(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 107678982 A
(43)申请公布日 2018.02.09

(21)申请号 201710532526.8

(22)申请日 2017.07.03

(30)优先权数据
62/370,230 2016.08.02 US
15/275,337 2016.09.23 US

(71)申请人 三星电子株式会社
地址 韩国京畿道水原市

(72)发明人 颂蓬·保罗·奥莱瑞兹 张牧天

(74)专利代理机构 北京铭硕知识产权代理有限公司 11286
代理人 曾世骁 张云珠

(51)Int.Cl.
G06F 12/14(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)

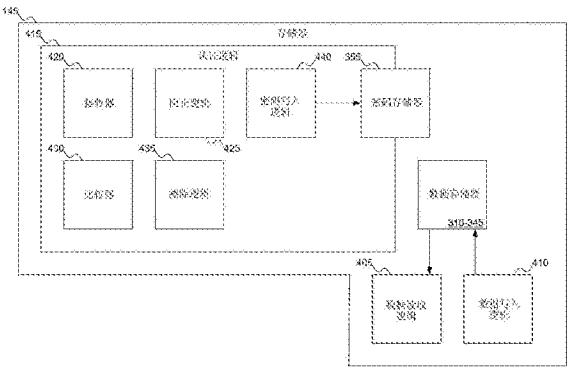
权利要求书2页 说明书15页 附图14页

(54)发明名称

安全存储器及在智能存储装置中执行数据清理的方法

(57)摘要

公开了一种安全存储器及在智能存储装置中执行数据清理的方法。公开了一种安全存储器。该存储器可包括:用于数据的数据存储器、用于从数据存储器读取数据的数据读取逻辑、和用于向数据存储器写入数据的数据写入逻辑。可存储密码的密码存储器。接收器可从存储器控制器接收密码。比较器可将接收的密码与存储的密码进行比较。如果接收的密码与存储的密码不匹配,则擦除逻辑可将数据存储器中的数据擦除。最后,阻止逻辑可阻止来自存储器控制器的对存储器的访问,直到比较器完成它的操作之后为止。



CN 107678982 A

1.一种存储器，包括：

数据存储器，用于存储针对第一用户的数据；

数据读取逻辑，用于从数据存储器读取数据；

数据写入逻辑，用于向数据存储器写入数据；

密码存储器，用于存储密码；

接收器，用于从存储器控制器接收密码；

比较器，用于将接收的密码与存储的密码进行比较；

擦除逻辑，用于：如果接收的密码与存储的密码不同，则擦除数据存储器中的数据；

阻止逻辑，用于阻止来自存储器控制器的对数据存储器的访问，直到比较器完成操作之后为止；

其中，接收的密码或存储的密码不用于对存储在存储器中的数据进行加密。

2.如权利要求1所述的存储器，其中，阻止逻辑能够执行操作以阻止来自存储器控制器的对数据存储器的访问，直到擦除逻辑完成操作之后为止。

3.如权利要求1所述的存储器，还包括：密码写入逻辑，用于将接收的密码写入密码存储器。

4.如权利要求1所述的存储器，还包括：串行存在检测SPD，用于指明存储器是否正在安全模式下运行。

5.如权利要求4所述的存储器，其中，如果SPD指明存储器不是正在安全模式下运行，则阻止逻辑允许存储器控制器访问数据存储器，而无需调用比较器。

6.如权利要求1所述的存储器，其中，如果阈值数量的接收的密码都与存储的密码不同，则擦除逻辑能够执行操作以擦除数据存储器中的数据。

7.如权利要求1所述的存储器，其中，存储器从包括以下项的集合得到：易失性存储器模块、非易失性存储器模块、以及易失性存储器装置与非易失性存储器装置的任何组合。

8.如权利要求1所述的存储器，还包括寄存器时钟驱动器RCD，其中，RCD包括所述接收器、所述比较器、所述擦除逻辑和所述阻止逻辑。

9.一种防止对存储器的未授权访问的方法，包括：

确定存储器已复位；

确定存储器正在安全模式下运行还是在非安全模式下运行；

如果存储器正在安全模式下运行，则：

针对用户选择密码；

将所述密码发送到存储器；

接收对存储器的访问，

其中，所述密码不用于对存储器中存储的数据进行加密。

10.如权利要求9所述的方法，还包括：如果存储器正在非安全模式下运行，则在不使用密码的情况下接收对存储器的访问。

11.如权利要求9所述的方法，其中，将所述密码发送到存储器的步骤包括：向存储器发送阈值次数的所述密码。

12.如权利要求9所述的方法，其中，接收对存储器的访问的步骤包括：接收对经过擦除的存储器的访问。

13.如权利要求9所述的方法,还包括:

测量从存储器复位开始的时长;

如果从存储器复位开始的时长大于阈值,则向存储器发送软件引起的复位。

14.一种防止对存储器的未授权访问的方法,包括:

将指示存储器正在安全模式下运行的信号从存储器发送到存储器控制器;

从存储器控制器接收密码;

将接收的密码与存储的密码进行比较;

如果接收的密码与存储的密码不匹配,则:

对存储器进行擦除;

授权存储器控制器对存储器的访问,

其中,接收的密码或存储的密码不用于对存储在存储器中的数据进行加密。

15.如权利要求14所述的方法,还包括:如果接收的密码与存储的密码不匹配,则将接收的密码存储在存储器中。

16.如权利要求14所述的方法,还包括:如果接收的密码与存储的密码匹配,则授权存储器控制器对存储器的访问。

17.如权利要求14所述的方法,还包括:在对存储器进行擦除之前,对接收的密码与存储的密码进行阈值次数的比较。

18.如权利要求14所述方法,还包括:

从存储器控制器接收复位命令;

响应于所述复位命令使存储器复位。

19.如权利要求14所述的方法,其中,将指明存储器正在安全模式下运行的信号从存储器发送到存储器控制器的步骤包括:从存储器控制器接收关于存储器是否正在安全模式下运行的请求。

20.如权利要求14所述的方法,其中,从存储器控制器接收密码的步骤包括:向存储器控制器请求密码。

安全存储器及在智能存储装置中执行数据清理的方法

[0001] 本申请要求于2016年8月2日提交的序列号为62/370,230的美国临时专利申请的权益,所述申请的全部公开通过引用合并于此以用于各种目的。

技术领域

[0002] 发明构思总体上涉及存储器,更具体地涉及一种可被保护以防止对存储于存储器中的数据进行未授权的访问的存储器。

背景技术

[0003] 非易失性存储器(NVM)的内容是永久性的。当用作长期的存储装置时,期待且想要这样行为:期望数据的保存。

[0004] 但是非易失性存储器在存储器空间的使用上可存在问题。通常出于安全原因,保存在存储器空间中的许多形式的数据都想要是临时的。NVM打破了这一假设,并且如果NVM被盗或它的资源重新分配则造成风险。例如,当事实上客户数据被存储在NVM上时,基于云计算的网络服务可将客户数据存储在它所认为的易失性存储器。例如,如果网络服务没有明确擦除存储器内容而被终止,则数据将会被另一用户获得,就好像NVM被盗或NVM的资源被提供给另一云用户。

[0005] 仍需要一种用于使存储器被保护以防止对存储器模块(特别是利用NVM的存储器模块)进行未授权的访问的方法。

发明内容

[0006] 本发明构思的一方面提供了一种存储器,所述存储器可包括:数据存储器,用于存储针对第一用户的数据;数据读取逻辑,用于从数据存储器读取数据;数据写入逻辑,用于向数据存储器写入数据;密码存储器,用于存储密码;接收器,用于从存储器控制器接收密码;比较器,用于将接收的密码与存储的密码进行比较;擦除逻辑,用于:如果接收的密码与存储的密码不同,则擦除数据存储器中的数据;阻止逻辑,用于阻止来自存储器控制器的对数据存储器的访问,直到比较器完成操作之后为止;其中,接收的密码或存储的密码不用于对存储在存储器中的数据进行加密。

[0007] 阻止逻辑能够执行操作以阻止来自存储器控制器的对数据存储器的访问,直到擦除逻辑完成操作之后为止。

[0008] 所述存储器还可包括:密码写入逻辑,用于将接收的密码写入密码存储器;串行存在检测SPD,用于指明存储器是否正在安全模式下运行,其中,如果SPD指明存储器不是正在安全模式下运行,则阻止逻辑允许存储器控制器访问数据存储器,而无需调用比较器。

[0009] 如果阈值数量的接收的密码都与存储的密码不同,则擦除逻辑能够执行操作以擦除数据存储器中的数据。

[0010] 存储器可从包括以下项的集合得到:易失性存储器模块、非易失性存储器模块、以及易失性存储器装置与非易失性存储器装置的任何组合。

[0011] 所述存储器还可包括寄存器时钟驱动器RCD，其中，RCD包括所述接收器、所述比较器、所述擦除逻辑和所述阻止逻辑。

[0012] 根据本发明构思的另一方面，提供了一种防止对存储器的未授权访问的方法，所述方法可包括：确定存储器已复位；确定存储器正在安全模式下运行还是在非安全模式下运行；如果存储器正在安全模式下运行，则：针对用户选择密码；将所述密码发送到存储器；接收对存储器的访问，其中，所述密码不用于对存储器中存储的数据进行加密。

[0013] 如果存储器正在非安全模式下运行，则在不使用密码的情况下接收对存储器的访问。

[0014] 将所述密码发送到存储器的步骤可包括：向存储器发送阈值次数的所述密码。接收对存储器的访问的步骤可包括：接收对经过擦除的存储器的访问。

[0015] 所述方法还可包括：测量从存储器复位开始的时长；如果从存储器复位开始的时长大于阈值，则向存储器发送软件引起的复位。

[0016] 根据本发明构思的另一方面，提供了一种防止对存储器的未授权访问的方法，所述方法可包括：将指示存储器正在安全模式下运行的信号从存储器发送到存储器控制器；从存储器控制器接收密码；将接收的密码与存储的密码进行比较；如果接收的密码与存储的密码不匹配，则：对存储器进行擦除；授权存储器控制器对存储器的访问，其中，接收的密码或存储的密码不用于对存储在存储器中的数据进行加密。

[0017] 如果接收的密码与存储的密码不匹配，则将接收的密码存储在存储器中；如果接收的密码与存储的密码匹配，则授权存储器控制器对存储器的访问。在对存储器进行擦除之前，对接收的密码与存储的密码进行阈值次数的比较。

[0018] 所述方法还可包括：从存储器控制器接收复位命令；响应于所述复位命令使存储器复位。

[0019] 将指明存储器正在安全模式下运行的信号从存储器发送到存储器控制器的步骤可包括：从存储器控制器接收关于存储器是否正在安全模式下运行的请求。从存储器控制器接收密码的步骤可包括：向存储器控制器请求密码。

附图说明

[0020] 图1示出根据发明构思的实施例的具有使用安全存储器的各种主机的数据中心。

[0021] 图2示出图1的主机的额外的细节。

[0022] 图3示出图1的存储器的细节。

[0023] 图4示出图1的存储器的另一种示图。

[0024] 图5示出图3-图4的存储器使用从图3的存储器控制器接收的密码确定是授权对存储在图3-图4的存储器中的数据的访问还是擦除图3-图4的存储器中存储的数据。

[0025] 图6示出根据发明构思的实施例的图1的可在两个用户之间共享资源的存储器的示例。

[0026] 图7A-图7C示出根据发明构思的实施例的图3的存储器控制器请求对图1的存储器的访问的示例过程的流程图。

[0027] 图8示出根据发明构思的实施例的图3的存储器控制器选择密码以请求对图1的存储器的访问的示例过程的流程图。

[0028] 图9A-图9C示出根据发明构思的实施例的图1的存储器确定是授权图3的存储器控制器对数据的访问还是擦除数据的示例过程的流程图。

[0029] 图10示出根据发明构思的实施例的图4的删除逻辑从图1的存储器删除数据的示例过程的流程图。

具体实施方式

[0030] 现在将详细参考附图中示出其示例的本发明构思的实施例。在下面的详细描述中，为了透彻地理解本发明构思阐述了许多具体的细节。然而，应该理解的是，本领域的普通技术人员可在无需这些具体细节的情况下实施本发明构思。在其他情况下，已知的方法、过程、组件、电路和网络未被详细描述，以免不必要地模糊实施例的方面。

[0031] 将理解的是，虽然此处的术语第一、第二等可被用于描述各种元件，但是这些元件不应被这些术语所限制。这些术语仅被用于将一个元件与另一元件相区别。例如，在不脱离本发明构思的范围的情况下，第一模块可称为第二模块，同样地，第二模块可被称为第一模块。

[0032] 此处用于描述本发明构思的术语仅被用于描述具体实施例的目的，而不是意在限制本发明构思的目的。除非上下文另有清楚地说明，否则如在本发明构思和权利要求的描述中所使用的，单数形式意在包括复数形式。将理解的是，此处使用的术语“和/或”指并且包含一个或多个相关联的列出的项目的所有可能的组合。还将理解的是，术语“包括”当在说明书中被使用时表示存在陈述的特征、整数、步骤、操作、元件和/或组件，但是不排除存在或添加一个或更多个其他特征、整数、步骤、操作、元件、组件和/或上述项的组。附图的组件和特征不一定是按比例绘制的。

[0033] 安全的非易失性存储器(NVM)模块可被用于存储器空间中。NVM可配备密码和认证逻辑：来自于NVM的数据可仅在用户具有匹配密钥的情况下被访问。

[0034] 安全模块的控制流可进行如下操作：

[0035] 1)存储器控制器在复位(无论是硬件引起的复位(诸如上电)或软件引起的复位)时读取双线存储器模块(DIMM)串行存在检测(SPD)的SPD以确定DIMM是否具有安全模式。

