(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 101770552 B
(45)授权公告日 2012.07.04

(21)申请号 200810247043.4

(22)申请日 2008.12.31

(73)专利权人 北京联想软件有限公司
地址 100085 北京市海淀区信息产业基地创业路6号4层

(72)发明人 徐琳

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 逯长明

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

(56)对比文件
US 5060263 A,1991.10.22,
CN 1750458 A,2006.03.22,

审查员 胡丽丽

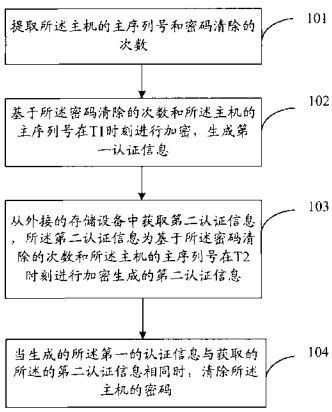
权利要求书 1 页 说明书 8 页 附图 7 页

(54)发明名称

清除计算机密码的方法及装置

(57)摘要

本发明实施例涉及一种不需要客服部门参与,用户自己可以在家生成认证文件,并根据该认证文件清除或者重置计算机密码的方法和设备及其系统。用户在设置计算机密码时,提示用户生成一个认证文件,当以后用户密码丢失时,可以通过一种特别的方式登录计算机并提供当初生成的认证文件,当认证文件通过验证后即允许用户清除或者重设该计算机的密码。以及在用户成功清除或者重设密码以后,可以选择重新生成认证文件。本发明实施例在一定程度上降低了售后成本,保证了系统的安全性。



CN 101770552 B

1. 一种清除计算机密码的方法，其特征在于，在 BIOS 检测到用户启动密码清除流程时，所述方法包括：

提取所述主机的主序列号和密码清除的次数；

基于所述密码清除的次数和所述主机的主序列号在 T1 时刻进行加密，生成第一认证信息；

从外接的存储设备中获取第二认证信息，所述第二认证信息为基于所述密码清除的次数和所述主机的主序列号在 T2 时刻进行加密生成的第二认证信息；所述 T2 时刻早于所述 T1 时刻；

当生成的所述第一认证信息与获取的所述的第二认证信息相同时，清除所述主机的密码。

2. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：在密码清除成功时，将密码清除的次数加 1。

3. 根据权利要求 1 至 2 任一项所述的方法，其特征在于，所述基于所述密码清除的次数和所述主机的主序列号在 T1 时刻进行加密，生成第一认证信息具体包括：

对所述密码清除的次数进行取模运算，得到一个序号；

根据所述序号查询预设密钥序列中对应的密钥；

利用所查询到的密钥对所述主序列号进行加密，生成第一认证信息。

4. 一种清除计算机密码的装置，其特征在于，所述装置包括：

提取单元，用于在 BIOS 检测到用户启动密码清除流程时，提取所述主机的主序列号和密码清除的次数；

生成单元，用于根据所述密码清除的次数和所述主机的主序列号在 T1 时刻进行加密，生成第一认证信息；

获取单元，用于从外接的存储设备中获取第二认证信息，所述第二认证信息为基于所述密码清除的次数和所述主机的主序列号在 T2 时刻进行加密生成的第二认证信息；所述 T2 时刻早于所述 T1 时刻；

清除单元，用于当生成的所述第一认证信息与获取的所述的第二认证信息相同时，清除所述主机的密码。

5. 根据权利要求 4 所述的装置，其特征在于，所述装置还包括：

计数单元，用于在密码清除成功时，将密码清除的次数加 1。

6. 根据权利要求 4 所述的装置，其特征在于，所述生成单元包括：

运算单元，用于对所述密码清除的次数进行取模运算，得到一个序号；

查询单元，用于根据所述序号查询预设密钥序列中对应的密钥；

认证信息生成单元，用于利用所查询到的密钥对所述主序列号进行加密，生成第一认证信息。

清除计算机密码的方法及装置

技术领域

[0001] 本发明涉及计算机领域，特别涉及一种清除计算机密码的方法及装置。

背景技术

[0002] 目前的计算机系统，为了用户数据的安全性，一般都要求用户去设置开机密码、硬盘密码，该密码一般由用户自己保存。用户在使用过程中，很容易把自己设置的密码忘掉。在种情况下，一般有两种解决方式：

[0003] 一种方式是：在用户忘记他所设置的开机密码或者硬盘密码时，通常会向计算机供应商的客服部门寻求帮助，客服部门通常会采用实时时钟芯片(RTC，Real-Time Clock)放电或者用特别的基本输入输出系统(BIOS，Basic Input-output System)刷新工具来为用户清除密码。但是，无论RTC放电还是特别的BIOS刷新工具清除密码，都必须计算机在现场和客户服务的人员面对面的进行，因此会造成售后成本的增加。

[0004] 另一种方式是：当用户忘记他所设置的开机密码或者硬盘密码时，通过电话联系计算机供应商的客服部门，客服部门通过让用户提供身份证复印件、注册联系电话等等信息以证明其身份，当验证用户身份后，再让用户提供贴在计算机的主序列号，之后，客服部门通过该主序列号生成一串验证号码给用户，用户在拿到这串验证号码后，可以用一种特别的方式进入计算机并输入该串验证号码，并在验证通过后，计算机才允许用户清除他所设置的密码。但是，在用户拿到该计算机的这串验证号码后，在忘记该计算机的开机密码或硬盘密码时，每次都可以用同样的方式进入计算机对原密码进行清除。也就是说，该验证号码将成为该计算机的“万能密码”，从而造成日后更换该计算机的使用者，前使用者也可以用“万能密码”进入该计算机，而给后使用者的数据造成安全隐患。

[0005] 在对现有技术的研究和实践过程中，本发明的发明人发现，现有解决用户忘记开机密码或硬盘密码时，需要联系计算机供应商的客服部门来清除和重置密码，无法进一步的降低售后成本；此外，客服部门重置的密码有可能会成为该计算机的“万能密码”，会给后续使用者的数据造成安全隐患，降低了系统的安全性。因此，设计一种安全的计算机密码清除方法，使用户可以自己在家中将密码清除或者重置密码，成为当前发展的趋势。

