

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 7 月 7 日 (07.07.2016)



(10) 国际公布号
WO 2016/106911 A1

- (51) 国际专利分类号:
G06F 12/14 (2006.01)
- (21) 国际申请号: PCT/CN2015/071556
- (22) 国际申请日: 2015 年 1 月 26 日 (26.01.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410851200.8 2014 年 12 月 30 日 (30.12.2014) CN
- (71) 申请人: 北京兆易创新科技股份有限公司
(GIGADEVICE SEMICONDUCTOR (BEIJING) INC.) [CN/CN]; 中国北京市海淀区学院路 30 号科大天工大厦 A12 层 01-15 室, Beijing 100083 (CN)。
- (72) 发明人: 李宝魁 (LI, Baokui); 中国北京市海淀区学院路 30 号科大天工大厦 A12 层 01-15 室, Beijing 100083 (CN)。 王景华 (WANG, Jinghua); 中国北京市海淀区学院路 30 号科大天工大厦 A12 层 01-15 室, Beijing 100083 (CN)。 王南飞 (WANG, Nanfei); 中国北京市海淀区学院路 30 号科大天工大厦 A12 层 01-15 室, Beijing 100083 (CN)。

- (74) 代理人: 北京润泽恒知识产权代理有限公司
(BEIJING RISEHIGH INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: METHOD AND DEVICE FOR PROTECTING INFORMATION OF MCU CHIP

(54) 发明名称: 一种 MCU 芯片的信息保护方法和装置

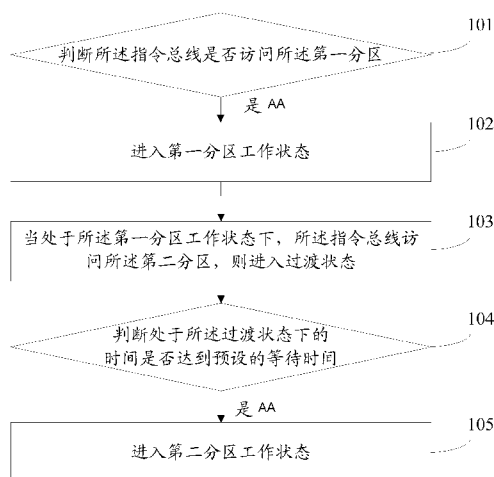


图1 / Fig.1

101 DETERMINE WHETHER COMMAND BUS IS ACCESSING FIRST SUB-AREA
102 ENTER FIRST SUB-AREA OPERATIONAL STATE
103 WHEN IN FIRST SUB-AREA OPERATIONAL STATE, AND COMMAND BUS ACCESSES SECOND SUB-AREA, ENTER TRANSITIONAL STATE
104 DETERMINE WHETHER AMOUNT OF TIME OF BEING IN TRANSITIONAL STATE REACHES PRESET WAITING TIME
105 ENTER SECOND SUB-AREA OPERATIONAL STATE
AA YES

(57) Abstract: A method and device for protecting information of an MCU chip, the MCU chip comprising a command bus, a data bus, a flash memory controller and a flash memory user area, the flash memory controller being used for dividing the flash memory user area into a first sub-area and a second sub-area. The method comprises: when the command bus accesses the flash memory user area, determining whether the command bus is accessing the first sub-area (101); if so determined, entering a first sub-area operational state (102); when in the first sub-area operational state, and the command bus accesses the second sub-area, entering a transitional state (103); determining whether the amount of time of being in the transitional state reaches a preset waiting time (104); if so determined, entering a second sub-area operational state (105). The method and device are used to protect programs from being stolen by a client, and also protect against a situation wherein companies collaboratively developing a program are able to steal programs from one another.

(57) 摘要: 一种 MCU 芯片的信息保护方法和装置, 所述 MCU 芯片包括指令总线、数据总线、闪存控制器和闪存用户区; 所述闪存控制器用于将闪存用户区划分为第一分区和第二分区; 所述的方法包括: 当所述指令总线访问所述闪存用户区时, 判断所述指令总线是否访问所述第一分区 (101); 若是, 则进入第一分区工作状态 (102); 当处于所述第一分区工作状态下, 所述指令总线访问所述第二分区, 则进入过渡状态 (103); 判断处于所述过渡状态下的时间是否达到预设的等待时间 (104); 若是, 则进入第二分区工作状态 (105); 所述方法和装置用以保护程序不被客户窃取, 同时保护合作开发程序的公司不能相

互窃取对方的程序。

WO 2016/106911 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种 MCU 芯片的信息保护方法和装置

本申请要求在 2014 年 12 月 30 日提交中国专利局、申请号为 201410851200.8、发明名称为“一种 MCU 芯片的信息保护方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本申请涉及电子电路技术领域，特别是涉及一种 MCU 芯片的信息保护方法和一种 MCU 芯片的信息保护装置。

背景技术

随着集成电路技术的不断提高，MCU(Micro Control Unit，微控制单元)芯片的应用越来越广泛，小到儿童玩具，大到工程机械，都需要用到 MCU 芯片。MCU 芯片通常包含 CPU (Central Processing Unit，中央处理器)、闪存 (Flash Memory)、SRAM (Static Random Access Memory，静态随机存储器)和各种外围设备。在 MCU 芯片掉电时，闪存的内容不会丢失，而 SRAM 的内容则会丢失。闪存通常会被分为两个独立的区域：
10 一个是闪存用户区，用来存储用户的程序；另一个是闪存信息区，用来存放 MCU 芯片的配置信息。SRAM 一般用作片上缓存。

对于 MCU 芯片的方案商而言，也就是基于 MCU 芯片开发程序和外围电路的厂商，程序最终会烧写到 MCU 芯片的闪存用户区中，由于方案商的核心价值在于所开发的程序，故需要保证程序绝对安全，不能被他人窃取。MCU 芯片的信息保护方案的目标就是保护闪存用户区的内容不被他人窃取。目前市场上的 MCU 芯片的产品在信息保护方案方面，都只是对其闪存用户区的内容整体地保护，无法满足两家公司合作开发程序的需求。因为它只能保护闪存用户区的内容不被客户窃取，而不能阻止合作开发程序的公司相互窃取对方的程序。

25 因此，目前需要本领域技术人员迫切解决的一个技术问题就是：提出一种 MCU 芯片的信息保护方案，用以保护程序不被客户窃取，同时保护合作开发程序的公司不能相互窃取对方的程序。

发明内容

本申请实施例所要解决的技术问题是提供一种 MCU 芯片的信息保护方法，用以保护程序不被客户窃取，同时保护合作开发程序的公司不能相互窃取对方的程序。

5 相应的，本申请实施例还提供了一种 MCU 芯片的信息保护装置，用以保证上述方法的实现及应用。

为了解决上述问题，本申请公开了一种 MCU 芯片的信息保护方法，所述 MCU 芯片包括指令总线、数据总线、闪存控制器和闪存用户区；所述闪存控制器用于将闪存用户区划分为第一分区和第二分区；所述的方法包括：

10

当所述指令总线访问所述闪存用户区时，判断所述指令总线是否访问所述第一分区；

若是，则进入第一分区工作状态；在所述第一分区工作状态下，允许所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

15

当处于所述第一分区工作状态下，所述指令总线访问所述第二分区，则进入过渡状态；在所述过渡状态下，暂停所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

