



[12] 发明专利申请公开说明书

[21] 申请号 02802339.0

[43] 公开日 2003 年 12 月 31 日

[11] 公开号 CN 1465002A

[22] 申请日 2002.7.6 [21] 申请号 02802339.0

[30] 优先权

[32] 2001.7.10 [33] EP [31] 01116594.1

[86] 国际申请 PCT/EP02/07548 2002.7.6

[87] 国际公布 WO03/007132 德 2003.1.23

[85] 进入国家阶段日期 2003.3.7

[71] 申请人 迈克纳斯公司

地址 德国弗赖堡

[72] 发明人 彼得·穆勒 佐拉恩·迈卓维克
曼弗雷德·朱克 乔奇姆·里特
斯蒂芬·齐默尔曼[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

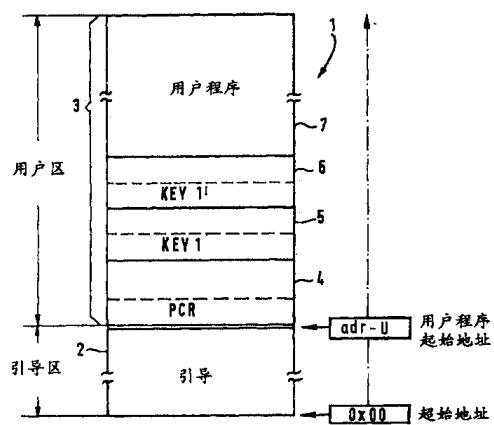
代理人 付建军

权利要求书 3 页 说明书 10 页 附图 4 页

[54] 发明名称 处理器中带数据安全的存储器设备

[57] 摘要

公开了处理器(10)中使用的存储器设备(1)。存储器设备(1)和处理器(10)集成在一块芯片上，存储器设备(1)包括初始化程序使用的第一存储器部分(2)和用于用户程序的第二存储器部分(3)。经过第一组数据接口(16、18)，能对第一存储器部分(2)进行读写，经过第二组数据接口(16、17、18)，能对第二存储器部分(3)进行读写。第一和/或第二存储器部分(2、3)包括可逐块寻址的存储器块(4、5、6、7)。第一存储器块(4)含有一个保护控制寄存器(PCR)，PCR 中含有各个数据接口的可编程的启用或禁用信息。在加电时对保护控制寄存器(PCR)进行查询。第二存储器和第三存储器块(5、6)用于保存口令字(Key 1, Key 1')，该口令字与存储器设备(1)中的加密和识别程序相关。



1. 处理器（10）所使用的存储器设备（1）集成在一块芯片上，处理器设备（1）包括第一存储器部分（2），例如初始化或引导程序所使用的存储器部分，和第二存储器部分（3），例如，用户程序所使用的存储器部分；

- 经过第一组接口（16、17、18），能对第一存储器部分（2）进行写和/或读，经过第二组数据接口（16、17、18），能对存储器器第二部分（3）进行写或读；

- 第一和/或第二存储器部分（2、3）含有可逐块寻址的存储器块（4、5、6、7）；

- 第一存储器块（4）包括一个保护控制寄存器 PCR，含有对第一组和第二组数据接口（16、18；16、17、18）的可编程启用和/或禁用信息；并且

- 在初始化程序允许查询或编程之前，先进行保护控制寄存器（PCR）查询。

2. 如权利要求 1 中所述的存储器设备，其特征在于，第一组数据接口包括独立于处理器（10）的数据接口（16、18）。

3. 如权利要求 2 中所述的存储器设备（1），其特征在于，第二组数据接口包括独立于处理器（10）的数据接口（16、18）和由处理器控制的数据接口（17）。

4. 如权利要求 1 到 3 中的任一个所述的存储器设备（1），其特征在于，第二和第三存储器块（5、6）用于保存一个口令字（Key 1, Key 1'），该口令字与第一和/或第二存储器部分（2、3）中的解密和/或加密程序相联系。

5. 如权利要求 4 中所述的存储器设备（1），其特征在于，假设在保护控制寄存器 PCR 中没有设定相关的禁用信息，那么经过第二组数据接口（16、17、18），只有使用口令字（Key 1, key 1'）进行识别的授权访问和包含在第一和/或第二存储器部分（2、3）中的初始化程序、

通过程序取消。

14. 如权利要求 1~13 的任一个中所述的存储器设备 (1)，其特征在于，通过电路装置，可编程保护位 (已设定保护位) 防止存储器设备 (1) 的任何意外擦除，该可编程保护位插在用户程序中。

