备证书中的从设备验证密钥所述加密签名的第二随机数据验证签名并解密，比较确认；并在比较主设备计算机发出加密签名的第一随机数据和从设备发传送回来的加密签名的第一随机数据后确认从设备验证通过。

所述步骤 A25）后还包括下列步骤：

步骤 A26）主从设备的双端验证完成，主设备计算机启动后，主设备计算机进行计算机平台进行完整性检验，主设备计算机和第一射频识别装置建

立的通信传输链路相互访问数据，主设备计算机的主板 BIOS 能够确认主设备计算机的安全锁定认证加电复位动作由第一射频识别装置发出。

所述开关休眠状态包括计算机的加电启动，待机启动，进入休眠状态，从休眠状态中唤醒中的一种或者一种以上的组合。

所述的安全锁定启动模式，包括正常启动模式，密码分发模式，射频识别安全锁定模式。

所述主设备证书包括证书有效期，证书唯一性标识，主设备唯一性标识，从设备验证密钥；所述从设备证书包括证书有效期，证书唯一性标识，从设备唯一性标识，主设备验证密钥。

所述密钥为 RSA、Diffie-Hellman、ECC 算法中的公私钥对。

所述密钥为 DES、3DES、IDEA、RC4、RC5、AES 算法中的共享对称密钥。

本发明的有益效果是：本发明的射频识别的计算机安全锁定认证系统和方法，在计算机和移动设备都具备射频识别（RFID）功能时，将移动设备的射频识别（RFID）芯片作为安全锁定钥匙，实现计算机的动态安全锁定。由于移动终端越来越成为人们生活中不可分割的一部分，本发明移动终端可以方便地替代现有的 USB key 和专有 IC 卡钥匙的安全功能，可以提高计算机安全锁定的安全性，而又无须修改硬件；其在主设备计算机不加电时，移动终端工作在射频识别主动工作模式，移动终端和主设备认证通过之后，也能方便地进行安全认证和开机的操作，同时，安全认证的数字设备证书由用户计算机定制，便于用户管理，既方便而使用中又不受限制。

附图说明

图 1 为本发明射频识别的计算机安全锁定认证主设备计算机结构示意图；

图 2 为本发明射频识别的计算机安全锁定认证从设备移动终端结构示意图；

图 3 为本发明射频识别的计算机安全锁定认证方法中主从设备证书生成及交换过程流程图；

图 4 为本发明射频识别的计算机安全锁定认证方法中安全锁定认证过程

流程图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图 1~4 及实施例，对本发明的射频识别的计算机安全锁定认证系统和方法进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

本发明的射频识别的计算机安全锁定认证系统和方法，在主设备计算机具有第一射频识别装置和从设备移动终端具有第二射频识别装置的情况下，主设备计算机的第一射频识别装置在被动模式下工作，从设备移动终端的第二射频识别装置主动模式下。在安全锁定认证过程中，从设备移动终端的第二射频识别装置主动向主设备计算机的第一射频识别装置发出认证请求，在认证通过后，主设备计算机的第一射频识别装置发出系统加电信号，主设备计算机启动。

本发明的射频识别的计算机安全锁定认证系统包括主设备计算机和从设备移动终端。

本发明的主设备计算机指可以进行安全锁定认证的计算机设备，可以是笔记本计算机、个人计算机、服务器或者其他需要较高安全等级的计算机设备。

本发明的从设备移动终端指用于与主设备计算机交互，进行安全锁定认证的移动通信设备，其可以是手机、PDA、MP3、MP4 或者其他便携电子设备。

如图 1 所示，主设备计算机包括中央处理器（CPU），计算机主板，计算机电源，外围设备（如键盘等）等，本发明的主设备计算机还包括安全锁定控制器以及第一射频识别装置。

安全锁定控制器可以是嵌入式控制器（Embed Controller，EC）或者是南桥上的其他专有连接部件，其可以集成到主设备计算机的主板及电源间的计算机电源控制电路上，对计算机的电源开关休眠状态进行控制。