20 判断处于所述过渡状态下的时间是否达到预设的等待时间；

若是，则进入第二分区工作状态；在所述第二分区工作状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区，但允许所述数据总线访问所述第二分区。

优选地，所述方法还包括：

25 在所述 MCU 芯片复位后，进入初始状态；在所述初始状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区和第二分区。

优选地，所述 MCU 芯片包括 CPU，所述 CPU 为哈佛结构；所述预

设的等待时间与 CPU 的特性相关；若所述 CPU 为 ARM Cortex-M3，则所述预设的等待时间为 20 个 CPU 时钟周期。

优选地，所述 MCU 芯片包括闪存信息区，所述闪存信息区包括选项字节；所述的方法还包括：

5 依据所述选项字节确定所述闪存用户区的读保护状态；

若为零级读保护状态，则允许对所述闪存用户区进行读取、写入和擦除；

10 若为一级读保护状态，则允许对所述第一分区进行读取、写入和擦除，仅在所述闪存用户区启动时允许对所述第二分区进行读取、写入和擦除；

若为二级读保护状态，则仅在所述闪存用户区启动时允许对所述第一分区和第二分区进行读取、写入和擦除。

优选地，

在所述零级读保护状态下，所述选项字节允许修改；

15 在所述一级读保护状态下，所述选项字节允许修改，若基于所述选项字节从所述一级读保护状态修改为零级读保护状态，则所述闪存用户区中的全部信息将被擦除；

在所述二级读保护状态下，所述选项字节禁止修改。

20 优选地，所述 MCU 芯片设计有私有设备，仅在输出有第一分区使能信号时正常工作的私有设备为第一设备，以及，仅在输出有第二分区使能信号时正常工作的私有设备为第二设备；所述方法还包括：

若处于所述第一分区工作状态，或者，第一分区过渡状态，则输出第一分区使能信号；若处于所述第二分区工作状态，或者，第二分区过渡状态，则输出第二分区使能信号。

25 优选地，所述设备包括静态随机存储器 SRAM。

优选地，所述第一分区位于闪存用户区的前半段地址空间，所述第二分区位于闪存用户区的后半段地址空间。

本申请实施例还公开了一种 MCU 芯片的信息保护装置, 所述 MCU 芯片包括指令总线、数据总线、闪存控制器和闪存用户区; 所述闪存控制器用于将闪存用户区划分为第一分区和第二分区; 所述的装置包括:

5 第一判断模块, 配置为当所述指令总线访问所述闪存用户区时, 判断所述指令总线是否访问所述第一分区; 若是, 则调用第一进入模块;

第一进入模块, 配置为进入第一分区工作状态; 在所述第一分区工作状态下, 允许所述指令总线访问所述闪存用户区, 允许所述数据总线访问所述第一分区, 但禁止所述数据总线访问所述第二分区;

10 第二进入模块, 配置为当处于所述第一分区工作状态下, 所述指令总线访问所述第二分区, 则进入过渡状态; 在所述过渡状态下, 暂停所述指令总线访问所述闪存用户区, 允许所述数据总线访问所述第一分区, 但禁止所述数据总线访问所述第二分区;

第二判断模块, 配置为判断处于所述过渡状态下的时间是否达到预设的等待时间; 若是, 则调用第三进入模块;

15 第三进入模块, 配置为进入第二分区工作状态; 在所述第二分区工作状态下, 允许所述指令总线访问所述闪存用户区, 禁止所述数据总线访问所述第一分区, 但允许所述数据总线访问所述第二分区。

优选地, 所述装置还包括:

20 第四进入模块, 配置为在所述 MCU 芯片复位后, 进入初始状态; 在所述初始状态下, 允许所述指令总线访问所述闪存用户区, 禁止所述数据总线访问所述第一分区和第二分区。

优选地, 所述 MCU 芯片包括闪存信息区, 所述闪存信息区包括选项字节; 所述的装置还包括:

25 确定模块, 配置为依据所述选项字节确定所述闪存用户区的读保护状态;

第一保护模块, 配置为在为零级读保护状态时, 允许对所述闪存用户区进行读取、写入和擦除;

第二保护模块, 配置为在为一级读保护状态时, 允许对所述第一分

区进行读取、写入和擦除，仅在所述闪存用户区启动时允许对所述第二分区进行读取、写入和擦除；

第三保护模块，配置为在为二级读保护状态时，仅在所述闪存用户区启动时允许对所述第一分区和第二分区进行读取、写入和擦除。

5 优选地，

在所述零级读保护状态下，所述选项字节允许修改；

在所述一级读保护状态下，所述选项字节允许修改，若基于所述选项字节从所述一级读保护状态修改为零级读保护状态，则所述闪存用户区中的全部信息将被擦除；

10 在所述二级读保护状态下，所述选项字节禁止修改。

优选地，所述 MCU 芯片设计有私有设备，仅在输出有第一分区使能信号有效时正常工作的私有设备为第一设备，以及，仅在输出有第二分区使能信号有效时正常工作的私有设备为第二设备；所述装置还包括：

15 第一输出模块，配置为在处于所述第一分区工作状态，或者，第一分区过渡状态时，输出第一分区使能信号；

第二输出模块，配置为在处于所述第二分区工作状态，或者，第二分区过渡状态时，输出第二分区使能信号。

20 本申请实施例还公开了一种在其上记录有用于执行权利要求 1 所述方法的程序的计算机可读记录介质。

与现有技术相比，本申请实施例包括以下优点：

25 在本申请实施例中，在 MCU 芯片中的闪存控制器将闪存用户区划分为第一分区和第二分区，当指令总线访问闪存用户区时，闪存用户区可以正常接受指令总线的访问，但是数据总线访问分区将受到限制。例如，当指令总线访问第一分区时，数据总线只能访问第一分区，不能访问第二分区。如果指令总线从访问第一分区转为访问第二分区，则暂停指令总线访问闪存用户区，并且在达到预设的等待时间时，指令总线又可以

访问闪存用户区，此时数据总线不能访问第一分区，只能访问第二分区。
本申请实施例在指令总线访问闪存用户区时，只允许数据总线访问指令总线所访问的分区，可以保护在闪存用户区中的程序不被合作开发程序的其他公司窃取。

5 在本申请实施例中，还对 MCU 芯片设置有读保护级别，根据闪存信息区中的选项字节，确定该 MCU 芯片对闪存的读保护级别，限制对于闪存用户区的操作。在两家公司合作开发 MCU 芯片中的程序时，当某个公司开发完毕后，可以提高闪存用户区的读保护级别，以限制其他公司读取器烧录到闪存用户区的程序，从而避免合作开发程序的公司相互窃取
10 对方的程序。此外，如果有人想通过降低读保护级别的方式去窃取获得访问闪存用户区的程序的权限，闪存用户区中的全部程序都将被擦除，进一步保护了公司的开发成果。

 在本申请实施例中，可以将分区划分给不同合作开发的公司，并且可以将外围设备设计为某一分区的私有设备，每个分区具有对应的分区
15 使能信号，而分区使能信号可以控制其所对应的私有设备。例如，根据分区使能信号，可以开启或关闭对应私有设备的部分或全部功能，避免了合作开发的公司所开发的程序运行的中间结果，被其他合作公司得到。