发明内容

[0006] 本发明实施例提供一种清除计算机密码方法、计算机及清除计算机密码系统，以便于用户在家清除计算机密码，降低售后成本，提高系统的安全性。

[0007] 为此，本发明实施例提供一种清除计算机密码方法，在BIOS检测到用户启动密码清除流程时，所述方法包括步骤：

[0008] 提取所述主机的主序列号和密码清除的次数；

[0009] 基于所述密码清除的次数和所述主机的主序列号在T1时刻进行加密，生成第一认证信息；

[0010] 从外接的存储设备中获取第二认证信息，所述第二认证信息为基于所述密码清除

的次数和所述主机的主序列号在 T2 时刻进行加密生成的第二认证信息；所述 T2 时刻早于所述 T1 时刻；

[0011] 当生成的所述第一认证信息与获取的所述的第二认证信息相同时，清除所述主机的密码。

[0012] 相应的，本发明实施例还提供一种计算机，包括主板，所述主板包括：

[0013] 提取单元，用于在 BIOS 检测到用户启动密码清除流程时，提取所述主机的主序列号和密码清除的次数；

[0014] 生成单元，用于根据所述密码清除的次数和所述主机的主序列号在 T1 时刻进行加密，生成第一认证信息；

[0015] 获取单元，用于从外接的存储设备中获取第二认证信息，所述第二认证信息为基于所述密码清除的次数和所述主机的主序列号在 T2 时刻进行加密生成的第二认证信息；所述 T2 时刻早于所述 T1 时刻；

[0016] 判断单元，用于判断生成的所述第一认证信息与获取的所述的第二认证信息是否相同，并发送判断结果；

[0017] 清除单元，用于在接收到判断单元发送相同的判断结果时，清除所述主机的密码。

[0018] 本发明实施例再提供一种清除计算机密码系统，所述系统包括计算机的主板和与其连接的存储设备，其中，

[0019] 所述存储设备，用于存储第二认证信息，所述第二认证信息为基于密码清除的次数和主机的主序列号在 T2 时刻进行加密生成的第二认证信息；

[0020] 所述主板，用于在 BIOS 检测到用户启动密码清除流程时，提取所述主机的主序列号和密码清除的次数；根据所述密码清除的次数和所述主机的主序列号在 T1 时刻进行加密，生成第一认证信息；从外接的存储设备中获取第二认证信息；所述 T2 时刻早于所述 T1 时刻；在判断生成的所述第一认证信息与获取的所述的第二认证信息相同是，清除所述主机的密码。

[0021] 由上述技术方案可知，本发明实施例提供一种不需要客服部门参与，用户可以在家利用外接存储设备中存储的认证信息清除计算机的密码。当用户的密码丢失时，可以通过一种特别的方式登录计算机，并通过外接存储设备提供的认证信息，然后对比通过外接设备得到的认证信息与根据所提起到的主机序列号和密码清除次数生成的认证信息，如果二者相同，则允许用户清除或者重设该计算机的密码。由此可见，采用本发明实施例所述技术方案后，无需客服部门介入，为企业节省了服务成本；在认证过程中，无需增加特别的硬件设备，不但节省了成本，也避免了由于硬件损坏造成的无法完成认证的隐患，从而提高了系统的安全性。

附图说明

[0022] 图 1 为本发明实施例中清除计算机密码的方法的流程图；

[0023] 图 2 为本发明实施例中第二认证信息的生成方法的具体应用实例；

[0024] 图 3 为本发明实施例中第一认证信息的生成过程的流程图；

[0025] 图 4 为利用本发明实施例中清除计算机密码的方法的具体应用实例图；

[0026] 图 5 为本发明实施例中利用所述生成的信息文件清除计算机密钥的方法的应用

实施例的流程图；

[0027] 图 6 为本发明实施例中认证信息的生成设备的结构示意图；

[0028] 图 7 为本发明实施例中计算机的一种结构示意图；

[0029] 图 8 为本发明实施例中清除计算机密码系统的一种结构示意图。

具体实施方式

[0030] 本发明实施例提供了一种不需要客服部门参与，当用户忘记设置的密码时，用户可以自己在家完成认证并清除或者重置密码。也就是说，用户在设置计算机密码时，并在完成计算机密钥设置后，选择密钥重设置功能，提示用户生成一个认证文件，并将该认证文件存储在外接于所述计算机上存储设备中，比如 U 盘等，当以后用户密码丢失时，可以通过一种特别的方式登录计算机并将所述外接存储设备插入到所述计算机中提供当初生成的认证文件，在该认证文件通过验证后即允许用户清除或者重设该计算机的密码；当用户成功清除或者重设密码以后，可以选择重新生成认证文件，这样上次的认证文件就失效了，这就在一定程度上保证了系统的安全性。

[0031] 下面我们将结合附图，对本发明的最佳实施方案进行详细描述。

[0032] 请参阅图 1，为本发明实施例中清除计算机密码的方法的流程图，在 BIOS 检测到用户启动密码清除流程时，所述方法包括：

[0033] 步骤 101：提取所述主机的主序列号和密码清除的次数；

[0034] 步骤 102：基于所述密码清除的次数和所述主机的主序列号在 T1 时刻进行加密，生成第一认证信息；所述第一认证信息的实现过程详见下图 3。

[0035] 优选地，可以根据所述第一认证信息生成第一安全认证信息，所述第一安全认证信息可以由所述第一认证信息中的部分或者全部的认证码组成，比如，第一认证信息为一串字符，而该串字符有十个认证码组成，而所述第一认证文件可以只包括第一认证码，也可以包括第一和第二认证码的组合，或者是所有十种认证码的组合，本实施例不作限制。

[0036] 步骤 103：从外接的存储设备中获取第二认证信息，所述第二认证信息为基于所述密码清除的次数和所述主机的主序列号在 T2 时刻进行加密生成的第二认证信息；

