[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 12/00
G06F 13/00 G06F 9/06

[12]发明专利申请公开说明书

[21]申请号 01114762.8

[43]公开日 2001年10月17日

[11]公开号 CN 1317744A

[22]申请日 2001.5.30 [21]申请号 01114762.8

[71]申请人 深圳市朗科科技有限公司
地址 518131 广东省深圳市深南中路2070号电子科技大厦C座24A
[72]发明人 邓国顺 成晓华 向 锋

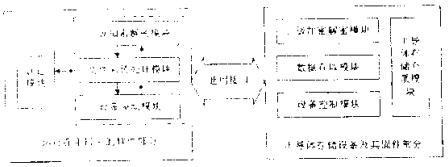
[74]专利代理机构 深圳睿智专利事务所
代理人 陈鸿荫

权利要求书4页 说明书12页 附图页数12页

[54]发明名称 一种半导体存储装置

[57]摘要

一种半导体存储装置，包括用于存储数据的半导体存储设备及 其固件部分、连接半导体存储设备与主机系统的通用接口和运行在 主机中的软件部分，其半导体存储设备及其固件部分包括设备控制 模块、半导体存储介质模块、数据存取模块和二级加密解密模块，其运行在主机中的软件部分包括一级加密解密模块、文件系统处理 模块、设备驱动模块、用户认证模块、用户控制模块。本发明提供 用户认证和数据加解密功能，使得在没有采取保密措施的主机上操 作存取保密信息成为可能。



ISSN1008-4274

01.05.08

权 利 要 求 书

1. 一种半导体存储装置，包括用于存储数据的半导体存储设备及其固件部分、连接半导体存储设备与主机系统的通用接口和运行在主机中的软件部分，其特征在于，所述半导体存储设备及其固件部分包括：

（a）设备控制模块，完成对设备的初始化，对设备的控制，对通用接口的控制和数据的接受、发送；

（b）半导体存储介质模块，使用的半导体存储介质可以是快闪存储器（Flash Memory）、DRAM、EEPROM、SRAM、FRAM 或者 MRAM，由一块或多块芯片按各种现有寻址方式连接；

（c）数据存取模块，将从通用接口接受到的文件数据和专用数据存入半导体存储介质中，或者从半导体存储介质中读取文件数据和专用数据，并传回通用接口；

所述运行在主机中的软件部分包括：

（d）一级加密解密模块，将欲存入半导体存储设备的数据进行加密，将从半导体存储设备中读出的数据进行解密；

（e）文件系统处理模块，按照文件系统所要求的格式执行读操作和写操作，解释来自主机的文件操作指令并把该指令转换为半导体存储设备操作指令；

（f）设备驱动模块，①按照所选用通用接口的协议建立主机与半导体存储设备之间的连接；②接受文件系统处理模块传来的操作指令和数据并按照所选用通用接口的协议要求格式发送给半导体存储设备；③从通用接口接受半导体存储设备返回的数据和状态信息，并发送给文件系统处理模块。

2. 根据权利要求 1 所述的一种半导体存储装置，其特征在于，所述运行在主机中的软件部分还包括：

（g）用户认证模块，将用户的认证信息和从用于存储数据的半导体存储设备中读取的认证信息加以比较后反馈比较结果，若匹配

则用户获得使用该设备的权利，否则该用户被拒绝使用。该模块还支持通过认证的用户修改其存储在半导体存储设备中的用户认证信息，修改后的用户认证信息被写入半导体存储设备。

（h）用户控制模块，支持通过认证的用户选择免除用户认证过程的设置；免除后，支持用户恢复要求用户认证过程的设置。该模块还支持通过认证的用户选择免除数据加密解密过程的设置；免除后，读写到半导体存储设备的数据不经过第一和第二加密解密模块进行加密解密；免除后，用户可以恢复数据加密解密功能的设置。

3. 根据权利要求 1 或 2 所述的一种半导体存储装置，其特征在于，所述半导体存储设备及其固件部分还包括：

（i）二级加密解密模块，将通过通用接口接受到的数据进行加密或者将从半导体存储介质中读取的数据进行解密。

4. 根据权利要求 3 所述的一种半导体存储装置，其特征在于所述半导体存储介质中有专用信息区，用于存储设备描述信息、用户认证信息、用户认证选择信息、数据加密解密选择信息。

5. 根据权利要求 3 所述的一种半导体存储装置，其特征在于所述通用接口为有线通用接口，如 USB 接口、IEEE1394 接口等；或者为无线通用接口，如蓝牙（Bluetooth）接口、IrDA 红外接口、HomeRF 接口、IEEE802.11a 接口、IEEE802.11b 接口等。

6. 根据权利要求 3 所述的一种半导体存储装置，所述（g）用户认证模块中的用户认证功能的实现可以是结合现有技术的软、硬件设计实现的要求用户提供密码，或者检测用户的指纹，或者检测用户的视网膜微血管分布图，或者检测用户的声纹。

7. 根据权利要求 3 所述的一种半导体存储装置，其特征在于，所述设备控制模块包括通用接口控制器（22）和微处理器单元（21），

所述微处理器单元（21），用以控制通用接口控制器（22）和半导体存储介质（1）的工作，所述通用接口控制器（22）与所述半导体存储介质（1）相连，所述微处理器单元（21）与半导体存储介质（1）、通用接口控制器（22）、二级加密解密模块（25）相连，所有连接皆可用于数据和信息的双向交流，所述运行在主机中的软件部分包括主机中安装的驱动程序（Driver）和用户认证模块以及用户控制模块，所述驱动程序运行于主机的上层操作系统和下层操作系统之间，处理上层操作系统对半导体存储设备的读写要求；所述用户认证模块以及用户控制模块运行于主机的上层操作系统之上，对企图读写半导体存储设备的用户进行资格认证；在所述微处理器单元（21）中固化有固件程序，所述固件程序的运行，实现对半导体存储介质（1）的读、写或擦除操作。

8. 根据权利要求 7 所述的一种半导体存储装置，其特征在于所述设备控制模块中还包括休眠及唤醒电路（24），分别同时与微处理器单元（21）和通用接口控制器（22）相连并受其控制，以实现在空闲时使本装置进入休眠状态，有操作请求时又被激活进入唤醒状态的功能。

9. 根据权利要求 7 所述的一种半导体存储装置，其特征在于所述设备控制模块还具有写保护功能。

10. 根据权利要求 9 所述的一种半导体存储装置，其特征在于所述设备控制模块还包括写保护开关电路（4），利用开关 S1 对半导体存储介质（1）提供物理保护，使其内容不被改写或擦除，所述写保护开关电路（4）分别与微处理器（21）和半导体存储介质（1）相连。

11. 根据权利要求 9 所述的一种半导体存储装置，其特征在于所述微处理器单元（21）和所述通用接口控制器（22）合并为一个

功能单元，使用同时具有微处理功能和通用接口控制功能的一个集成电路模块。

12. 根据权利要求 11 所述的一种半导体存储装置，其特征在于所述驱动程序把上层主机操作系统要求读写操作的标准磁盘读写操作命令转换成半导体存储设备的特定读写操作命令，并对转换后的读写操作命令打包后发给底层操作系统，由底层操作系统把此特定读写操作命令通过通用接口发送给微处理器（21）中的固件程序，由固件程序执行读写操作。

13. 根据权利要求 12 所述的一种半导体存储装置，其特征在于所述用于存储数据的半导体存储介质采用快闪存储器 (1)，所述驱动程序把上层主机操作系统要求读操作的标准磁盘读操作命令转换成快闪存储器的特定读操作命令，并对转换后的读操作命令进行打包后发给底层操作系统，由底层操作系统把读操作命令通过通用接口发送给微处理器（21）中的固件程序，由固件程序执行读操作；所述驱动程序把上层主机操作系统要求写存储器的标准的磁盘写操作命令转换成三个不同的内部操作：读、擦除和写：首先驱动程序执行一个内部读操作，把写位置的原有内容读出来并保存，然后驱动程序执行一个内部擦除操作以清除写位置的所有数据，最后驱动程序把需要写的新数据和原有数据结合在一起，并对结合后的数据执行一个内部写操作。

01·06·08

说 明 书

一种半导体存储装置

本发明涉及电数字数据处理，尤其涉及数据处理系统的存储器，具体的说是一种半导体存储装置。

当今科学技术发展的一个明证是计算机技术按摩尔定律飞速发展，在计算速度越来越快、存储容量越来越大的同时，还越来越小型化、轻便化，出现了便携式笔记本电脑和手持式数据处理系统例如国际流行的个人数字助理（PDA）。传统的磁盘存储器和磁盘驱动器因体积太大、笨重和存取速度太慢而不适用，人们开发出新的装置，例如美国专利 US 6,148,354 《通用串行总线个人电脑闪存盘的结构》(《ARCHITECTURE FOR A UNIVERSAL SERIAL BUS-BASED PC FLASH DISK》)，该专利中公开了一种采用 USB 标准接口连接于主机的快闪存储盘。包括快闪存储器（flash memory），可实现 USB 标准功能的连接器（USB connector）、电子接口（electrical interface）、逻辑接口（logical interface）、应用数据包提取器(application packet extractor)和应用命令译码器（application command interpreter）等，实现了将快闪存储器用于 PC 机的目的。但是在因特网日益普及、电子商务迅速发展的今天，缺乏对用户的认证限制，缺乏对所存储的信息内容的保密处理，限制了这种快闪盘的用途。而且该 USB PC 闪存盘在连接于 PC 机后，始终处于激活状态，能耗较大，不符合当前节能环保的世界主题。

针对现有技术的不足，本发明的目的在于提出一种半导体存储装置，提供用户认证及数据加密与解密功能，对使用该半导体存储装置的用户加以身份认证，并对存入该半导体存储装置中的信息进行加密保护，加密信息在读出时再被解密；同时提供休眠与唤醒功能，以减少能耗；并提供写保护开关电路，对该快闪存储器中的数据提供双重保护，防止病毒侵入。