附图说明

 图 1 是本申请的一种 MCU 芯片的信息保护方法实施例的步骤流程图；
20 图 2 是本申请的一种基于哈佛结构 CPU 的 MCU 芯片的系统结构示意图；
 图 3 是本申请的一种 MCU 芯片闪存控制器的工作流程示意图；
 图 4 是本申请的一种 MCU 芯片的信息保护装置实施例的结构框图。

具体实施方式

25 为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

 下面介绍了本申请实施例的一种 MCU 芯片的信息保护方案。

通过闪存信息区的若干控制位来控制闪存控制器的读保护级别。闪存控制器的读保护级别分三级，各级别的特征如下：

零级读保护：闪存用户区完全开放，可以任意读、写和擦除。闪存信息区也一样完全开放。

5 一级读保护：从闪存用户区启动可以正常访问闪存用户区；其他启动方式（包括从其他位置启动以及 JTAG (Joint Test Action Group, 联合测试工作组)）等调试手段均不能访问闪存用户区，读、写和擦除等操作都不行。在此级别下，可以访问闪存信息区，但如果修改控制位将闪存控制器的读保护级别改为零级，闪存用户区的内容会全部被擦除。

10 二级读保护：从闪存用户区启动可以正常访问闪存用户区；其他启动方式（包括从其他位置启动以及 JTAG 等调试手段）均不可用。在此级别下，闪存信息区只可读，不可写，也不可擦除。

在上述的 MCU 芯片的信息保护方案中，将闪存用户区作为一个整体来保护的。如果 MCU 芯片的程序完全由一家公司来开发，采用此方案可以满足需求。但随着 MCU 芯片应用日趋复杂，MCU 芯片的程序会越来越复杂。将会有两家公司甚至多家公司合作开发程序的需求。而该 MCU 芯片信息保护方案是满足不了的。因为它只能保护闪存用户区的内容不被客户窃取，不能阻止合作开发程序的公司之间相互窃取对方的程序。基于这样的需求，本申请实施例进一步提出了一种 MCU 芯片的信息保护方案。

20

应用本申请实施例的 MCU 信息保护方案，可以满足两家公司合作开发 MCU 芯片程序的需求。本申请实施例将闪存用户区分为两个分区，合作开发程序的两家公司可分别将自己开发的程序烧写到属于自己的分区中。本申请实施例可以保证两家公司的程序之间既可以正常实现相互调用，又不能相互窃取对方分区中的程序，同时保护程序不被客户窃取。

25

另外，如果 SRAM 和其他外围设备都由是合作的两家公司共享，程序有可能通过这些共享资源被合作方窃取。对此，本申请实施例还可以将特定 SRAM 或外围设备划分给某一方作为私有设备，拓宽了本申请实施例

的应用范围。

参照图 1，示出了本申请的一种 MCU 芯片的信息保护方法实施例的步骤流程图，所述 MCU 芯片可以包括指令总线、数据总线、闪存控制器和闪存用户区；所述闪存控制器可以用于将闪存用户区划分为第一分区
5 和第二分区；

参照图 2 所示的本申请的一种基于哈佛结构 CPU 的 MCU 芯片的系统结构示意图，MCU 芯片通常包含 CPU、总线、闪存、闪存控制器、SRAM、各种主设备和从设备（外围设备）等等。其中，所述总线可以包括指令
10 总线、数据总线和系统总线。在具体实现中，CPU 通过指令总线、数据总线和系统总线与总线互联矩阵相连。指令总线负责读取指令；数据总线负责数据访问；系统总线负责访问外围设备。

MCU 芯片的闪存控制器是连接总线和闪存的桥梁。闪存控制器有同样的三条总线与总线互联矩阵相连，其中指令总线负责接受 CPU 的取指令访问；数据总线负责接受 CPU 的数据访问；它的配置寄存器是通过系统总线被访问的。SRAM 以及各种外围设备都是连接在总线互联矩阵上的。在本申请实施例中，在两家公司合作开发 MCU 芯片的程序时，可以将两个分区分别划分给合作开发程序的两家公司，并且可以将外围设备
15 设计为某一分区的私有设备，每个分区具有对应的分区使能信号，私有设备会受闪存控制器输出的分区使能信号控制。

在具体实现中，“访问”包含所有的操作。MCU 芯片的总线有读操作和写操作，那么总线访问包含读操作和写操作。闪存具有读操作、写操作和擦除操作，那么对闪存的访问就包含读操作、写操作和擦除操作。

所述的方法具体可以包括如下步骤：

25 步骤 101，当所述指令总线访问所述闪存用户区时，判断所述指令总线是否访问所述第一分区；若是，则执行步骤 102；

步骤 102，进入第一分区工作状态；在所述第一分区工作状态下，允许所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一

分区，但禁止所述数据总线访问所述第二分区；

步骤 103，当处于所述第一分区工作状态下，所述指令总线访问所述第二分区，则进入过渡状态；在所述过渡状态下，暂停所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

步骤 104，判断处于所述过渡状态下的时间是否达到预设的等待时间；若是，则执行步骤 105；

步骤 105，进入第二分区工作状态下；在所述第二分区工作状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区，但允许所述数据总线访问所述第二分区。

应用本申请实施例，至少具有如下两个优点：第一，保护闪存的内容不被终端客户窃取；第二，确保合作开发程序的两家公司不能相互窃取对方的程序。

合作开发程序的两家公司一定有一家开发主程序的，另一家是开发库函数的。此处将开发主程序的公司称为第一公司，开发库函数的公司称为第二公司。两家公司对应的分区分别是第一分区和第二分区。第一分区位于前半段地址空间，第二分区位于后半段地址空间。这样便于 MCU 芯片启动时率先执行第一公司的程序。本申请实施例的 MCU 芯片信息保护的方法可以分为三部分来描述：第一部分是分区保护工作方式；第二部分是读保护级别的定义及使用方法；第三部分是私有设备的实现方法。前两部分是在闪存控制器中实现的；第三部分是根据闪存控制器输出的分区使能信号在私有设备中实现的。

第一部分：分区保护工作方式。

在闪存用户区启动时，闪存用户区可以正常接受 CPU 指令总线的访问，并可以受限制的接受 CPU 数据总线的访问，但不接受其他主设备的访问。参照图 3 所示的本申请的一种 MCU 芯片闪存控制器的工作流程示意图，具体的步骤如下所示：

1、MCU 芯片复位，闪存控制器处于初始状态。在所述初始状态下，

指令总线可以访问所有分区，数据总线不能访问任何分区。

2、判断指令总线是否在访问闪存用户区；若是，则执行步骤 3，若否，则返回步骤 1。

3、判断指令总线访问的是否为第一分区；若是，则执行步骤 4，若否，则执行步骤 9。

4、进入第一分区工作状态。在所述第一分区工作状态下，指令总线可以访问所有分区，数据总线可以访问第一分区但不能访问第二分区（若访问第二分区，返回错误响应）。

5、判断指令总线是否在访问闪存用户区；若否，则返回步骤 4，即如果指令总线没有访问闪存用户区，则保持在当前状态（第一分区工作状态）；若是，执行步骤 6。

6、判断指令总线访问的是否为其他分区（第二分区）；如果指令总线访问的是当前工作的分区（第一分区），保持当前状态，即返回步骤 4，如果指令总线访问的是其他分区（第二分区），则执行步骤 7。