计算机电源开关休眠状态包括计算机的加电启动，待机启动，进入休眠状态，从休眠状态中唤醒等。

所述安全锁定控制器还包括安全锁定模式控制单元，用于设定主设备计算机的安全锁定控制模式。

较佳地，所述的安全锁定启动模式，可以包括正常启动模式，密码分发模式，射频识别安全锁定模式等。

当然，所述的安全锁定启动模式，也可以还包括 USB key 安全锁定模式，以及 IC 卡安全锁定模式等各种安全锁定模式等。

所述第一射频识别装置包括第一射频识别安全锁定认证单元，其与安全锁定控制器相连，用于与从设备移动终端在射频识别链路上交互，利用主设备证书与从设备移动终端进行安全锁定认证。

本发明实现的射频识别芯片控制安全锁定认证的主设备计算机，其将第一射频识别装置连接在主设备计算机的安全锁定控制器上。

本发明的第一射频识别装置工作在非常低的待机功耗，等待外部从设备移动终端上的第二射频识别装置通过射频识别连入的被动模式下。

如图 2 所示，从设备移动终端包括移动终端主板，移动终端电源，第二射频识别装置，其中：

所述第二射频识别装置包括第二射频识别安全锁定认证单元，用于与主设备计算机在射频识别链路上交互，通过从设备证书与主设备计算机进行安全锁定认证，控制计算机电源开关休眠状态的安全锁定。

所述第一射频识别装置和第二射频识别装置还包括工作模式设定单元，用于控制设定主设备计算机第一射频识别装置和从设备移动终端的第二射频识别装置的工作模式为主动模式或者被动模式。

当工作在主动模式下时，工作模式设定单元控制移动终端电源对第二射频识别装置进行供电，由此产生非接触式设备的射频能量场，其相当于一个射频识别读卡器；当工作在被动模式下时，工作模式设定单元控制第二射频识别装置仿真成为射频标签（如 IC 卡），此时不需要任何外部供电或较低的外部电流，其接受主设备计算机的射频识别信号，由外部设备感应电压进行工作，并通过感应完成主从设备间的应用功能交换，其相当于一个射频识别标签。

当主设备没有启动，从设备移动终端对主设备计算机进行加电启动安全

锁定认证时，工作模式设定单元控制第二射频识别装置在主动模式下工作，完成安全锁定认证工作；当主设备已经启动，从设备移动终端对主设备计算机只是在待机启动，进入休眠状态，从休眠状态中唤醒等，工作模式设定单元既可以控制第二射频装置在主动模式下工作，也可以在被动模式工作，完成安全锁定认证。

所述第一射频识别装置和第二射频识别装置还包括保存单元，用于保存主设备证书和从设备证书，并在射频识别认证过程中，将主设备证书提供给第一射频识别安全锁定认证单元，将从设备证书提供给第二射频识别安全锁定认证单元进行安全锁定认证。

保存单元保存设备证书，将设备证书的信息保存后，除射频识别安全锁定认证单元外，其他任何程序无法读取此从设备证书信息。

本发明实现的控制主设备计算机安全锁定认证的从设备移动终端，其通过工作模式设定单元，利用移动终端电源向第二射频识别装置供电，使第二射频识别装置在主动模式下工作，向主设备计算机的第一射频识别装置发射射频信号，建立射频识别链路，然后第二安全锁定认证单元和第一安全锁定认证单元在射频识别链路上利用第二射频识别装置的保存单元保存的从设备证书与主设备计算机的主设备证书交互，进行主设备计算机安全锁定认证。

本领域的普通技术人员可以理解，作为具有射频识别功能的能够进行安全锁定的主设备计算机和从设备移动终端，本发明所述的第一射频识别装置和第二射频识别装置还包括现有公知的射频识别访问单元，用于和第一射频识别装置进行通讯，完成数据传输通信工作，其所遵循的现有国际标准可以是射频标签标准，包括 SONY Felica、ISO/IEC 14443 TYPE A、ISO/IEC 14443 TYPE B、ISO/IEC15693、ISO18092、ISO18000－3，在本发明中，引用这些标准，不再一一赘述。