一种半导体存储装置，包括用于存储数据的半导体存储设备及

其固件部分、连接半导体存储设备与主机系统的通用接口和运行在主机中的软件部分，所述半导体存储设备及其固件部分包括：

（a）设备控制模块，完成对设备的初始化，对设备的控制，对通用接口的控制和数据的接收、发送；

（b）半导体存储介质模块，使用的半导体存储介质是快闪存储器（Flash Memory）、DRAM、EEPROM、SRAM、FRAM 或者 MRAM，由一块或多块芯片按各种现有寻址方式连接；

（c）数据存取模块，将从通用接口接收到的文件数据和专用数据存入半导体存储介质中，或者从半导体存储介质中读取文件数据和专用数据，并传回通用接口；

所述运行在主机中的软件部分包括：

（d）一级加密解密模块，将欲存入半导体存储设备的数据进行加密，将从半导体存储设备中读出的数据进行解密；

（e）文件系统处理模块，按照文件系统所要求的格式执行读操作和写操作，解释来自主机的文件操作指令并把该指令转换为半导体存储设备操作指令；

（f）设备驱动模块，①按照所选用通用接口的协议建立主机与半导体存储设备之间的连接；②接受文件系统处理模块传来的操作指令和数据并按照所选用通用接口的协议要求格式发送给半导体存储设备；③从通用接口接受半导体存储设备返回的数据和状态信息，并发送给文件系统处理模块。

（g）用户认证模块，将用户的认证信息和从用于存储数据的半导体存储设备中读取的认证信息加以比较后反馈比较结果，若匹配则用户获得使用该设备的权利，否则该用户被拒绝。该模块还支持通过认证的用户修改其用户认证信息，修改后的用户认证信息被写入半导体存储设备。

（h）用户控制模块，支持通过认证的用户选择免除用户认证过程的设置；免除后，支持用户恢复要求用户认证过程的设置。该模块还支持通过认证的用户选择免除数据加密解密过程的设置；免除后，读写到半导体存储设备的数据不需要经过第一和第二加密解密

模块进行加密解密；免除后，用户可以恢复数据加密解密功能的设置。

所述半导体存储设备及其固件部分还包括：

（i）二级加密解密模块，将通过通用接口接受到的数据进行加密或者将从半导体存储介质中读取的数据进行解密。

所述半导体存储介质中有专用信息区，用于存储设备描述信息、用户认证信息、用户认证选择信息、数据加密解密选择信息。

所述设备控制模块包括通用接口控制器（22）和微处理器单元（21），所述微处理器单元（21），用以控制通用接口控制器（22）和半导体存储介质（1）的工作，所述通用接口控制器（22）与所述半导体存储介质（1）相连，所述微处理器单元（21）与半导体存储介质（1）、通用接口控制器（22）、二级加密解密模块（25）相连，所有连接皆可用于数据和信息的双向交流，所述运行在主机中的软件部分包括主机中安装的驱动程序（Driver）和用户认证模块以及用户控制模块，所述驱动程序运行于主机的上层操作系统和下层操作系统之间，处理上层操作系统对半导体存储设备的读写要求；所述用户认证模块以及用户控制模块运行于主机的上层操作系统之上，对企图读写半导体存储设备的用户进行资格认证；在所述微处理器单元（21）中固化有固件程序，所述固件程序的运行，实现对半导体存储介质（1）的读、写、擦除操作。

所述设备控制模块中还包括休眠及唤醒电路（24），分别同时与微处理器单元（21）和通用接口控制器（22）相连并受其控制，以实现在空闲时使本装置进入休眠状态，有操作请求时又被激活进入唤醒状态的功能。所述设备控制模块还具有写保护功能。

所述驱动程序把上层主机操作系统要求读写操作的标准磁盘读写操作命令转换成半导体存储设备的特定读写操作命令，并对转换后的读写操作命令打包后发给底层操作系统，由底层操作系统把此特定读写操作命令通过通用接口发送给微处理器（21）中的固件程序，由固件程序执行读写操作。

本发明采用独特设计，在半导体存储装置中提供用户认证和数据加解密功能，使该半导体存储装置可以存入重要的保密信息，并通过用户认证及数据加密解密模块对使用该半导体存储装置的用户加以身份认证，方便用户操作和携带保密数据，使得在没有采取保密措施的主机上操作存取保密信息成为可能。本发明提供具有写保护开关的硬保护功能，在物理上保护半导体存储设备的内容不被改写或擦除，防止数据丢失，防止病毒侵入。本发明提供休眠及唤醒电路在主机无操作命令时，使半导体存储设备进入休眠状态，降低能耗。本发明使用新型半导体存储介质和通用通道接口，可实现无驱动器、无外接电源的活动外存，并可带电插拔、即插即用、无需关机；存取速度快，容量大大超过软磁盘；体积小，携带方便，不易损坏；可同时连接二十多个快闪存储装置到数据系统上，可使用于任何支持通用通道的数据处理系统。

下面结合附图对本发明作进一步详细说明：

图 1 是本发明半导体存储装置的软硬件功能模块示意图；

图 2 是本发明半导体存储装置的用户认证及数据加密解密工作流程示意图；

图 3 是本发明采用有线通用接口实施例的结构原理框图；

图 4 是本发明采用 USB 接口的结构原理框图；

图 5 是本发明采用 IEEE1394 接口的结构原理框图；

图 6 是本发明采用 USB 接口时写保护开关电路原理图；

图 7 是本发明采用 USB 接口时微处理器和休眠及唤醒电路的电路原理图；

图 8 是本发明采用 USB 接口时直流电源变换器的电路原理图；

图 9 是本发明采用 USB 接口时接口控制器的电路原理图；

图 10 是本发明采用 USB 接口和快闪存储器实施例的控制管理软件系统示意图；

图 11 是本发明采用 USB 接口和快闪存储器实施例的驱动程序流程图；

01.06.03

图 12 是本发明的采用 USB 接口和快闪存储器实施例的固件流程图。

如图 1 是本发明半导体存储装置的软硬件功能模块示意图，包括由通用接口相连接的运行在主机中的软件部分和用于存储数据的半导体存储设备及其固件部分。

这里通用接口指有线通用接口或者无线通用接口，例如 USB 接口、IEEE1394 接口、蓝牙（Bluetooth）接口、IrDA 红外接口、HomeRF 接口、IEEE802.11a 接口、IEEE802.11b 接口。

运行在主机中的软件部分中包括用户认证模块、用户控制模块、级加密解密模块、文件系统处理模块和设备驱动模块。其中，用户认证模块接受用户输入的认证信息，同时从半导体存储设备中读取所存储的认证信息，并将二者加以比较后反馈比较结果，若匹配则用户获得使用该设备的权利，否则该用户被拒绝使用；用户认证模块还支持通过认证的用户修改其用户认证信息，修改后的用户认证信息被写入半导体存储设备。用户控制模块支持通过认证的用户选择免除用户认证过程的设置；免除后，支持用户恢复要求用户认证过程的设置。用户控制模块还支持通过认证的用户选择免除数据加密解密过程的设置；免除后，读写到半导体存储设备的数据不需要经过第一和第二加密解密模块进行加密解密；免除后，用户可以恢复数据加密解密功能的设置；一级加密解密模块将欲存入半导体存储设备的数据进行加密，将从半导体存储设备中读出的数据进行解密；文件系统处理模块按照文件系统所要求的格式执行读操作和写操作，解释来自主机的文件操作指令并把该指令转换为半导体存储设备操作指令；设备驱动模块的功能包括：①按照所选用通用接口的协议建立主机与半导体存储设备之间的连接；②接受文件系统处理模块传来的操作指令和数据并按照所选用通用接口的协议要求格式发送给半导体存储设备；③从通用接口接受半导体存储设备返回的数据和状态信息，并发送给文件系统处理模块。

在用于存储数据的半导体存储设备及其固件部分中包括 级加

密解密模块、数据存取模块、设备控制模块和半导体存储介质模块。其中，二级加密解密模块将通过通用接口接受到的数据加密或者将从半导体存储介质模块中读取的数据进行解密；数据存取模块将从通用接口接受到的文件数据和专用数据存入半导体存储介质中，或者从半导体存储介质中读取文件数据和专用数据，这里专用数据是指设备本身的信息、用户认证信息、用户认证选择信息、数据加密解密选择信息；设备控制模块对半导体存储设备进行初始化、控制半导体存储设备、通用接口和数据的接受和发送；半导体存储介质模块中所用的半导体存储介质可以是快闪存储器、DRAM、EEPROM、SRAM、FRAM 或者 MRAM，一块或多块芯片的组合。

本发明中二级加密解密模块或者用户认证模块或者用户控制模块也可以舍弃不用。

如图 2 是本发明半导体存储装置的工作流程示意图，在开始状态用户认证模块向半导体存储介质请求提出所存储的用户认证信息并与用户输入的用户认证信息比较，设置认证检验标志，若相同则允许使用，否则拒绝使用。进入使用的用户可能要求读文件、写文件、修改用户认证信息，这三种操作都需要通过认证检验标志的检验，若通过检验，则写文件和修改后的密码经过一级加密模块加密和二级加密模块加密后存入半导体存储介质；读文件则从半导体存储介质中读出文件并经过二级解密模块和一级解密模块解密。

用户控制模块支持通过认证的用户选择免除用户认证过程的设置。免除后，任何用户都可以不经过用户认证过程使用半导体存储设备进行数据存储，在免除用户认证的状态下，任何用户都可以恢复要求用户认证过程的设置。用户认证模块还支持通过认证的用户选择免除数据加密解密功能，免除后，任何用户所读写到半导体存储设备的数据不需要经过第一加密解密模块和第二加密解密模块进行加密和解密，在免除数据加密解密的状态下，任何用户都可以恢复数据加密解密功能的设置。半导体存储介质中有专用信息区，用于存储设备描述信息、用户认证信息、用户认证选择信息、数据加密解密选择信息。

