[19] 中华人民共和国国家知识产权局

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

[12] 发明专利申请公布说明书

[21] 申请号 200810171493.X

[43] 公开日 2009 年 4 月 1 日

[11] 公开号 CN 101398872A

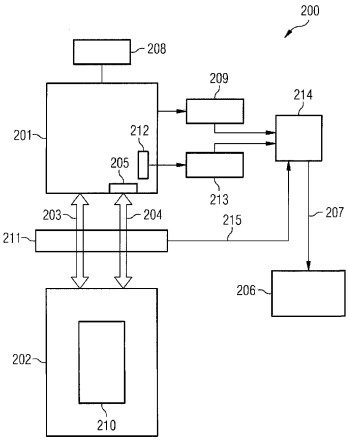
[22] 申请日 2008.9.26
[21] 申请号 200810171493.X
[30] 优先权
[32] 2007. 9.26 [33] US [31] 11/861288
[71] 申请人 英飞凌科技股份公司
地址 德国新比贝格
[72] 发明人 G·D·詹宁斯 J·巴斯托
P·埃德 M·戈德克 R·奈特
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王洪斌 刘春元
权利要求书 3 页 说明书 9 页 附图 4 页

[54] 发明名称

保护口令免受未授权访问的方法和数据处理单元

[57] 摘要

本申请提供了保护口令免受未授权访问的方法和数据处理单元。 保护口令免受未授权访问的方法的一个实施例包括：在存储器中存储表示至少部分口令的数据，将数据分配给多个指令中的至少一个，将多个指令作为处理器可执行代码存储在存储器中，以及阻止将处理器可执行代码作为数据从存储器读出。



1、 保护口令免受未授权访问的方法，包括：

在存储器中存储表示至少部分口令的数据；

将数据分配给多个指令中的至少一个；

将多个指令作为处理器可执行代码存储在存储器中；以及

阻止将处理器可执行代码作为数据从存储器读出。

2、 如权利要求1所述的方法，进一步包括：

允许将处理器可执行代码作为将由处理器执行的代码读出；

允许将可允许读出的处理器可执行代码转移至处理器。

3、 如权利要求1所述的方法，进一步包括将数据作为处理器可执行代码的部分进行存储。

4、 如权利要求1所述的方法，进一步包括将数据构建到多个指令中的至少一个中。

5、 如权利要求1所述的方法，其中多个指令中的至少一个是立即指令。

6、 如权利要求1所述的方法，进一步包括执行处理器可执行代码以获取表示至少部分口令的数据。

7、 如权利要求1所述的方法，其中阻止将处理器可执行代码作为数据从存储器中读出包括：控制对其中存储处理器可执行代码的存储器地址范围或存储器的访问。

8、 如权利要求1所述的方法，其中阻止将处理器可执行代码作为数据从存储器中读出包括：限制数据读访问对其中存储处理器可执行代码的存储器地址范围或存储器的访问。

9、 如权利要求2所述的方法，其中允许将处理器可执行代码作为将由处理器执行的代码读出包括：允许指令读访问对其中存储处理器可执行代码的存储器地址范围或存储器的访问。