在主设备计算机和从设备移动终端在进行加电启动安全锁定认证时，从设备移动终端的工作模式控制单元将从设备移动终端的第二射频识别装置控制为主动工作模式，通过通常的射频通讯协议建立射频链路，在安全锁定控制器的安全锁定模式控制单元设定主设备计算机为射频识别安全锁定模式时，第二安全锁定认证单元与主设备的第一射频识别装置中的第一安全锁定

认证单元在访问单元建立的射频识别链路上进行安全锁定认证，在安全认证通过后，第一射频识别装置向安全锁定控制器发送认证通过命令，安全锁定控制器通知计算机加锁或者解锁，控制控制计算机电源开关休眠状态的安全锁定。

同样，主设备计算机在待机启动状态，进入休眠状态，从休眠状态中唤醒时，也通过第二射频识别装置向第一射频识别装置发出认证请求而得到安全锁定认证后加锁或者解锁主设备计算机。

因此，在本发明实施例中，只以在计算机没有开启状态下，主设备计算机和从设备移动终端利用射频识别装置进行安全锁定认证，实现主设备计算机安全锁定认证后的安全加电开启的过程，对其他计算机电源开关休眠状态的安全锁定，其安全锁定认证过程与加电过程相同，本发明中不再一一赘述。

本发明移动终端替代现有的 USB key 和专有钥匙的安全锁定认证功能，提高计算机安全锁定的安全性，既方便又无须对硬件做大的改动；其在主设备计算机不加电时，也能方便地进行安全认证和开机的操作。

如图 3 和图 4 所示，下面详细说明本发明的非接触式计算机安全锁定方法：

步骤 1：安全锁定控制器设定主设备计算机在正常启动模式下启动，然后第一射频识别装置生成主设备证书和从设备证书，安全锁定控制器设定主设备计算机为密码分发模式。

然后，在主设备计算机启动之后，主设备计算机的第一射频识别装置生成主设备证书和从设备证书。

较佳地，主设备证书包括证书有效期，证书唯一性标识，主设备唯一性标识，从设备验证密钥。

从设备证书包括证书有效期，证书唯一性标识，从设备唯一性标识，主设备验证密钥。

主设备和从设备验证密钥可以采用非对称密钥的公私钥对，或者共享的对称密钥。

主设备和从设备验证密钥所采用的加密算法，由生产厂商分别预置在主设备计算机和从设备移动终端中。

因此，本发明主设备和从设备验证密钥可以是非对称算法密钥对中的密钥，如 RSA 算法（是基于数论的公钥密码体制，由 Rivest、Shamir 与 Adleman 三人合作开发，因此叫 RSA 算法）、Diffie-Hellman 算法、ECC（Elliptic Curves Cryptography）或其他非对称密钥算法的非对称密钥，所述加密算法的认证密钥对由该算法的密钥中心生成或者预存。

认证密钥根据设备情况也可以选择对称密钥算法，如 DES（Data Encryption Standard）、3DES、IDEA（IDEA（International Data Encryption Algorithm，国际数据加密算法）、RC4、RC5、AES（Advanced Encryption Standard，高级加密标准）或者其他对称密钥算法的密钥，此时认证密钥为一个随机数或变换产生。

如果采用非对称密钥方式，从设备证书验证密钥将包含从设备公钥和主设备私钥；主设备证书验证密钥将包含主设备公钥和从设备私钥。

本发明实施例中，采用非对称密钥方式，对主设备计算机和从设备移动终端的安全锁定认证过程进行详细描述，对对称密钥方式，其过程基本相同，因此本发明实施例中不再一一赘述。

较佳地，主设备证书和从设备证书生成后，设备证书的信息保存后，其他任何程序无法读取此主设备证书和从设备证书。在发现从设备移动终端丢失或损坏时，主设备计算机可以删除和更新第一射频识别装置内部保存主设备证书。在主设备证书和从设备证书的证书有效期到达时，主设备计算机和从设备移动终端将收到射频识别装置的证书更新通知，并提示用户重复证书生成过程进行设备证书更新。