如图 3 的结构原理框图所示，本发明采用有线通用接口实施例的结构包括半导体存储介质 1、存储控制电路 2、直流电源变换器 3、写保护开关 4。半导体存储介质 1 包括一个或一个以上半导体存储器模块，用于存储数据和控制信息；存储控制电路 2 控制半导体存储设备，实现半导体存储设备与主机之间的通讯、在半导体存储介质中的数据读写、所读写数据的加密解密功能；直流电源变换器 3 从通用通道取得供电源为半导体存储设备供电，为使图面清楚简洁，图中未画连接线；写保护开关 4 具有硬件保护功能，保护半导体存储介质中的内容不会被改变或擦除。存储控制电路 2 控制存储介质 1 并检查写保护开关 4 的状态。

存储控制电路 2 包括主机连接接口 20、接口插座 23、接口控制器 22、微处理器 21、休眠及唤醒电路 24、二级数据加解密模块 25。主机连接接口连接半导体存储设备和主机，这里所述的主机包括但不限于各种个人计算机、数码相机、PDA、Pocket PC、小型计算机、数据处理工作站以及各种需要存储装置的专用数据处理系统。一级数据加密解密模块 25 实现用户在通过认证的前提下将数据加密写入或解密读出半导体存储介质 1。

对用户进行身份认证的方法，可以是要求用户输入密码，并验证该密码是否正确，如果输入密码不正确，可以允许有限次数的重试，始终不正确，则拒绝读写半导体存储介质 1。对用户进行身份认证的方法，可以是要求用户提供密码，还可以是结合现有技术提供的软硬件验证用户的指纹、瞳孔、声纹，只有其指纹和瞳孔、声纹的特征符合的用户才被允许读写半导体存储器 1，必须说明不限于此处罗列的，其他种类用户认证识别办法结合在本发明的半导体存储装置中也属于本发明的保护范围。

休眠及唤醒电路 24 在主机无操作命令时，使快闪存储装置进入休眠状态，降低能耗，在主机有操作命令时将快闪存储装置从休眠状态中唤醒激活进入正常操作状态。

接口控制器 22 通过接口插座与主机连接电缆相连，接口控制器在微处理器 21 和休眠及唤醒电路 24 的控制下工作，接收主机来的

命令，并控制其与半导体存储介质 1 之间的数据操作。微处理器 21 还控制半导体存储介质 1 和休眠及唤醒电路 24、二级数据加密解密模块 25、查询写保护开关 4。

接口控制器 22 和微处理器 21 可以合而为一，使用同一模块。

本发明的半导体存储装置在外型结构上设计成一个整体，全部元器件容纳于单一壳体内，布置于电路板上，在驱动软件的驱动下实现存储功能。本发明的快闪存储装置没有机械转动部件，工作时整个装置处于静止状态，其体积可以做得非常小，像大拇指一样大，便于携带和使用。作为本发明的一个实施例，半导体存储装置也可以没有壳体。

如图 4 所示是本发明采用通用串行总线 USB 接口的一个实施例。本实施例的半导体存储介质采用快闪存储器，并采用 USB 连接接口使半导体存储介质与主机相连，采用 USB 插座 231 作为接口插座，采用 USB 接口控制器 221 控制半导体存储设备与主机之间的命令信息和数据的传输。USB 接口控制器 221 和微处理器 21 可以是同一模块。在该模块和快闪存储器之间有二级加密解密模块 25。根据 USB 标准，直流电源变换器 3 通过 USB 插座 231 从主机接入电源。

USB 已成为新的个人电脑行业标准，当今所有配置为奔腾 II 或以上电脑及兼容机均带有 USB 接口，因此本实施例快闪存储装置可替代现有软驱和软盘成为这些电脑的标准件。

如图 5 所示是本发明采用 IEEE 1394 接口的一个实施例。本实施例采用 IEEE 1394 连接接口 202 使半导体存储设备与主机相连，采用 IEEE 1394 插座 232 作为接口插座，采用 IEEE 1394 接口控制器 222 控制半导体存储设备与主机之间的命令信息和数据的交换和传输。根据 IEEE 1394 标准，直流电源变换器 3 与 IEEE 1394 插座 232 接入主机电源。

图 6 是本发明采用 USB 接口时半导体存储介质 1 采用快闪存储器的电路原理图，采用快闪存储器芯片 D1，本发明不限于示于图中的只有一个闪存芯片的实施例，也可以使用多个闪存芯片按各种现有寻址方式连接和管理。如图 6 所示，其快闪存储器芯片 D1 用于存

储数据，它可以采用但不限于一片或多片型号为TC58V64FT/128FT/256FT/512FT/100FT/K9F6408/K9F2808/K9F2808/K9F5608/K9K1208的芯片，该芯片D1的5脚与写保护开关S1的5脚连接。

图7是本发明采用USB接口、快闪存储器时的微处理器和休眠及唤醒电路的电路原理图，微处理器用于控制USB控制器221、快闪存储器1和休眠及唤醒电路24。它含有微处理器芯片D4及两个型号为4053的多路模拟开关芯片D5、D6，芯片D5的12、1、3脚、D6的12脚短接后接芯片D4的12脚，芯片D5的13、2、5脚、D6的13脚短接后接芯片D4的13脚；芯片D5的11、10、9脚和D6的11脚分别接芯片D4的44、1、2、3脚；芯片D4的DATA0~DATA7脚分别与USB控制器221的芯片D2以及快闪存储器芯片D1对应的接线脚相连；芯片D5的4号脚接快闪存储器D1的4号脚，芯片D6的14脚接快闪存储器D1的42脚；芯片D5的14、15脚接D2的15、16脚。

休眠及唤醒电路24含有三极管V1、电容C4、二极管V2、电阻R5~R9；三极管V1的基极经电阻R9、电容C4和电阻R8后接通串行总线接口控制器22的芯片D2的12脚，三极管V1的发射极接微处理器芯片D4的4脚。

图8是本发明采用USB接口、快闪存储器的直流电源变换器的电路原理图；采用三端电源D3，并在其端口1 VSS和端口2 VOUT之间并联连接电容器C3和C6，将输入电压VCC-BUS转换成输出电压FVCC-33。

图9是采用USB接口、快闪存储器的实施例的接口控制器的电路原理图，其USB接口控制器221可采用但不限于型号为PDIUSBD12的芯片D2、晶振Y1、电容C1~C2、C7~C8、电阻R1~R3、R10、发光二极管V3；晶振Y1、电容C1~C2互相串接形成闭合回路，在晶振Y1的两端分别接芯片D2的22和23脚，芯片D2的25、26脚分别经电阻R1、R2接通用串行总线插座23的2、3号脚。该USB接口控制器221负责USB数据流的输入输出及其控制，符合USB1.0

及 1.1 或 2.0 标准，具有可与大多数单片机相接的快速且简单的并行接口，并可实现 DMA 的功能。

本发明采用 USB 接口和快闪存储器时无需驱动器和外接电源，在控制管理软件的控制下工作，其控制管理软件包括用户认证模块、上层操作系统、驱动程序（Driver）、底层操作系统和固件程序（Firmware），如图 10 所示。固件程序是被固化在微处理器 21 中的管理程序，固件程序与底层操作系统互动，驱动程序被装载在主机的底层操作系统和上层操作系统之间，并与底层操作系统和上层操作系统互动。驱动程序与固件程序的流程图如图 11 和图 12 所示。

下面以采用 USB 接口和快闪存储器的半导体存储设备为例，结合附图 11、图 12、图 10 说明本发明在控制管理软件系统的控制下的工作过程。

当插入半导体存储设备，主机操作系统通过对 USB 接口的自动检测，立即激活用户认证模块和驱动程序，提示用户输入或修改用户认证信息，驱动程序即执行初始化操作，并指示上层操作系统产生一个相应的可移动存储装置配置（或称为活动存储装置配置），上层操作系统即为插入的该存储装置产生可移动存储装置配置并分配相应的装置符。当用户点击装置符时，驱动程序检查用户认证标志，并根据该标志作出判断，接受通过认证的用户或拒绝未通过认证的用户存取半导体存储设备。此后驱动程序进入等候操作请求状态。

当半导体存储设备插入到主机的 USB 接口时，被激活的还有固件程序，微处理器 21 立即开始执行固化在其中的固件程序，进行初始化，此时上层操作系统会查询 USB 接口芯片 D2，D2 会产生中断请求传送给微处理器 21，微处理器 21 通过对 USB 接口芯片 D2 中断请求的响应而与上层操作系统取得联系，操作系统根据 USB 接口芯片 D2 与微处理器 21 所反馈的各种特性状态或标志，通知 USB 接口芯片 D2 与微处理器 D4 进行有关的初始设置，为下一步数据交换做好准备。初始化完毕固件程序即进入等待状态，等待操作请求。

当该半导体存储设备从主机的 USB 接口拔出时，固件程序立即终止执行。主机操作系统自动检测到这一事件立即通知驱动程序；

驱动程序执行有关处理，并指示操作系统消除与该半导体存储设备对应的可移动存储装置配置；上层主机操作系统取消相应的可移动存储装置符。

当上层主机操作系统要求读操作时，会把读操作命令送给驱动程序。由于该操作命令属于标准的磁盘读操作命令，不符合快闪存储器的读操作方式要求，因此驱动程序把该读操作命令转换成快闪存储装置的特定操作命令。之后，驱动程序进一步对转换后的操作命令进行 USB 打包，并把打包后的读操作命令发给底层操作系统，由底层操作系统把读操作命令通过 USB 接口发送给微处理器 21 中的固件程序，由固件程序执行读操作，即 USB 接口控制器 D2 接到读操作命令后通知微处理器 D4，而微处理器 D4 在固件程序控制下从快闪存储器 D1 中读取所要求的数据送入二级解密模块进行解密后，将数据及相关信息通过 USB 接口传给底层操作系统，并把读取的数据及状态信息经 USB 接口通过底层操作系统返回给驱动程序，驱动程序中包含一级加密解密模块，该模块对所读数据进行解密，并把解密后的数据和状态信息发送给上层操作系统。