10、保护口令免受未授权访问的方法，包括：

将表示至少部分口令的数据分布到多个数据部分中；

将每个数据部分与多个指令中的至少一个进行组合；

将包括组合的数据部分的多个指令作为处理器可执行代码存储在存储器

中；以及

阻止将处理器可执行代码作为数据从存储器读出。

11、如权利要求10所述的方法，进一步包括：

允许将处理器可执行代码作为将由处理器执行的代码读出；以及

允许将可允许读出的处理器可执行代码转移至处理器。

12、如权利要求10所述的方法，其中组合包括将每个数据部分嵌入多个指令中的一个。

13、如权利要求10所述的方法，进一步包括执行处理器可执行代码以获取表示至少部分口令的数据。

14、如权利要求10所述的方法，进一步包括将组合的数据部分分布于在整个处理器可执行代码内。

15、数据处理单元，包括：

存储器，用于存储表示至少部分口令的数据，所述存储器进一步将多个指令作为处理器可执行代码进行存储；

控制单元，用于将数据分配给多个指令中的至少一个；以及

电路装置，用于阻止将处理器可执行代码作为数据从存储器读出。

16、如权利要求15所述的数据处理单元，电路装置进一步允许将处理器可执行代码作为将由处理器执行的代码读出；并且

电路装置进一步允许将可允许读出的处理器可执行代码转移至处理器。

17、如权利要求15所述的数据处理单元，存储器进一步将数据作为处理器可执行代码的部分进行存储。

18、如权利要求15所述的数据处理单元，控制单元进一步将数据构建到多个指令中的至少一个中。

19、如权利要求15所述的数据处理单元，其中多个指令中的至少一个是立即指令。

20、如权利要求15所述的数据处理单元，还包括：

处理器，用于处理指令并且具有指令输入端口，处理器进一步执行处理器可执行代码以便当经由指令输入端口接收处理器可执行代码时获取表示至少部分口令的数据；

电路装置进一步将可允许读出的处理器可执行代码转移至处理器的指令输

入端口。

21、如权利要求15所述的数据处理单元，电路装置还包括用于将存储器耦合到处理器的总线装置，所述总线装置具有总线监视电路以用于控制对其中存储处理器可执行代码的存储器地址范围或存储器的访问。

22、数据处理单元，包括：

控制单元，用于将表示至少部分口令的数据分布到多个数据部分中，控制单元进一步将每个数据部分与多个指令中的一个进行组合；

存储器，用于将包括组合的数据部分的多个指令作为处理器可执行代码进行存储；以及

电路装置，用于阻止将处理器可执行代码作为数据从存储器读出。

23、如权利要求22所述的数据处理单元，电路装置进一步允许将处理器可执行代码作为将由处理器执行的代码读出；并且

电路装置进一步允许将可允许读出的处理器可执行代码转移至处理器。

24、如权利要求22所述的数据处理单元，其中控制单元被配置成将每个数据部分嵌入多个指令中的一个。

25、如权利要求22所述的数据处理单元，还包括：

处理器，用于处理指令并且具有指令输入端口，并且进一步执行处理器可执行代码以便当经由指令输入端口接收处理器可执行代码时获取表示至少部分口令的数据；

电路装置，进一步将可允许读出的处理器可执行代码转移至处理器的指令输入端口。

保护口令免受未授权访问的方法和数据处理单元

技术领域

本发明大体上涉及一种保护口令免受未授权（unauthorized）访问的方法和数据处理单元。

附图说明

图1示出了根据本发明实施例的数据流程图；

图2示出了根据本发明实施例的数据处理单元；

图3示出了根据本发明实施例的方法的流程图；

图4示出了根据本发明另一个实施例的方法的流程图；

具体实施方式

以下的详细描述解释了本发明的示例性实施例。此描述不应理解为限制，而仅为了说明本发明的一般原理。然而，本发明的范围仅由权利要求定义并且不意在受以下描述的示例性实施例的限制。

术语“口令”通常意为一些被保密的并且必须被提供以获得对一些其它信息或资源的访问的信息。此处的术语“口令”也被用于表示信息的表示或编码。例如，口令可以由字母、数字和特殊符号的序列来定义。其它也能被称为口令的序列可以由另一个二进制数序列来表示或编码。

根据本发明的一个实施例，所提供的保护口令免受未授权访问的方法包括：在存储器中存储表示至少部分口令的数据，将数据分配给多个指令中的至少一个，将所述多个指令作为处理器可执行代码存储在存储器中，以及阻止将处理器可执行代码作为数据从存储器读出。

根据本发明的另一个实施例，所提供的保护口令免受未授权访问的方法包括：将表示至少部分口令的数据分布（distribute）到多个数据部分中，将每个数据部分与多个指令中的至少一个进行组合，将包括组合的数据部分的多个指令作为处理器可执行代码存储在存储器中，以及阻止将处理器可执行代码作为数