解密和/或加密程序，才可能对第二存储器部分（3）进行读和/写，例如，在程序更新的范围内。

6. 如权利要求5中所述的存储器设备（1），其特征在于，使用保护控制寄存器（PCR）中设置的禁用信息，经过第一组数据接口（16、18）对第一存储器部分（2）进行写和/或读是不可能的，即使访问是授权的。

7. 如权利要求1~6中所述的存储器设备（1），其特征在于，如果发生至少引起第二存储器部分（3）中的用户程序改变或擦除的退出或加电失败时，处理器（10）进入一个等待状态。

8. 如权利要求7中所述的存储器设备（1），其特征在于，启动信息结束等待状态，而启动信息启动以起始地址（adr-U）开始的用户程序的更新。

9. 如权利要求1~8的任一个中所述的存储器设备（1），其特征在于，通过使用全局擦除信息，第一和第二存储器部分（2、3）是可擦除的。

10. 如权利要求9中所述的存储器设备（1），其特征在于，通过在事先指定的处理器（10）的终端进行预先指定的级别配置，可以初始化全局擦除信息。

11. 如权利要求10中所述的存储器设备（1），其特征在于，在处理器（10）的内置条件下，预先指定的终端是不可访问的，尤其是经过一块母板。

12. 如权利要求1~11的任一个中所述的存储器设备（1），其特征在于，在发生程序更新时，如果新的程序也包括对各个数据接口（16、17、18）的禁用信息，则在任何时间段内，不擦除已经存在于保护控制寄存器（PCR）中的禁用信息，而是在保护寄存器中保持不变。

13. 如权利要求1~12的任一个中所述的存储器设备（1），其特征在于，在初始化程序中，通过保护控制寄存器查询，启动对相关的数据接口（16、17、18）的禁用，经过内部控制信号（25、26、27）实现，这些内部控制信号既不能直接取消，也不能间接取消，也不能

处理器中带数据安全的存储器设备

本发明涉及处理器上一种带数据安全的存储器设备。通过防止对相应的存储器设备中的加密程序和口令字的访问，本发明支持使用公钥、私钥或口令字的传统加密技术的保护功能。这些敏感的数据包含在处理器芯片上的随机存取存储器中，例如，一种电可写和可读快擦写存储器。这样带来的优点是，不能直接读出随机存储器的内容，而只能间接地通过数据接口。有名的外部可访问数据接口包括一些标准数据接口，例如，联合测试行动小组 JTAG(Joint Test Action Group)、通用异步接收发射器 UART(Universal Asynchronous Receiver/Transmitter)或通用串行总线 USB(Universal Serial Bus)，它们都允许串行访问。正如在 USB 的情形下，有的接口的功能必须由处理器中的特定的程序支持，而有的接口从外部进行控制，与处理器完全独立。如果有必要，则可以通过其他一些数据接口，获得快速的并行访问，这些接口可能与处理器相关，也可能独立，可能是标准的，也可能是非标准的。作为一个规则，对于这样的并行接口，要对大量的终端功能进行切换，例如，以便 32 位的数据和地址能够并行地输入或输出。

如果终端用户或第三方在未经允许的情况下想获得加密过程的内容，一般来说，会访问到已加密的数据内容。这些数据可能是保存的或传输的数据。一个例子是，在未经授权的情况下，对采用 MP3 压缩技术的收费乐曲进行传播和复制。对数据加密可以防止这一点，但必须对个体的或全局的加密程序进行保密。如果对数据的解密有很大兴趣，则必须假定，通过互连网或其他渠道，辅助程序传播迅速，并使得加密无效。

本发明的一个目的是，为保存在处理器上的数据连同加密或解密程序提供保护。尤其是，保护加密或解密程序，防止未经授权的读取、

改变或擦除。但是，对于授权的终端用户，可以在任何时候进行程序更新。保护的级别是由用户预先专门指定的，而不是由处理器的生产商指定。在下面的正文中，为了语言的简练，将加密和解密合在一起，共同使用一个术语“加密”来表示。

这里，术语“用户”指的是一个人，他以组件的形式，从半导体生产商购买处理器，安装到有特定用途的电路中，生产出一种设备或装置。最后，设备或装置经购买后，由终端用户直接投入使用，或作为另一个设备或装置的一部分。

通过权利要求1中所要求的特征来实现该目的。其他的优点和研制结果将在相关的权利要求中描述。

本发明的基本思想基于这样一个事实，即需要保护的存储器设备集成在微处理器上，由具有不同可访问性的第一存储器部分和第二存储器部分组成。将存储器设备集成在芯片上，允许组合使用硬件和软件保护性措施，而对分离的存储器设备则不能。第一存储器部分有一个初始化程序，在解密过程中也作为一个引导程序，第二存储器部分有一个用户程序，例如，对接收到的数据进行解密和/或解码的程序。这些数据可能是，例如，根据MP3标准编码的音频数据，为了防止未授权接收，而另外采用公共或秘密口令字进行加密。解密程序可能是相同的，在引导区有相当安全的解密程序，或者组成第二存储器部分中的用户程序的一部分。