在设备证书生成之后，主设备计算机的第一射频识别装置设置到密码分发模式，此时主设备计算机将等待从设备移动终端的关联请求。

步骤 2：当主设备计算机的第一射频识别装置与从设备移动终端第二射频识别装置关联，建立射频识别通信链路时，第一射频识别装置和第二射频识别装置之间交互，交换从设备证书给从设备移动终端，并获取和保存从设备移动终端信息，安全锁定控制器设置主设备计算机的启动模式为射频识别安全锁定模式。

从设备移动终端移动到足够近的距离时，主设备计算机的第一射频识别

装置接收到从设备移动终端的第二射频识别装置主动发射的射频信号，通过公知（如通常的ISO/IEC 14443 TYPE A/B、ISO18092、ISO/IEC15693、ISO18000—3 等协议技术标准）的交互，建立射频识别通信链路，建立关联。

在从设备移动终端与主设备计算机关联之后，主设备计算机第一射频识别装置传递主设备证书给从设备移动终端的第二射频识别装置，从设备移动终端第二射频识别装置将移动终端信息（如设备信息或用户信息）传递到主设备计算机。主设备计算机会保存移动终端信息，用于在从设备移动终端丢失和损坏时，通过再次与新的从设备移动终端相关联，重新恢复从设备证书。

从设备移动终端的第二射频识别装置保存主设备验证证书，用于对主设备计算机进行安全锁定认证。

主设备计算机可以保存对应多个不同从设备移动终端的主设备证书，从设备移动终端也可以保存对应多个主设备计算机的从设备证书。主从设备使用设备标识区分对应的设备。用户可以将从设备证书加密保存在其它设备上，比如 USB key 或特殊的服务器上，便于在移动设备遗失或损坏时，方便的恢复用户开机功能。

如果主设备计算机有多个对应不同从设备移动终端的主设备证书，从设备移动终端有对应多个主设备计算机的从设备证书时，其通过不同的标识识别的主从设备证书。

主设备计算机的安全锁定控制器设置主设备计算机的安全锁定方式为射频识别安全锁定模式。

主设备计算机的安全锁定控制器可以在射频识别安全锁定模式下通过安全锁定认证，启动主设备计算机，然后将其启动模式改变为其他模式，如正常启动模式，密码分发模式或者 USB key 安全锁定模式。

在设置主设备计算机为射频识别安全锁定模式之后，主设备计算机的安全锁定控制器控制计算机的主板和电源或与加电相关的单元，使主设备计算机在不接受射频识别认证成功的指令，则主设备计算机无法加电启动。

步骤 3：主设备计算机第一射频识别装置与从设备移动终端的第二射频识别装置关联，建立射频识别通信链路时，利用主设备证书和从设备证书进行安全锁定验证并确认后，安全锁定控制器控制计算机电源开关休眠状态为

主设备计算机加电启动。

步骤31：如图4所示，在主设备计算机设置了射频识别安全锁定模式后，启动主设备计算机时，在从设备移动终端移动到离主设备计算机足够近的距离时，主设备计算机的第一射频识别装置在被动模式下，接收到从设备移动终端的第二射频识别装置在主动模式下主动发射的射频信号，通过公知（如ISO/IEC 14443 TYPE A/B、ISO/IEC15693、ISO18092、ISO18000－3技术标准）的交互关联，建立射频识别通信链路。

步骤32：主从设备之间在无线射频识别链路上，利用主设备证书和从设备证书进行安全锁定验证，进行主设备安全锁定认证确认，然后安全锁定控制器控制计算机电源开关休眠状态为主设备计算机加电启动。

从设备移动终端的第二射频识别装置启动一个使用交换的验证密钥进行三次验证过程，如图3所示：

步骤321：由从设备移动终端的第二射频识别装置生成随机数RandomA，并将随机数RandomA在射频识别通信链路上发送给主设备计算机；

步骤322：主设备计算机中的第一射频识别装置收到随机数RandomA后，使用主设备证书中的从设备公钥通过非对称加密签名算法对随机数RandomA加密，并用主设备证书中的主设备私钥对随机数RandomA签名，形成签名TokenA，同时生成向从设备移动终端发送的另一个随机数据RandomB，将这三个数据一起传回从设备移动终端；