当上层主机操作系统要求写存储器时，会把该写操作命令发送给驱动程序。由于该操作命令属于标准的磁盘写操作命令，与快闪存储器要求的操作命令不一样，因此驱动程序会把它转换成快闪存储装置的特定操作命令。当写操作命令到达快闪存储器 D1 时，如果写位置已经包含有效数据，则新的数据无法直接写入，只有当有效数据被移动后，才能写入新的数据。基于这种原因，驱动程序把写操作转换成三个不同的内部操作：读、擦除和写。首先，驱动程序的一级加密解密程序需要写入的新数据进行加密，然后再执行一个内部读操作，把写位置的原有内容读出来并保存；然后再执行一个内部擦除操作，以清除写位置的所有数据；最后，把需要写的新数据和原有数据结合在一起，并对结合后的数据执行一个内部写操作。当上述三个操作都完成后，驱动程序把写操作的执行状态信息返回给上层操作系统，完成写操作。其操作过程是，当写操作命令至快闪存储器 D1 时，USB 接口控制器 D2 通知微处理器 D4，而微处理

器 D4 在固件程序控制下从 USB 接口控制芯片 D2 中读取相应的数据送入快闪存储器 D1。当操作系统要对快闪存储器 D1 进行擦写时，通用通道接口电路 D2 会通知微处理器 D4， D4 会送一串命令给快闪存储器 D1，从而擦除 D1 内相应区域的内容。驱动程序会对上述三个内部操作分别进行 USB 打包，并把打包后的操作发给底层操作系统，由底层操作系统通过 USB 接口发送给微处理器中的固件程序，固件程序执行该操作，并把操作后的数据及状态信息通过 USB 返回给底层操作系统，然后由底层操作系统发给驱动程序。

如图 12、图 11 所示，本发明半导体存储装置除支持上层主机操作系统要求的磁盘操作以外，还支持即插即用或其他特定操作，该即插即用和其他特定操作的请求来自上层主机操作系统，再经驱动程序处理成适合半导体存储设备的格式给底层操作系统按 USB 标准打包后经 USB 接口传给 USB 接口控制器 D2，在固件程序的控制下执行，并将执行结果信息给接口控制器 D2，经 USB 接口返还给上层主机操作系统。

01.06.08

说 明 书 附 图

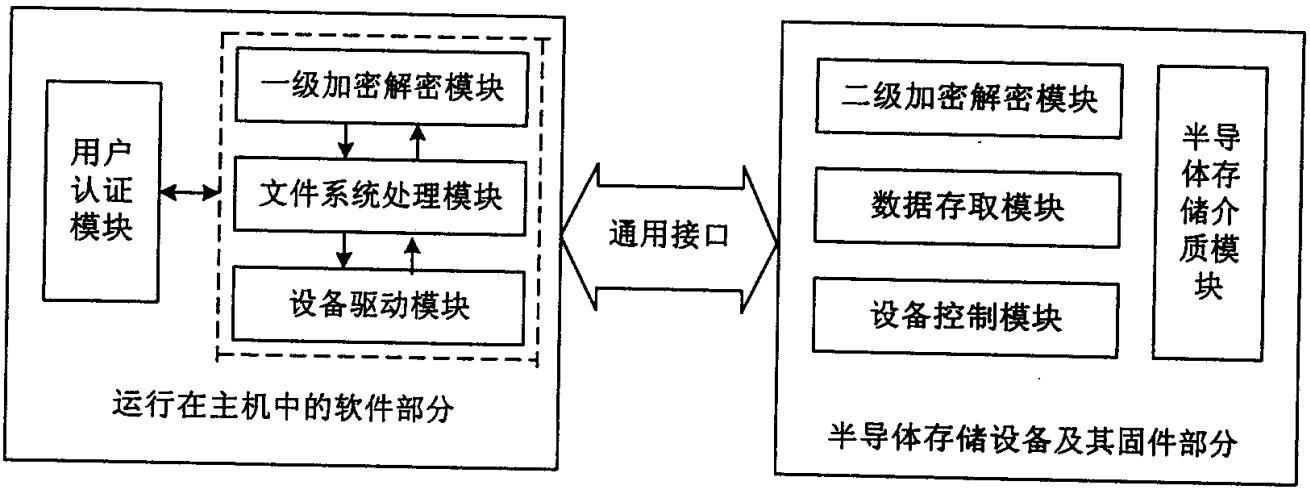


图 1

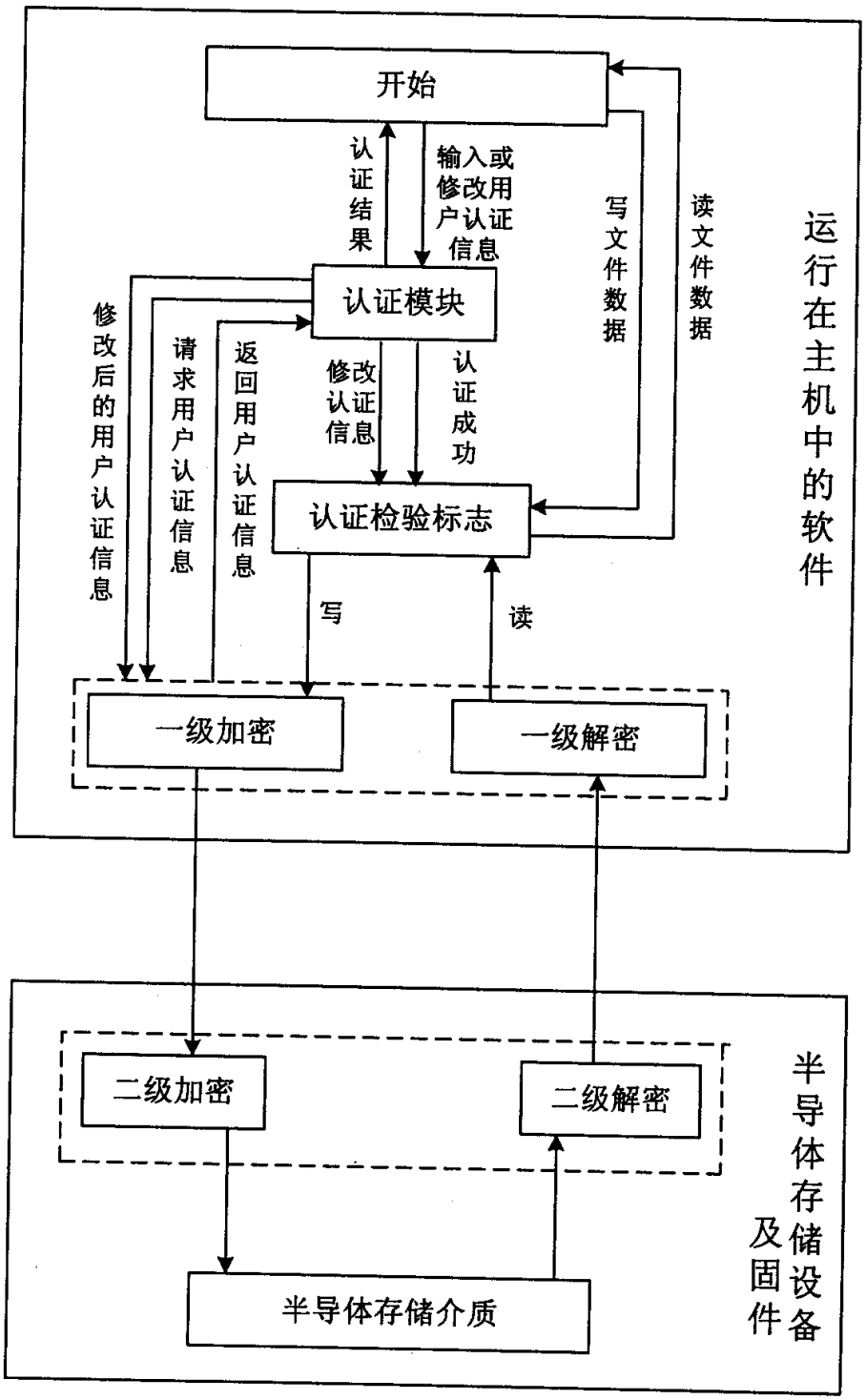

开始
认证结果
输入或修改用户认证信息
写文件数据
读文件数据
运行在主机中的软件
认证模块
修改后的用户认证信息
请求用户认证信息
返回用户认证信息
修改认证信息
认证成功
认证检验标志
写
读
一级加密
一级解密
二级加密
二级解密
半导体存储介质
半导体存储设备及固件