经过一个或数个外部接口，第一存储器部分是可编程的或可修改的，但不能经过处理器或由处理器控制的数据接口。这样，就不能经由一些程序而引起处理器读取、改变或毁坏初始化程序的内容，这些程序包含至少部分加密、解密或身份识别程序。第一存储器部分包含的基本功能总是足以对第二存储器部分中已改变或已毁坏的用户程序重新加载。第二存储器部分是可编程和可修改的，既可以通过外部数据接口，也可以通过处理器和由处理器控制的数据接口。

无论在正常操作过程中，还是当用户为终端用户提供程序更新时，处理器都不可避免要对第一存储器部分和第二存储器部分进行访问。

这样的程序更新有必要按预先指定期限进行，例如，改变单个的或成组相关联的加密程序或口令字，以便减少任何因加密方法意外或非法泄露引起的负面作用。然而，根据本发明，不进行程序更新也能够进行禁用。那样，通过设定禁用位，用户禁用所有的外部接口，换句话说，包括由处理器控制的那些接口。这样，正象上面提到的那样，处理器也总是根据正常的操作顺序访问存储器的两个部分。

本发明非常灵活，能够适应不同用户的不同保护要求，允许用户和专业人士使用。可以想到的一个用户应用是，例如，视频或音频数据的加密传输。通过本发明，只有授权的持执照者能通过处理器，为了处理器随后进行的操作或复制，对数据进行解密，但他或她不能将解密后的数据复制给第三方，因为这些数据不能通过任何外部可访问接口得到。与之相似的情形是，摩托车上的引擎由一个电子引擎管理系统控制，而其保密程序要防止被复制或修改。

授权或身份检查是通过受保护的加密程序进行的，利用保存在存储器的第一或第二部分中的公开或非公开的关键字和以加密形式获得的程序，以一种公开的方式进行交互。只有所有部分都吻合，才可能进行解密，进而对接收到的数据的使用才有意义，或更新保存的程序。

第二存储器部分，如果有必要的话，和第一存储器部分分成不同的存储器块，这样在程序更新时，就能够逐块进行修改或擦除，进而避免新旧程序之间的冲突。

在第一存储器部分或第二存储器部分中的第一存储器块中包含一个保护控制寄存器，含有针对每一个数据接口的可编程的启用和禁用信息，对第一存储器部分和第二存储器部分经由该数据接口的读出/写入进行启用或禁用。只要还没有启动禁用信息，就可以经由所有的外部数据接口，包括由处理器控制的接口，对第一和第二存储器部分进行访问。这样就允许生产商或用户对初始化或用户程序进行修改、调整或调试。在完成这些修改后，如果用户设定了外部可访问数据接口的禁用位，作为一个规则，在不毁坏已有的程序的情况下，任何人不能进行取消。这样，就能可靠地保护具有禁用信息的第一存储器块，

防止任何修改。通过已有的软件或保存的口令字，用户将自己识别为授权用户，就能够改变保护控制寄存器中的内容，也就是说，他们能够取消禁用。这样就允许用户在必要的情况下，对实际已禁用的处理器进行错误搜索。

对保护控制寄存器的查询最好一加电就进行，在初始化程序允许其他请求或编程操作之前，通过处理器的一个硬件实现的功能来完成。这些用于查询的硬件设计，对保护是很重要的，其优点是，任何程序无论是有意的，还是无意的，他们都是不可修改的。当然，有一点也是肯定的，即当电源接通或断开时，即使时间很短，也不能忽略对保护控制寄存器的查询。

第一存储器部分或第二存储器部分中的第二存储器块和第三存储器块用于对公开或保密的关键字进行双重保存。关键字也称作“口令字”，与第一存储器部分或第二存储器部分中的加密程序相联系。无论用户喜欢的保护用的是公开可访问的，还是不可公开访问的，也就是说，是不公开的，还是保密的关键字，对于本发明来说，都是不重要的，而只决定于所要的保护。本发明并没有改变两种系统的优点和不足，但在两种情形下，对受保护数据内容的访问是禁用的，或者说，至少更困难一些。

第二存储器部分中的第四存储器块相对较大，用于保存用户程序。作为一个规则，在程序更新事件中，将取代这个程序。用户程序的内容连同口令字允许处理器对接收到的数据进行解密和解码。当然，防止未授权访问，不仅可用于解密端，还可用于加密端。