[0037] 优选地，可以根据所述第二认证信息生成第二安全认证信息，所述第二安全认证信息可以由所述第二认证信息中的部分或者全部的认证码组成，

[0038] 步骤 104：当生成的所述第一的认证信息与获取的所述的第二认证信息相同时，清除所述主机的密码。

[0039] 优选的，所述方法还包括：在步骤 104 进行密码清除成功时，密码清除的次数加 1。

[0040] 优选的，所述 T2 时刻早于所述 T1 时刻。

[0041] 其中，在步骤 103 中，从外接的存储设备中获取第二认证信息，所述第二认证信息为基于所述密码清除的次数和所述主机的主序列号在 T2 时刻进行加密生成的第二认证信息，所述第二认证信息的实现过程详见下图 2。

[0042] 为了便于本领域技术人员的理解，下面先介绍一下认证信息的生成过程，请参阅图 2，为本发明实施例中第二认证信息的生成方法的流程图，在本实施例中存储设备以 U 盘为例，但并不限于此，

[0043] 如图 2 所示，用户在设置完计算机密码后，可以在 BIOS 界面中选择密码重设置

(Password Reset)功能，进行认证信息的生成，并将生成的认证信息存储在认证文件中。其用户的认证文件的生成过程具体包括：

[0044] 步骤 201：BIOS 在检测到用户进行密码设置后，BIOS 提示用户插入 U 盘；

[0045] 步骤 202：BIOS 检测是否有 U 盘插入，若是，执行步骤 203；否则，继续检测用户是否已插入 U 盘；

[0046] 步骤 203：当 BIOS 检测到用户插入的 U 盘后，BIOS 检测 U 盘是否可用，若是，则执行步骤 204，否则，执行步骤 208；

[0047] 步骤 204：若可用，则开始生成认证信息；即 BIOS 提取本机的主序列号和密码清除的次数进行加密，生成第二认证信息；

[0048] 其中，BIOS 从非易失性随机访问存储器 (NVRAM，Non-Volatile Random Access Memory) 中提取本机的主序列号和密码清除的次数（还可以为密钥重设置的次数等）；对所述认证信息的生成次数进行取模运算，得到一个序号；根据所述序号查询预设密钥序列中对应的密钥；利用所查询到的密钥对主序列号进行加密，生成第二认证信息；更进一步可以取加密结果的固定位置和固定长度信息作为第二认证信息。

[0049] 步骤 205：将携带有认证信息的认证文件写入 U 盘的根目录；

[0050] 步骤 206：显示用户的认证文件已生成信息；

[0051] 步骤 207：用户在看到认证文件已生成的信息后，拔掉 U 盘。

[0052] 步骤 208：若不可用，则提示用户更换 U 盘，之后，继续执行步骤 203。

[0053] 由此可知，本发明实施例提供一种不需要客服部门参与，用户自己可以在家生成认证文件，并根据该认证文件清除或者重置计算机密码。用户在设置计算机密码时，提示用户生成一个认证文件，当以后用户密码丢失时，可以通过一种特别的方式登录计算机并将 U 盘插入到计算机中提供当初生成的认证文件，当认证文件通过验证后即允许用户清除或者重设该计算机的密码。在一定程度上降低了售后成本，保证了系统的安全性。

[0054] 请参阅图 3，为本发明实施例中第一认证信息的生成的流程图，包括：

[0055] 步骤 301：BIOS 提取本机的主序列号和密码清除的次数；

[0056] 步骤 302：对所述密码清除的次数进行取模运算，得到一个序号；

[0057] 步骤 303：BIOS 根据所述序号查询密钥序列中对应的密钥；

[0058] 步骤 304：BIOS 利用所查询到的密钥对主序列号进行加密，生成第一认证信息；

[0059] 步骤 305：BIOS 将生成的认证信息写入计算机的认证文件。

[0060] 在本实施例中，对认证文件中生成的认证信息进行了特别的处理，比如，预先在主机的 NVRAM 预先存储一个专门的密钥序列，可以包括 10 个密钥或者更多，本实施例不作限制。在 BIOS 提取主机的主序列号和密码清除的次数后，对所述密码清除的次数进行取模运算，得到一个序号（即密钥在密钥序列中的序号），由于根据提取到的密码清除的次数不同，根据该次数计算出的模也不同，即得到的序号不同，而由于序号不同，在密钥序列中查找到对应的密钥也不同，而根据查找到的对所述主序列号进行加密，就形成了不同的认证信息。本实施例中所述这种方法可以使系统的安全性更高。

[0061] 还请参阅图 4，为本发明实施例中清除计算机密码的方法的具体应用实例图，在该实施例中，BIOS 在检测到用户启动密码清除流程时，所述方法包括：

[0062] 步骤 401：在判断允许密码重置功能打开时，从检测到带有认证文件的存储设备

中获取认证信息；

[0063] 步骤 402：根据所述获取认证信息中得到的密码清除的次数对本机的主序列号进行加密，生成认证信息；

[0064] 步骤 403：在判断所述获取的认证信息与生成的认证信息相同时，允许用户进入密钥清除流程。

[0065] 在步骤 401 之前，所述方法还包括：

[0066] 从 NVRAM 中读取密码设置信息，判断密码设置信息中的密码口令是否正确，若正确，则允许打开密码设置，否则，锁定计算机；

[0067] 在判断允许密码重置功能打开时，显示用来提示用户需要插入带有认证文件的存储设备信息；

[0068] 在检测到有存储设备插入时，判断所述存储设备中是否存在认证文件；若有，则在判断所述认证文件可用时，执行所述从带有认证文件的存储设备中获取认证信息的步骤。

[0069] 优选的，所述方法还包括：当用户成功清除或者重设密码以后，选择重新生成认证文件，所述重新生成认证文件包括：

[0070] 在检测到插入的存储设备可用时，提取主机的主序列号和密码清除的次数；

[0071] 根据所述主序列号和密码清除的次数生成认证信息，将所述认证信息写入认证文件；

[0072] 将所述写入认证信息的认证文件写入存储设备的根目录。

[0073] 还请参阅图 5，为本发明实施例中利用所述生成的认证文件中的认证信息清除计算机密钥的方法的应用实施例的流程图，在用户输入多次密码开机不成功时，用户选择重置密码功能，并从客服部门拿到验证码后，可以按照下述步骤清除密码，具体包括：