7、进入第一分区过渡状态。在所述第一分区过渡状态下，暂停响应指令总线，数据总线可以访问第一分区但不能访问第二分区（若访问第二分区，返回错误响应）。

8、在过渡状态下等待时间是否已到达预设的等待时间；若是，则执行步骤 9；若否，则返回步骤 7。

9、进入第二分区工作状态。在所述第二分区工作状态下，指令总线可以访问所有分区，数据总线可以访问第二分区但不能访问第一分区（访问第一分区，返回错误响应）。

10、判断指令总线是否在访问闪存用户区；若否，则返回步骤 9，即如果指令总线没有访问闪存用户区，则保持在当前状态（第二分区工作状态）；若是，执行步骤 11。

11、判断指令总线访问的是否为其他分区（第一分区）；如果指令总线访问的是当前工作的分区（第二分区），保持当前状态，即返回步骤 9，如果指令总线访问的是其他分区（第一分区），则执行步骤 12。

12、进入第二分区过渡状态。在所述第二分区过渡状态下，暂停响应指令总线，数据总线可以访问第二分区但不能访问第一分区（若访问第一分区，返回错误响应）。

13、在过渡状态下等待时间是否已到达预设的等待时间；若是，则
5 执行步骤 4；若否，则返回步骤 12。

在本申请的具体应用的一种示例中，在过渡状态中的预设等待时间的长短与 MCU 芯片的 CPU 的特性相关。哈佛结构 CPU 通过指令总线读取指令，通过数据总线完成数据访问，两者是并行工作的。CPU 通过指令总线取得要执行的指令，经过指令解析得出是否需要数据访问以及需
10 要访问哪个地址的数据，然后通过数据总线完成相应数据访问。

从指令总线读取指令到数据总线完成相应数据访问要经过若干周期。过渡状态的作用就是在阻止针对其他分区的指令总线访问完成的同时，让之前针对当前工作分区的指令所对应的数据访问都完成，然后再跳转到新的工作分区。等待时间需足够长，以确保之前针对当前工作分区的
15 指令所对应的数据访问都完成。以 ARM Cortex-M3 为例，等待时间可设置为 20 个 CPU 时钟周期。

第二部分：读保护级别的定义及使用方法。

在本申请的一种优选实施例中，所述 MCU 芯片可以包括闪存信息区，
20 所述闪存信息区可以包括选项字节；所述的方法还可以包括如下步骤：

步骤 S11，依据所述选项字节确定所述闪存用户区的读保护状态；

步骤 S12，若为零级读保护状态，则允许对所述闪存用户区进行读取、
写入和擦除；

步骤 S13，若为一级读保护状态，则允许对所述第一分区进行读取、
25 写入和擦除，仅在所述闪存用户区启动时允许对所述第二分区进行读取、
写入和擦除；

步骤 S14，若为二级读保护状态，则仅在所述闪存用户区启动时允许
对所述第一分区和第二分区进行读取、写入和擦除。

在本申请的一种优选实施例中，其特征在于，

在所述零级读保护状态下，所述选项字节允许修改；

在所述一级读保护状态下，所述选项字节允许修改，若基于所述选项字节从所述一级读保护状态修改为零级读保护状态，则所述闪存用户
5 区中的全部信息将被擦除（为确保闪存用户区的内容不被窃取，用户区内容擦除完毕之后，零级读保护才生效）。

在所述二级读保护状态下，所述选项字节禁止修改。

在具体实现中，读保护级别可以由闪存信息区中的若干字节来控制，
10 这些字节为选项字节。在本申请实施例中对于控制的方法随意，只要能区分不同的读保护级别并且方便读保护级别之间的切换即可。例如，用 1 个字节来控制，当该字节的值为 A5 时，读保护状态为零级；当该字节的值为 CC 时，读保护级别为二级；当该字节为除 A5 和 CC 之外的其他值时，读保护级别为一级。

在 MCU 芯片程序的开发过程中，读保护级别的使用方法可以为如下
15 所示。刚出厂的 MCU 芯片先交到第二公司，此时读保护级别为零级保护状态，闪存用户区是空的。第二公司将他们开发的程序烧写到闪存用户区的第二分区中。第二公司可以在零级读保护状态下调试程序。正式生产时，第二公司要在把芯片交给第一公司之前将读保护级别修改为一级读保护。第一公司将他们开发的程序烧写到闪存用户区的第一分区。此
20 时，闪存用户区的第一分区存有第一公司的程序，第二分区存有第二公司的程序，读保护级别为一级读保护。第一公司要在此状态下完成两家公司程序的联合调试。正式生产时，第一公司要在把芯片交给客户之前将读保护级别修改为二级读保护。

25 第三部分：私有设备的实现方法。

在本申请的一种优选实施例中，所述 MCU 芯片可以根据特定需求设计私有设备，仅在输出有第一分区使能信号时正常工作的私有设备为第一设备，以及，仅在输出有第二分区使能信号时正常工作的私有设备为

第二设备；所述方法还可以包括如下步骤：

步骤 S21，若处于所述第一分区工作状态，或者，第一分区过渡状态，则输出第一分区使能信号；

5 步骤 S22，若处于所述第二分区工作状态，或者，第二分区过渡状态，则输出第二分区使能信号。

在本申请实施例中，私有设备是通过闪存控制器输出的分区使能信号控制的设备。每个分区可以对应 1 比特分区使能信号。分区使能信号表示对应分区处于工作状态。第一分区使能信号在第一分区工作状态和第一分区过渡状态下为 1，其他状态下为 0；第二分区使能信号在第二分区工作状态和第二分区过渡状态下为 1，其他状态下为 0。控制的方法就是根据特定分区使能信号的状态，开启或关闭相应设备的部分或全部功能。

例如，若想让某私有 SRAM 只允许第一公司的程序读，可以用第一分区使能信号来作为 SRAM 读通路的使能信号；若想让某私有设备的运算结果寄存器只允许第二公司的程序读，可以用第二分区使能信号来选通结果寄存器的读通路；若想让某私有设备只允许第一公司的程序配置，可以用第一分区使能信号来作为设备寄存器的配置使能信号。

当然，在实际中也可以不设计私有设备。比如全部的设备可以为共享，本申请实施例对此不加以限制。

20 需要说明的是，对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请实施例并不受所描述的动作顺序的限制，因为依据本申请实施例，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本申请
25 实施例所必须的。

参照图 4，示出了本申请的一种 MCU 芯片的信息保护装置实施例的结构框图，所述 MCU 芯片可以包括指令总线、数据总线、闪存控制器和

闪存用户区。所述闪存控制器用于将闪存用户区划分为第一分区和第二分区；具体可以包括如下模块：

第一判断模块 201，配置为当所述指令总线访问所述闪存用户区时，判断所述指令总线是否访问所述第一分区；若是，则调用第一进入模块 202；

第一进入模块 202，配置为进入第一分区工作状态；在所述第一分区工作状态下，允许所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

在本申请的一种优选实施例中，所述第一分区位于闪存用户区的前半段地址空间，所述第二分区位于闪存用户区的后半段地址空间。

第二进入模块 203，配置为当处于所述第一分区工作状态下，所述指令总线访问所述第二分区，则进入过渡状态；在所述过渡状态下，暂停所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