[0036] 2)如果DIMM不具有安全模式，则系统正常进行。

[0037] 3)否则，存储器控制器通过新定义的模式寄存器集(MRS)命令向DIMM发送密码。

[0038] 4)如果该密码被识别，则DIMM被解锁并且DIMM按照常规DIMM进行操作。DIMM可向存储器控制器发送信号，授权对DIMM的访问。可通过DQ总线传输该“认证”信号。然后系统可正常进行操作。

[0039] 5)如果该密码不被识别，则DIMM可要求存储器控制器重试。重试信号也可通过DQ总线被发送。然后存储器控制器可通过MRS命令重新发送密钥。

[0040] 6)如果重试的次数超过阈值，则DIMM可停止允许存储器控制器重试。DIMM转而通过DQ总线向存储器控制器发送“不授权”信号。然后DIMM可在授权存储器控制器访问DIMM之前擦除它的内容。

[0041] 图1示出根据本发明构思的实施例的具有使用安全存储器的各种主机的数据中心。在图1中，数据中心105可包括各种主机(也可被称为服务器)，诸如主机110、主机115、主机120和主机125。数据中心105可支持可被任何用户使用的客户机(诸如客户机130)。客户

机130上的用户可从数据中心105有效地“租赁”任何服务所需的资源。例如，数据中心105可向用户提供购买可被送达到他的/或她的家的产品的能力；数据中心105可向用户“租赁”存储器以在选择商品并完成支付期间存储用户的购物车。虽然图1示出数据中心105包括四个主机110、115、120和125和一个客户机130，但是本发明构思的实施例可支持任何数量的主机和/或客户机。由于为了本公开的目的而主机110、主机115、主机120和主机125是可互换，因此对主机110的进一步的参考也意图包括对主机110、主机120和主机125的参考。

[0042] 图1示出包括网络135的数据中心105。网络135可采用任何期望的形式，包括局域网(LAN)、广域网(WAN)、全球网络(诸如因特网)和有线或无线网络。此外，网络135可以是这些网络的任何组合，从而允许数据中心是分布式的而不是位于单个地理位置。

[0043] 尽管可在数据中心105内的主机110、主机115、主机120和主机125中的任何一个主机中发现相同的细节，但图1也示出了主机110的细节。主机110被示出为包括处理器140、存储器145、电可擦除可编程只读存储器(EEPROM)150和存储器装置155。处理器140可以是任何种类的处理器：例如，Intel Xeon、Celeron、Itanium或Atom处理器、AMD Opteron处理器、ARM处理器等。存储器145可以是任何种类的存储器，诸如动态随机存取存储器(DRAM)、永久性随机存取存储器(PRAM)、静态随机存取存储器(SRAM)、铁电随机存储器(FRAM)或非易失性随机存取存储器(NVRAM)(诸如磁阻随机存取存储器(MRAM))。此外，存储器145可以是混合存储器，其中，混合存储器在单个存储器模块中包括易失性存储器装置和非易失性存储器装置的任何期望的组合。但是与传统存储器模块相反，如下文所描述的，存储器145可以是安全存储器模块。存储器装置155可以是任何种类的存储器装置，包括传统的硬盘驱动器或闪存和其他可能的存储器装置。

[0044] EEPROM 150可存储重要产品数据(VPD)160。如下文描述，尽管存储器145可指定存储器145自身是安全存储器还是不是安全存储器，重要产品数据160可提供针对这一信息的备用资源。虽然图1示出重要产品数据160被存储在EEPROM 150内，但是本发明构思的实施例可支持使用任何其他存储介质。例如，EEPROM 150可被可擦除可编程只读存储器(EPROM)或闪存、或一些其他替代物代替。

[0045] 图2示出图1的主机110、主机115、主机120和主机125的额外的细节。参照图2，通常地，主机110、主机115、主机120和主机125包括一个或更多个处理器140，其中，处理器140可包括可被用于协调主机110、主机115、主机120和主机125的组件的操作的存储器控制器205和时钟210。处理器140也可耦接到存储器145，其中，存储器145可包括例如随机存取存储器(RAM)、只读存储器(ROM)或其他状态保持介质。处理器140也可耦接到存储装置155和网络连接器215，其中，网络连接器215可以是例如以太网连接器或无线连接器。处理器140也可连接到总线220，其中，可使用输入/输出引擎230管理的用户界面225和输入/输出端口附接到总线220。

[0046] 图3示出图1的存储器145的细节。在图3中，存储器145可包括寄存器时钟驱动器(RCD)305和存储器芯片310、存储器芯片315、存储器芯片320、存储器芯片325、存储器芯片330、存储器芯片335、存储器芯片340和存储器芯片345。虽然图3示出了典型的具有8个存储数据的芯片的DRAM模块，但是本发明构思的实施例可包括其他类型的且包括任何期望数量的芯片或芯片替代物的存储器模块。

[0047] 存储器控制器205可与存储器145连接。存储器控制器205可将读取和写入数据的

命令直接发送到存储器片310-存储器片345。存储器控制器205也可与RCD 305连接以使用命令/地址信号和时钟信号。

[0048] 在存储器145已经执行了复位操作后，存储器控制器205可确定存储器145是否正在安全模式下运行。复位操作可以是硬件引起的复位(诸如当图1的主机110最初上电)或者软件引起的复位(诸如当存储器控制器205通知存储器145用户的资源租赁已结束(将在下文描述))。存储器控制器205可通过查询串行存在检测(SPD)350来确定存储器145是否正在安全模式下运行。可选地，如以上参照图1所描述的，存储器控制器205可从EEPROM访问图1的重要产品数据160，其中，重要产品数据160可指示存储器145是否正在安全模式下运行。

[0049] 如果存储器145不是正在安全模式下运行，则存储器控制器205可按照传统惯例访问存储器145。但是如果存储器145正在安全模式下运行，则存储器控制器205可尝试向存储器145认证以获取访问。(注意在这里的上下文中，“认证以获取访问”不意味着存储器控制器205可被拒绝访问存储器145，而是如下文所述，仅在存储器145已经擦除了任何先前的数据之后才可允许存储器控制器205访问存储器145)。存储器控制器205可通过模式寄存器设置(MRS)命令向RCD 305发送密码。然后RCD 305可将接收的密码与存储在存储器355中的密码进行比较。如果接收的密码与存储的密码匹配，则存储器控制器205可被授权对存储器145的访问：该信号可通过DQ总线被发送。否则，存储器145可将存储在存储器芯片310-存储器芯片345中的任何数据擦除，之后，存储器控制器205可被授权对存储器145的访问。

[0050] 为促进进一步的访问，RCD 305也可将接收的密码存储在存储器355中，使存储器控制器205能够在将来使用接收的密码向存储器145进行认证。RCD305也可重写在存储器305中现有的密码，以防止原来存储的密码在将来被接受。擦除存储的密码也可以是擦除存储在存储器145中的数据的一部分，也是为了防止原来存储的密码在将来被接受。

[0051] 存储器控制器205可以以任何期望的方式产生密码。示例方法可以是：产生随机的密码；从预定的密码列表中选择密码；产生用户ID的散列；或者使用可信平台模块(TPM)产生密码。本发明构思的实施例也可支持产生密码的其他技术。

[0052] 本发明概念的实施例比传统的系统具有一些优点。通过提供保护存储器145的机制，一个用户能够读取另一用户的数据的危险被显著地降低。但是因为用户的数据当被存储在存储器中时不被加密，所以不需要包括加密逻辑以管理加密的数据。由于不需要花时间执行加密/解密，所以省掉对数据进行加密的需要也减少了从存储器145访问数据所需的时间。

[0053] 针对传统系统的有用的比方可以是将存储器与银行的保险箱系统比拟。要从银行中的保险箱访问东西，必须出示该保险箱的钥匙。如果用户随后需要访问不同保险箱中的数据，则第一个保险箱必须被关闭并且下一个保险箱被打开。这与对数据进行加密的传统系统相似：要访问任何具体的数据，则那个数据必须被解密，而这使访问变得缓慢。

[0054] 相反地，存储器145可与房子比拟，用于访问存储器145的密码可与门的钥匙比拟。直到门被打开为止，房子的内容受到保护。门一旦被打开，数据可被自由地访问而没有延迟：由于数据不被加密，所以不会引起进一步的延迟。

[0055] 图4示出图1的存储器145的另一种示图。与示出存储器145的具体实施例的图3相反的，图4示出存储器145的更抽象的表示。存储器145可包括可存储实际用户数据的数据存储器310-数据存储器345、以及可从数据存储器310-数据存储器345读取数据的数据读取逻

辑405和向数据存储器310-数据存储器345写入数据的数据写入逻辑410。

[0056] 存储器145也可包括可确定用户是否将被授权访问存储器145的认证逻辑415。如上所述，“被授权访问”不意味着存在用户可能不被允许使用存储器145的可能性，而是在用户被授权访问之前，存储器145可将数据存储器310-数据存储器340中的任何数据擦除。认证逻辑415可包括接收器420、阻止逻辑425、比较器430和擦除逻辑435。接收器420可从图3的存储器控制器205接收密码。在认证逻辑415确定在图3的存储器控制器205被授权访问之前数据存储器310-数据存储器345是否应被擦除时，阻止逻辑425可阻止来自图3的存储器控制器205的对存储器145的访问。比较器430可将从图3的存储器控制器205接收的密码与存储在密码存储器355中的密码进行比较来看密码是否匹配。如果它们不匹配，则擦除逻辑435可在图3的存储器控制器205被授权访问存储器145之前将数据存储器310-数据存储器345的内容擦除。

[0057] 擦除逻辑435可按照适合于存储器145采用的形式的任何方式运行。例如，如果存储器145仅使用易失性存储器，则擦除逻辑435可通过防止数据存储器310-数据存储器345中的值的刷新足够长时间，使得数据存储器310-数据存储器345中存储的所有值丢失(即，存储在数据存储器310-数据存储器345中的任何值都不再被存储)，从而有效地对存储器145进行擦除。(这一过程将花费多长时间可取决于数据存储器310-数据存储器345的具体类型和形式、以及其他的因素，诸如与数据存储器310-数据存储器345的制造相关的偏心距。例如，如果存储器145使用易失性存储器并且处于寒冷的环境中，则由于存储器145的内容可能不在合理的时间内妥协，所以擦除逻辑435可能需要向存储器145写入值以对存储器145进行擦除。)在本发明构思的其他实施例中，按照所期望的，擦除逻辑435可用常数值(诸如0或1)重写数据存储器310-数据存储器345中存储的值。在本发明构思的其他实施例中，擦除逻辑435可执行设计的写序列以擦除任何值。这样的序列的示例可包括由美国国防部(DoD)或其他政府机构和非政府组织设计的序列。例如，诸如序列可包括将所有的0，然后所有的1，然后随机的模式写入存储器。在可使用闪存的本发明构思的另一实施例中，在图3的存储器控制器205被授权访问存储器145之前，存储器145中的所有数据块(或至少包含有效数据的那些块)可遭受直接垃圾收集。

[0058] 认证逻辑415也可包括密码写入逻辑440。密码写入逻辑440可将密码写入密码存储器355。例如，如果从图3的存储器控制器205接收的密码与密码存储器355中存储的密码不匹配，则在擦除逻辑435将数据存储器310-数据存储器345的内容擦除后，密码写入逻辑440可将从图3的存储器控制器205接收的密码写入密码存储器355。以这种方式，图3的存储器控制器205之后可使用相同的密码向存储器145认证，任何其他存储器控制器将不能认证(除非其他存储器控制器设法产生相同密码这样不可能的事件)，从而保护用户的数据免受未授权的访问。

[0059] 在图3-图4中，由系统确定何时使存储器145复位。即，存储器145不知道任何特定的用户租赁了存储器145多久。因此，图3的存储器控制器205(或图1的数据中心105的服务提供商)可通过计时器追踪用户已经访问存储器145的时长。一旦用户的租赁已经到期，图3的存储器控制器205(或图1的主机110的任何其他期望的组件)可向存储器145(或更一般地，向图1的服务器110)发出软件引起的复位命令，该复位命令可保护用户的数据不被另一用户读取。

[0060] 在图3-图4中，密码存储器355被示出为与SPD 350分离。但是如果需要，本发明构思的一些实施例可将密码存储在SPD 350的未使用的部分或供应商指定的区域中。这样的方法可避免引入新的仅用于密码的存储器。

[0061] 图5示出图3-图4的存储器145使用从图3的存储器控制器205接收的密码确定是授权对图3-图4的存储器145中存储的数据的访问还是擦除存储在图3-图4的存储器145中的数据。在图4中，接收器420可从图3的存储器控制器205接收密码505。然后比较器430可将接收的密码505与从密码存储器355读取的存储的密码510进行比较。如果接收的密码505与存储的密码510匹配，则比较结果515可指示图3的存储器控制器205可被授权立即访问图4的存储器145；否则，比较结果515可指示图3的存储器控制器205应被阻止，直到图3-图4的数据存储器310-数据存储器345中存储的数据被图4的擦除逻辑435擦除。