[0074] 步骤 501：用户选择重置密码功能；

[0075] 步骤 502：在开机时选择特定方式登陆计算机，比如在开机时按下“Fn+F？”键；

[0076] 步骤 503：BIOS 检测到开机时该按键按下时，即启动密码清除流程；

[0077] 步骤 504：BIOS 判断读取到的是否允许密码重置功能 (Password Reset) 打开，若可以，则执行步骤 505；否则，执行步骤 516：锁定计算机 (Lock PC)；

[0078] 在该步骤 504 中，BIOS 从 NVRAM 中读取 Password Reset 字段信息，并判断是否允许密码重置功能打开，若可以，显示用来提示用户需要插入带有认证文件的 U 盘信息。如果不能读取 Password Reset 字段信息，则失败，报错。

[0079] 步骤 505：BIOS 提示用户插入带有认证文件的 U 盘；

[0080] 步骤 506：BIOS 检测是否有 U 盘插入，若有，执行步骤 507；否则，继续检测是否有 U 盘插入；

[0081] 步骤 507：检测插入的 U 盘是否可用，若是，则执行步骤 508；否则执行步骤 509：提示用户当前 U 盘不可用，之后执行步骤 516；

[0082] 步骤 508：检测 U 盘上根目录上是否有可用的认证文件，若是，则执行步骤 510；否则执行步骤 511：提示用在 U 盘上没有可用的认证文件，之后执行步骤 516；

[0083] 步骤 510：从 U 盘上可用的认证文件中读出认证文件中的认证信息，

[0084] 步骤 512：提取本机的主序列号和密码清除的次数；

[0085] 步骤 513：根据密码清除的次数对本机主序列号进行加密，生成认证信息；

[0086] 步骤 514 :判断所述获取的认证信息与生成的认证信息是否相同,若相同,则执行步骤 515 ;否则,执行步骤 516 ;

[0087] 步骤 515 :若相同,则允许用户进入密钥清除流程 ;即如果两个认证信息的内同一致时,则允许用户进入密码清除流程。

[0088] 步骤 516,若不同,则提示用户认证失败,要求提供正确的认证文件,并执行步骤 517,即锁定计算机。

[0089] 需要说明的是,读取 U 盘中认证文件中的认证信息和生成的认证信息,在时间上没有先后顺序,即可以是先生成认证信息,也可以是读取 U 盘中认证文件中的认证信息,也可以是生成认证信息和读取的认证信息同时。本实施例不作限制。

[0090] 由此可知,本发明实施例提供一种不需要客服部门参与,用户自己可以在家生成认证文件,并根据该认证文件清除或者重置计算机密码的方法和设备。用户在设置计算机密码时,提示用户生成一个认证文件,当以后用户密码丢失时,可以通过一种特别的方式登录计算机并提供当初生成的认证文件,当认证文件通过验证后即允许用户清除或者重设该计算机的密码。以及在用户成功清除或者重设密码以后,可以选择重新生成认证文件。在一定程度上降低了售后成本,保证了系统的安全性。此外,当用户感觉当前认证文件可能外泄存在安全隐患时,可以选择重新生成新的认证文件,在新的认证文件生成时,旧的认证文件就自动失效了,从而提高了系统的安全性。

[0091] 相应的,本发明实施例还提供一种认证信息的生成设备,用于在检测到用户进行密码设置后,选择重设置功能时,生成认证文件,其结构示意图详见图 6,所述设备包括 :提取单元 61、生成单元 62 和存储单元 63,其中,所述提取单元 61,用于在检测到插入的存储设备可用时,提取主机的主序列号和密码清除的次数 ;所述生成单元 62,用于根据所述提取单元 61 提取的主序列号和密码清除的次数生成认证信息,将所述认证信息写入认证文件 ;所述存储单元 63,用于将写入认证信息的认证文件存储到存储设备中。

[0092] 所述设备还包括 :密钥预设单元,用于在在主机的认证文件中预先存储专门的密钥序列。

[0093] 所述生成单元 62 包括 :运算单元、查询单元、认证信息生成单元和写入单元,其中,所述运算单元,用于对所述密码清除的次数进行取模运算,得到一个序号 ;所述查询单元,用于根据所述序号查询密钥预设单元中存储的密钥序列中对应的密钥 ;所述认证信息生成单元,用于利用所查询到的密钥对主序列号进行加密,生成认证信息 ;所述写入单元,用于将认证信息生成单元生成的所述认证信息写入认证文件。

[0094] 所述设备还包括 :检测单元和更换信息显示单元,其中,所述检测单元,用于检测插入的存储设备是否可用,若可用,则通知提取单元 61 ;否则,通知更换信息显示单元 ;所述更换信息显示单元,用于显示用来提示用户需要更换存储设备的信息。

[0095] 所述设备还包括 :生成信息显示单元,用于显示写入认证信息的认证文件已生成信息。

[0096] 本实施例中所述设备中各个单元的功能和作用详见上述方法中对应的实现过程,在此不再详细的描述。

[0097] 本发明实施例还提供一种计算机,包括主板,所述主板包括 :提取单元 70、生成单元 71、获取单元 72、判断单元 73 和清除单元 74,其结构示意图如图 7 所示。其中,所述提取

单元 70，用于在 BIOS 检测到用户启动密码清除流程时，提取所述主机的主序列号和密码清除的次数；所述生成单元 71，用于根据所述密码清除的次数和所述主机的主序列号在 T1 时刻进行加密，生成第一认证信息；所述获取单元 71，用于从外接的存储设备中获取第二认证信息，所述第二认证信息为基于所述密码清除的次数和所述主机的主序列号在 T2 时刻进行加密生成的第二认证信息；所述判断单元 73，用于判断生成的所述第一的认证信息与获取的所述的第二认证信息是否相同，并发送判断结果；所述清除单元 74，用于在接收到判断单元发送相同的判断结果时，清除所述主机的密码。

[0098] 所述主板还包括：计数器，用于在密码清除成功时，将密码清除的次数加 1。

[0099] 所述生成单元包括：运算单元、查询单元和认证信息生成单元，其中，所述运算单元，用于对所述密码清除的次数进行取模运算，得到一个序号；所述查询单元，用于根据所述序号查询预设密钥序列中对应的密钥；所述认证信息生成单元，用于利用所查询到的密钥对所述主序列号进行加密，生成第一认证信息。