第二判断模块 204，配置为判断处于所述过渡状态下的时间是否达到预设的等待时间；若是，则调用第三进入模块 205；

第三进入模块 205，配置为进入第二分区工作状态；在所述第二分区工作状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区，但允许所述数据总线访问所述第二分区。

在本申请的一种优选实施例中，所述 MCU 芯片包括 CPU，所述 CPU 为哈佛结构；所述预设的等待时间与 CPU 的特性相关；若所述 CPU 为 ARM Cortex-M3，则所述预设的等待时间为 20 个 CPU 时钟周期。

在本申请的一种优选实施例中，所述装置还可以包括如下模块：

第四进入模块，配置为在所述 MCU 芯片复位后，进入初始状态；在所述初始状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区和第二分区。

在本申请的一种优选实施例中，所述 MCU 芯片包括闪存信息区，所述闪存信息区包括选项字节；所述的装置还可以包括如下模块：

确定模块，配置为依据所述选项字节确定所述闪存用户区的读保护状态；

第一保护模块，配置为在为零级读保护状态时，允许对所述闪存用户区进行读取、写入和擦除；

- 5 第二保护模块，配置为在为一级读保护状态时，允许对所述第一分区进行读取、写入和擦除，仅在所述闪存用户区启动时允许对所述第二分区进行读取、写入和擦除；

第三保护模块，配置为在为二级读保护状态时，仅在所述闪存用户区启动时允许对所述第一分区和第二分区进行读取、写入和擦除。

- 10 在本申请的一种优选实施例中，

在所述零级读保护状态下，所述选项字节允许修改；

在所述一级读保护状态下，所述选项字节允许修改，若基于所述选项字节从所述一级读保护状态修改为零级读保护状态，则所述闪存用户区中的全部信息将被擦除；

- 15 在所述二级读保护状态下，所述选项字节禁止修改。

在本申请的一种优选实施例中，所述 MCU 芯片可以根据特定需求设计私有设备，仅在输出有第一分区使能信号时正常工作的私有设备为第一设备，以及，仅在输出有第二分区使能信号时正常工作的私有设备为第二设备；所述装置还包括：

- 20 第一输出模块，配置为在处于所述第一分区工作状态，或者，第一分区过渡状态时，输出第一分区使能信号；

第二输出模块，配置为在处于所述第二分区工作状态，或者，第二分区过渡状态时，输出第二分区使能信号。

- 25 在本申请的一种优选实施例中，所述外围设备可以包括静态随机存储器 SRAM。

对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

本申请实施例还提供了一种在其上记录有用于上述实施例的程序的计算机可读记录介质。

所述计算机可读记录介质包括用于以计算机（例如计算机）可读的形式存储或传送信息的任何机制。例如，机器可读介质包括只读存储器（ROM）、随机存取存储器（RAM）、磁盘存储介质、光存储介质、闪存存储介质、电、光、声或其他形式的传播信号（例如，载波、红外信号、数字信号等）等。

本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

本领域内的技术人员应明白，本申请实施例的实施例可提供为方法、装置、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

本申请实施例是参照根据本申请实施例的方法、终端设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在

流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

5 这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上，使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

10 尽管已描述了本申请实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请实施例范围的所有变更和修改。

15 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，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、物品或者终端设备不仅包括那些要素，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、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的
20 过程、方法、物品或者终端设备中还存在另外的相同要素。

以上对本申请所提供的一种 MCU 芯片的信息保护方法和一种 MCU 芯片的信息保护装置，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据
25 本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求 书

1、一种 MCU 芯片的信息保护方法，其特征在于，所述 MCU 芯片包括指令总线、数据总线、闪存控制器和闪存用户区；所述闪存控制器用于将闪存用户区划分为第一分区和第二分区；所述的方法包括：

5 当所述指令总线访问所述闪存用户区时，判断所述指令总线是否访问所述第一分区；

若是，则进入第一分区工作状态；在所述第一分区工作状态下，允许所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

10 当处于所述第一分区工作状态下，所述指令总线访问所述第二分区，则进入过渡状态；在所述过渡状态下，暂停所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

判断处于所述过渡状态下的时间是否达到预设的等待时间；

15 若是，则进入第二分区工作状态；在所述第二分区工作状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区，但允许所述数据总线访问所述第二分区。

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：

20 在所述 MCU 芯片复位后，进入初始状态；在所述初始状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区和第二分区。

3、根据权利要求 1 所述的方法，其特征在于，所述 MCU 芯片包括 CPU，所述 CPU 为哈佛结构；所述预设的等待时间与 CPU 的特性相关；若所述 CPU 为 ARM Cortex-M3，则所述预设的等待时间为 20 个 CPU 时钟周期。

25 4、根据权利要求 1 所述的方法，其特征在于，所述 MCU 芯片包括闪存信息区，所述闪存信息区包括选项字节；所述的方法还包括：

依据所述选项字节确定所述闪存用户区的读保护状态；

若为零级读保护状态，则允许对所述闪存用户区进行读取、写入和

擦除；

若为一级读保护状态，则允许对所述第一分区进行读取、写入和擦除，仅在所述闪存用户区启动时允许对所述第二分区进行读取、写入和擦除；

- 5 若为二级读保护状态，则仅在所述闪存用户区启动时允许对所述第一分区和第二分区进行读取、写入和擦除。

5、根据权利要求4所述的方法，其特征在于，

在所述零级读保护状态下，所述选项字节允许修改；

- 10 在所述一级读保护状态下，所述选项字节允许修改，若基于所述选项字节从所述一级读保护状态修改为零级读保护状态，则所述闪存用户区中的全部信息将被擦除；

在所述二级读保护状态下，所述选项字节禁止修改。

- 15 6、根据权利要求1所述的方法，其特征在于，所述MCU芯片设计有私有设备，仅在输出有第一分区使能信号时正常工作的私有设备为第一设备，以及，仅在输出有第二分区使能信号时正常工作的私有设备为第二设备；所述方法还包括：

若处于所述第一分区工作状态，或者，第一分区过渡状态，则输出第一分区使能信号；若处于所述第二分区工作状态，或者，第二分区过渡状态，则输出第二分区使能信号。

- 20 7、根据权利要求6所述的方法，其特征在于，所述设备包括静态随机存储器SRAM。

8、根据权利要求1所述的方法，其特征在于，所述第一分区位于闪存用户区的前半段地址空间，所述第二分区位于闪存用户区的后半段地址空间。

25

9、一种MCU芯片的信息保护装置，其特征在于，所述MCU芯片包括指令总线、数据总线、闪存控制器和闪存用户区；所述闪存控制器用于将闪存用户区划分为第一分区和第二分区；所述的装置包括：

第一判断模块，配置为当所述指令总线访问所述闪存用户区时，判断所述指令总线是否访问所述第一分区；若是，则调用第一进入模块；

第一进入模块，配置为进入第一分区工作状态；在所述第一分区工作状态下，允许所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

第二进入模块，配置为当处于所述第一分区工作状态下，所述指令总线访问所述第二分区，则进入过渡状态；在所述过渡状态下，暂停所述指令总线访问所述闪存用户区，允许所述数据总线访问所述第一分区，但禁止所述数据总线访问所述第二分区；