据从存储器读出。

根据本发明的另一个实施例，所提供的数据处理单元包括：存储器，用于存储表示至少部分口令的数据，所述存储器进一步将多个指令作为处理器可执行代码进行存储；控制单元，用于将数据分配至多个指令中的至少一个；以及电路装置（arrangement），用于阻止将处理器可执行代码作为数据从存储器读出。

根据本发明的另一个实施例，所提供的数据处理单元包括：控制单元，用于将表示至少部分口令的数据分布到多个数据部分中，所述控制单元进一步将每个数据部分与多个指令中的一个进行组合；存储器，用于将包括组合的数据部分的多个指令作为处理器可执行代码进行存储；以及电路装置，用于阻止将处理器可执行代码作为数据从存储器读出。

说明性地，口令和/或关于如何获取（retrieve）口令的一些信息与被作为处理器可执行代码存储在存储器中的多个指令相联系（link）。由于将处理器可执行代码作为数据从存储器读出被阻止，所以口令被保护免受未授权访问。

根据本发明的一个实施例，允许将处理器可执行代码作为将由处理器执行的代码读出，并且允许将可允许读出的处理器可执行代码转移至处理器。

根据本发明的一个实施例，通过执行处理器可执行代码来获取表示口令的数据。

表示口令的数据可以被作为处理器可执行代码的部分来存储。它们可以被构建（build）到处理器可执行代码的指令中。根据本发明的实施例，多个指令中的至少一个是立即指令。

处理器可执行代码可以包括附加指令以用于执行安全相关过程。表示口令的数据所分配到的多个指令可以被分布于整个处理器可执行代码内。这样，口令就具有更强的免受未授权访问的保护。

在其中安全和不安全代码由单个处理器执行的数据处理系统中，需要安全方法来控制对关键硬件资源的访问。这样的关键硬件资源的例子可以是用于加密（cryptographic）操作的基于保密硬件（secret hardware）的密钥。对硬件资源的访问应仅当确定的安全代码片段（piece）在系统中执行时才是可能的。

这能够例如通过使用用于安全访问的单独的（附加的）处理器、通过使用具有硬件安全线程的处理器、或通过使用状态机控制对指令和数据存储器的访问来实现。可替换地，口令可以被用于控制对硬件资源的访问。

当使用口令来控制对资源的访问时，通常希望保持口令保密以便其仅对被授权使用资源者是已知的而对其它人不可用。例如，在其中安全和非安全代码由单个处理器执行的数据处理系统中，对资源安全访问的形成可以通过使用仅当安全代码被执行时才能被访问的口令来提供。因为在某一点需要使用口令，所以口令必须在系统中是可用的，但是必须保护对口令的访问免受攻击者读取和使用。换句话说，必须保护口令免受未授权访问。

图 1 示出了根据本发明一个实施例的数据流程图。

口令 101 由存储在存储器中的数据 102 表示。数据 102 包括多个数据部分 103、104、105、106 和 107。数据部分被单独地分配给多个指令 108、109 和 110 中的一个。在所示的例子中，数据部分 103 分配给第一指令 108（“指令 1”），数据部分 104 被分配给第二指令 109（“指令 2”）等等。指令被作为处理器可执行代码存储在存储器中。这意味着代码仅能够被执行而不能作为数据读出。分配给指令 108、109 和 110 的数据部分可以作为处理器可执行代码的部分来存储。

为达此目的，在所描述的实施例中使用所谓的立即指令。这些是其中指令所引用的数据被构建到指令中的指令，并且不需要取数据。指令 108、109 和 110 可以是允许使用内部指令常量的汇编指令，其能够在不使用附加数据总线的情况下被加载到微处理器的寄存器中。ARM926 是能够按这种方式使用的处理器的例子。立即指令中所使用的数据通常很短并且可能仅为 1 字节。在所示的例子中，第一指令 108 包括分配的数据 111 和 112，第二指令 109 包括分配的数据 113 和 114，第三指令 110 包括分配的数据 115。在该情况下，分配的数据 111 对应于数据部分 103，分配的数据 112 对应于数据部分 105 等等。可替换地，立即指令可以不包括数据部分 103、104、105、106 和 107，取而代之其它信息可用于获取密码，例如到其中存储数据 102 的其它指令或存储位置的链接（link）或指针。