图 2

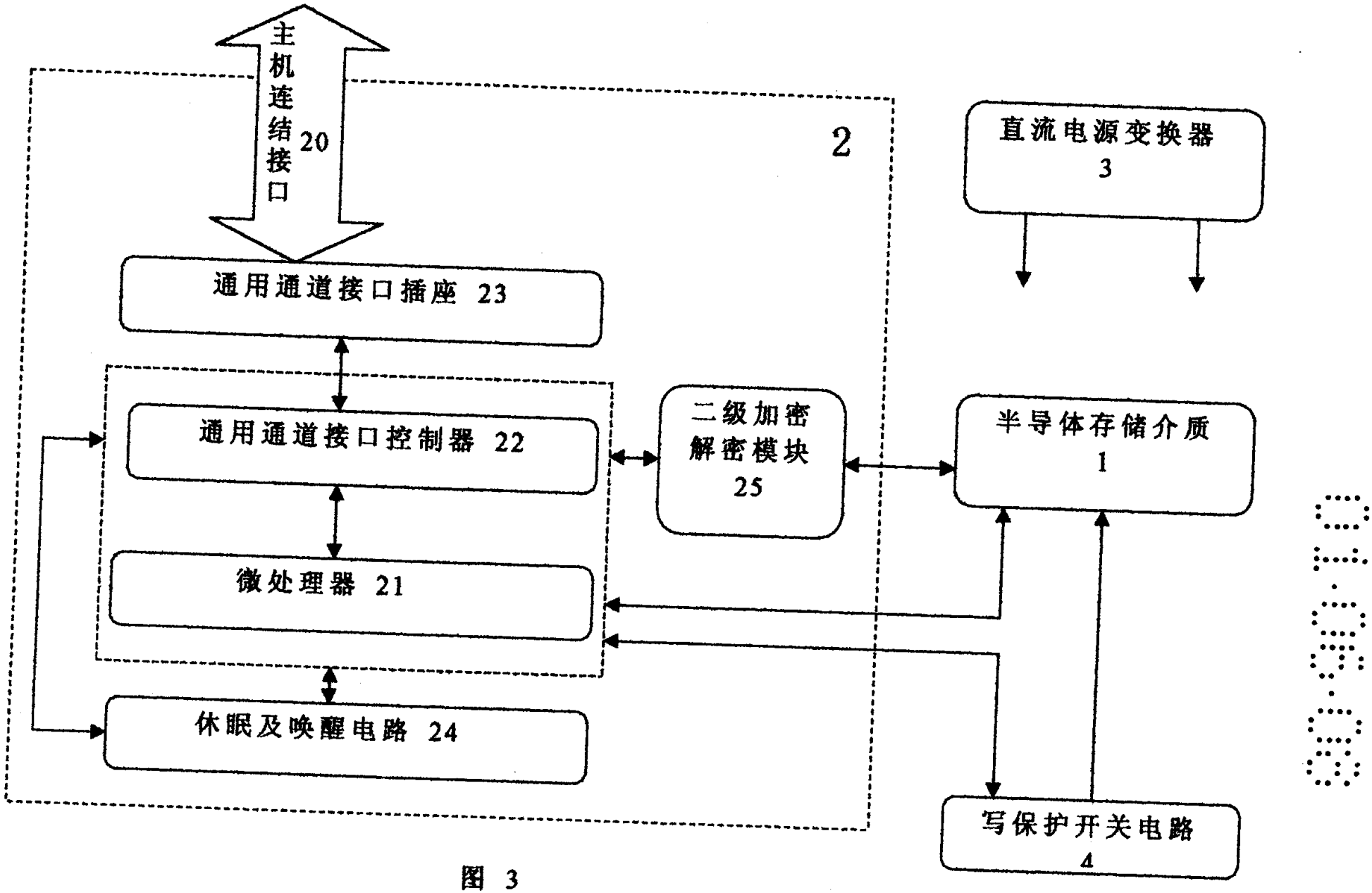

主机连结接口 20
2
直流电源变换器 3
通用通道接口插座 23
通用通道接口控制器 22
二级加密解密模块 25
半导体存储介质 1
微处理器 21
休眠及唤醒电路 24
写保护开关电路 4

图 3

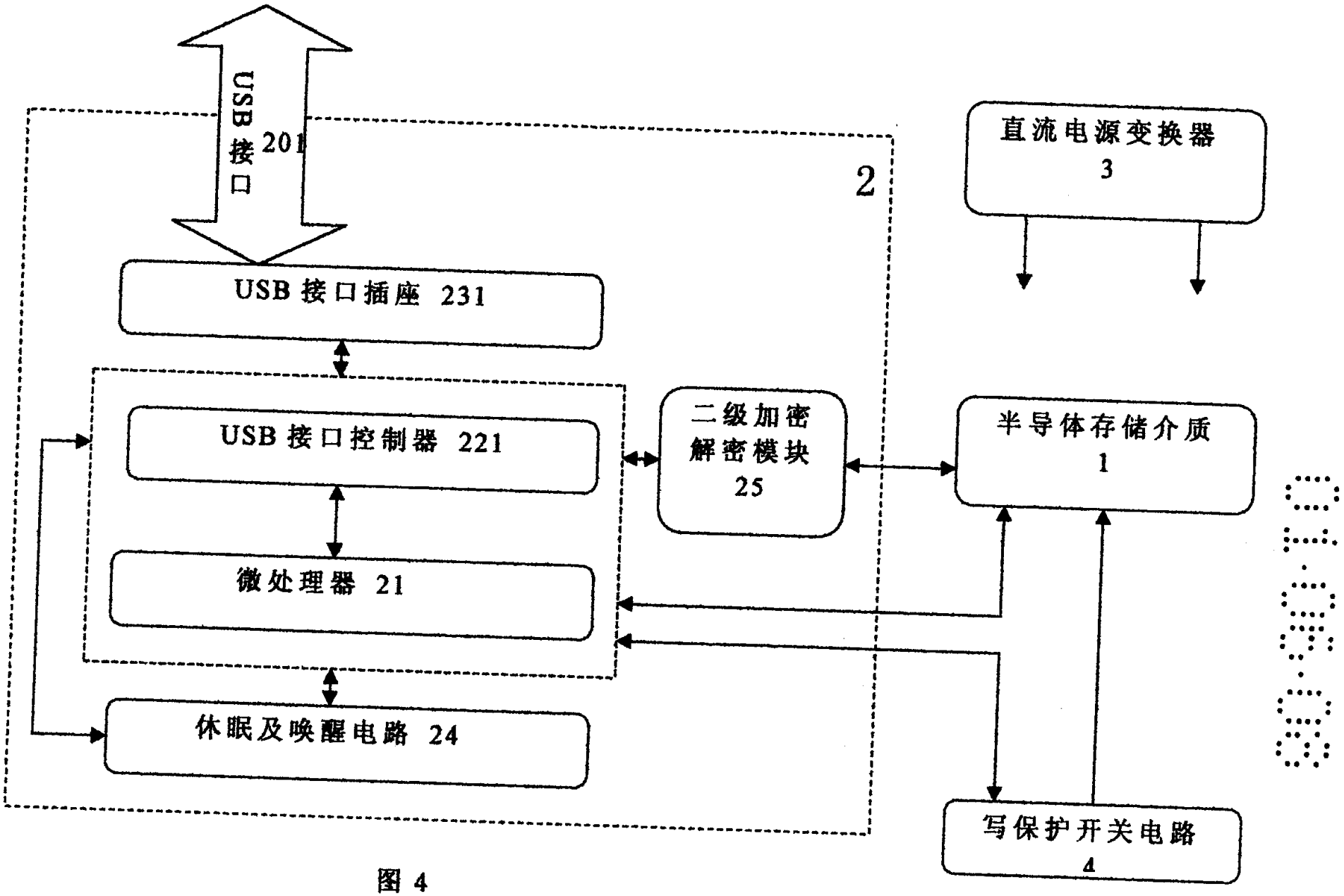

USB 接口 201
2
直流电源变换器 3
USB 接口插座 231
USB 接口控制器 221
二级加密解密模块 25
半导体存储介质 1
微处理器 21
休眠及唤醒电路 24
写保护开关电路 4

图 4

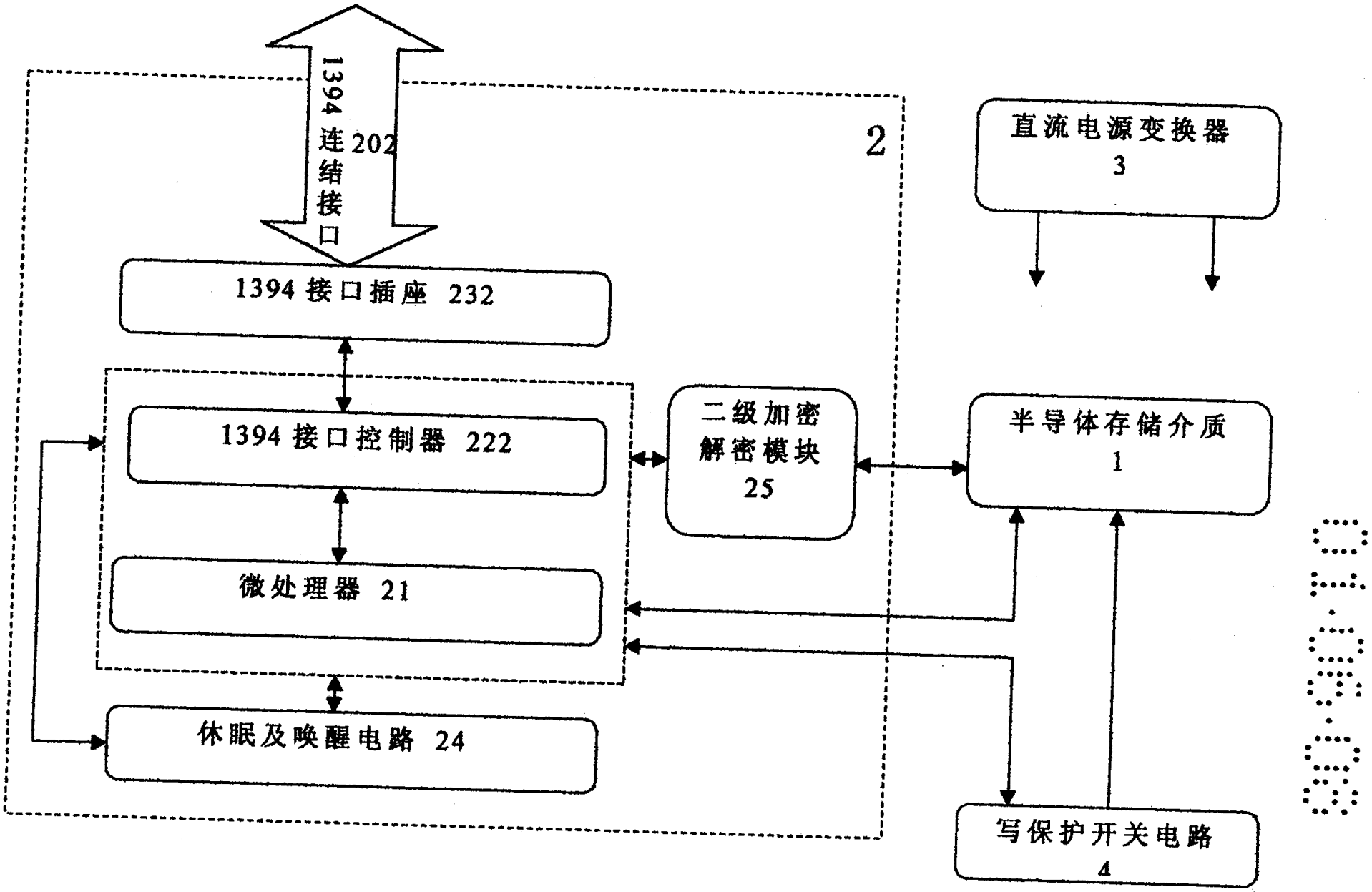

1394 连结接口 202
2
直流电源变换器 3
1394 接口插座 232
1394 接口控制器 222
二级加密解密模块 25
半导体存储介质 1
微处理器 21
休眠及唤醒电路 24
写保护开关电路 4