步骤323：从设备移动终端的第二射频识别装置收到主设备计算机传来的数据后，使用从设备证书中的主设备公钥对签名TokenA利用相应的非对称加密算法进行验证确认，然后使用从设备证书中的从设备私钥利用相应的非对称加密算法进行解密，得到解密结果随机数RandomA，比较解密结果与随机数RandomA相等后确认主设备计算机验证通过。

步骤324：从设备移动终端的第二射频识别装置使用从设备证书中的主设备公钥对随机数RandomB利用非对称加密算法加密，并使用从设备私钥对随机数RandomB签名，形成签名TokenB，并将加密结果和签名TokenB及签名数据TokenA这三个数据一起传回主设备计算机；

步骤325：主设备计算机的第一射频识别装置使用主设备证书中的从设

备公钥对 TokenB 利用相应的非对称算法验证确认，然后用主设备私钥对从从设备移动终端接收到的加密结果利用相应的非对称加密算法进行解密，得到解密结果，比较解密结果与随机数 RandomB 相等后确认

同时，比较发出签名数据 TokenA 和收到的签名数据 TokenA 是否相等，如果相等则确认从设备验证通过。

如果上述验证过程全部完成，则主从设备的双端验证完成，则从设备移动终端向主设备计算机发出加电启动指令，主设备计算机的第一射频识别装置接收到指令后，向主设备计算机的安全锁定控制器发出加电启动指令，主设备计算机加电启动操作系统。

步骤 326：如果主从设备的双端验证完成，主设备计算机启动后，主设备计算机进行计算机平台进行完整性检验，确认第一射频识别装置与系统连接，并且主设备计算机和第一射频识别装置能够通过射频协议建立的通信传输链路相互访问数据，同时主设备计算机的主板 BIOS 能够确认主设备计算机的安全锁定认证加电复位动作由第一射频识别装置发出。

在本发明方法中，如果任何一步骤验证比较结果为否，则终止主从设备的安全锁定认证。

需要说明的是，当主设备计算机在启动状态，主设备计算机和从设备移动终端建立射频识别链路，交互而进行安全锁定认证的加锁或者解锁主设备计算机的过程中，主设备计算机的第一射频识别装置可以在主动模式下，即作为射频识别读卡器；而相应地，从设备移动终端工作在被动模式下，即作为射频识别标签，建立射频识别通信链路，进行安全锁定认证的加锁和解锁。此时，用户可以设定安全锁定的级别，可以进行操作系统的锁定、计算机关机锁定和屏幕锁定等。

本发明的射频识别的计算机安全锁定认证系统和方法，在计算机和移动设备都具备射频识别功能时，将移动设备的射频识别芯片作为安全锁定钥匙，实现计算机的动态安全锁定。由于移动终端越来越成为人们生活中不可分割的一部分，本发明移动终端可以方便地替代现有的 USB key 和专有钥匙的安全功能，可以提高计算机安全锁定的安全性，而又无须修改硬件；其在主设备计算机不加电时，也能方便地进行安全认证和开机的操作，同时，安全认

证的数字设备证书由用户计算机定制，便于用户管理，既方便而使用中又不受限制。

本实施例是为了更好地理解本发明进行的详细的描述，并不是对本发明所保护的范围的限定，因此，本领域普通技术人员不脱离本发明的主旨未经创造性劳动而对本发明所做的改变在本发明的保护范围内。