由于包含立即指令的代码被微处理器执行，所以微处理器在内部寄存器中建立完全（complete）口令，即表示口令的数据。这可以通过在将口令加载到内部寄存器时使用移位（shift）操作和“或”操作来实现。这能够直至一个或多个完全 32 位寄存器已经被加载口令才完成。

在一个实施例中，表示口令 101 的数据 102 被分布于立即指令 108、109 和 110 中的整个安全访问代码内。安全访问代码包括一个或多个附加指令 116 以用

于执行安全相关过程。由于口令访问命令被分布于整个安全访问代码内，所以如果代码没有被完全执行，则完全口令对微处理器而言不可用。安全访问代码能够执行安全访问，例如检查中断被禁止（disabled），以及检查调用（call）例程的源。

参考图2，示意性的框图示出了以下将要讨论的根据本发明另一个实施例的数据处理单元。

数据处理单元200包括微处理器201和存储器202，所述微处理器201和存储器202经由数据总线203及指令总线204相耦合。指令总线连接至微处理器的指令输入端口205。数据处理单元还包括安全关键硬件资源206，例如用于加密操作的基于保密硬件的密钥。对该硬件资源的访问受安全访问信号207保护，其继而受口令保护。

每当数据处理单元200被重置和引导时，口令都会被赋予新值。实现此目的的好方法是从随机数字发生器208中取值。随机数字发生器208所递送的口令被微处理器201编程到不能被读出的硬件寄存器209中，例如当紧接在初始化之后，数据处理单元处于安全状态时。当系统仍处于安全状态时，口令也被嵌入存储在存储器202中的一段安全访问代码210。为了实现此目的，使用立即指令。口令或密钥必须分割成指令适合的片段。大小由所使用的指令集来确定，例如加载记忆区（load mnemonic）中常量字段的大小。表示口令的数据被嵌入多个立即指令，其形成安全访问代码210的一部分。此处微处理器201担当向多个指令中的至少一个分配数据的控制单元。微处理器201也能够被视为将表示至少部分口令的数据分布至多个数据部分中的控制单元，控制单元进一步将每个数据部分与多个指令中的一个进行组合。

安全访问代码210通过硬件来保护。总线监视器（watcher）211仅允许针对其中通过指令总线204保护安全访问代码的存储器的总线访问。这意味代码仅能够被微处理器201执行，并且不能被作为数据从存储器读出。通过总线监视器211针对来自任何总线的数据访问对相应的存储区域进行保护和闭锁(lock)。总线监视器211的硬件能够被视为用于阻止将处理器可执行代码作为数据从存储器202读出的电路装置。因此口令在微处理器对非安全代码的执行期间被保护。如果安全访问代码被非法访问（被重写，或作为数据读取）或试图这样做，则总线监视器211的检测电路将会产生安全警报，锁定（lock off）对

安全硬件资源 206 的访问直至下一次重置，或简单地重置系统（例如数据处理单元）。

也可以使对口令的访问依赖于集成电路的特定安全状态。这可以通过硬件来实现。利用不正确的安全状态访问口令会引发安全警报。

当要求访问硬件资源 206 的应用或例程需要使用口令时，安全访问代码 210 经由指令总线 204 和指令输入端口 205 被加载到微处理器中并被立即执行。当安全访问代码被执行时，微处理器在内部寄存器 212 中构建完全口令，即表示口令的数据。这可以通过在将口令加载至内部寄存器 212 中时使用移位和“或”操作来实现。这能够直至一个或多个完全 32 位寄存器已经被加载口令才完成。之后微处理器将口令写入比较硬件寄存器 213。安全访问电路 214 将硬件寄存器 209 的内容和比较硬件寄存器 213 的内容进行比较。仅当比较硬件寄存器 213 包含口令的正确值并且没有从警报信号 215 检测到总线监视器 211 的安全警报条件时，才激活安全访问信号 207。