图 5

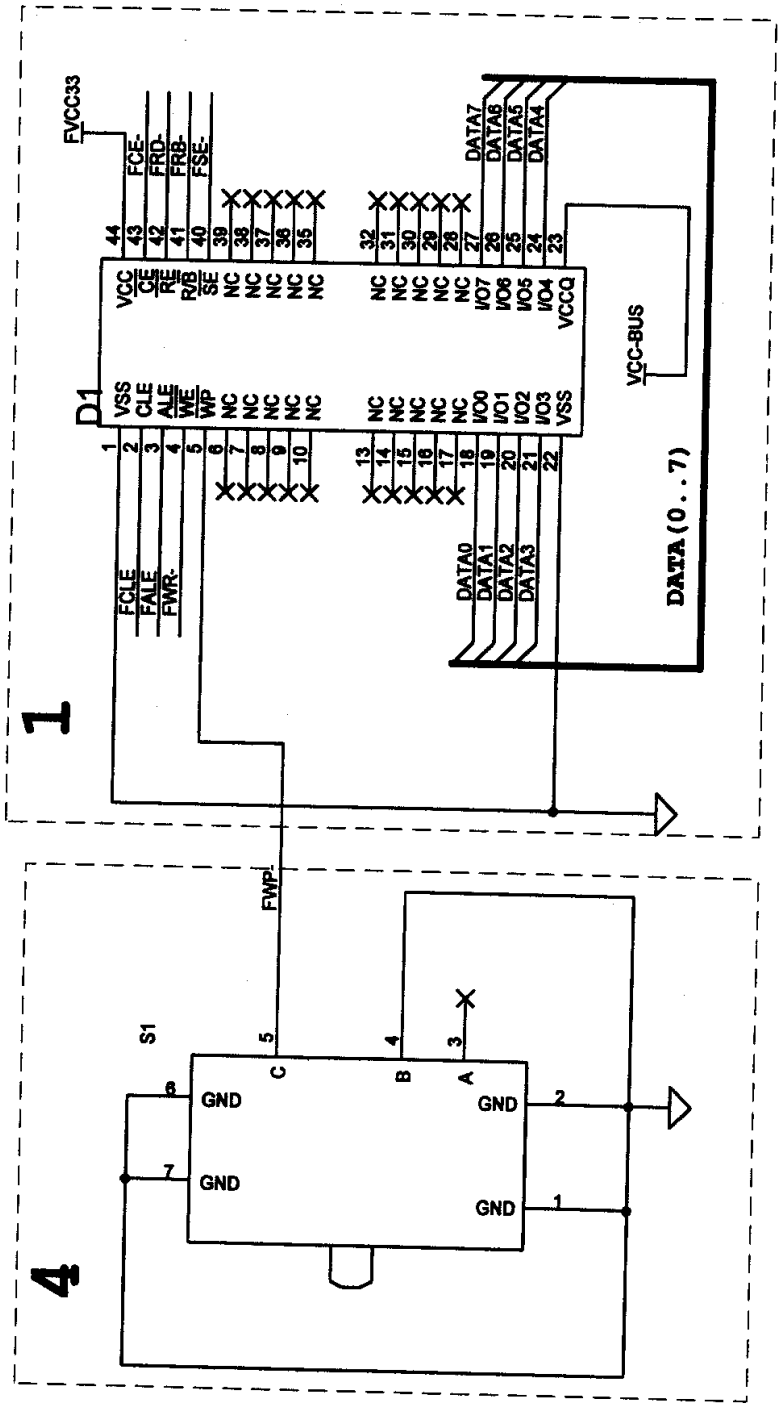

FVCC33
FCE-
FRD-
FRB-
FSE-
DATA7
DATA6
DATA5
DATA4
VCC
CLE
RE
R/B
SE
NC
I/O7
I/O6
I/O5
I/O4
VCCQ
VCC-BUS
D1
VSS
CLE
ALE
WE
WP
I/O0
I/O1
I/O2
I/O3
VSS
DATA0
DATA1
DATA2
DATA3
DATA(0..7)
FCLE
FALE
FWR-
1
FWP
S1
GND
GND
GND
GND
4

图 6

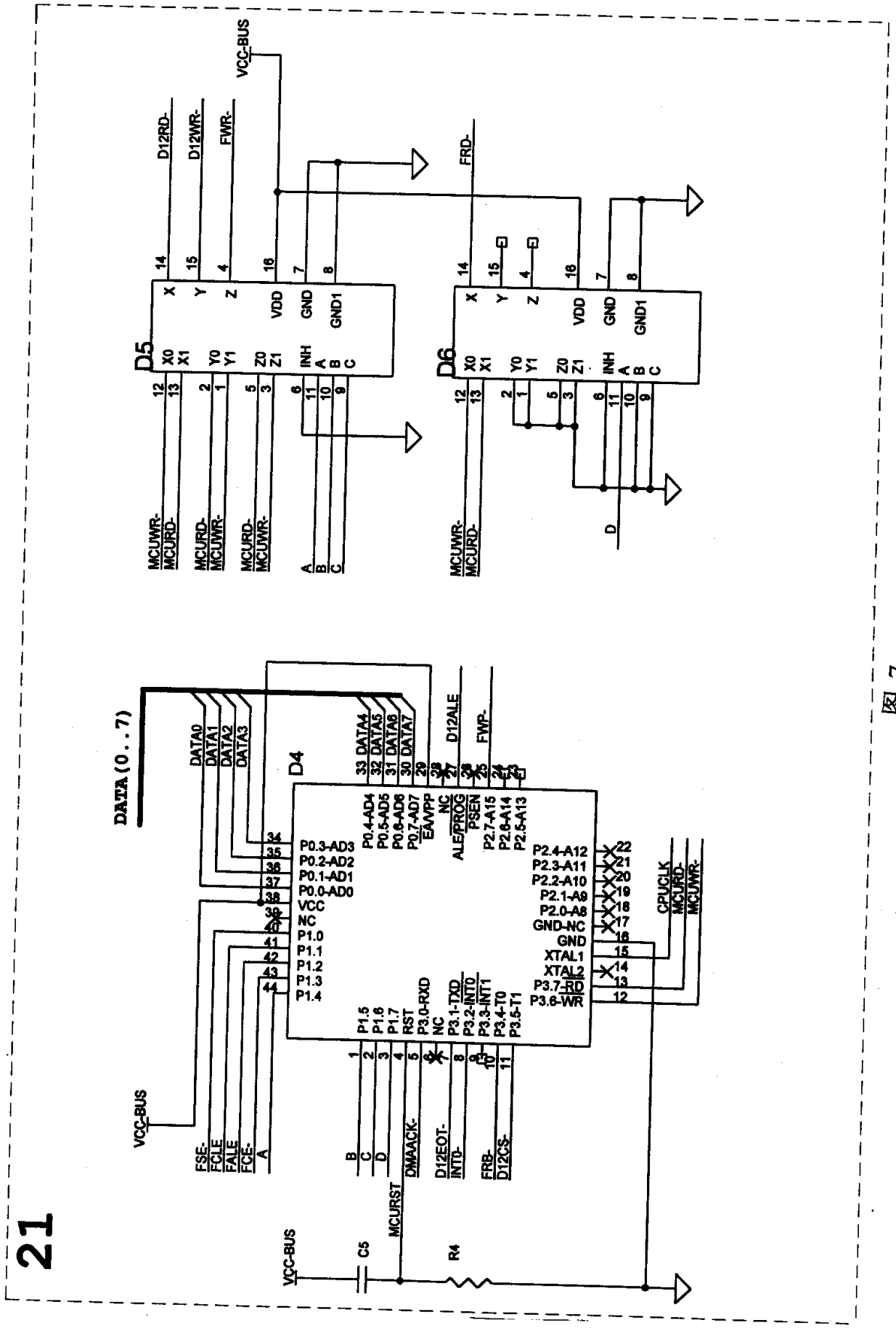
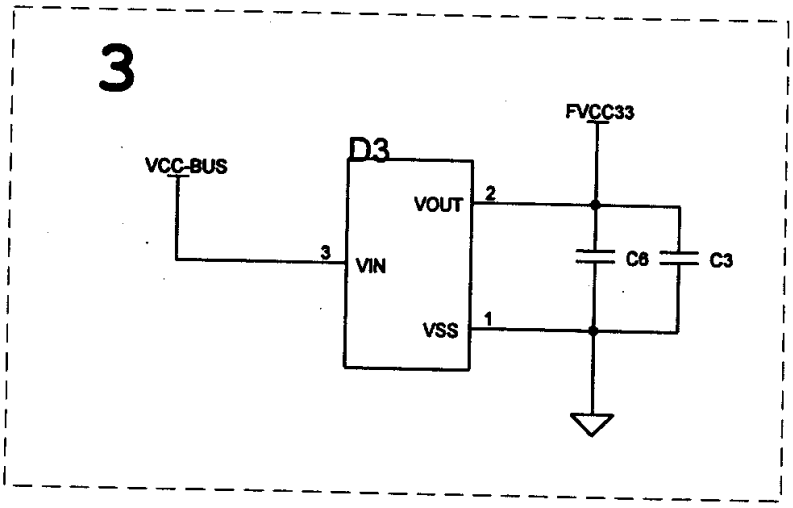