参照提供的一些附图，现在更加详细地解释本发明和一些有用的研制成果，在这些附图中：

图1 表示集成在处理器芯片上的存储器单元的分区情况；

图2 表示一个带有接口存储器位置的保护控制寄存器；

图3 表示一个初始化顺序流程图；

图4 表示一个程序更新流程图；

图5 表示一个作为本发明的实施例的处理器。

图 1 表示装在处理器 10 (参照图 5) 上的存储器设备 1 的分区情况。第一存储器部分 2, 开始地址为 0x00, 有一个初始化程序, 该程序也称为“引导程序”。对于程序设计来说, 第一存储器部分 2 只为用户和生产商提供有限访问, 即只能通过这些独立于处理器操作的数据接口。在生产过程中, 为了加载初始化程序, 经由相应的不可访问的芯片连接, 有可能对第一存储器部分进行强制访问。

当处理器接通时, 启动了初始化程序。它也包括一些程序, 对用户或终端用户的真实性或身份进行检查, 并支持对处理器控制的数据接口的读写操作。初始化程序还至少包括解密程序的一部分, 它们对第二存储器部分的再编程是必要的, 这需要在处理器的帮助下, 而且是在这一存储器部分是空的或故障时, 例如, 一个方法是经由处理器控制的数据接口输入加密了的新程序。

在第一存储器部分 2 的后面是第二存储器部分 3 (用户区), 包含有用户程序, 其地址分配到存储器块, 以用户开始地址 adr-u 开始。第一存储器块 4 包含一个保护控制寄存器 PCR, PCR 中含有对各个数据接口的启用或禁用信息。在第一存储器块 4 中, 为了保存更多数据, 可增加一些空间。

第一存储器块 4 的后面是第二存储器块 5 及第三存储器块 6, 它们必须各自都含有口令字 “Key 1” 和 “Key 1'”, 分配到终端用户或终端用户组。这两个口令字是相同的, 必须分开放在可擦除区中, 以便在再编程时至少保证有一个口令字有效。如果没有口令字, 是不可能对接收到的数据解密的。在再编程过程中, 对处于不同控制区的第二存储器块 5 和第三存储器块 6 中的原有的口令字用新的口令字代替。第二存储器块 5 和第三存储器块 6 足够大, 如果有必要, 它们可以为其他加密程序保存更多的口令字。

用户程序本身放在第四存储器块 7 中。存储器块足够大, 能够保存当前和以后的用户程序。不同的访问级别以及对第一存储器部分 2 和第二存储器部分 3 的最终要求的禁用, 由使用块地址的硬件控制。例如, 处理器的编程信号在逻辑上与第一存储器部分 2 的区信号相结

合，方法是，不形成对存储器设备 1 的全局启用信号或存储器块启用信号。然而，如果第一存储器部分 2 编址时与一个数据接口相连，而该数据接口独立于处理器，那么，如果不设定寄存器 PCR 的相关禁用信号，就不能消除全局的或存储器块启用信号。以一种类似的方式，通过将块地址或地址范围信号与存储器设备 1 及相关的数据接口的读或写信号相结合，从而控制第二存储器部分 3 中的块 4 到块 7。在图 1 中的实施例中，存储器块 4、5、6 与第二存储器部分 3 相关联。以这样的方式，保护装置就获得了最大的灵活性，因为通过再编程(更新)，就可以改变访问授权或口令字。如果保护控制寄存器 PCR 或口令字 Key 1 和 Key 1' 使用的寄存器 5 和寄存器 6 在第一存储器部分 2 中，就不能经过处理器进行再编程，已设计的数据就将访问授权和口令字永久固定。因为对外部可访问数据接口的电子禁用不允许对数据的读取。

图 2 表示了在第一存储器块 4 中的保护控制寄存器 PCR。对于每一个数据接口，保护控制寄存器有一个位置，保存值“1”或“0”。值“1”表示，经过相关的数据接口，可以对存储器设备 1 进行读写。当然，这个启用状态不会使预先指定访问可能性无效，例如，经过由处理器控制的数据接口，永远不能访问第一存储器部分 2。选择“1”，取决于用于存储器设备 1 的有关技术。在快擦写存储器中，在擦除后，所有单元的状态都为“1”，所以对于这种存储器类型，必须选逻辑状态 #1# 为启用信号。相应地，#0# 则代表禁用读写或擦除操作的信号。当加电时，经触发后，寄存器内容中的每一位相应设置为状态“1”或“0”。或许，经过永久相连的输出读取线，PCR 寄存器已经用作一个状态寄存器使用。在操作过程中，只能通过改变保护控制寄存器的内容或通过关机，才能改变这样的状态寄存器的内容。处于加电状态的状态寄存器内容，只能从状态“1”变到状态“0”，并且取决于 PCR 寄存器的内容。其他方向上的改变是不可能的，因为经过外部可访问数据接口，禁用信号“0”禁用了对保护控制寄存器 PCR 的访问。