安全访问代码 210 包含附加指令 116 以用于执行安全访问，例如检查中断被禁止，以及检查调用例程的源。授权帧（frame）可以被执行，此处调用模块通过读出链接寄存器（例如 ARM 系统上的 R14）并且将其与允许地址的列表相比较来确定。另外，可以针对未授权返回地址来检查本地堆栈帧。这确保了获取口令的功能仅能够被授权的软件部分使用。调用安全访问代码的例程可以完全通过硬件来保护。表示口令的数据可以在以预定方式加扰（scramble）的多个部分中返回调用例程，从而要求调用例程必须在能够使用它之前以已定义方式对数据进行去扰（descramble）。

由于口令访问命令（指令 108、109、110）被分布于整个安全访问代码内，所以如果代码不被完全执行，则完全口令将对于微处理器而言不可用。在安全访问代码 210 的执行时，数据处理单元 200 能够被强制进入安全状态。因此能够实现：仅当安全代码被微处理器 201 执行时才准予对硬件资源 206 的访问。

安全访问信号 207 仅能够通过将正确值写入硬件比较寄存器 213 来激活。将错误值写入寄存器将会引起安全访问信号被锁定直至对数据处理单元 200 的下一次重置。只要口令具有合理的长度，试图随机猜测口令的攻击者极可能失败。这是因为攻击者仅能猜一次，之后数据处理单元 200 必须被重置才能有另一次尝试。在这一点，使用随机数字发生器 208 产生新口令。这意味强力攻击

比口令长度暗示（imply）花费长得多的时间，系统性的（systematic）攻击也不起作用。

口令的使用也能够利用附加硬件来保护。在这种情况下，硬件检查口令是否已经被全部读取。如果没有，则口令不能被使用，并且将被拒绝。

这样，硬件资源 206 通过硬件和软件的组合来保护，其优点在于：软件能够依据所需的保护等级而增强。数据处理单元 200 能够是单元或集成至单个集成电路中的系统。其也可以是包括若干集成电路和/或其它件设备的系统。

图 3 示出了根据本发明一个实施例的方法的流程图。

在 301 中，表示至少部分口令的数据被存储在存储器中。例如，这能够由与数据存储器 202 相耦合的微处理器 201 来执行。耦合可以由数据总线 203 提供。

在 302 中，数据被分配至多个指令中的至少一个。这还可以由微处理器 201 来执行。指令可以是立即指令，其允许使用内部指令常量。利用这些，可以执行汇编指令以便在不是必须使用附加数据总线的情况下将数据加载到微处理器的寄存器中。

在 303 中，将多个指令作为处理器可执行代码存储在存储器中。如图 1 所示，所分配的数据 111、112、113、114 和 115 可以与指令 108、109 和 110 一起存储。在这个例子中，它们形成存储器 202 中的处理器可执行代码 210 的一部分。可替换地，所分配的数据可以保持或能够被存储在另一个存储器位置。提供各数据和其被分配到的指令之间联系的一些信息可以包括在指令中。

在 304 中，阻止将处理器可执行代码作为数据从存储器读出。例如，总线监视器 211 控制对存储器 202 中存储处理器可执行代码 210 的区域的总线访问。任何数据读或写访问都通过总线监视器硬件被阻止。总线监视器阻止任何经由数据总线 203 访问处理器可执行代码 210 的尝试。因此口令 101，更确切地，表示口令的数据 102，被保护免受未授权访问。

图 4 示出了根据本发明另一个实施例的方法的流程图。

在 401 中，表示至少部分口令的数据被分布到多个数据部分中。例如，这能够由微处理器 201 来执行。表示口令 101 的数据 102 被分割为片段 103、104、105、106 和 107。