[0100] 本实施例中所述设备中各个单元的功能和作用详见上述方法中对应的实现过程，在此不再详细的描述。

[0101] 此外，本发明实施例还提供一种清除密码系统，包括存储设备和主板，其中，所述存储设备，用于存储第二认证信息，所述第二认证信息为基于所述密码清除的次数和所述主机的主序列号在 T2 时刻进行加密生成的第二认证信息；所述主板，用于在检测到用户启动密码清除流程时，提取所述主机的主序列号和密码清除的次数；根据所述密码清除的次数和所述主机的主序列号在 T1 时刻进行加密，生成第一认证信息；从外接的存储设备中获取第二认证信息；判断生成的所述第一的认证信息与获取的所述的第二认证信息是否相同，在接收到判断单元发送相同的判断结果时，清除所述主机的密码。

[0102] 请参阅图 8，为本发明实施例中一种清除计算机密码系统的应用实例图。

[0103] 如图 8 所示，该清除密码系统包括主板，所述主板包括硬盘驱动器 (HDD，Hard Disk Drive)81、BIOS 管理设备 82、非易失性随机访问存储器 NVRAM83 和存储设备 84，其中，BIOS 管理设备 82（即 BIOS 管理程序）负责整个程序流程的管理，其中包括验证文件的生成，以及密码的清除。NVRAM83 是一块存储介质，用于存储生成验证文件时、清除密码时用到的一些变量、密码和密码清除的次数等，都保存在 NVRAM 上。BIOS 管理设备也负责和硬盘驱动器 81 进行交互，并利用存储设备 85 中存储的认证文件来完成硬盘密码的清除和设置。

[0104] 其中，所述 BIOS 管理设备 82 包括：认证信息的生成设备 821 和清除计算机密码的设备 822，所述认证信息的生成设备 811，用于检测到用户在 HDD 上进行密码设置后，在 BIOS 界面上选择重设置功能时，若检测到插入的所述存储设备（比如 U 盘）可用，则从 NVRAM 中提取主机的主序列号和密码清除的次数；根据所述提取的主序列号和密码清除的次数生成认证信息，将所述认证信息写入认证文件，并将写入认证信息的认证文件存储到存储设备中；具体包括：提取单元、生成单元和存储单元，其具体功能和作用的实现过程详见上述，在此不再赘述。

[0105] 所述清除计算机密码的设备 822，用于在检测到用户启动密码清除流程时，若从 NVRAM 读取到允许密码重置功能打开，并在检测到带有认证文件的存储设备插入时，则从所述认证文件中获取认证信息；以及提取本机的主序列号和密码清除的次数；根据所述密码清除的次数对本机的主序列号进行加密，生成认证信息；并在判断所述获取的认证信息和

生成的认证信息相同时，允许用户进入密钥清除流程。

[0106] 清除计算机密码的设备 822 具体包括：提取单元 822、生成单元 823、获取单元 824、判断单元 825 和清除单元 826，其具体功能和作用的实现过程详见上述，在此不再赘述。

[0107] 由此可知，本发明实施例提供一种不需要客服部门参与，用户自己可以在家生成认证文件，并根据该认证文件清除或者重置计算机密码的方法和设备。用户在设置计算机密码时，提示用户生成一个认证文件，当以后用户密码丢失时，可以通过一种特别的方式登录计算机并提供当初生成的认证文件，当认证文件通过验证后即允许用户清除或者重设该计算机的密码。以及在用户成功清除或者重设密码以后，可以选择重新生成认证文件。在一定程度上降低了售后成本，保证了系统的安全性。由此可见，采用本发明实施例所述技术方案后，无需客服部门介入，为企业节省了服务成本；在认证过程中，无需增加特别的硬件设备，不但节省了成本，也避免了由于硬件损坏造成的无法完成认证的隐患；当用户感觉当前认证文件可能外泄存在安全隐患时，可以选择重新生成新的认证文件，在新的认证文件生成时，旧的认证文件就自动失效了，从而提高了系统的安全性。

[0108] 通过以上实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

[0109] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

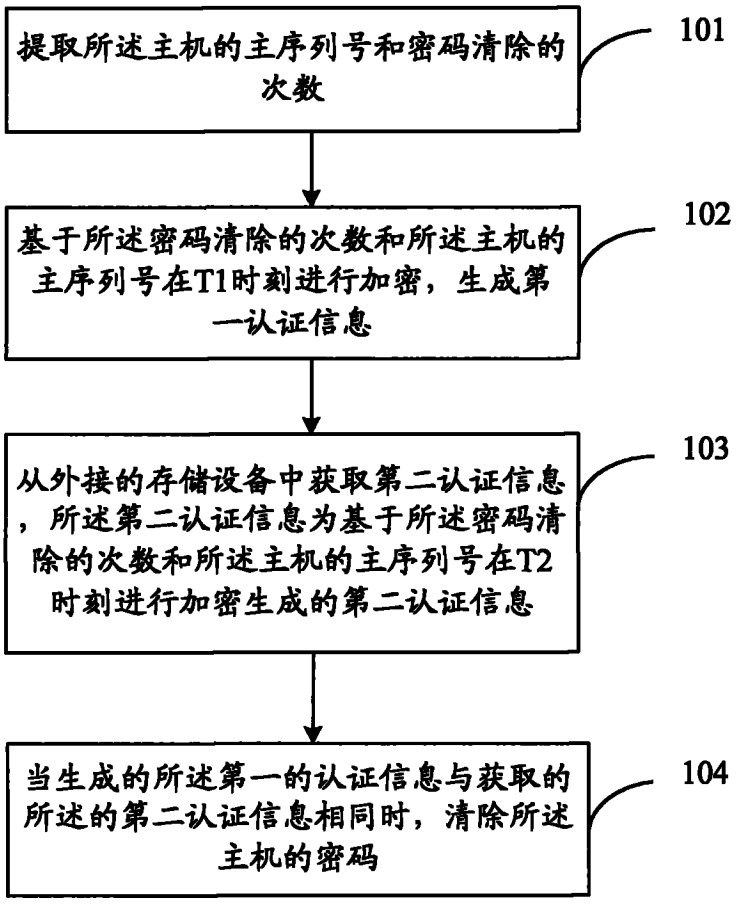

提取所述主机的主序列号和密码清除的次数
101
基于所述密码清除的次数和所述主机的主序列号在T1时刻进行加密，生成第一认证信息
102
从外接的存储设备中获取第二认证信息，所述第二认证信息为基于所述密码清除的次数和所述主机的主序列号在T2时刻进行加密生成的第二认证信息
103
当生成的所述第一的认证信息与获取的所述的第二认证信息相同时，清除所述主机的密码
104