第二判断模块，配置为判断处于所述过渡状态下的时间是否达到预设的等待时间；若是，则调用第三进入模块；

第三进入模块，配置为进入第二分区工作状态；在所述第二分区工作状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区，但允许所述数据总线访问所述第二分区。

10、根据权利要求 9 所述的装置，其特征在于，所述装置还包括：

第四进入模块，配置为在所述 MCU 芯片复位后，进入初始状态；在所述初始状态下，允许所述指令总线访问所述闪存用户区，禁止所述数据总线访问所述第一分区和第二分区。

11、根据权利要求 9 所述的装置，其特征在于，所述 MCU 芯片包括闪存信息区，所述闪存信息区包括选项字节；所述的装置还包括：

确定模块，配置为依据所述选项字节确定所述闪存用户区的读保护状态；

第一保护模块，配置为在为零级读保护状态时，允许对所述闪存用户区进行读取、写入和擦除；

第二保护模块，配置为在为一级读保护状态时，允许对所述第一分区进行读取、写入和擦除，仅在所述闪存用户区启动时允许对所述第二分区进行读取、写入和擦除；

第三保护模块，配置为在为二级读保护状态时，仅在所述闪存用户

区启动时允许对所述第一分区和第二分区进行读取、写入和擦除。

12、根据权利要求 11 所述的装置，其特征在于，

在所述零级读保护状态下，所述选项字节允许修改；

5 在所述一级读保护状态下，所述选项字节允许修改，若基于所述选项字节从所述一级读保护状态修改为零级读保护状态，则所述闪存用户区中的全部信息将被擦除；

在所述二级读保护状态下，所述选项字节禁止修改。

13、根据权利要求 9 所述的装置，其特征在于，所述 MCU 芯片设计有私有设备，仅在输出有第一分区使能信号有效时正常工作的私有设备
10 为第一设备，以及，仅在输出有第二分区使能信号有效时正常工作的私有设备为第二设备；所述装置还包括：