图 3 中的流程图表示了加电时所发生的事件。加电启动了对保护控制寄存器中的各个位置的查询。例如，这里假设为芯片上的快速存储器，逻辑“1”状态对应于“启用”，逻辑“0”状态对应于“禁用”。图 3 中以三种外部可访问数据接口为例：一个 JTAG 接口、一个并行接口和一个测试接口。如果各接口是启用的，分别是用一个功能框来标记的，那么，就能经过这个接口，读取或改变存储器设备 1 的数据。通过在引导区启动一个到起始地址 0x00 的跳转，结束了读或写操作。然而，如果是在加电后从 PCR 寄存器中读出禁用信息，立即发生到引导开始地址 0x00 的跳转，将不能够经过接口对存储器设备 1 的任何部分进行读或写。以这种方式，就不能忽略 PCR 寄存器的禁用信息，因为硬件控制的查询是在第一系统时钟周期，一加电，就作为第一步立即发生的。相比之下，程序从引导存储器地址 0x00 开始，代表的是纯软件操作。

下一步，程序从引导开始地址 0x00 开始，启动了是否加载新的用户程序的请求，例如，程序更新。这愿望可以通过信号来指示，例如，手动操作一个输入键（更新键）。如果是这样设计的（设置了键），则将启动一个编程模式，在图 4 中的流程图将更加详细地解释。

如果没有设计程序更新，则将进行一次检查，检查在第二存储器部分中是否包含有一个完整而有效的用户程序。如果检查的结果是否定的，因为用户程序不完整，则将启动一个等待状态，当前的程序将被中断。如果用户程序是完整而有效的，将启动一个到用户程序起始地址 adr-U 的跳转。这样，保留了含有初始化程序（引导程序）的第一存储器部分 2。处理器 10（参照图 5）现在已作好解密和解码的准备，并在内部对接收到的数据进行处理。然而，正如前面所提到的，不能够通过外部可访问接口传输已解密的数据。

在更新键请求之后，通过在“否”分支中插入一个可编程保护位（已设定保护位），能提供防止由于不小心而擦除整个存储器设备 1 的进一步保护，因为这时用户程序还在初始化程序段中。在用户程序的编程过程当中，可设定保护位，防止存储器设备 1 被全部或部份擦

除，而这是当前执行程序修改或出错的结果。只有在关掉设备，且通过更新键来给出信号以表示输入新的用户程序，才能忽略保护位。在这种情况下，是否已设定保护位，要由用户判断，由该用户编制和传播新的用户程序。

图 4 的流程图表示在用户程序的更新操作过程中发生的事件的顺序，而这是由编程模式来初始化的。首先，要做一个身份识别检查。如果这一检查的结果是否定的，编程模式将立即中断，且启动和指示一个等待状态。如果身份识别成功，在下一步，将删除含有关键字“Key 1”的第三存储器块 6。紧接着，查询保护控制寄存器 PCR 是否含有一个禁用位“0”和新内容是否也是一个禁用位，如果情况不是这样，将擦除 PCR 寄存器。初看起来，这个查询有一些奇怪，但却有下列用途。首先，明确的是，必须改变保护控制寄存器 PCR 的内容，或保持启用状态。在这些情形下，在加载新的程序之前，可以擦除 PCR。然而，如果检查表明，保护控制寄存器的前面内容是一个禁用位，要加载的程序也含有一个禁用位，将不能擦除保护控制寄存器 PCR。这就保证了，包含在保护控制寄存器中的禁用信息在再编程过程中的任何时候不会变成无效，也就是说，甚至在较短时间内也不会。在保护控制寄存器 PCR 接收到它的新内容之后，能够加载新的用户程序进入第四存储器块 7。而在加载之前，最好先擦除旧用户程序。

应该注意到，在用户程序编制的整个过程中，擦除第三存储器块 6 中的口令字“Key 1’”。程序的解密过程，要用到在第的二个存储器块 5 中口令字“Key 1”。在新的程序已加载到第四存储器块 7 之后，接收到的程序把新的口令字“Key 1’”写入第三存储器块 6 中。作为再编程的最后一步，擦除第二存储器块 5 中的旧口令字“Key 1”，并用一个新的口令字代替。这就完成了再编程。