21
D5
D6
D4
VCC-BUS
D12RD-
D12WR-
FWR-
FRD-
MCUWR-
MCURD-
DATA(0..7)
DATA0
DATA1
DATA2
DATA3
D12ALE
FWP-
FSE-
FCLE
FALE
FCE-
DMAACK-
D12EOT-
INT0-
FRB-
D12CS-
MCURST
C5
R4
CPUCLK

图 7


3
FVCC33
VCC-BUS
D3
VOUT
2
3
VIN
C6
C3
VSS
1

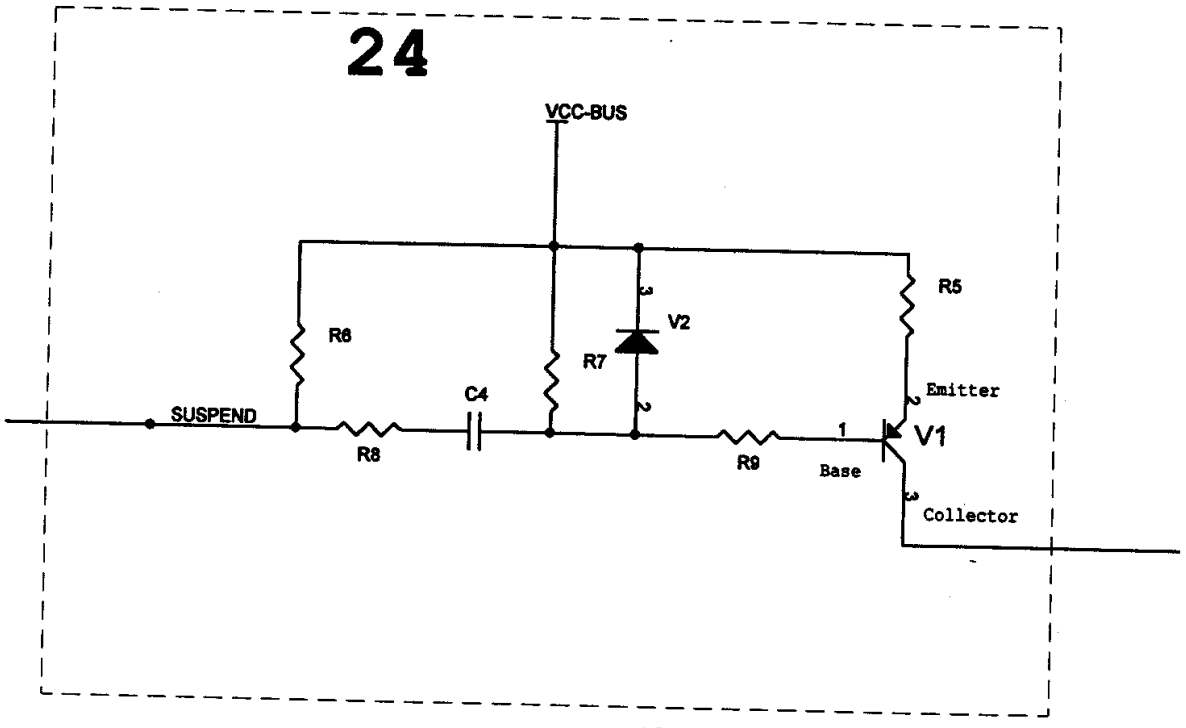

24
VCC-BUS
R5
R6
V2
R7
Emitter
C4
SUSPEND
1
V1
R8
R9
Base
Collector

图 8

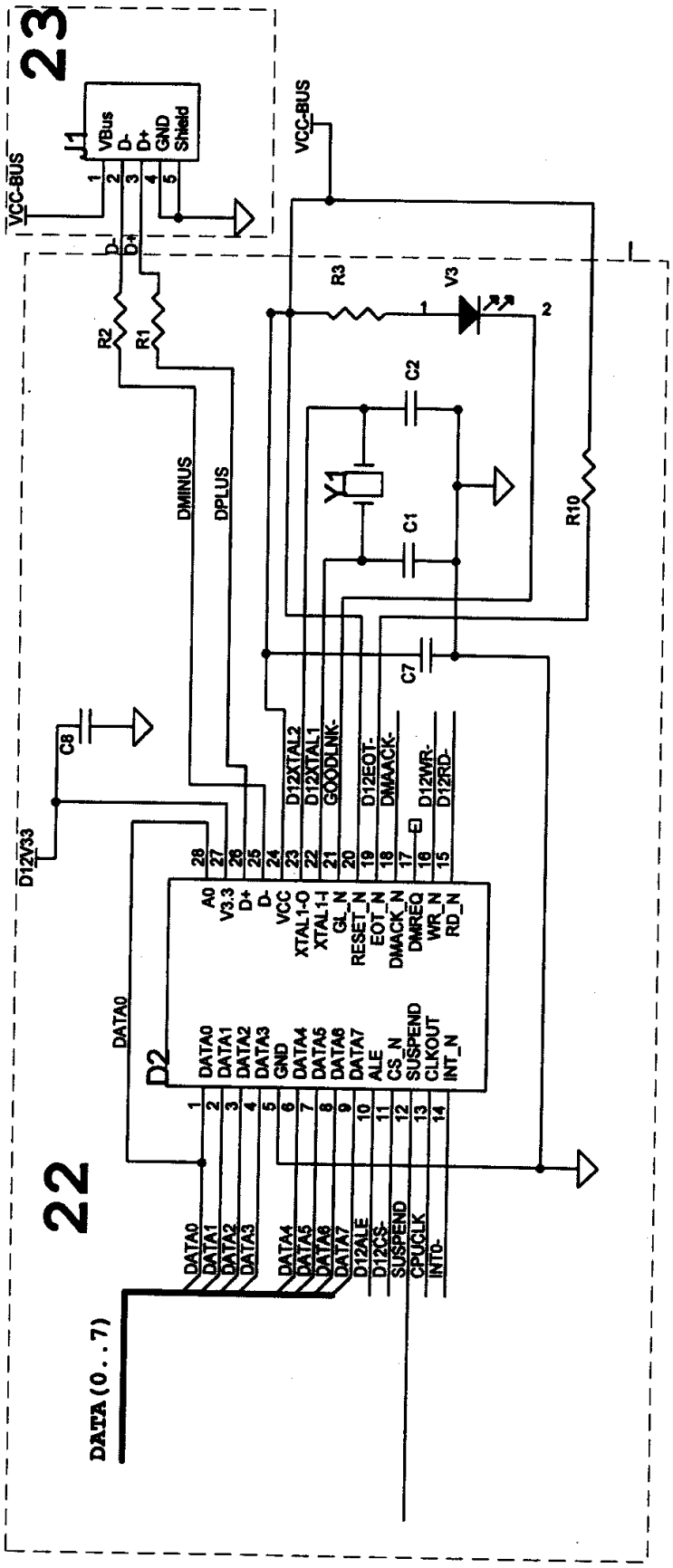

23
J1
VBus
D-
D+
GND
Shield
VCC-BUS
VCC-BUS
D-
D+
R2
R1
R3
V3
C2
Y1
C1
R10
C7
C8
DMINUS
DPLUS
D12V33
D2
A0
V3.3
D+
D-
VCC
XTAL1-O
XTAL1-I
GL_N
RESET_N
EOT_N
DMACK_N
DMREQ
WR_N
RD_N
D12XTAL2
D12XTAL1
GOODLNK-
D12EOT-
DMAACK-
D12WR-
D12RD-
DATA0
DATA1
DATA2
DATA3
GND
DATA4
DATA5
DATA6
DATA7
ALE
CS_N
SUSPEND
CLKOUT
INT_N
22
DATA0
DATA1
DATA2
DATA3
DATA4
DATA5
DATA6
DATA7
D12ALE
D12CS-
SUSPEND
CPUCLK
INT0-
DATA(0..7)