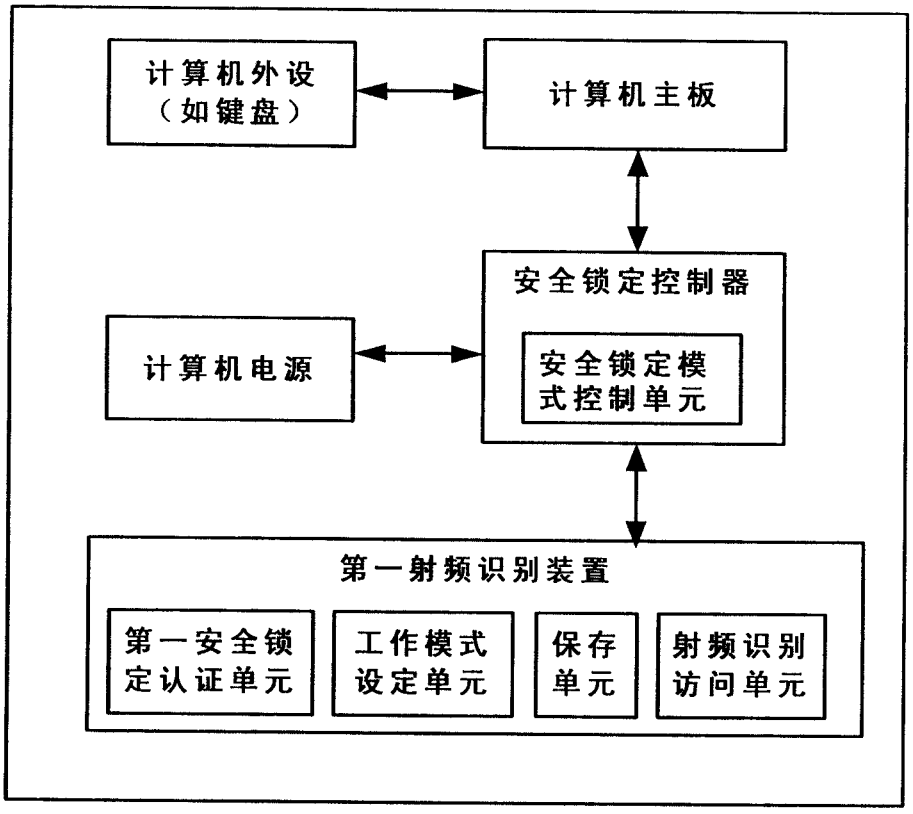

计算机外设
（如键盘）
计算机主板
安全锁定控制器
计算机电源
安全锁定模式控制单元
第一射频识别装置
第一安全锁定认证单元
工作模式设定单元
保存单元
射频识别访问单元