从流程图 4 可知，有一点是明显的，即再编程从擦除第三存储器块 6 中的口令字开始，到擦除第二存储器块 5 并写入新的口令字结束。这样，第三存储器块 6 及第二存储器块块 5 的状态可以表明，是否已完成用户程序的编程或是否在完成之前就退出了。在后一种情况下，

对第三存储器块 6 和第二存储器块块 5 的内容进行简单的逻辑比较，结果将表明用户程序是否已经完整有效。如果用户程序无效，正象图 3 中表明的那样，处理器将进入一个等待模式，要结束这一模式，必须在用户起始地址 adr-U，开始一个新的程序。

在流程图 3 和图 4 中，没有表示出对存储器设备 1 的全部内容的全局擦除。这是能启动的，例如，通过在处理器 10 的预设终端预先进行级别配置。即使在处理器最坏的操作条件下，这一状态也不会发生。所以，最好将全局擦除与完全不规则的操作条件相联系。全局擦除的目的是，在特定条件下由保护控制寄存器 PCR 取消禁用，而不会使从存储器设备中读取任何保护性数据变得可能。作为擦除的结果，这些数据消失了。现在可以对整个存储器设备 1 进行再编程。编程是有点麻烦的，因为还不能经过处理器控制的数据接口，加载第一存储器部分，而只能经过独立于处理器的接口。通过全局擦除，即使由于错误加载而使处理器中有了一个繁杂或错误的程序，生产商或用户还是能在禁用之后使用处理器。了解全局擦除知识的第三方不能访问存储器内容。这样就完全保证了保护功能。

图 5 中，以方框图的形式，表示了本发明的一个实施例，给出了对于保护功能必须的功能单元。处理器 10 含有一个处理器核心 11，其输入、输出与内部数据总线 12、内部地址总线 13 相连。因为总线 12 和总线 13 还未阐明，所以可以设计成高速并行总线，例如各自都含有 32 条线。另外，可能有效率不够高的内部总线连接，它们将处理器的各个功能单元互连。系统时钟信号 c1 为处理器 10 提供时钟，系统时钟信号由芯片上时钟发生器 14 提供。

处理器核心 11 中需要处理的数据和地址来自静态随机存取存储器 15 (SRAM)、快擦除存储器 1 或数据接口 16、17、18，且经过数据总线 12 或地址总线 13。数据和地址也有可能从数据接口 16 直接传到处理器核心。在图 5 的实施例中，下面的外部可访问数据接口直接连到数据总线 12 和地址总线 13：一个 JTAG 接口 16、一个 USB 接口 17 和一个并行接口 18。经过一个合适的程序控制器，USB 数据接口

17 和处理器核心 11 协同工作。接口 JTAG16 和并行接口 18 独立于处理器核心 11，能比较方便地输入数据和地址。

利用地址产生器 19，各个地址形成存储器区信号 adr-I。在与接口 16、17 和 18 相关联的逻辑设备 20、21 和 22 中，这些地址范围信号分别都和 PCR 寄存器中相关的禁用或启用信号相结合，形成控制信号 25、26 和 27，分别对接口 16、17 和 18 禁用和启用。