图 1

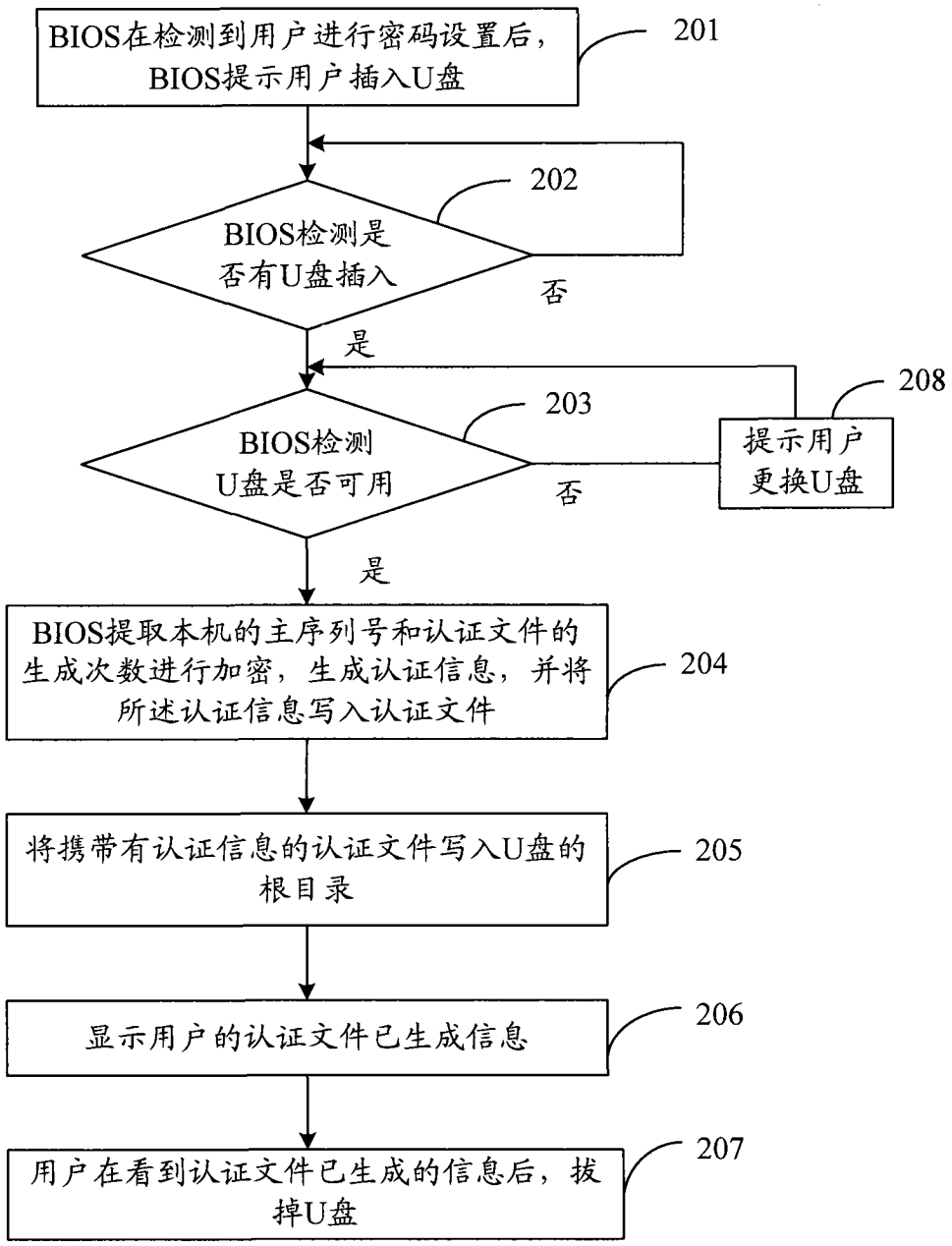

BIOS在检测到用户进行密码设置后，BIOS提示用户插入U盘
201
BIOS检测是否有U盘插入
202
否
是
BIOS检测U盘是否可用
203
否
提示用户更换U盘
208
是
BIOS提取本机的主序列号和认证文件的生成次数进行加密，生成认证信息，并将所述认证信息写入认证文件
204
将携带有认证信息的认证文件写入U盘的根目录
205
显示用户的认证文件已生成信息
206
用户在看到认证文件已生成的信息后，拔掉U盘
207