[0062] 图5也示出了阈值520的使用。在本发明构思的一些实施例中，比较器430可执行对接收的密码505与存储的密码510的单次比较，以确定是否授权图3的存储器控制器205访问图3-图4的存储器145。但是本发明构思的其他实施例可允许图3的存储器控制器205提供多个接收的密码505。例如，在比较器确定接收的密码505与存储的密码510不匹配之后，图4的认证逻辑415可通过DQ总线向图3的存储器控制器205发送请求图3的存储器控制器205重新发送接收的密码505的信号。允许重试可防止数据的意外的改变：例如，由于当发送接收的密码505时的干扰。然后比较器430可测试接收的密码505达由阈值520所指定的次数，之后，如果没有发现匹配，则比较结果515可指定将数据从图3-图4的存储器145中的图3-图4的数据存储器310-数据存储器345擦除。阈值520可以被设置为任何期望的整数值；但是由于图3的存储器控制器205被暂时地阻止访问图3-图4的存储器145，直到本发明构思的实施例已经确定是否擦除图3-图4的数据存储器310-数据存储器345中的数据(如果需要，则执行擦除)为止，所以使阈值520保持较小的整数值会是有利的，以减少图3-图4的存储器控制器205被阻止的时间。

[0063] 图6示出根据本发明构思的实施例的可在两个用户之间共享资源的图1的存储器145的示例。在图6中，存储器145可包括存储器的两个部分605和610，这两个部分中的每个部分可被视作单独的存储器模块。例如，存储器145可以是具有被测量为兆兆字节或更大字节的容量的DIMM。由于存储器的该容量大于单个用户所需，所以将整个存储器145分配给单个用户是浪费的。相反，存储器145的一部分(诸如部分605)可被分配给用户，而将部分610留给包括另一用户的其他用户。

[0064] 两个存储器控制器205和620可使用接口615与存储器145连接。例如，存储器控制器205可与存储器145的部分605连接，存储器控制器620可与存储器145的部分610连接。以这种方式，尽管存储器145可存储两个不同用户的数据，但是每个用户仅可访问他们自己的数据，而不可访问其他用户的数据。这种机制保护了每个用户的数据。

[0065] 当一个用户对存储器145的部分的租赁结束时，可启动存储器145的软件引起的复位。例如，假设已经租赁了部分605的用户已经结束了对部分605的租赁。存储器145可随后被复位。当存储器145的软件引起的复位完成时，存储器控制器620可向存储器145提供它的密码。存储器控制器620可因此向存储器145认证它本身，重新获得对存储在部分610中的用户数据的访问。虽然软件引起的复位和认证过程可延迟对部分610中的用户数据的访问，但是这个延迟并不显著，并且甚至可能不会被用户注意到。

[0066] 另一方面，存储器控制器205可向存储器145提供新的密码。因为这个密码将(可能)不会被识别，所以存储器控制器205将不能向存储器145认证。因此，部分605可在另一用户可能租赁部分605之前被擦除，从而保护其数据先前被存储在部分605中的用户。

[0067] 虽然图6示出存储器145被划分为两部分605和610，但是本发明构思的实施例可支持在存储器145中的任何数量的部分。图6中的两个部分的使用仅是示例。此外，根据存储器145的实施例，存储器145可：针对存储器145的每个部分包括一个RCD；针对存储器145的所有部分包括一个RCD或者根本不包括RCD。

[0068] 图7A-图7C示出根据本发明构思的实施例的图3的存储器控制器205请求对图1的存储器145的访问的示例步骤的流程图。在图7A中，在框705，图3的存储器控制器205可确定图1的存储器145已复位(或者通过硬件引起的复位或者通过软件引起的复位)。在框710，存储器控制器205可确定图1的存储器145是否正在安全模式下运行：例如，通过从图3的SPD 350读取相关数据。在框715，如果图1的存储器145不是正在安全模式下运行，则图3的存储器控制器205可接收对图1的存储器145的访问。

[0069] 另一方面，如果图1的存储器145正在安全模式下运行，则在框720，图3的存储器控制器205可选择用于图1的存储器145的密码。在框725，响应于来自于图1的存储器145的请求，图3的存储器控制器205可向图1的存储器145发送密码。

[0070] 在框730(图7B)，图3的存储器控制器205可确定密码是否被接受。如上所述，图1的存储器145可通过DQ总线发送信号，以指示密码是否被接受并且图3的存储器控制器205是否被授权。如果密码未被接受，则在框735，图3的存储器控制205可接收重新发送密码的请求，并且控制可返回图7A的框720。可选地，在框740，图3的存储器控制器205可接收对图1的存储器145的访问，但是仅在图1的存储器145已擦除了图3-图4的数据存储器310-数据存储器345中的所有数据之后。框735和框740之间的不同表示存储器145是否已执行了阈值次数的密码比较：这是因为图3的存储器控制器205可能不知道阈值，图3的存储器控制器205可能仅能够对图1的存储器145做出的额外的密码请求进行响应。

[0071] 另一方面，如果密码被接受，则在框745，图3的存储器控制器205可接收对图1的存储器145的访问，而不需要图3-图4的数据存储器310-345中的数据被首先擦除。

[0072] 在框750(图7C)，图3的存储器控制器205可测量自图3的存储器控制器205被授权访问图1的存储器145以来已经过去了多长时间。在框755，图3的存储器控制器205可确定是否阈值量的时间(用户租赁图1的存储器145的时间量)已经过去。如果没有，则图3的存储器控制器205可等待一会并且再次测量已经过去了多长时间。一旦租赁的时间已经过去，在框760，图3的存储器控制器205可指示图1的存储器145执行软件引起的复位，在此之后处理结束。

[0073] 图8示出根据本发明构思的实施例的图3的存储器控制器205选择密码以请求对图1的存储器145的访问的步骤的流程图。在图8中，在框805，图3的存储器控制器205可产生随机密码以在向图1的存储器145的认证中使用。可选地，在框810，图3的存储器控制器205可从密码列表中选择密码以在向图1的存储器145的认证中使用。可选地，在框815，图3的存储器控制器205可将用户ID散列以产生密码，以在向图1的存储器145的认证中使用。可选地，在框820，图3的存储器控制器205可从可信平台模块获取密码以在向图1的存储器145的认证中使用。

[0074] 图9A-图9C示出根据本发明构思的实施例的图1的存储器145确定是授权图3的存储器控制器205访问数据还是擦除数据的示例步骤的流程图。在图9A中，在框905，图1的存储器145可接收了解图1的存储器145是否正在安全模式下运行的请求。在框910，图1的存储器145可向图3的存储器控制器205发送指示图1的存储器145是否在安全模式下运行的信号。在框915，图1的存储器145可从图3的存储器控制器205接收访问图1的存储器145的请求。

[0075] 在框920，图1的存储器145可确定其是否正在安全模式下运行。如果图1的存储器145不是正在安全模式下运行，则在框925，图1的存储器145可授权对图1的存储器145的访问。否则，在框930，认证逻辑415可从图3的存储器355访问图5的存储的密码。

[0076] 在框935(图9B)，图1的存储器145可向图3的存储器控制器205请求图5的密码505。在框940，图1的存储器145可从图3的存储器控制器205接收图5的密码505。在框945，图4的比较器430可将图5的接收的密码505与图5的存储的密码510进行比较。

[0077] 在框950，图4的认证逻辑415可确定图5的比较结果515，其中，比较结果515指示图5的接收的密码505与图5的存储的密码的比较是否指示匹配。如果匹配，则在框955，图1的存储器145可授权图3的存储器控制器205访问图1的存储器145。

[0078] 在框960(图9C)，假设图5的接收的密码505与图5的存储的密码510不匹配，则图4的认证逻辑415可确定是否已经发生了阈值次数的密码比较。如果没有发生阈值次数的密码比较，则控制返回到图9B的框935以使图1的存储器145向图3的存储器控制器205请求新的密码。否则，在框965，图4的擦除逻辑435可从图3-图4的数据存储器310-数据存储器345擦除数据。随后，在框970，图4的密码写入逻辑可将图5的接收的密码505写入图3的密码存储器355中，在此之后，在框975，图1的存储器145可授权图3的存储器控制器205访问图1的存储器145。

[0079] 在框980，不管图1的存储器145是在擦除了图3-图4的数据存储器310-数据存储器345中的数据的情况下还是在无需擦除图3-图4的数据存储器310-数据存储器345中的数据的情况下授权图3的存储器控制器205访问图1的存储器145，在框980，图1的存储器145可从图3的存储器控制器205接收信号以执行软件引起的复位，并且在框985，图1的存储器145可执行软件引起的复位，在此之后处理结束。

[0080] 图10示出根据本发明构思的实施例的图4的擦除逻辑435从图1的存储器145擦除数据的示例步骤的流程图。在图10中，在框1005，图4的擦除逻辑可在由用户使用过的存储器的块上执行垃圾收集。可选地，在框1010，图4的擦除逻辑435可用常数值重写图1的存储器145中的所有数据。可选地，在框1015，图4的擦除逻辑435可执行重写序列，诸如在图1的存储器145中的所有数据上全部写入0，然后全部写入1，然后写入随机模式。可选地，在框1020，图4的擦除逻辑可防止图1的存储器145中的小区被刷新，直到图1的存储器可保证所有的存储的数据值已丢失这样的时刻。

[0081] 在图7-图10中，示出了本发明构思的一些实施例。但是本领域的技术人员将清楚的是通过改变框的顺序、通过省略框或者通过包含未示出在附图中的链接也可能实现本发明构思的其他实施例。不论是否被描述，对流程图的所有这样的改变都被视为是本发明构思的实施例。

[0082] 以下描述意在提供可在其中实现本发明构思的特定方面的合适的机器的简洁的、

一般的说明。所述机器可至少部分地通过来自传统输入装置(诸如键盘、麦克风等)的输入、以及通过从另一机器接收的指令、与虚拟现实(VR)环境的交互、生物反馈或其他输入信号被控制。如此处使用的,术语“机器”意在广泛地包括单个机器、虚拟机器、或通信地耦接的机器、虚拟机器或装置一起运行的系统。示例机器包括计算装置(诸如个人计算机、工作站、服务器、便携式计算机、手持装置、电话、平板等)和运输装置(诸如私人或公共交通,例如,汽车、火车、出租车等)。

[0083] 机器可包括嵌入式控制器(诸如可编程或不可编程逻辑装置或阵列)、专用集成电路(ASIC)、嵌入式计算机、智能卡等。机器可利用一个或更多个连接连接到一个或更多个远程机器,诸如通过网络接口、调制解调器或其他通信耦合。机器可通过物理和/或逻辑网络(诸如内联网、互联网、局域网、广域网等)的方法互相连接。本领域的技术人员将理解网络通信可利用各种有线和/或无线短距离或长距离运营商和协议,包括射频(RF)、卫星、微波、电气电子工程协会(IEEE)802.11、蓝牙®、光学、红外线、电缆、激光等。

[0084] 本发明构思的实施例可通过参照或结合相关数据(包括函数、程序、数据结构、应用程序等)被描述,其中,所述相关数据当被机器访问时导致该机器执行任务或定义抽象数据类型或低级硬件环境。相关数据可被存储在例如易失性存储器和/或非易失性存储器(例如,RAM、ROM等)中,或被存储在其他存储器装置和它们的关联存储介质中,包括硬件驱动器、软盘、光学存储器、磁带、闪存、记忆棒、数字视频磁盘、生物存储器等。相关数据可以以包、串行数据、并行数据、传播信号等的形式通过传输环境(包括物理和/或逻辑网络)被传送,并可被以压缩或加密的格式使用。相关数据可在分布式环境中被使用,并被本地地和/或远程地存储以用于机器访问。

[0085] 本发明构思的实施例包括包含可由一个或更多个处理器执行的指令得有形的、非暂时性机器可读介质,其中,所述指令包含执行此处描述的本发明构思的元件的指令。

[0086] 已经参照所示实施例描述并示出了本发明构思的原理,将要理解的是,所示实施例可在不脱离这样的原理的情况下进行排列和细节上的修改,并且可以以任何期望的方式组合。而且,虽然前面的讨论集中在特定的实施例,但是还考虑其他的配置。具体地,尽管诸如“根据本发明构思的实施例”等表述被用于此处,但是这些表述意味着一般参考实施例的可能性,而不是意在将本发明构思限制于特定实施例。如此处使用的,这些术语可参考可结合在其他实施例中的相同或不同的实施例。

[0087] 上述示例性实施例不应被解释为限制其发明构思。虽然已经描述了一些实施例,但是本领域的技术人员将容易地认识到:在本质上不脱离本公开的新颖教导和优点的情况下可对那些实施例做出许多修改。因此,所有这样的修改都意在被包括在如权利要求所定义的本发明构思的范围内。

[0088] 本发明构思的实施例可扩展到下列声明而没有限制:

[0089] 声明1、本发明构思的实施例包括存储器,其中,该存储器包含:

[0090] 数据存储器,用于针对第一用户的数据;

[0091] 数据读取逻辑,用于从数据存储器读取数据;

[0092] 数据写入逻辑,用于向数据存储器写入数据;

[0093] 密码存储器,用于存储的密码;

[0094] 接收器,用于从存储器控制器接收密码;

[0095] 比较器，用于将接收的密码与存储的密码进行比较；

[0096] 擦除逻辑，用于如果接收的密码与存储的密码不同，则将数据存储器中的数据擦除；

[0097] 阻止逻辑，用于阻止来自存储器控制器的对数据存储器的访问，直到比较器完成操作为止，

[0098] 其中，接收的密码或存储的密码不用于对存储器中存储的数据进行加密。

[0099] 声明2、根据声明1，本发明构思的实施例包括存储器，其中，阻止逻辑能够执行操作以阻止来自存储器控制器的对数据存储器的访问。

[0100] 声明3、根据声明1，本发明构思的实施例包括存储器，其中，该存储器还包含将接收的密码写入密码存储器的密码写入逻辑。

[0101] 声明4、根据声明1，本发明构思的实施例包括存储器，其中，该存储器还包含指定存储器是否正在安全模式下运行的串行存在检测(SPD)。

[0102] 声明5、根据声明4，本发明构思的实施例包括存储器，其中，如果SPD指定存储器不是正在安全模式下运行，则阻止逻辑允许存储器控制器访问数据存储器，而无需调用比较器。