在 402 中，将每个数据部分与多个指令中的至少一个进行组合。这也可以

由微处理器 201 来执行。数据部分可以与指令一起被安排或与指令相联系。如果指令是立即指令，那么数据部分能够被构建成立即指令。

在 403 中，将包括组合的数据部分的多个指令作为处理器可执行代码存储在存储器中。图 1 中的数据 111、112、113、114 和 115 可以被视为与指令 108、109 和 110 组合的数据部分。指令和组合的数据部分能够被一起存储在存储器 202 中并且之后形成处理器可执行代码 210 的一部分。

在 404 中，阻止将处理器可执行代码作为数据从存储器读出。例如，总线监视器 211 控制对存储器 202 中存储处理器可执行代码 210 的区域的总线访问。任何数据读或写访问都通过总线监视器硬件被阻止。总线监视器阻止任何经由数据总线 203 访问处理器可执行代码 210 的尝试。因此口令 101，更确切地表示口令的数据 102，被保护免受未授权访问。

虽然已经特别参考附图详细描述了前述一些实施例，但发明者考虑到不同的实施例。

在本发明的一个实施例中，控制对其中存储处理器可执行代码的存储器地址范围或存储器的访问包括使用硬件单元。

本发明的一个实施例包括：当处理器可执行代码被作为数据读出或被改变时产生安全警报。

在本发明的一个实施例中，处理器可执行代码包括附加指令以用于执行安全相关过程。

在本发明的一个实施例中，多个指令中的至少一个被分布于整个处理器可执行代码内。

在本发明的一个实施例中，为了完全获取表示至少部分口令的数据，需要基本上执行所有处理器可执行代码。

本发明的一个实施例包括：每当集成电路被重置和引导时，向表示至少部分口令的数据分配新值。

在本发明的一个实施例中，向表示至少部分口令的数据分配新值包括使用随机数字发生器。

本发明的一个实施例包括：将表示至少部分口令的数据编程到不能被读出的硬件寄存器中；将所获取的数据写入硬件比较寄存器；以及如果硬件比较寄存器包含表示至少部分口令的数据的正确表示，则激活安全访问信号。

本发明的一个实施例包括：在激活安全访问信号时，使能（enable）对安全硬件资源的访问。

本发明的一个实施例包括：如果硬件比较寄存器包含表示至少部分口令的数据的不正确表示，则锁定安全访问信号。

本发明的一个实施例包括：保持锁定的安全访问信号被锁定直至集成电路被重置或引导。

本发明的一个实施例包括：执行软件例程，所述软件例程需要安全访问，所述安全访问需要表示至少部分口令的数据；以及使用硬件单元检查软件例程的完整性（integrity）和/或授权。