图 2

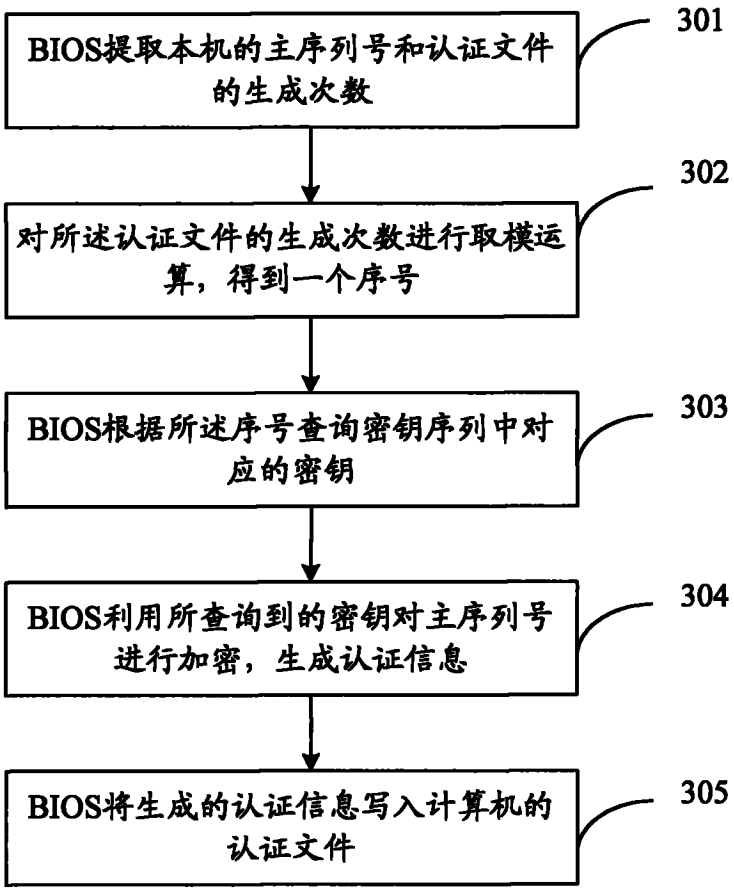

BIOS提取本机的主序列号和认证文件的生成次数
301
对所述认证文件的生成次数进行取模运算，得到一个序号
302
BIOS根据所述序号查询密钥序列中对应的密钥
303
BIOS利用所查询到的密钥对主序列号进行加密，生成认证信息
304
BIOS将生成的认证信息写入计算机的认证文件
305

图 3

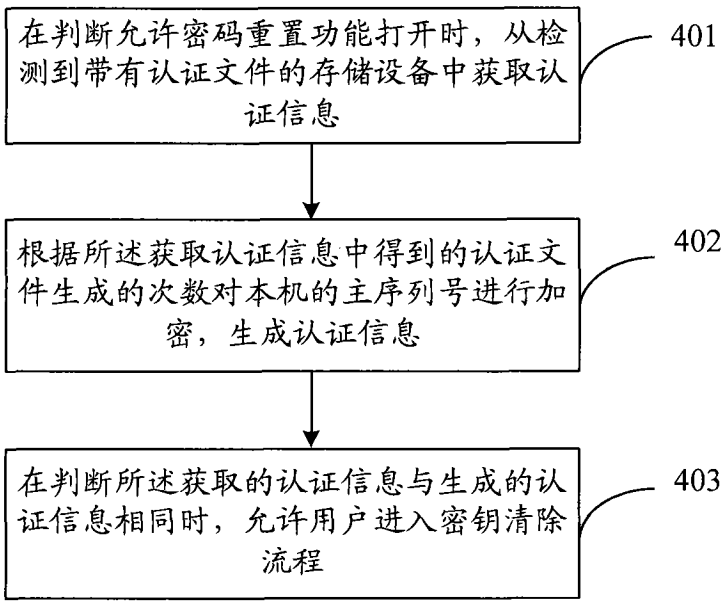

在判断允许密码重置功能打开时，从检测到带有认证文件的存储设备中获取认证信息
401
根据所述获取认证信息中得到的认证文件生成的次数对本机的主序列号进行加密，生成认证信息
402
在判断所述获取的认证信息与生成的认证信息相同时，允许用户进入密钥清除流程
403