[0103] 声明6、根据声明1，本发明构思的实施例包括存储器，其中，该存储器还包含指定存储器是否正在安全模式下运行的重要产品数据(VPD)。

[0104] 声明7、根据声明6，本发明构思的实施例包括存储器，其中，该存储器还包含存储VPD的电可擦除可编程只读存储器(EEPROM)。

[0105] 声明8、根据声明6，本发明构思的实施例包括存储器，其中，如果VPD指定存储器不是正在安全模式下运行，则阻止逻辑允许存储器控制器访问数据存储器，而无需调用比较器。

[0106] 声明9、根据声明1，本发明构思的实施例包括存储器，其中，如果阈值数量的接收的密码都与存储的密码不同，则擦除逻辑能够执行操作以将数据存储器中的数据擦除。

[0107] 声明10、根据声明1，本发明构思的实施例包括存储器，其中：

[0108] 该存储器还包含：第二数据存储器，存储针对第二用户的第二数据；

[0109] 数据读取逻辑能够执行操作以从第二数据存储器读取第二数据；

[0110] 数据写入逻辑能够执行操作以向第二数据存储器写入第二数据；

[0111] 密码存储器能够执行操作以存储第二密码；

[0112] 接收器能够执行操作以从第二存储器控制器接收第二密码；

[0113] 比较器能够执行操作以将接收的第二密码与存储的第二密码进行比较；

[0114] 擦除逻辑能够执行操作以：如果接收的第二密码与存储的第二密码不同，则将第二数据存储器中的第二数据擦除；

[0115] 阻止逻辑能够执行操作以：阻止来自第二存储器控制器的对第二数据存储器的访问，直到比较器完成操作之后为止。

[0116] 声明11、根据声明10，本发明构思的实施例包括存储器，其中，存储器控制器是第二存储器控制。

[0117] 声明12、根据声明1，本发明构思的实施例包括存储器，其中，存储器从包括以下项的集合得到：易失性存储器模块、非易失性存储器模块、以及易失性存储器装置与非易失性

存储器装置的任何组合。

[0118] 声明13、根据声明1，本发明构思的实施例包括存储器，其中，该存储器还包含包括接收器、比较器、擦除逻辑和阻止逻辑的寄存器时钟驱动器(RCD)。

[0119] 声明14、根据声明13，本发明构思的实施例包括存储器，其中，RCD还包含数据读取逻辑和数据写入逻辑。

[0120] 声明15、本发明的实施例包括一种方法，该方法包含：

[0121] 确定存储器已复位；

[0122] 确定存储器正在安全模式下运行还是正在非安全模式下运行，并且，

[0123] 如果存储器正在安全模式下运行，则：

[0124] 针对用户选择密码；

[0125] 将所述密码发送到存储器；

[0126] 接收对存储器的访问，

[0127] 其中，所述密码不用于对存储器中存储的数据进行加密。

[0128] 声明16、根据声明15，本发明构思的实施例包括一种方法，该方法还包含：如果存储器正在非安全模式下运行，则在不使用密码的情况下接收对存储器的访问。

[0129] 声明17、根据声明15，本发明构思的实施例包括一种方法，其中，将所述密码发送到存储器的步骤包括：将所述密码发送到存储器阈值次数。

[0130] 声明18、根据声明15，本发明构思的实施例包括一种方法，其中，接收对存储器的访问的步骤包括：接收对经过擦除的存储器的访问。

[0131] 声明19、根据声明15，本发明构思的实施例包括一种方法，其中，接收对存储器的访问的步骤包括：接收对存储在存储器中的数据的访问。

[0132] 声明20、根据声明15，本发明构思的实施例包括一种方法，其中，该方法还包含：

[0133] 测量从存储器复位开始的时长；

[0134] 如果从存储器复位开始的时长大于阈值，则向存储器发送软件引起的复位。

[0135] 声明21、根据声明15，本发明构思的实施例包括一种方法，其中，存储器从包括以下项的集合得到：易失性存储器模块、非易失性存储器模块、以及易失性存储器装置与非易失性存储器装置的任何组合。

[0136] 声明22、根据声明15，本发明构思的实施例包括一种方法，其中，该存储器包含分配给第一用户的第一部分和分配给第二用户的第二部分。

[0137] 声明23、根据声明15，本发明构思的实施例包括一种方法，其中，针对用户选择密码的步骤包括：产生随机密码。

[0138] 声明24、根据声明15，本发明构思的实施例包括一种方法，其中，针对用户选择密码的步骤包括：从可用密码的列表选择密码。

[0139] 声明25、根据声明15，本发明构思的实施例包括一种方法，其中，针对用户选择密码的步骤包括：将密码产生为用户的标识符的散列。

[0140] 声明26、根据声明15，本发明概念的实施例包括一种方法，其中，针对用户选择密码的步骤包括：从可信平台模块访问密码。

[0141] 声明27、本发明构思的实施例包括一种方法，其中，该方法包括：

[0142] 将指示存储器正在安全模式下运行的信号从存储器发送到存储器控制器；

[0143] 从存储器控制器接收密码；

[0144] 如果接收的密码与存储的密码不匹配，则：

[0145] 对存储器进行擦除；

[0146] 向存储器控制器提供对存储器的访问，

[0147] 其中，接收的密码或存储的密码不用于对存储在存储器中的数据进行加密。

[0148] 声明28、根据声明27，本发明构思的实施例包括一种方法，其中，该方法还包含：如果接收的密码与存储的密码不匹配，则将接收的密码存储在存储器中。

[0149] 声明29、根据声明27，本发明构思的实施例包括一种方法，其中，该方法还包含：如果接收的密码与存储的密码匹配，则向存储器控制器提供对存储器的访问。

[0150] 声明30、根据声明27，本发明构思的实施例包括一种方法，其中，该方法还包含：在对存储器进行擦除之前将接收的密码与存储的密码比较阈值次数。

[0151] 声明31、根据声明27，本发明构思的实施例包括一种方法，其中，该方法还包含：

[0152] 从存储器控制器接收复位命令；

[0153] 响应于所述复位命令使存储器复位。

[0154] 声明32、根据声明31，本发明构思的实施例包括一种方法，其中，响应于复位命令使存储器复位的步骤包括：对存储器中的所有数据执行垃圾收集。

[0155] 声明33、根据声明31，本发明构思的实施例包括一种方法，其中，响应于复位命令使存储器复位的步骤包括：对存储器中所有数据执行重写序列。

[0156] 声明34、根据声明31，本发明构思的实施例包括一种方法，其中，响应于复位命令使存储器复位的步骤包括：用常数对存储器中所有数据进行重写。

[0157] 声明35、根据声明31，本发明构思的实施例包括一种方法，其中，响应于复位命令使存储器复位的步骤包括：防止对存储器中的所有数据进行刷新，直到存储器中的所有数据不再存储在存储器中为止。

[0158] 声明36、根据声明27，本发明构思的实施例包括一种方法，其中，将存储器正在安全模式下运行的信号从存储器发送到存储器控制器的步骤包括：从存储器控制器接收关于存储器是否正在安全模式下运行的请求。

[0159] 声明37、根据声明27，本发明构思的实施例包括一种方法，其中，从存储器控制器接收密码的步骤包括：向存储器控制器请求密码。

[0160] 声明38、根据声明27，本发明构思的实施例包括一种方法，其中，存储器从包括以下项的集合得到：易失性存储器模块、非易失性存储器模块、以及易失性存储器装置与非易失性存储器装置的任何组合。

[0161] 声明39、根据声明27，本发明构思的实施例包括一种方法，其中，存储器包括分配给第一用户的第一部分和分配给第二用户的第二部分。

[0162] 声明40、本发明构思的实施例包括一种物品，该物品包含有形存储介质，该有形存储介质上存储有当被机器执行时引起以下操作的非暂时性指令：

[0163] 确定存储器已复位；

[0164] 确定存储器正在安全模式下运行还是在非安全模式下运行；

[0165] 如果存储器正在安全模式下运行，则：

[0166] 针对用户选择密码；

[0167] 将该密码发送到存储器；

[0168] 接收对存储器的访问，

[0169] 其中，该密码不用于对存储在存储器中的数据进行加密。

[0170] 声明41、根据声明40，本发明构思的实施例包括一种物品，其中，该有形存储介质上还存储有当被机器执行时引起以下操作的非暂时性指令：如果存储器正在非安全模式下运行，则在不使用密码的情况下接收对存储器的访问。

[0171] 声明42、根据声明40，本发明构思的实施例包括一种物品，其中，将该密码发送到存储器的步骤包括：将该密码发送到存储器阈值次数。

[0172] 声明43、根据声明40，本发明构思的实施例包括一种物品，其中，接收对存储器的访问的步骤包括：接收对经过擦除的存储器的访问。

[0173] 声明44、根据声明40，本发明构思的实施例包括一种物品，其中，接收对存储器的访问的步骤包括：接收对存储在存储器中的数据的访问。

[0174] 声明45、根据声明40，本发明构思的实施例包括一种物品，其中，该有形存储介质上还存储有当被机器执行时引起以下操作的非暂时性指令：

[0175] 测量从存储器复位开始的时长；

[0176] 如果从存储器复位开始的时长大于阈值，则向存储器发送软件引起的复位。

[0177] 声明46、根据声明40，本发明构思的实施例包括一种物品，其中，存储器从包括以下项的集合得到：易失性存储器模块、非易失性存储器模块、以及易失性存储器装置与非易失性存储器装置的任何组合。

[0178] 声明47、根据声明40，本发明构思的实施例包括一种物品，其中，存储器包括分配给第一用户的第一部分和分配给第二用户的第二部分。

[0179] 声明48、根据声明40，本发明构思的实施例包括一种物品，其中，针对用户选择密码的步骤包括：产生随机密码。

[0180] 声明49、根据声明40，本发明构思的实施例包括一种物品，其中，针对用户选择密码的步骤包括：从可用密码的列表选择密码。

[0181] 声明50、根据声明40，本发明构思的实施例包括一种物品，其中，针对用户选择密码的步骤包括：将密码产生为用户的标识符的散列。

[0182] 声明51、根据声明40，本发明构思的实施例包括一种物品，其中，针对用户选择密码的步骤包括：从可信平台模块访问密码。

[0183] 声明52、本发明构思的实施例包括一种物品，该物品包含有形存储介质，该有形存储介质上存储有当被机器执行时引起以下操作的非暂时性指令：

[0184] 将指示存储器正在安全模式下运行的信号从存储器发送到存储器控制器；

[0185] 从存储器控制器接收密码；

[0186] 将接收的密码与存储的密码进行比较；

[0187] 如果接收的密码与存储的密码不匹配，则：

[0188] 对存储器进行擦除；

[0189] 向存储器控制器提供对存储器的访问，

[0190] 其中，接收的密码或存储的密码不用于对存储在存储器中的数据进行加密。

[0191] 声明53、根据声明52，本发明构思的实施例包括一种物品，其中，该有形存储介质

上还存储有当由机器执行时引起以下操作的非暂时性指令，，导致：如果接收的密码与存储的密码不匹配，则将接收的密码存储在存储器中。

[0192] 声明54、根据声明52，本发明构思的实施例包括一种物品，其中，如果接收的密码与存储的密码匹配，则向存储器控制器提供对存储器的访问。

[0193] 声明55、根据声明52，本发明构思的实施例包括一种物品，其中，该有形存储介质上还存储有当被机器执行时引起以下操作的非暂时性指令：在对存储器进行擦除之前，将接收的密码与存储的密码比较阈值次数。

[0194] 声明56、根据声明52，本发明构思的实施例包括一种物品，其中，该有形存储介质上还存储有当被机器执行时引起以下操作的非暂时性指令：

[0195] 从存储器控制器接收复位命令；

[0196] 响应于复位命令使存储器复位。

[0197] 声明57、根据声明56，本发明构思的实施例包括一种物品，其中，响应于复位命令使存储器复位的步骤包括：对存储器中的所有数据执行垃圾收集。

[0198] 声明58、根据声明56，本发明构思的实施例包括一种物品，其中，响应于复位命令使存储器复位的步骤包括：对存储器中的所有数据执行重写序列。

[0199] 声明59、根据声明56，本发明构思的实施例包括一种物品，其中，响应于复位命令使存储器复位的步骤包括：用常数重写存储器中的所有数据。

[0200] 声明60、根据声明56，本发明构思的实施例包括一种物品，其中，响应于复位命令使存储器复位的步骤包括：防止对存储器中的所有数据的刷新，直到存储器中的所有数据不再存储在存储器中为止。

[0201] 声明61、根据声明52，本发明构思的实施例包括一种物品，其中，将存储器正在安全模式下运行的信号从存储器发送到存储器控制器的步骤包括：从存储器控制器接收针对存储器是否正在安全模式下运行的请求。

[0202] 声明62、根据声明52，本发明构思的实施例包括一种物品，其中，从存储器控制器接收密码的步骤包括：向存储器控制器请求密码。

[0203] 声明63、根据声明52，本发明构思的实施例包括一种物品，其中，存储器从包括以下项的集合得到：易失性存储器模块、非易失性存储器模块、以及易失性存储器装置与非易失性存储器装置的任何组合。