本发明的一个实施例包括：在以预定方式加扰的多个部分中返回表示至少部分口令的数据。

在本发明的一个实施例中，总线监视电路被配置成限制数据读访问对其中存储处理器可执行代码的存储器地址范围或存储器的访问。

在本发明的一个实施例中，总线监视电路被配置成允许指令读访问对其中存储处理器可执行代码的存储器地址范围或存储器的访问。

在本发明的一个实施例中，电路装置包括检测电路，所述检测电路用于当处理器可执行代码被作为数据读出或被改变时产生安全警报。

在本发明的一个实施例中，处理器可执行代码包括附加指令以用于执行安全相关过程。

在本发明的一个实施例中，多个指令中的至少一个被分布于整个处理器可执行代码内。

本发明的一个实施例包括具有引导电路的集成电路，所述引导电路用于每当集成电路被重置和引导时，向表示至少部分口令的数据分配新值。

本发明的一个实施例包括随机数字发生器以用于产生新值。

本发明的一个实施例包括：

硬件寄存器，用于接收表示至少部分口令的数据，所述硬件寄存器被配置为不能被读出；

硬件比较寄存器，用于将所获取的数据写入其中；以及

安全访问电路，用于在硬件比较寄存器包含表示至少部分口令的数据的正确表示的情况下激活安全访问信号。

本发明的一个实施例包括安全硬件资源并且被配置为在激活安全访问信号时使能对安全硬件资源的访问。

本发明的一个实施例配置为：如果硬件比较寄存器包含表示至少部分口令的数据的不正确表示，则锁定安全访问信号。

本发明的一个实施例包括具有引导电路的集成电路并且配置为保持锁定的安全访问信号被锁定直至集成电路被重置或引导。

本发明的一个实施例包括完整性检测电路，用于在软件例程在被处理器执行时需要安全访问的情况下检查软件例程的完整性，所述安全访问需要表示至少部分口令的数据。

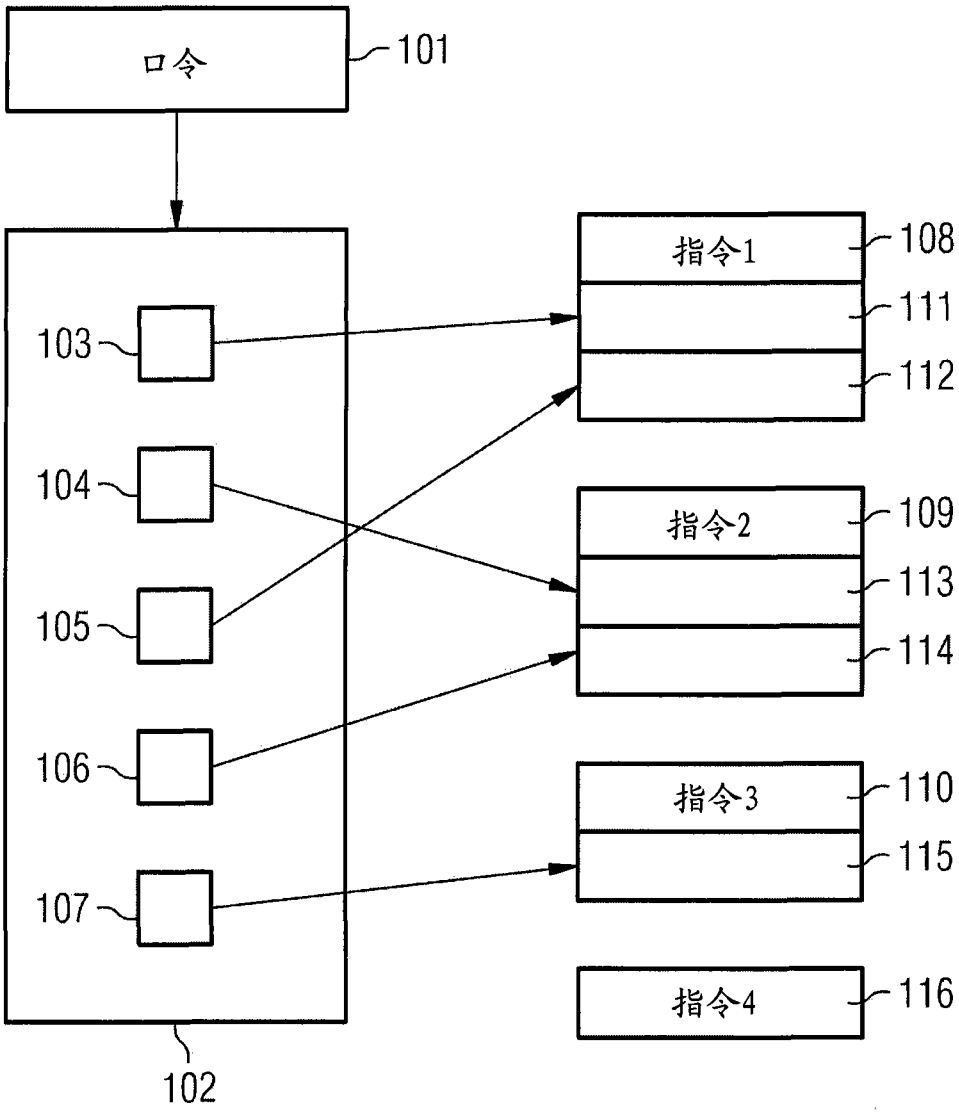

口令
101
103
104
105
106
107
102
指令1
108
111
112
指令2
109
113
114
指令3
110
115
指令4
116