图 9

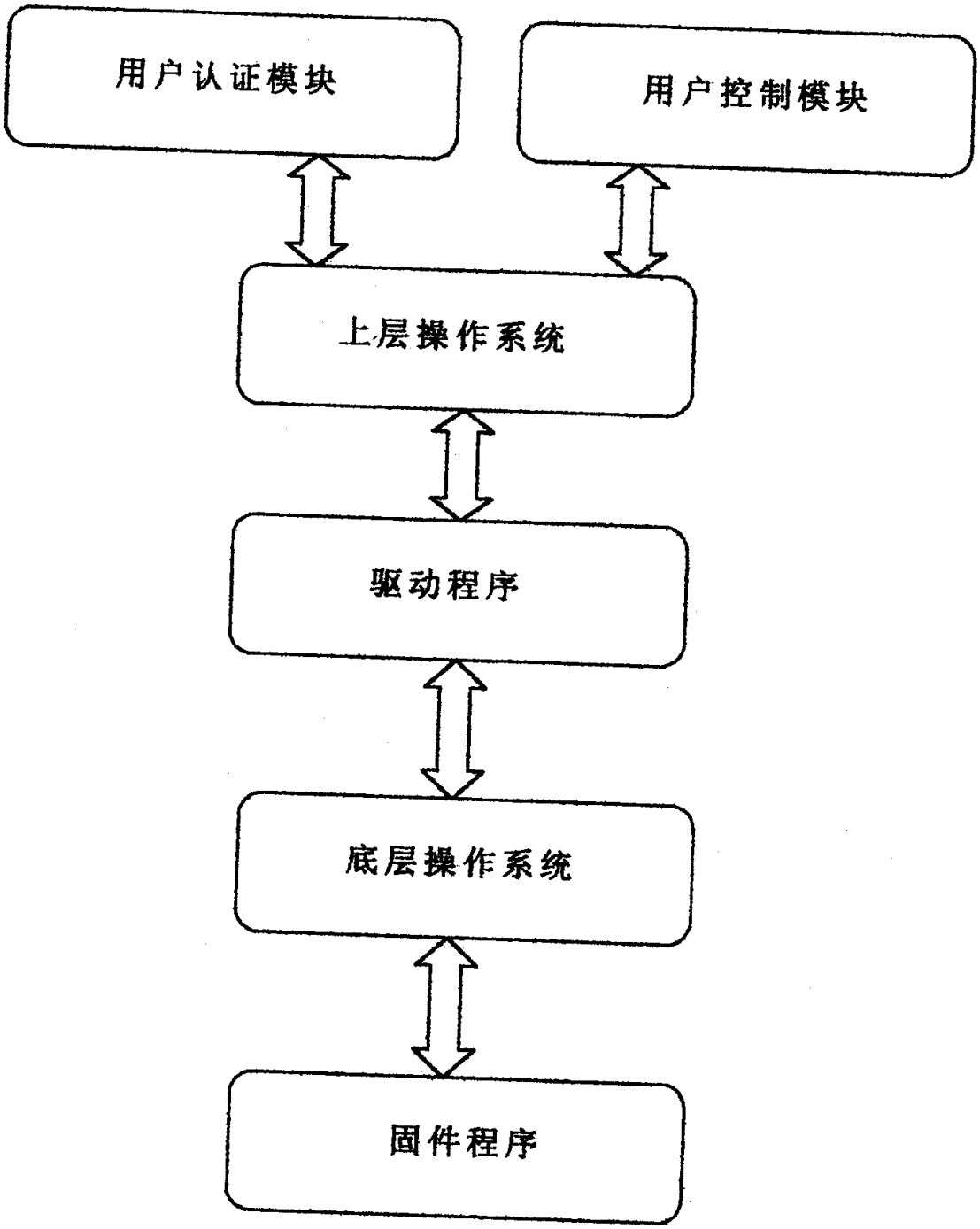


图 10

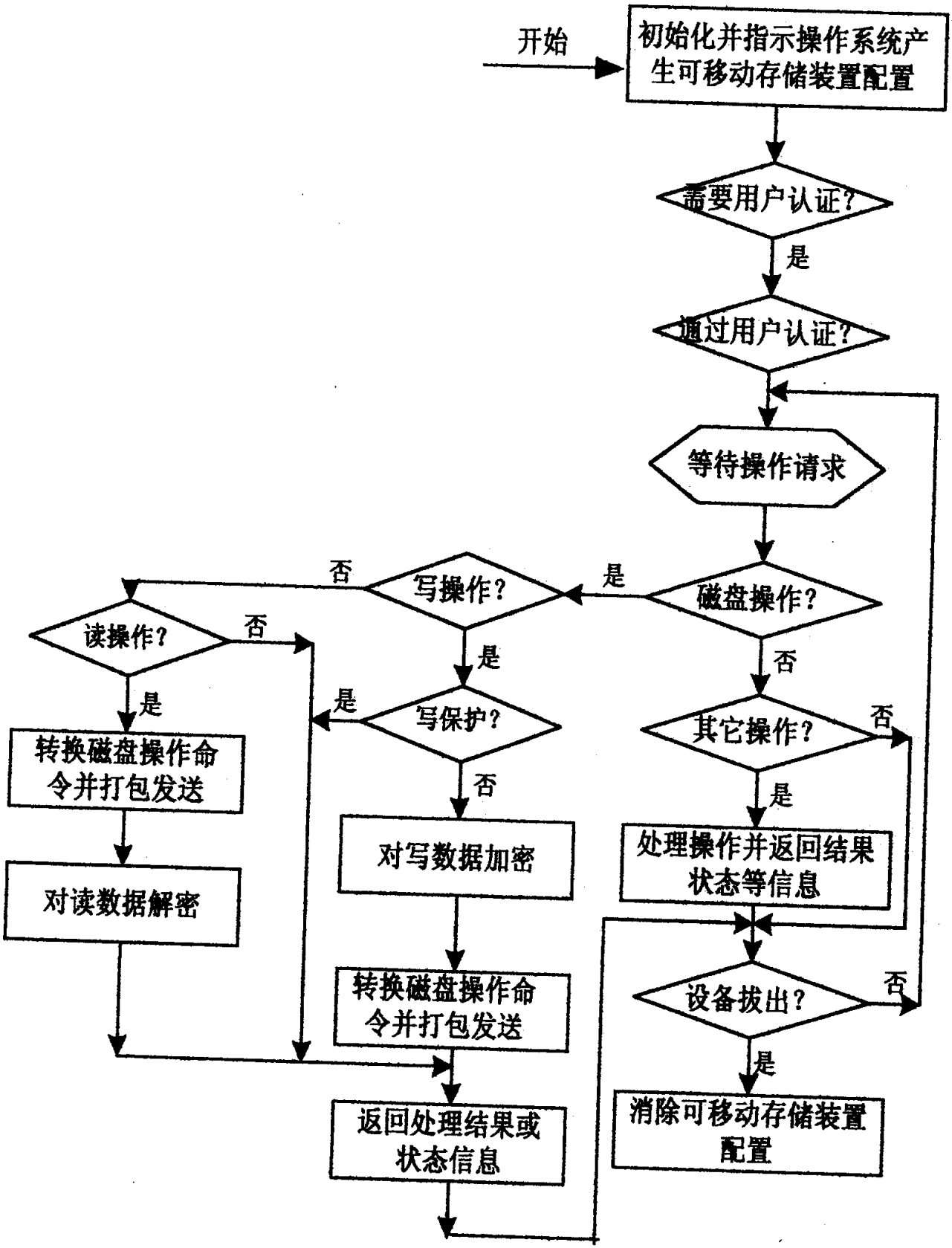

开始
初始化并指示操作系统产生可移动存储装置配置
需要用户认证?
是
通过用户认证?
等待操作请求
磁盘操作?
是
否
写操作?
否
读操作?
否
是
转换磁盘操作命令并打包发送
对读数据解密
是
写保护?
否
对写数据加密
转换磁盘操作命令并打包发送
返回处理结果或状态信息
否
其它操作?
否
是
处理操作并返回结果状态等信息
设备拔出?
否
是
消除可移动存储装置配置

图 11

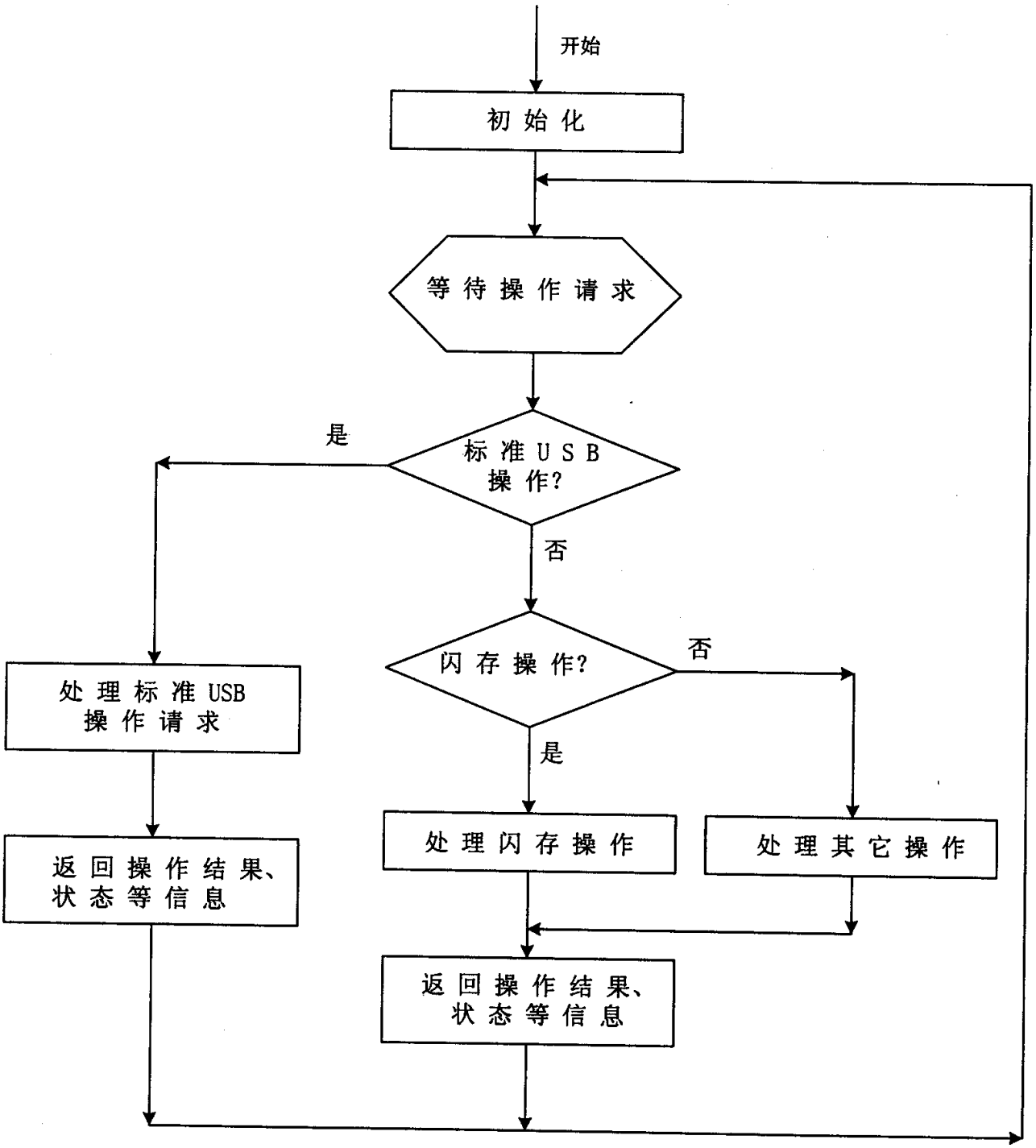

开始
初始化
等待操作请求
标准USB操作?
是
否
闪存操作?
否
是
处理标准USB操作请求
返回操作结果、状态等信息
处理闪存操作
处理其它操作
返回操作结果、状态等信息

图 12