[0204] 声明64、根据声明52，本发明构思的实施例包括一种物品，其中，存储器包括分配给第一用户的第一部分和分配给第二用户的第二部分。

[0205] 因此，鉴于这里描述的实施例的各种排列，以上详细描述和所附材料仅出于示意性的目的，而不应被理解为限制本发明构思的范围。因此，本发明构思所要求保护是如可进入权利要求及其等同物的精神和范围内的所有这样的变型。

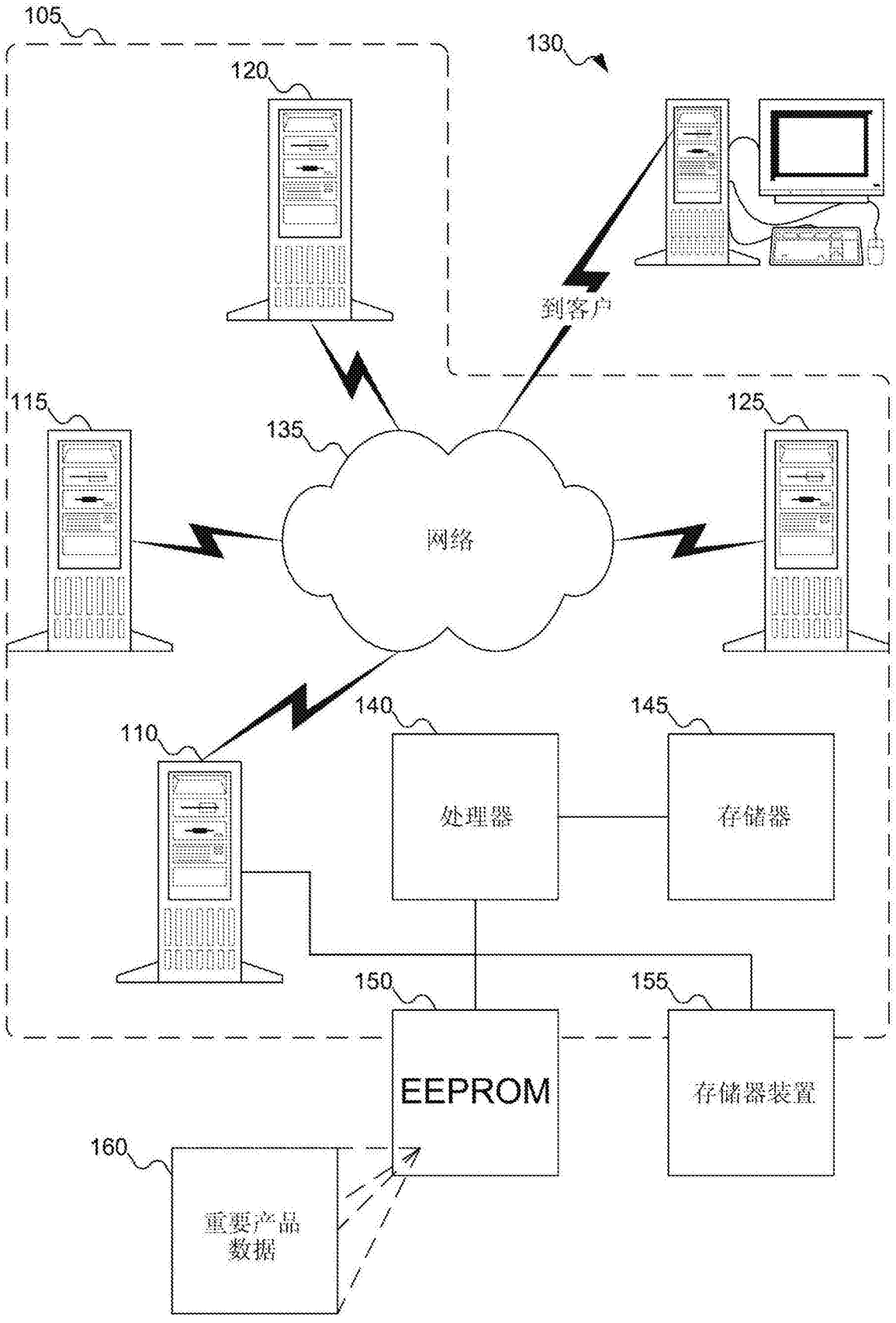

105
130
120
到客户
115
135
125
网络
110
140
145
处理器
存储器
150
155
EEPROM
存储器装置
160
重要产品
数据

图1

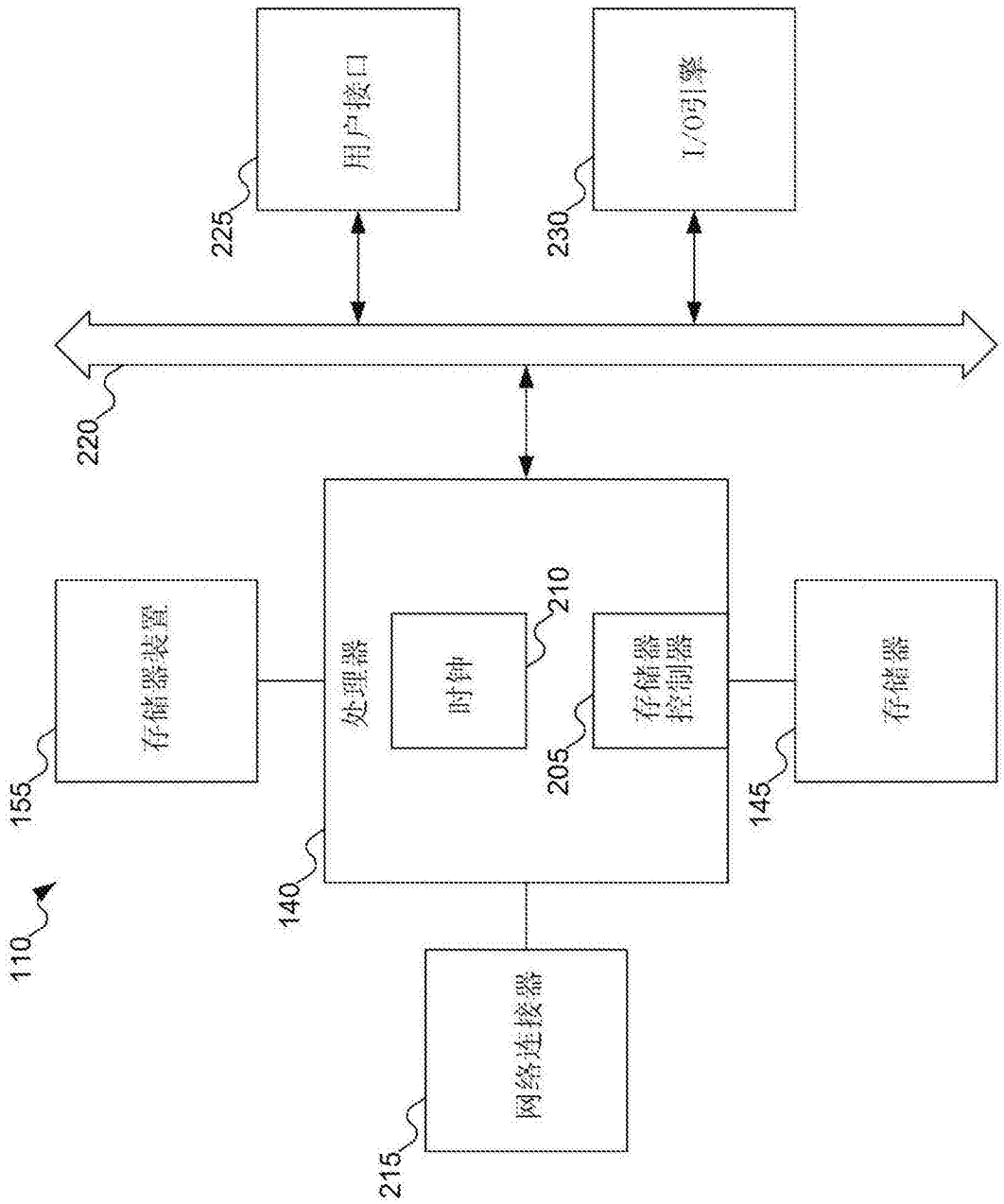

用户接口
225
I/O引擎
230
220
处理器
时钟
210
存储器控制器
205
存储器装置
155
存储器
145
140
110
网络连接器
215

图2

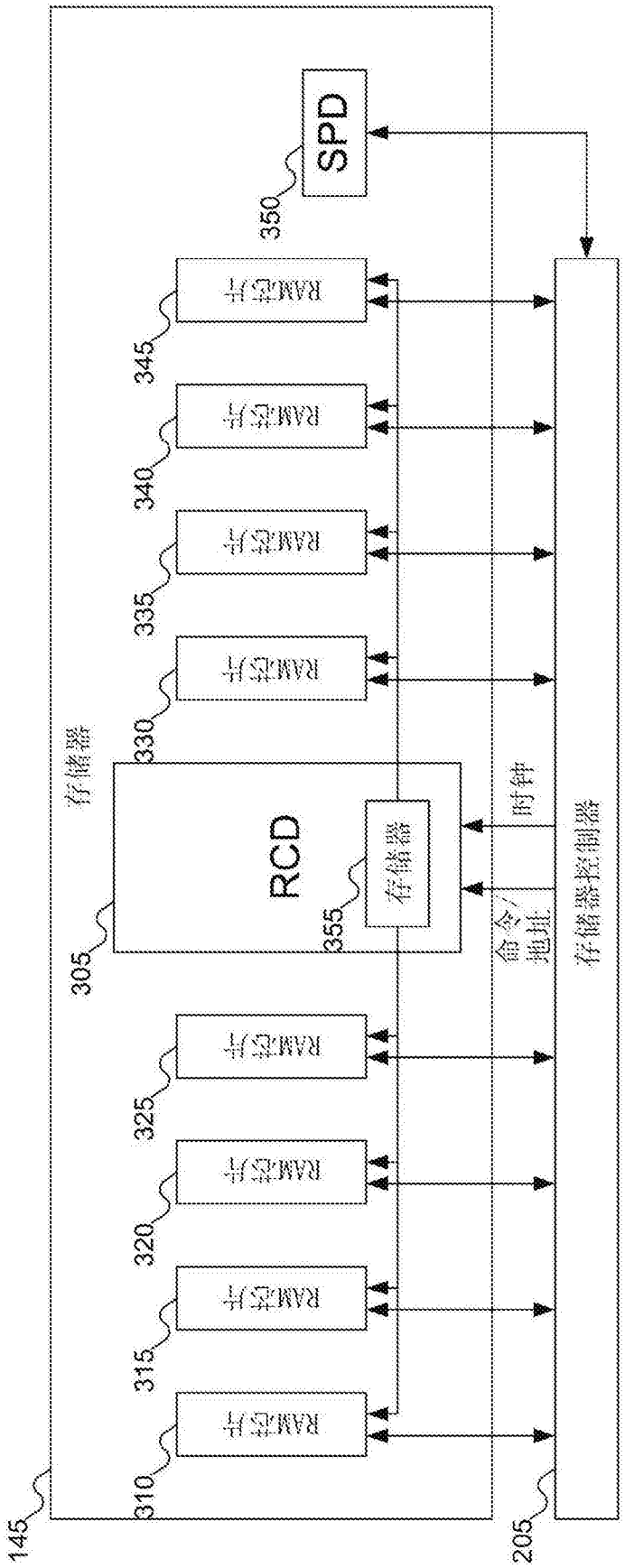

SPD
350
RAM芯片
345
RAM芯片
340
RAM芯片
335
RAM芯片
330
存储器
RCD
存储器
355
305
时钟
命令/地址
存储器控制器
RAM芯片
325
RAM芯片
320
RAM芯片
315
RAM芯片
310
145
205