图 1

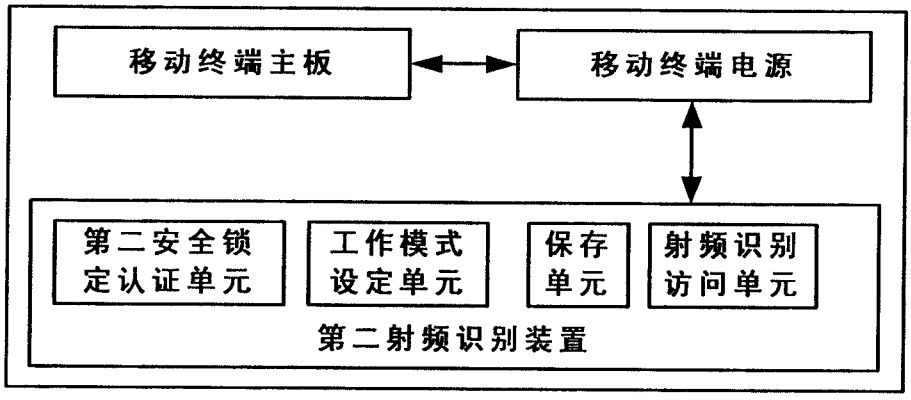

移动终端主板
移动终端电源
第二安全锁定认证单元
工作模式设定单元
保存单元
射频识别访问单元
第二射频识别装置

图 2

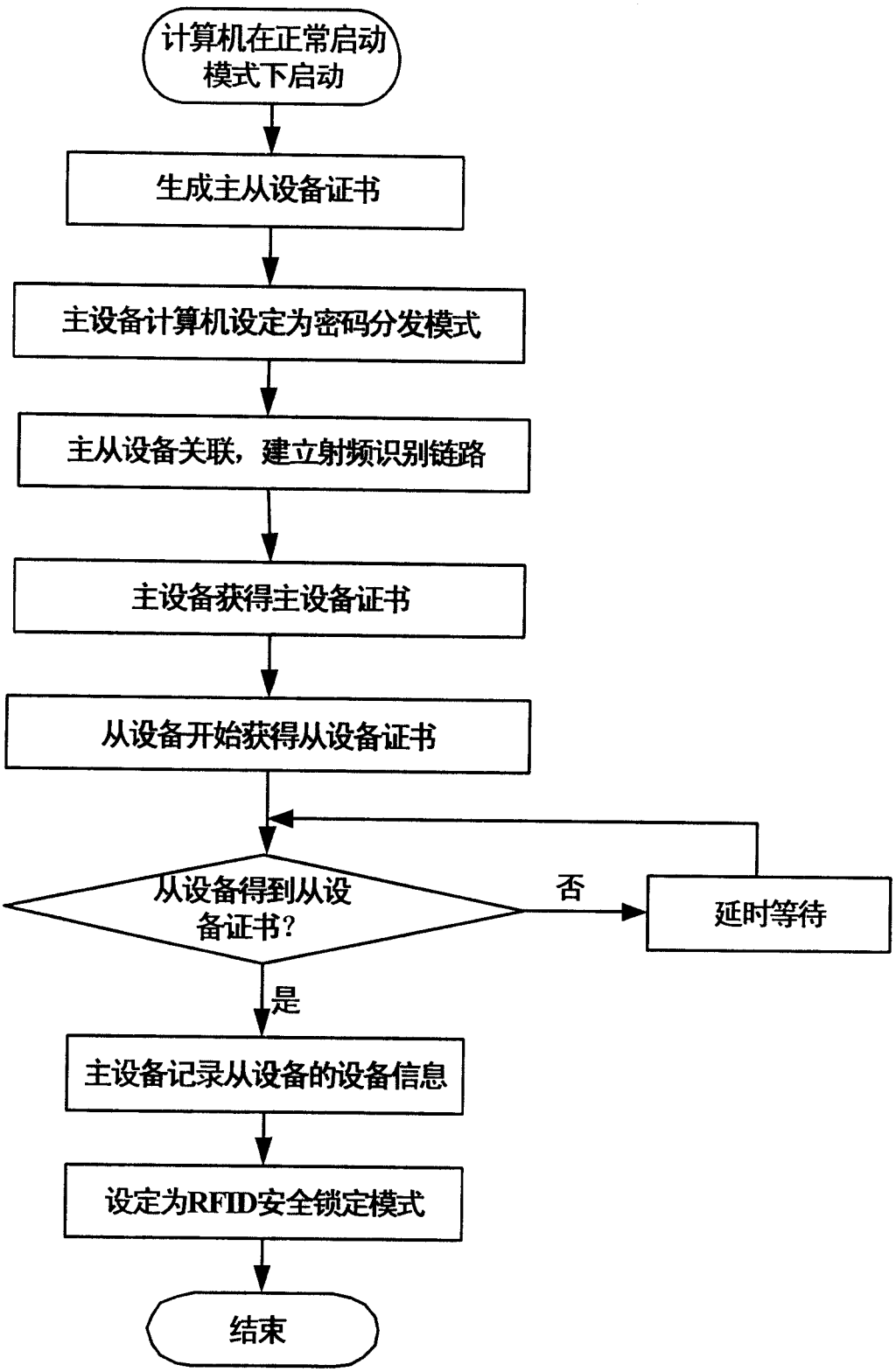

计算机在正常启动模式下启动
生成主从设备证书
主设备计算机设定为密码分发模式
主从设备关联，建立射频识别链路
主设备获得主设备证书
从设备开始获得从设备证书
从设备得到从设备证书?
否
延时等待
是
主设备记录从设备的设备信息
设定为RFID安全锁定模式
结束