图 4

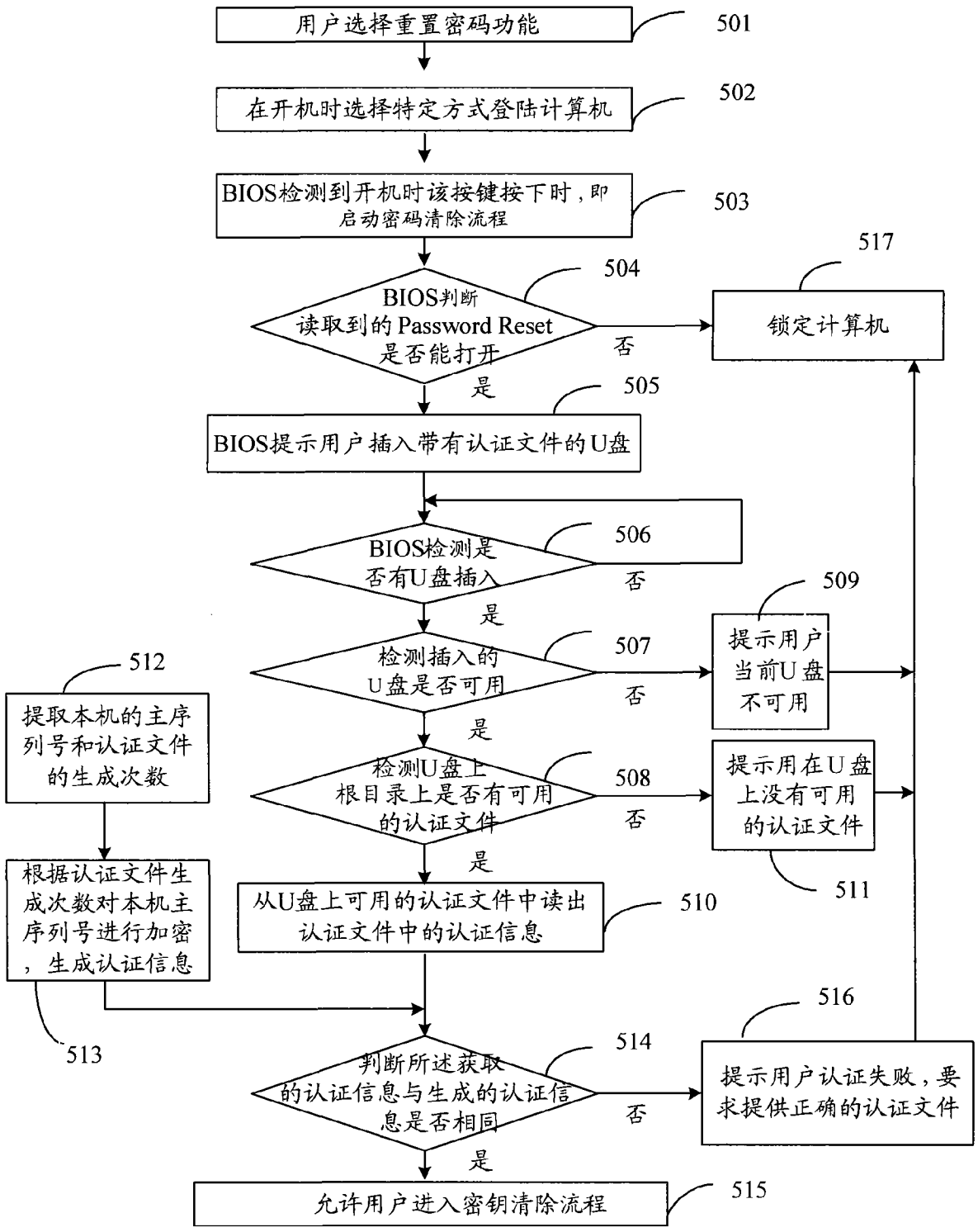

用户选择重置密码功能
501
在开机时选择特定方式登陆计算机
502
BIOS检测到开机时该按键按下时，即启动密码清除流程
503
BIOS判断读取到的Password Reset是否能打开
504
否
是
锁定计算机
517
BIOS提示用户插入带有认证文件的U盘
505
BIOS检测是否有U盘插入
506
否
是
检测插入的U盘是否可用
507
否
是
提示用户当前U盘不可用
509
检测U盘上根目录上是否有可用的认证文件
508
否
是
提示用在U盘上没有可用的认证文件
511
从U盘上可用的认证文件中读出认证文件中的认证信息
510
提取本机的主序列号和认证文件的生成次数
512
根据认证文件生成次数对本机主序列号进行加密，生成认证信息
513
判断所述获取的认证信息与生成的认证信息是否相同
514
否
是
提示用户认证失败，要求提供正确的认证文件
516
允许用户进入密钥清除流程
515

图 5

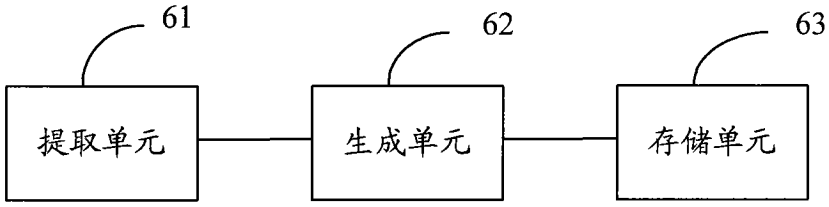


图 6

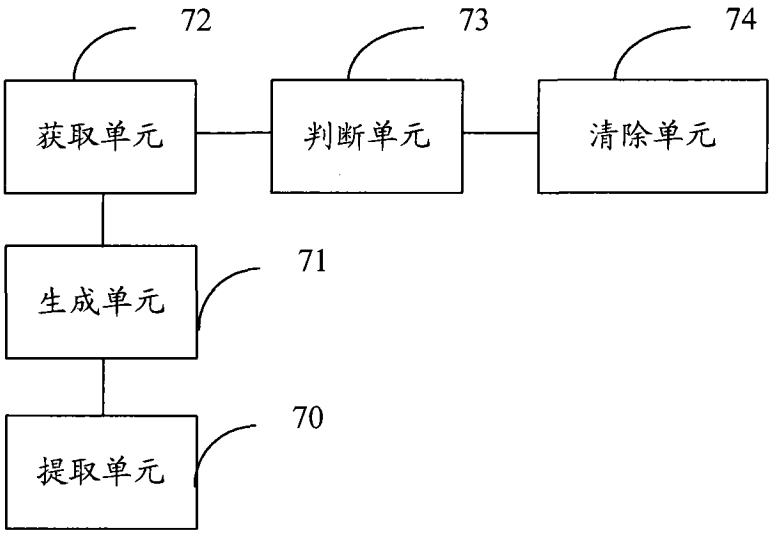


图 7

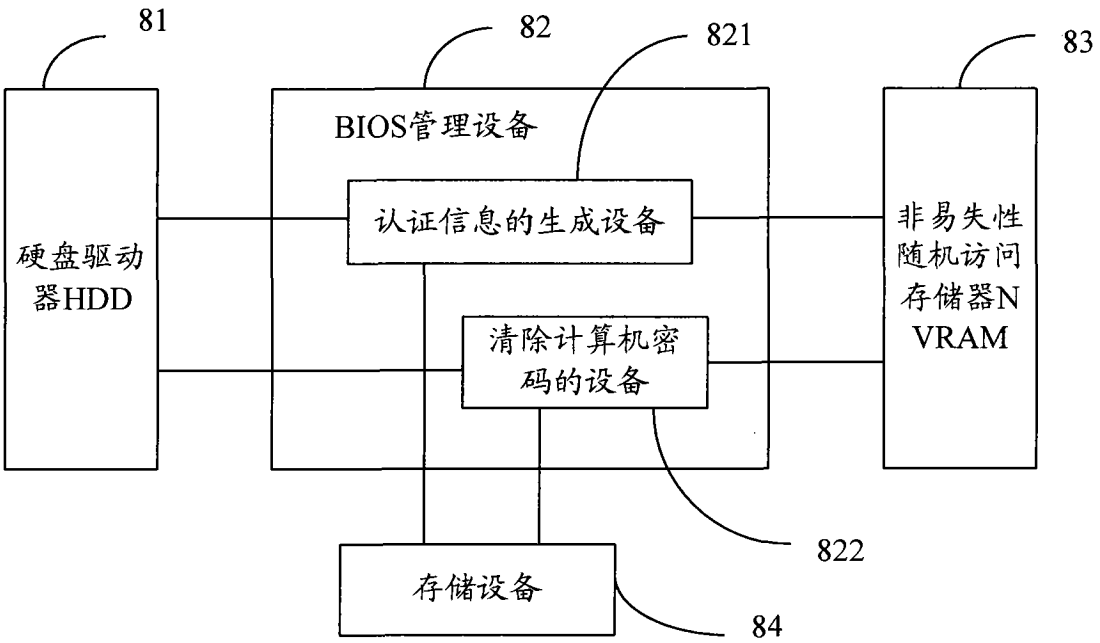

81
82
821
83
BIOS管理设备
硬盘驱动器HDD
认证信息的生成设备
非易失性随机访问存储器NVRAM
清除计算机密码的设备
822
存储设备
84

图 8