图3

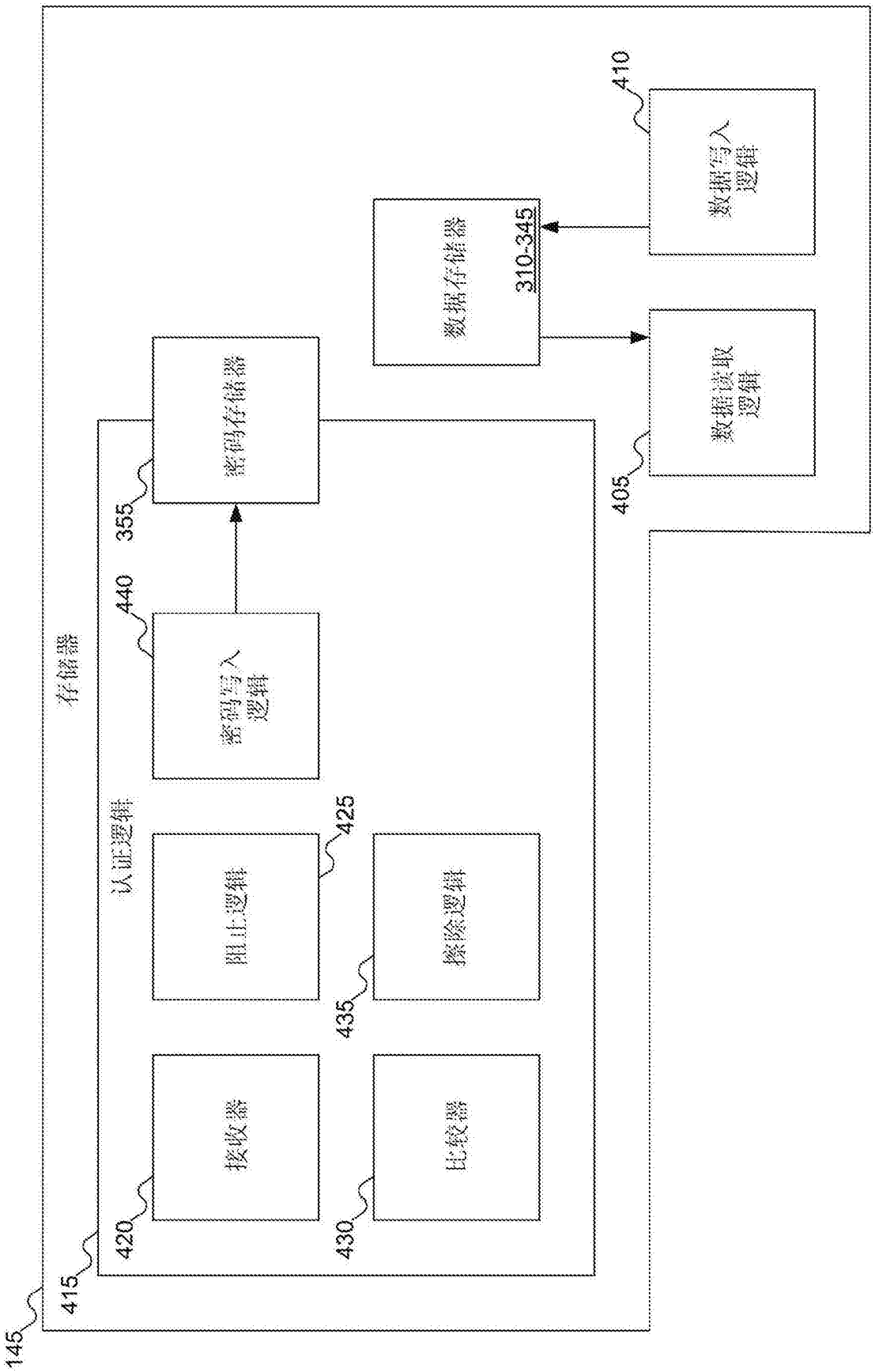

145
存储器
415
认证逻辑
420
接收器
430
比较器
435
擦除逻辑
425
阻止逻辑
440
密码写入逻辑
355
密码存储器
405
数据读取逻辑
310-345
数据存储器
410
数据写入逻辑