图1

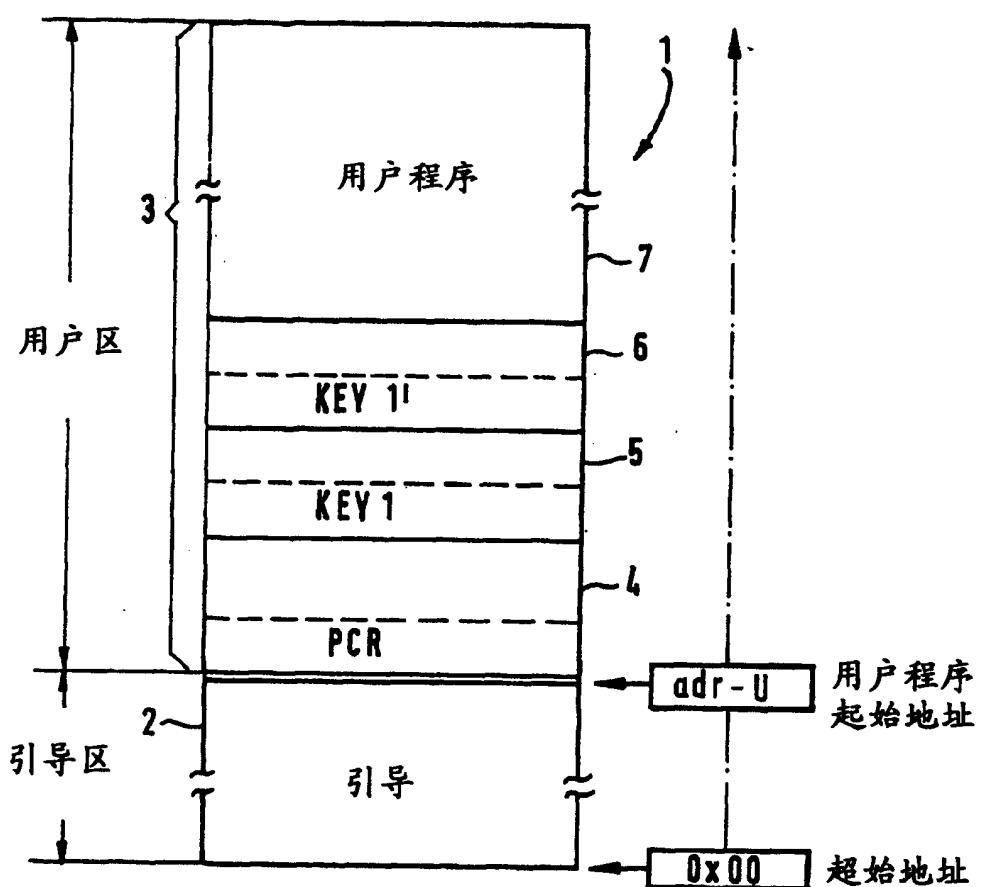


图2

X	X	X	X		X	PCR
JTAG 接口	USB 接口	并行 接口	UART 接口		测试 模式	读写
1	1	1	1		1	启用
0	0	0	0		0	禁用