第一输出模块，配置为在处于所述第一分区工作状态，或者，第一分区过渡状态时，输出第一分区使能信号；

15 第二输出模块，配置为在处于所述第二分区工作状态，或者，第二分区过渡状态时，输出第二分区使能信号。

14、一种在其上记录有用于执行权利要求 1 所述方法的程序的计算机可读记录介质。

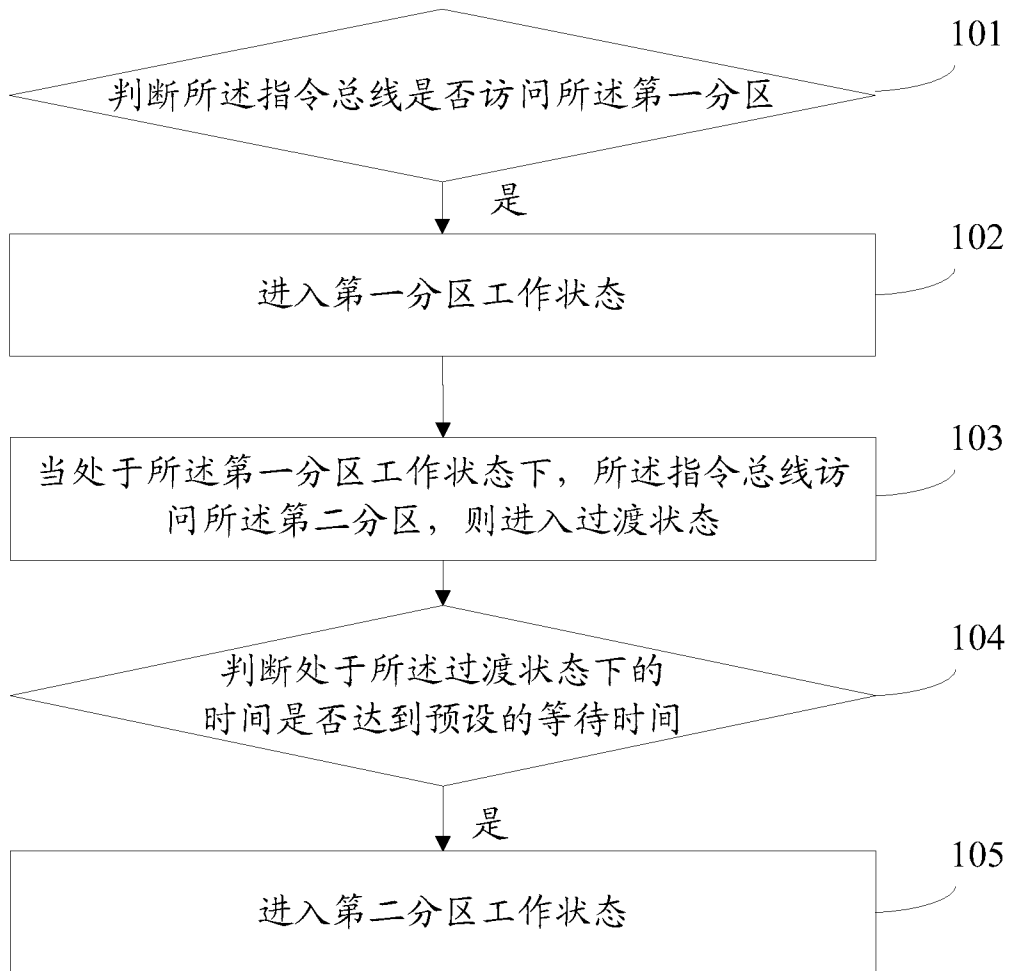


图 1

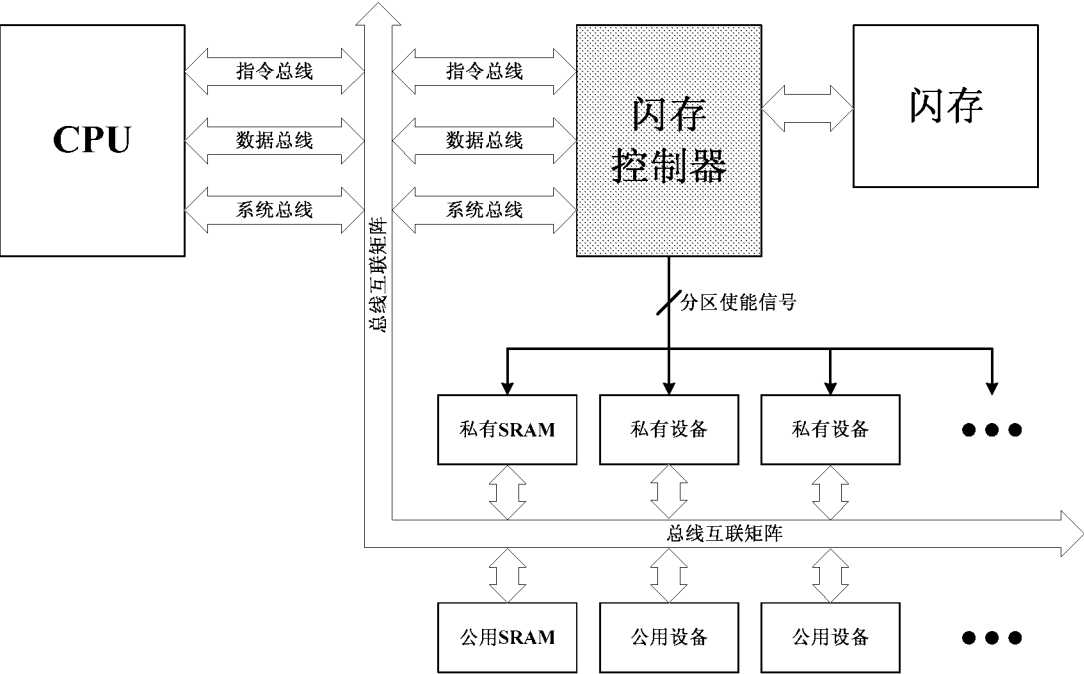


图 2

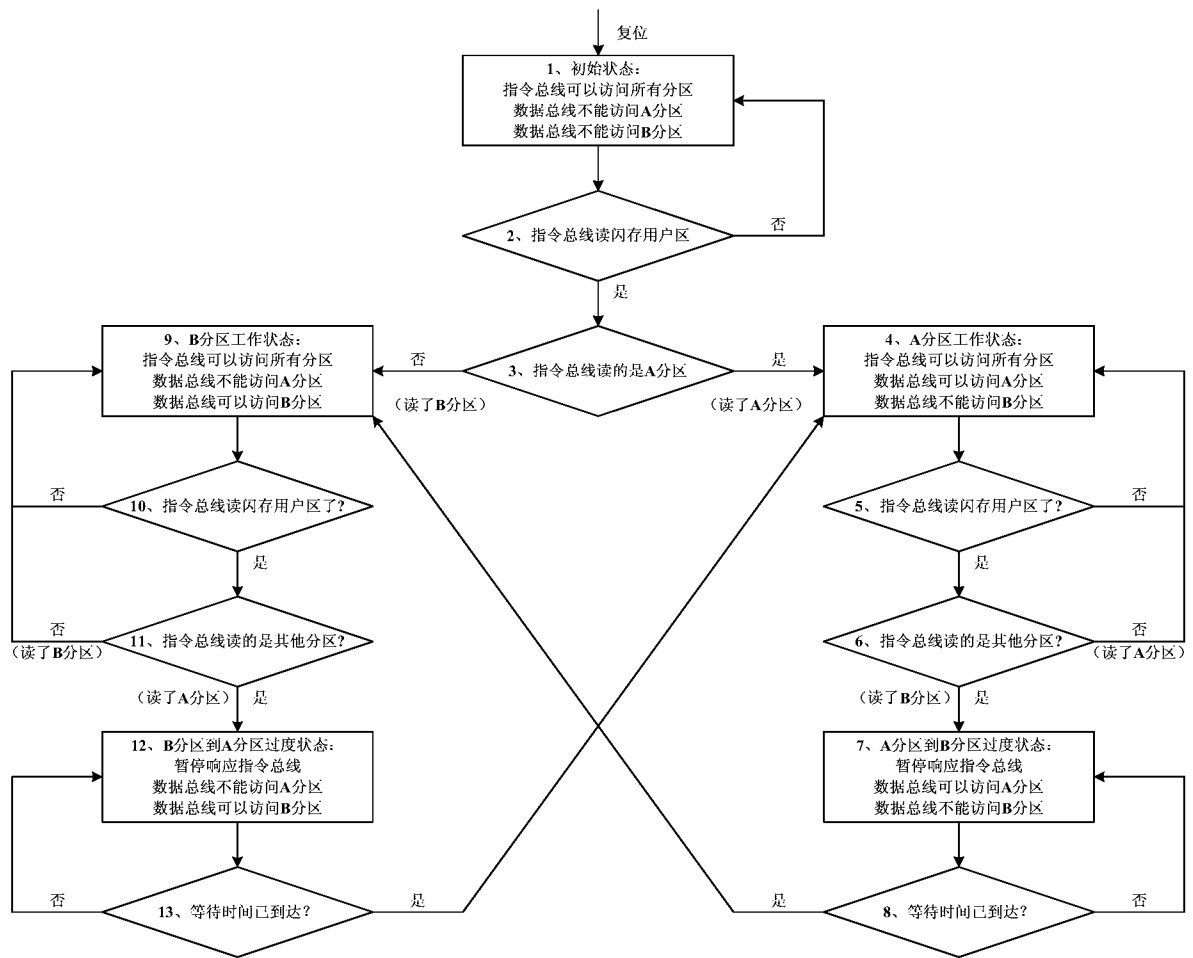


图 3

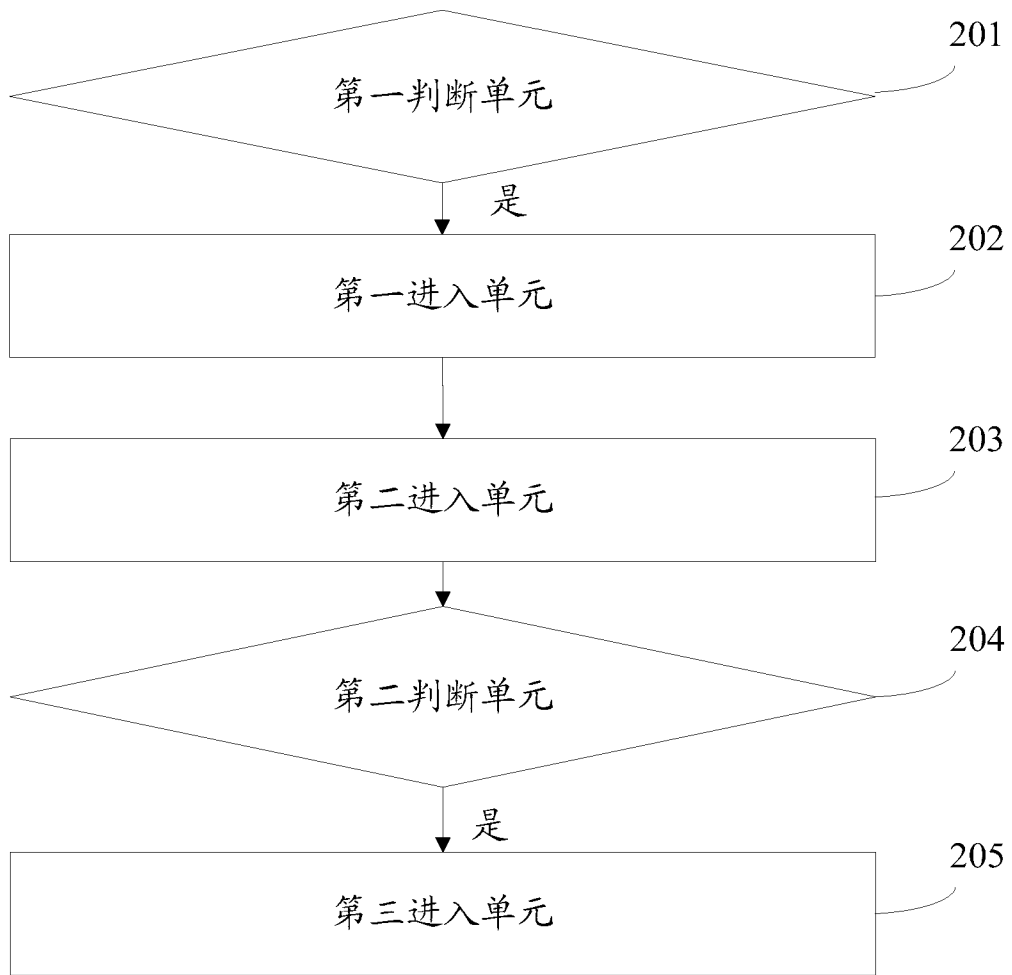


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/071556

A. CLASSIFICATION OF SUBJECT MATTER

G06F 12/14 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, WPI, CNPAT, USTXT, CNKI, IEEE: partition, flash memory, prevent, forbid+, user, access+, area, block, region, two, second, flash, sequen+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101566972 A (C*CORE TECHNOLOGY (SUZHOU) CO., LTD.), 28 October 2009 (28.10.2009), description, page 4, line 5 to page 6, line 1, and claims 1-2	1-14
A	CN 1595517 A (XI'AN SAMING TECHNOLOGY CO., LTD.), 16 March 2005 (16.03.2005), the whole document	1-14
A	CN 103229157 A (ADVANCED MICRO DEVICES, INC.), 31 July 2013 (31.07.2013), the whole document	1-14
A	CN 101315608 A (SAMSUNG ELECTRONICS CO., LTD.), 03 December 2008 (03.12.2008), the whole document	1-14
A	CN 1196524 A (NEC CORP.), 21 October 1998 (21.10.1998), the whole document	1-14
A	CN 1604791 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.), 06 April 2005 (06.04.2005), the whole document	1-14
A	US 2007136576 A1 (CHAMBERS, MICHAEL JOSEPH et al.), 14 June 2007 (14.06.2007), the whole document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 09 April 2015 (09.04.2015)	Date of mailing of the international search report 29 May 2015 (29.05.2015)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer WANG, Xun Telephone No.: (86-10) 62413643

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/071556

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101566972 A	28 October 2009	CN 101566972 B	08 December 2010
CN 1595517 A	16 March 2005	None	
CN 103229157 A	31 July 2013	US 2012144104 A1	07 June 2012
		WO 2012074998 A1	07 June 2012
		EP 2646925 A1	09 October 2013
		KR 20140071270 A	11 June 2014
		JP 2013545201 A	19 December 2013
CN 101315608 A	03 December 2008	KR 20080104591 A	03 December 2008
		US 2008301389 A1	04 December 2008
CN 1196524 A	21 October 1998	US 6101586 A	08 August 2000
		JPH 10228421 A	25 August 1998
		EP 0859319 A1	19 August 1998
		CN 1145885 C	14 April 2004
		KR 19980071365 A	26 October 1998
		KR 100319677 B	08 March 2002
CN 1604791 A	06 April 2005	CN 1284088 C	08 November 2006
		WO 03013586 B1	19 February 2004
		WO 03013586 A8	13 November 2003
		US 2003028639 A1	06 February 2003
		KR 20040019328 A	05 March 2004
		WO 03013586 A1	20 February 2003
		EP 1413116 A1	28 April 2004
		JP 2003122635 A	25 April 2003
		JP 4280036 B2	17 June 2009
US 2007136576 A1	14 June 2007	WO 2007067221 A2	14 June 2007