图4

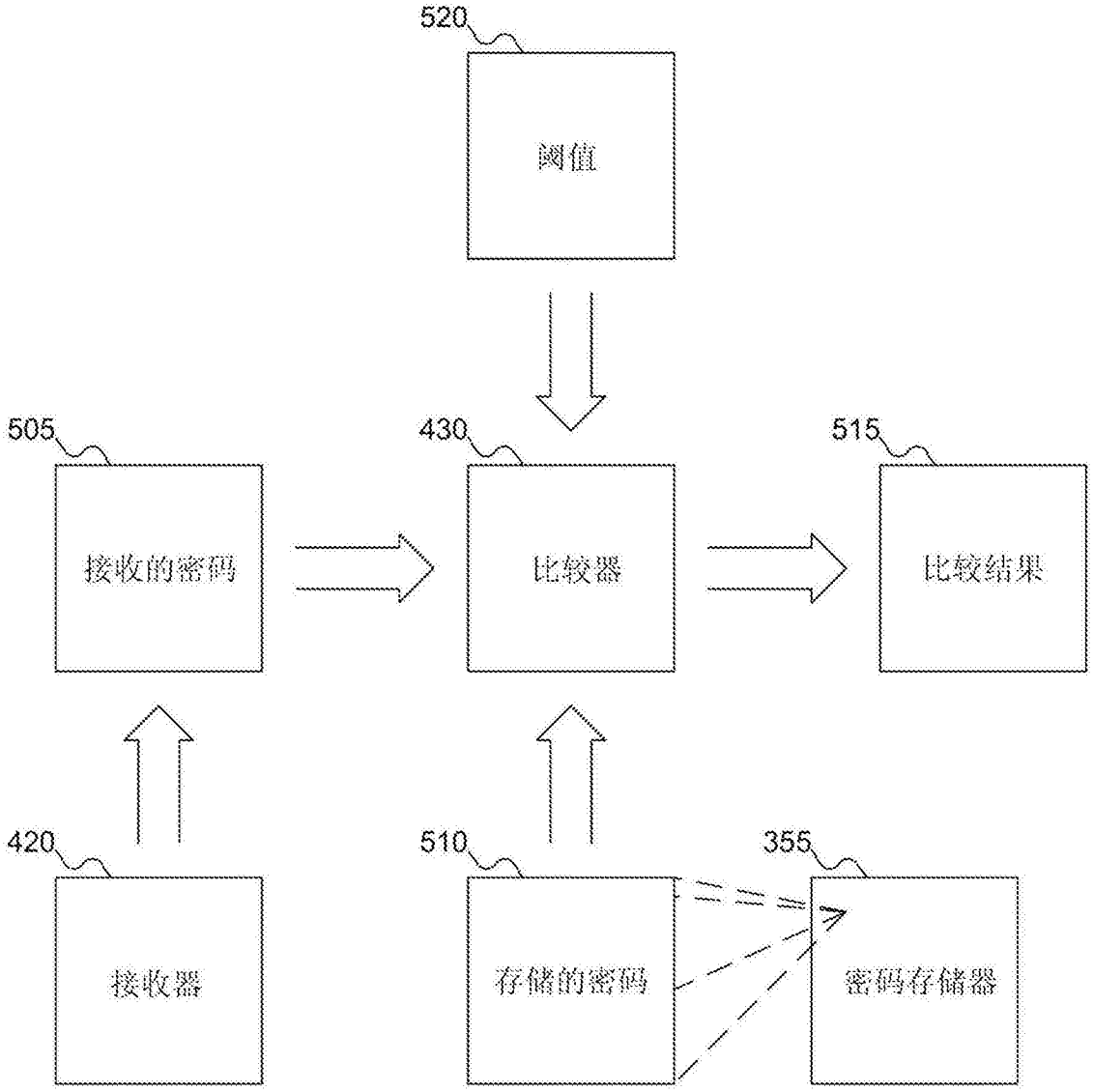


图5

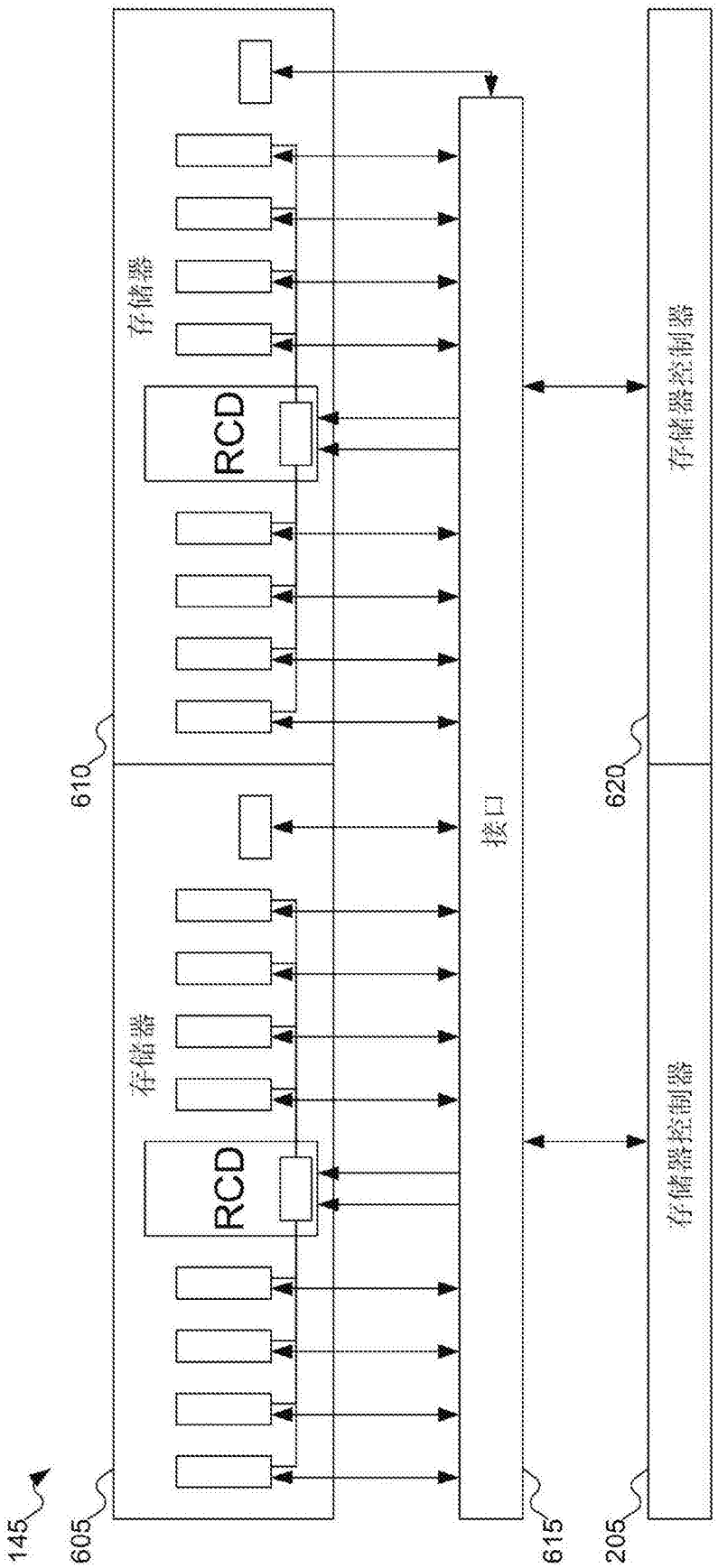


图6

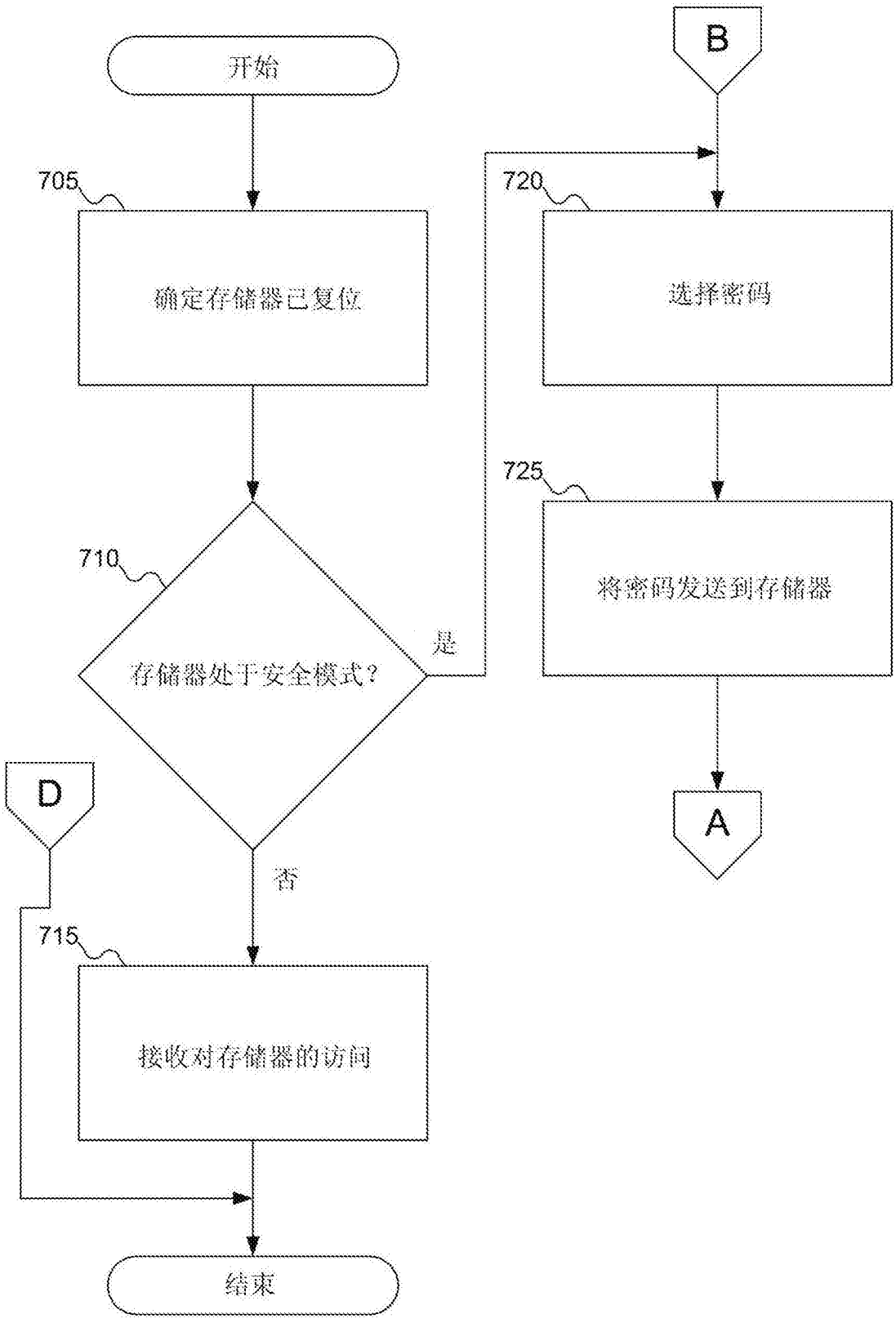

开始
705
确定存储器已复位
710
存储器处于安全模式?
是
否
D
715
接收对存储器的访问
结束
B
720
选择密码
725
将密码发送到存储器
A

图7A

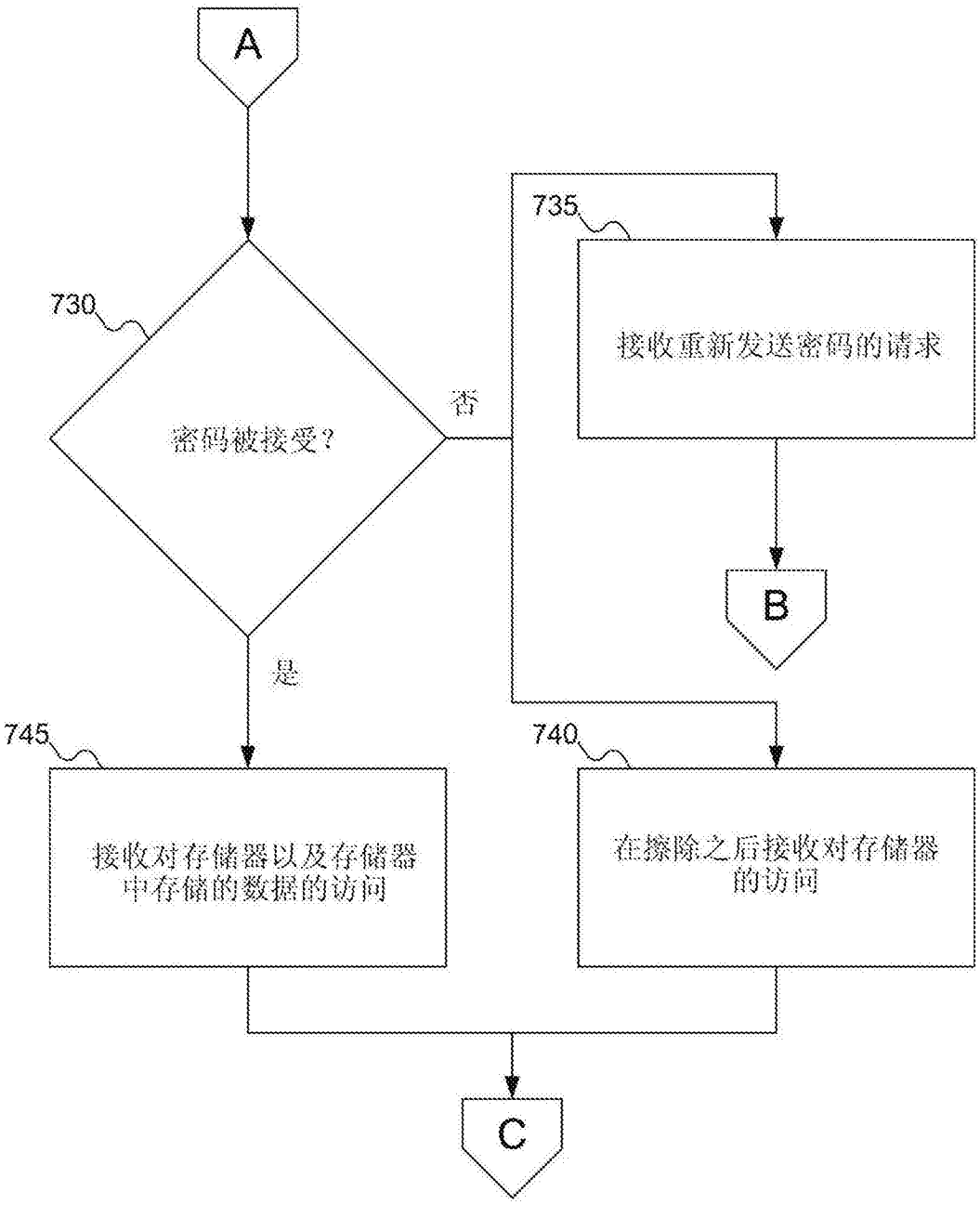

A
730
密码被接受？
否
是
735
接收重新发送密码的请求
B
745
接收对存储器以及存储器中存储的数据的访问
740
在擦除之后接收对存储器的访问
C

图7B

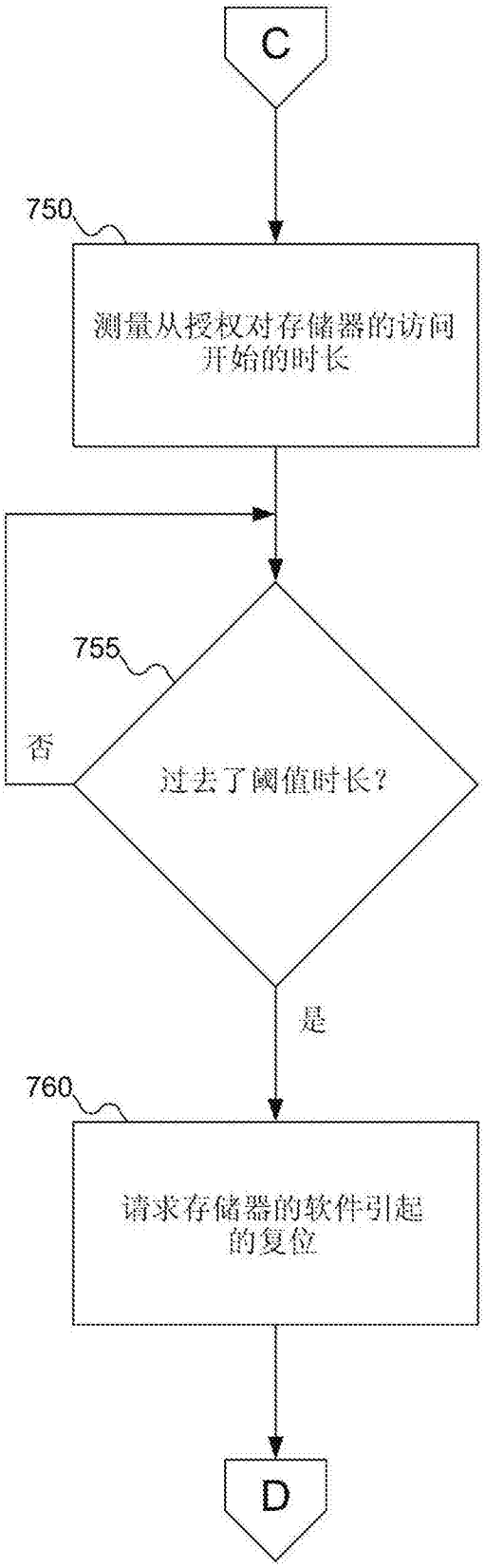

C
750
测量从授权对存储器的访问开始的时长
755
过去了阈值时长?
否
是
760
请求存储器的软件引起的复位
D

图7C

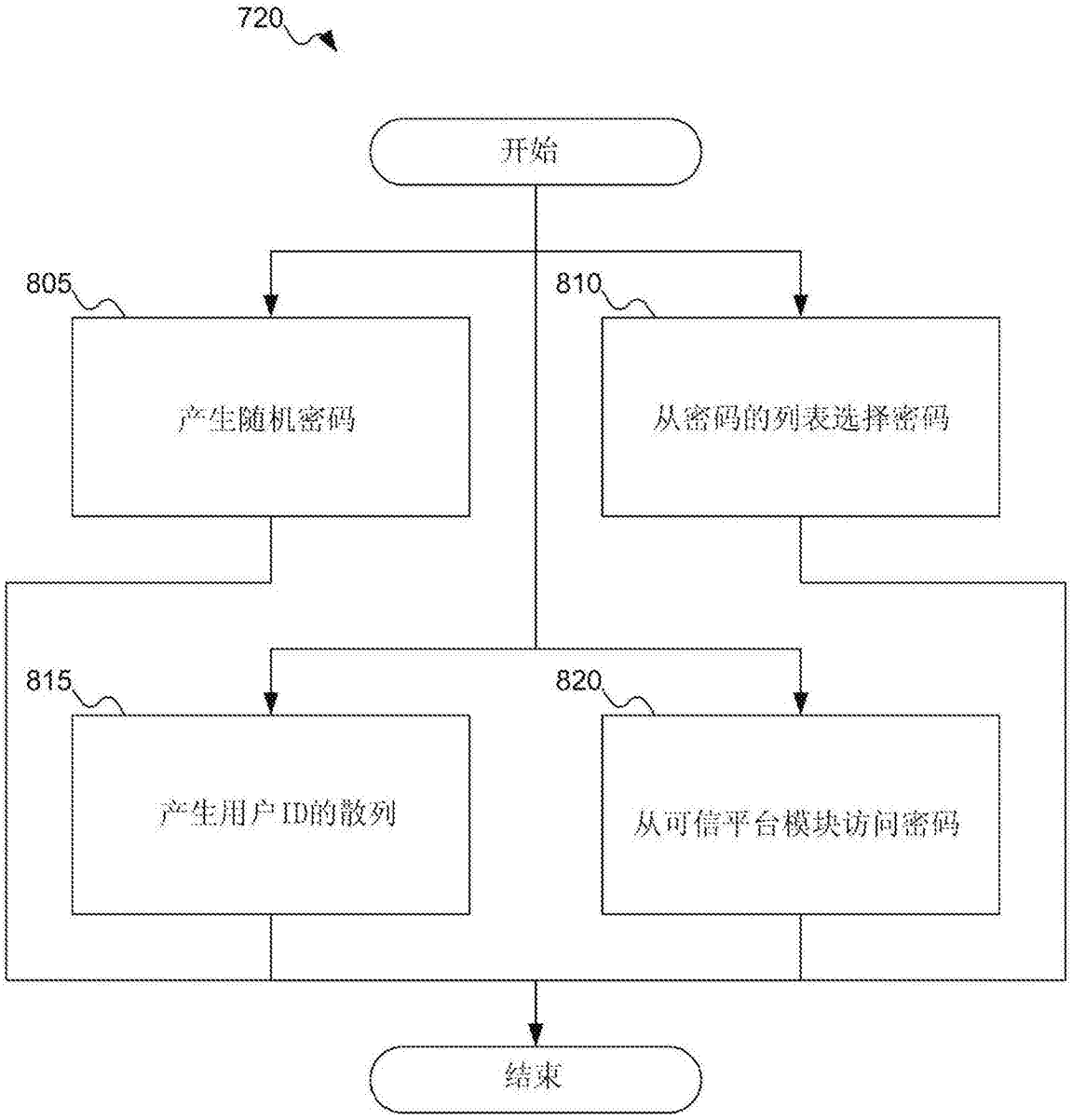

720
开始
805
产生随机密码
810
从密码的列表选择密码
815
产生用户ID的散列
820
从可信平台模块访问密码
结束

图8

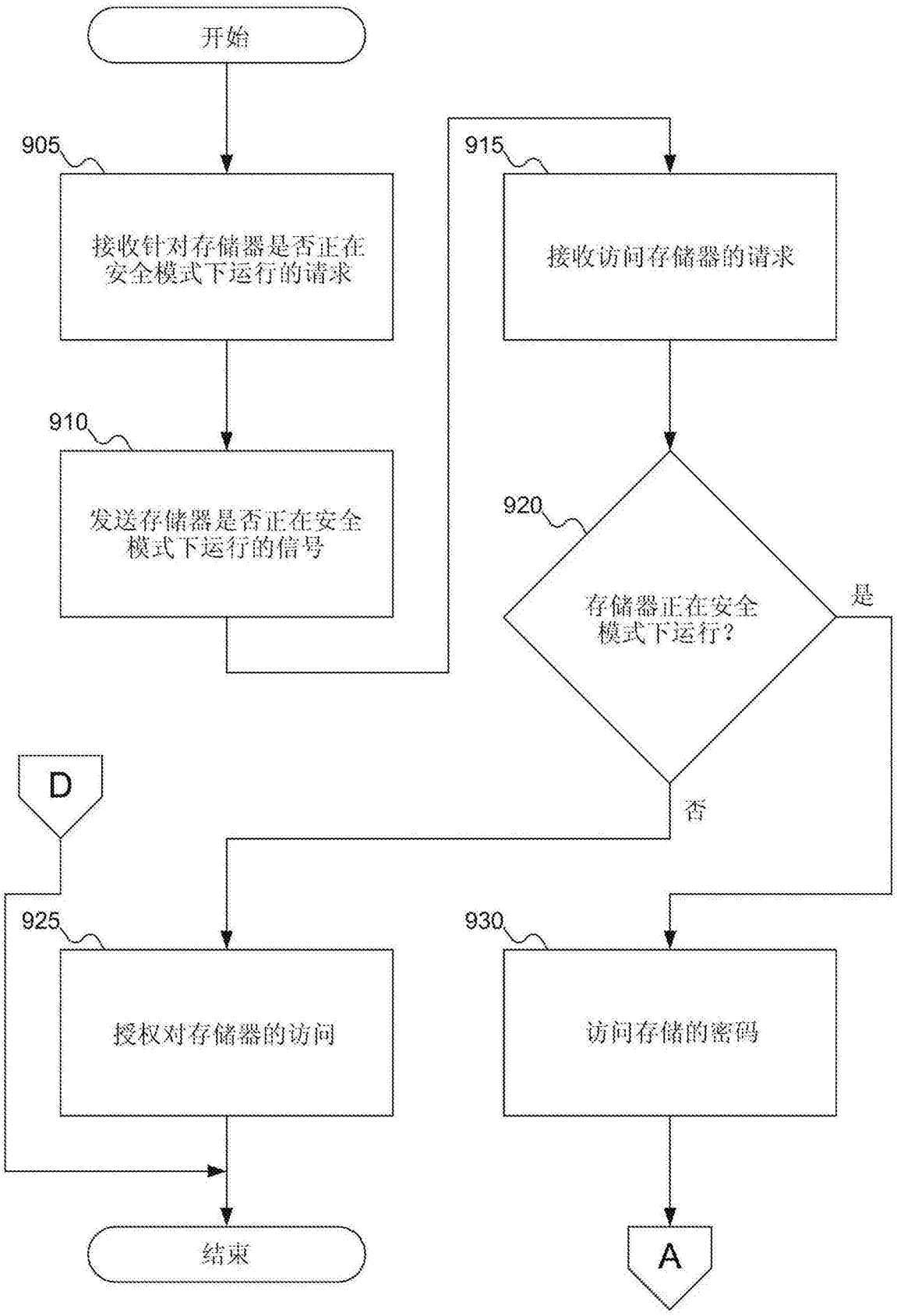

开始
905
接收针对存储器是否正在安全模式下运行的请求
910
发送存储器是否正在安全模式下运行的信号
915
接收访问存储器的请求
920
存储器正在安全模式下运行?
是
否
D
925
授权对存储器的访问
930
访问存储的密码
结束
A