图 3

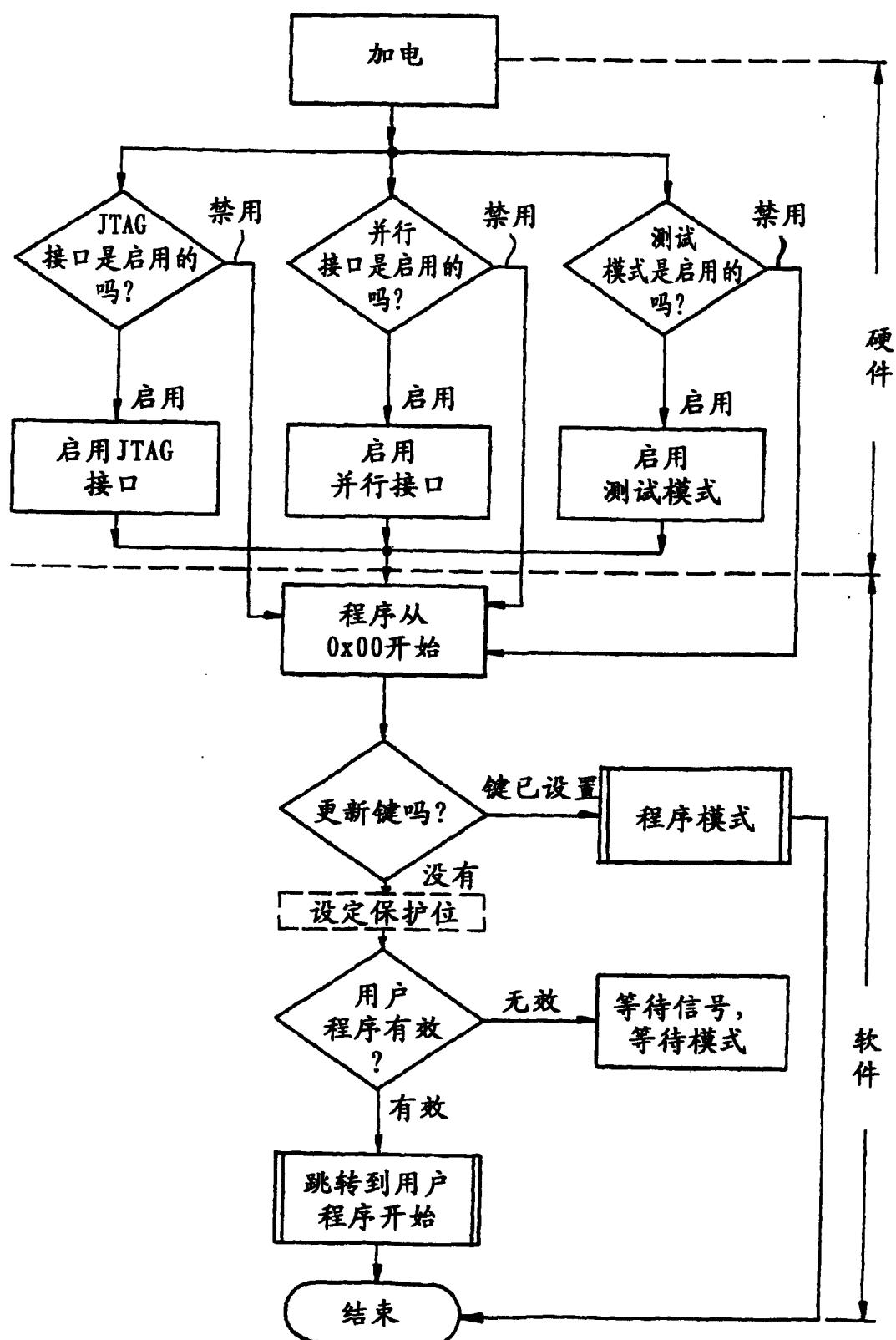


图 4

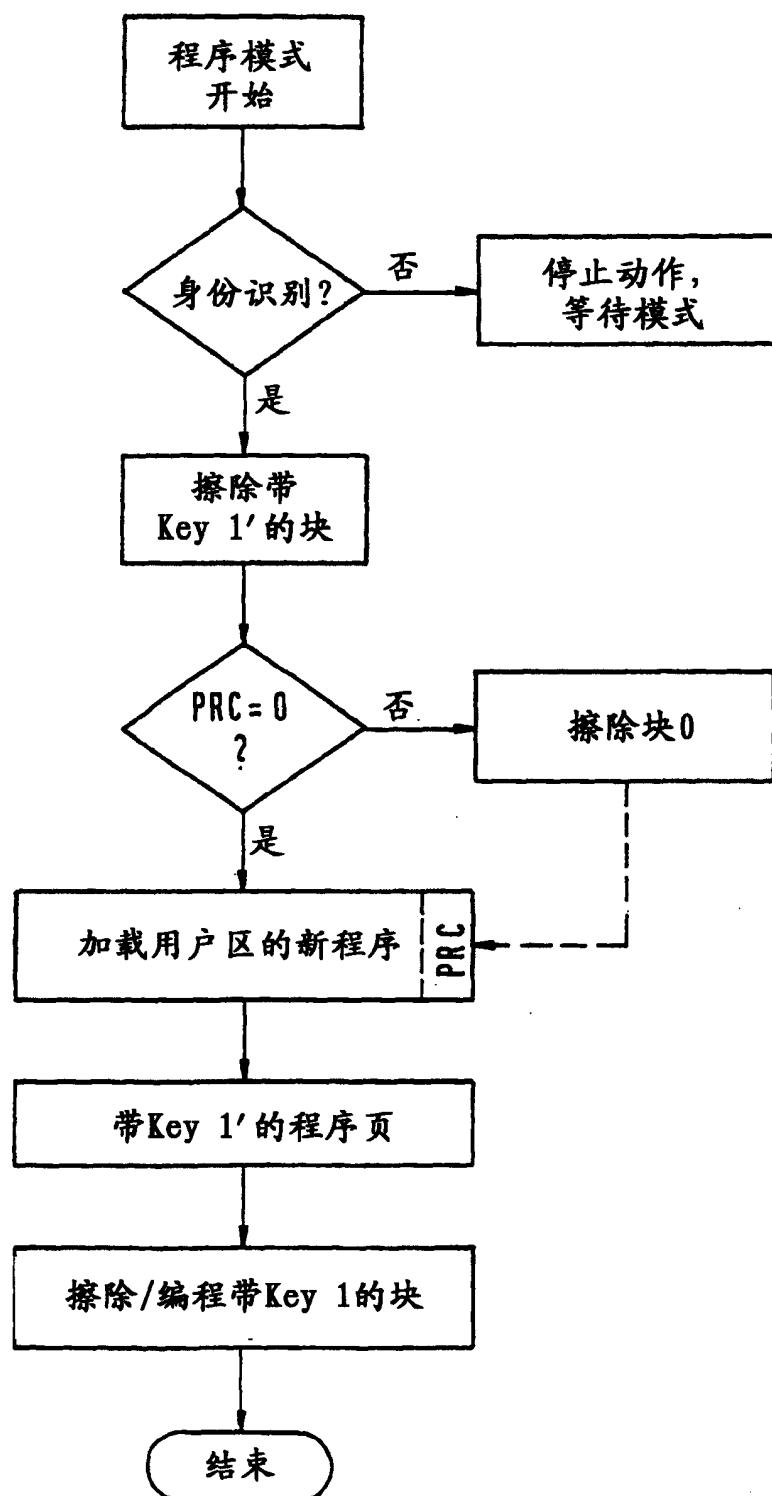


图 5