		WO 2007067221 A3	17 April 2008
		CN 101268650 A	17 September 2008
		JP 2009518742 A	07 May 2009
		KR 20080074848 A	13 August 2008
		GB 2443984 A	21 May 2008
		CN 103824032 A	28 May 2014
		US 7657754 B2	02 February 2010
		KR 101224322 B1	18 January 2013
		GB 0802864 D0	26 March 2008
		GB 2443984 B	27 October 2010
		JP 2013232219 A	14 November 2013

国际检索报告

国际申请号

PCT/CN2015/071556

A. 主题的分类

G06F 12/14(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

EPDOC, WPI, CNPAT, USTXT, CNKI, IEEE: 禁, 用户, 访问, 分区, 块, 两, 二, 闪存, 顺序, prevent, forbid+, user, access+, area, block, region, two, second, flash, sequen+

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 101566972 A (苏州国芯科技有限公司) 2009年 10月 28日 (2009 - 10 - 28) 说明书第4页第5行-说明书第6页第1行, 权利要求1-2	1-14
A	CN 1595517 A (西安三茗科技有限责任公司) 2005年 3月 16日 (2005 - 03 - 16) 全文	1-14
A	CN 103229157 A (超威半导体公司) 2013年 7月 31日 (2013 - 07 - 31) 全文	1-14
A	CN 101315608 A (三星电子株式会社) 2008年 12月 3日 (2008 - 12 - 03) 全文	1-14
A	CN 1196524 A (日本电气株式会社) 1998年 10月 21日 (1998 - 10 - 21) 全文	1-14
A	CN 1604791 A (松下电器产业株式会社) 2005年 4月 6日 (2005 - 04 - 06) 全文	1-14
A	US 2007136576 A1 (CHAMBERS, MICHAEL JOSEPH 等) 2007年 6月 14日 (2007 - 06 - 14) 全文	1-14

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2015年 4月 9日

国际检索报告邮寄日期

2015年 5月 29日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10)62019451

授权官员

王迅

电话号码 (86-10)62413643

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/071556

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101566972	A	2009年 10月 28日	CN	101566972	B	2010年 12月 8日
CN	1595517	A	2005年 3月 16日	无			
CN	103229157	A	2013年 7月 31日	US	2012144104	A1	2012年 6月 7日
				WO	2012074998	A1	2012年 6月 7日
				EP	2646925	A1	2013年 10月 9日
				KR	20140071270	A	2014年 6月 11日
				JP	2013545201	A	2013年 12月 19日
CN	101315608	A	2008年 12月 3日	KR	20080104591	A	2008年 12月 3日
				US	2008301389	A1	2008年 12月 4日
CN	1196524	A	1998年 10月 21日	US	6101586	A	2000年 8月 8日
				JP	H10228421	A	1998年 8月 25日
				EP	0859319	A1	1998年 8月 19日
				CN	1145885	C	2004年 4月 14日
				KR	19980071365	A	1998年 10月 26日
				KR	100319677	B	2002年 3月 8日
CN	1604791	A	2005年 4月 6日	CN	1284088	C	2006年 11月 8日
				WO	03013586	B1	2004年 2月 19日
				WO	03013586	A8	2003年 11月 13日
				US	2003028639	A1	2003年 2月 6日
				KR	20040019328	A	2004年 3月 5日
				WO	03013586	A1	2003年 2月 20日
				EP	1413116	A1	2004年 4月 28日
				JP	2003122635	A	2003年 4月 25日
				JP	4280036	B2	2009年 6月 17日
US	2007136576	A1	2007年 6月 14日	WO	2007067221	A2	2007年 6月 14日
				WO	2007067221	A3	2008年 4月 17日
				CN	101268650	A	2008年 9月 17日
				JP	2009518742	A	2009年 5月 7日
				KR	20080074848	A	2008年 8月 13日
				GB	2443984	A	2008年 5月 21日
				CN	103824032	A	2014年 5月 28日
				US	7657754	B2	2010年 2月 2日
				KR	101224322	B1	2013年 1月 18日
				GB	0802864	D0	2008年 3月 26日
				GB	2443984	B	2010年 10月 27日
				JP	2013232219	A	2013年 11月 14日

表 PCT/ISA/210 (同族专利附件) (2009年7月)