图9A

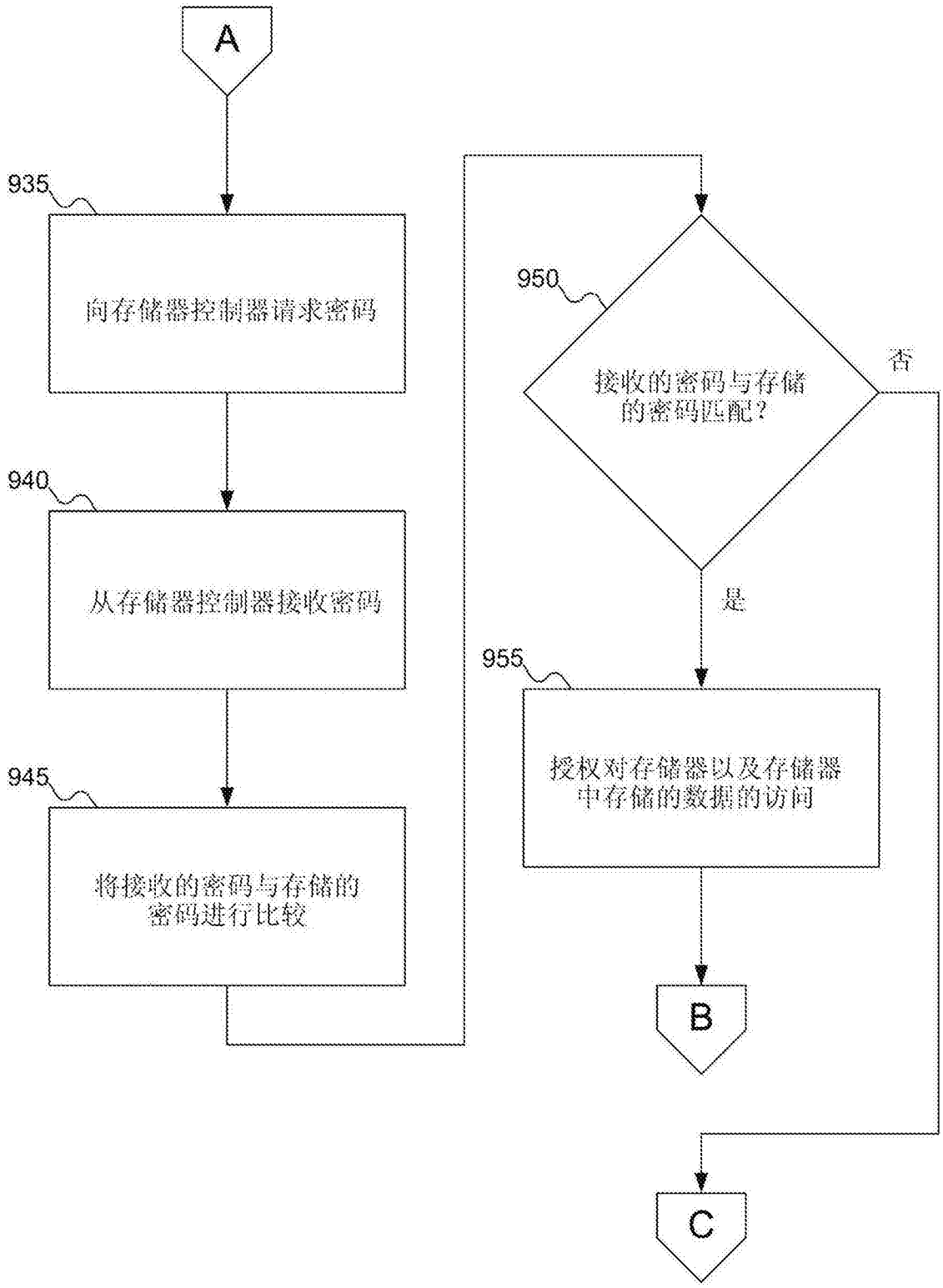

A
935
向存储器控制器请求密码
940
从存储器控制器接收密码
945
将接收的密码与存储的密码进行比较
950
接收的密码与存储的密码匹配?
否
是
955
授权对存储器以及存储器中存储的数据的访问
B
C

图9B

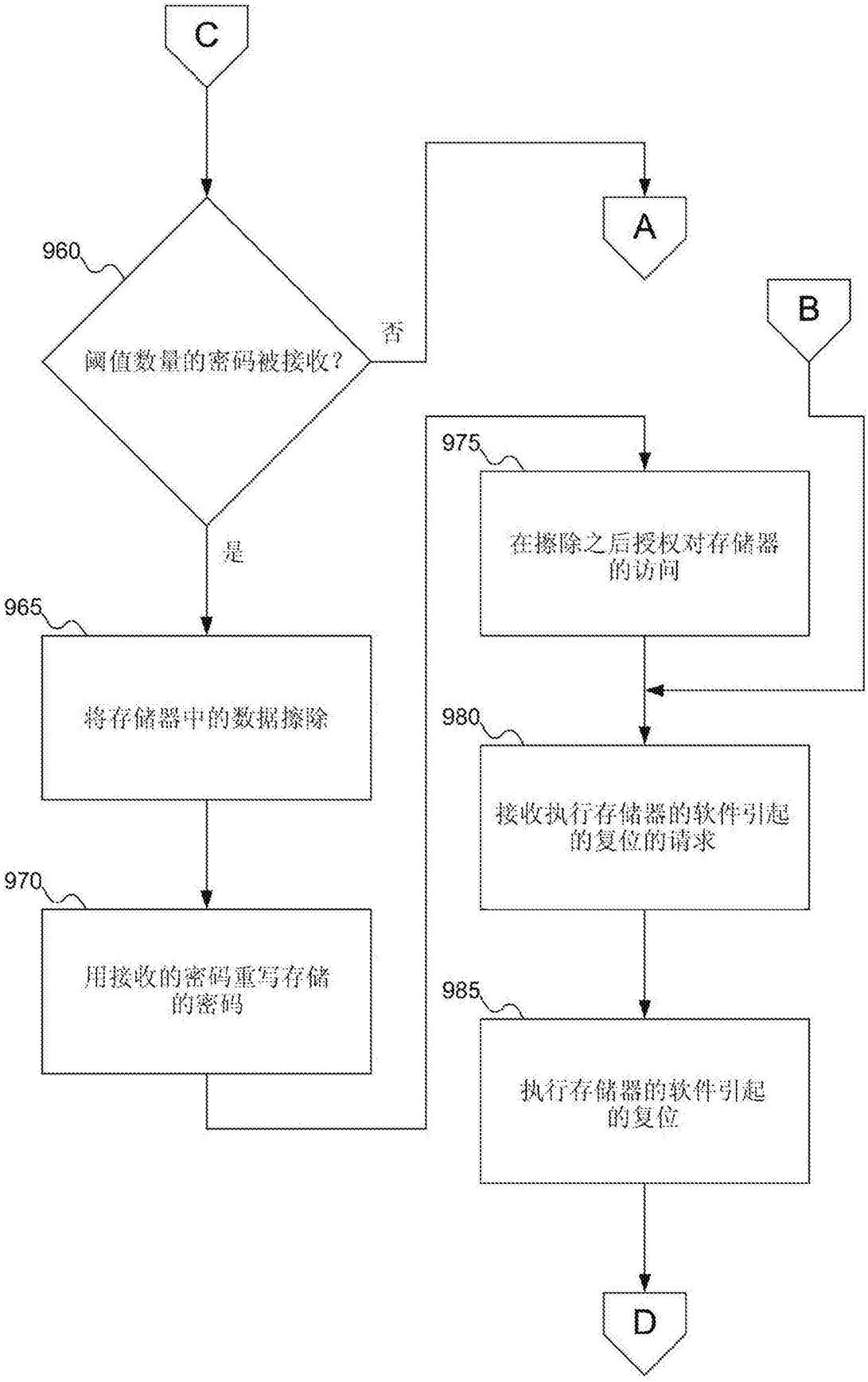

C
960
阈值数量的密码被接收?
否
是
A
B
965
将存储器中的数据擦除
970
用接收的密码重写存储的密码
975
在擦除之后授权对存储器的访问
980
接收执行存储器的软件引起的复位的请求
985
执行存储器的软件引起的复位
D

图9C

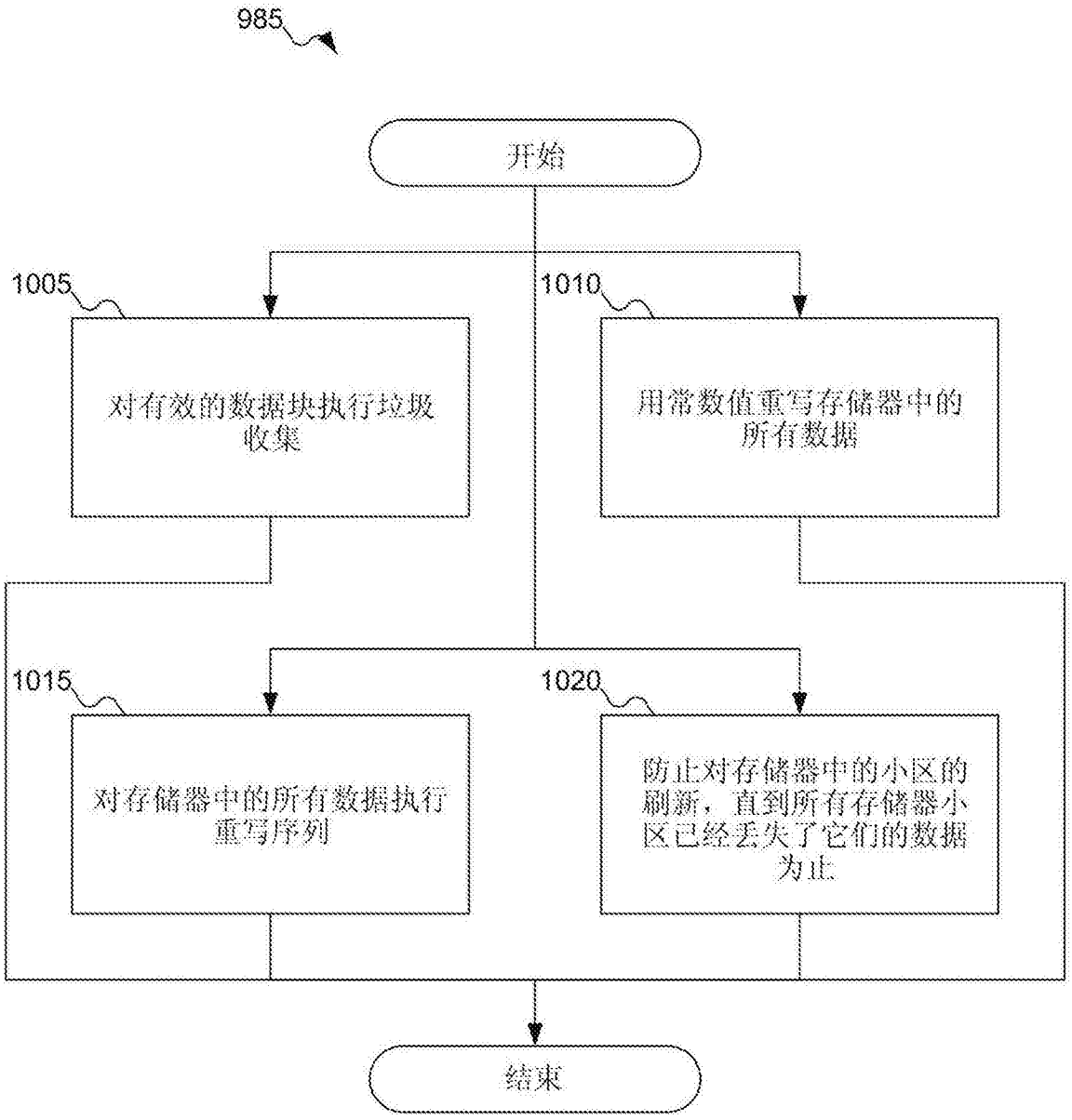

985
开始
1005
对有效的数据块执行垃圾收集
1010
用常数值重写存储器中的所有数据
1015
对存储器中的所有数据执行重写序列
1020
防止对存储器中的小区的刷新，直到所有存储器小区已经丢失了它们的数据为止
结束

图10