图 3

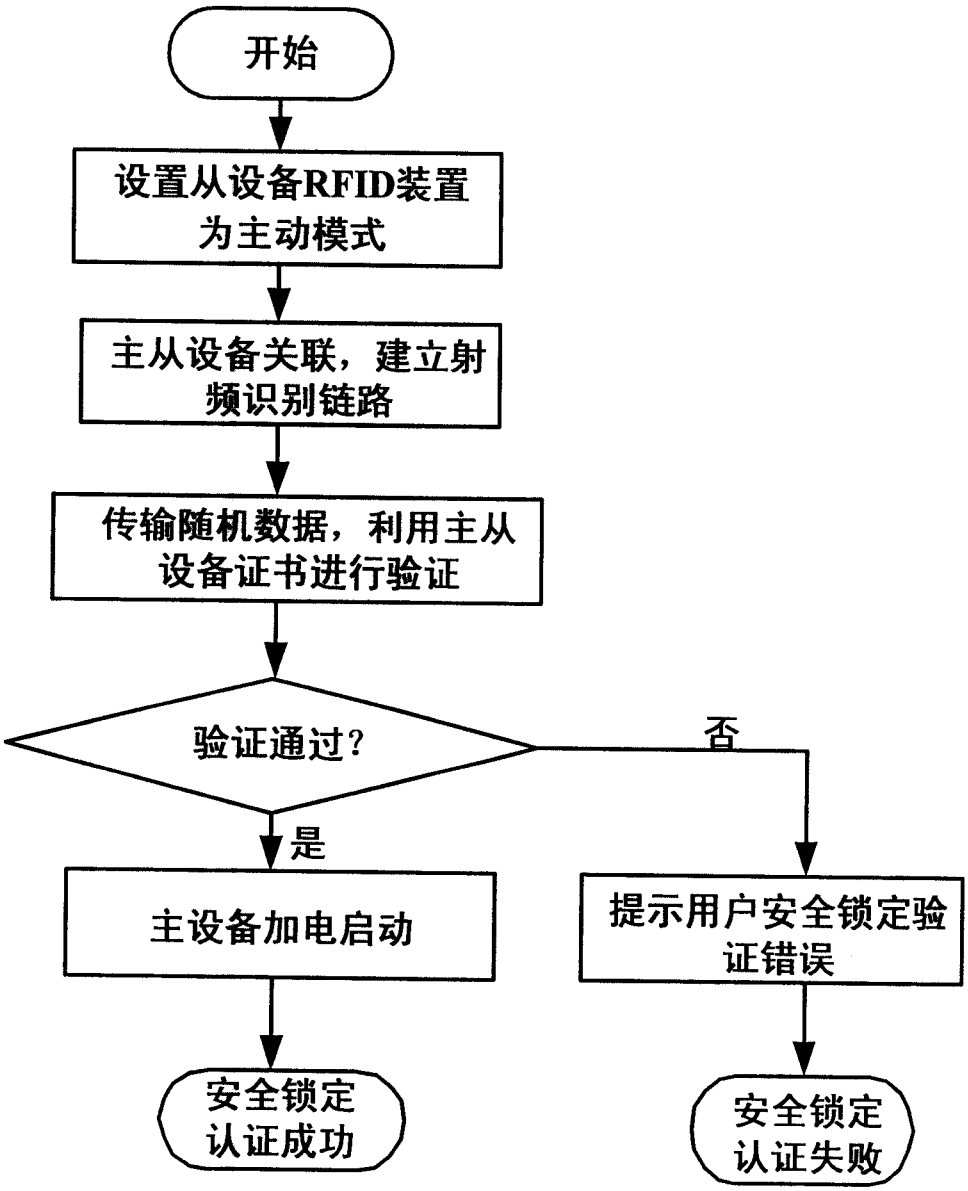

开始
设置从设备RFID装置为主动模式
主从设备关联，建立射频识别链路
传输随机数据，利用主从设备证书进行验证
验证通过？
否
是
主设备加电启动
提示用户安全锁定验证错误
安全锁定认证成功
安全锁定认证失败

图 4