图 1

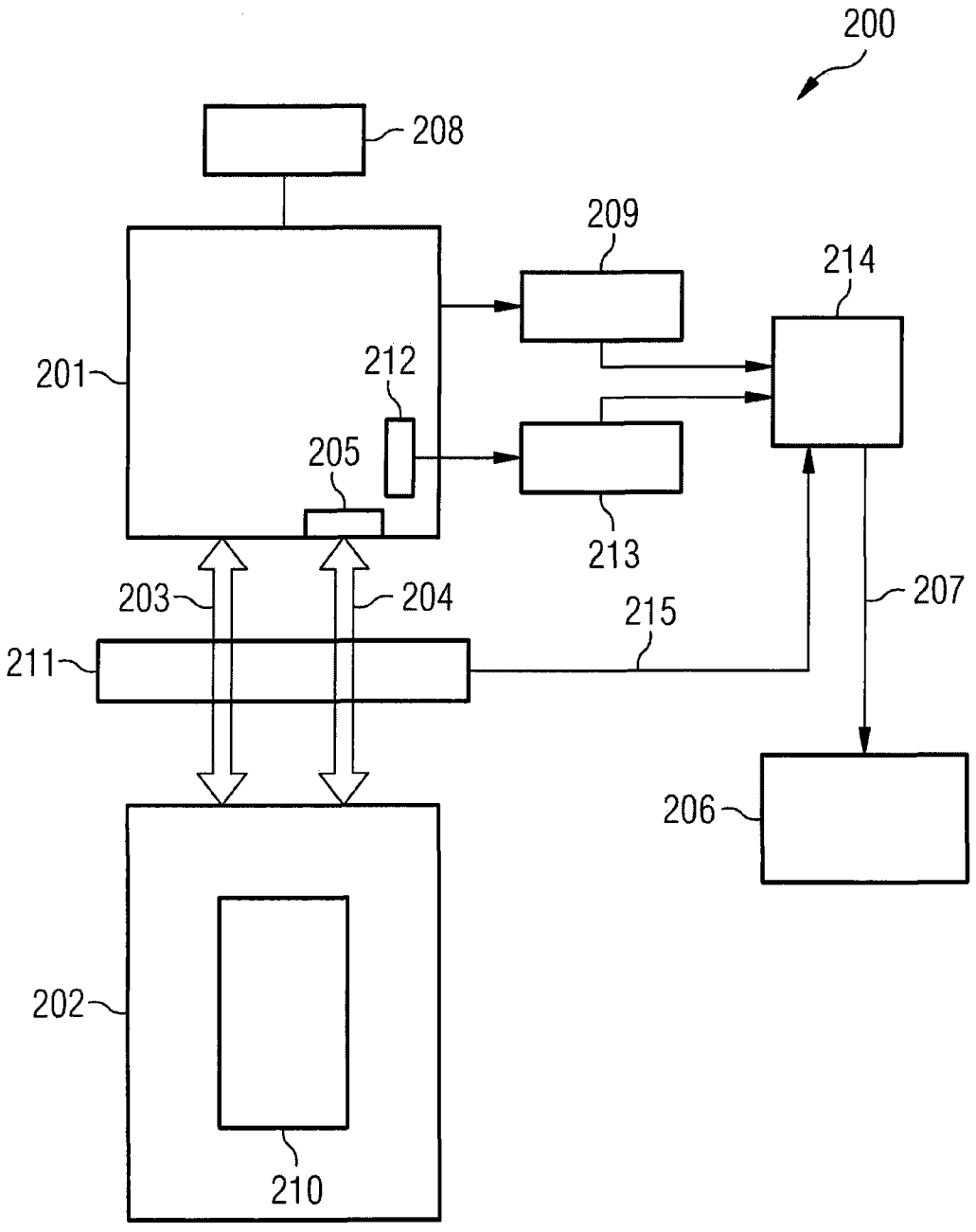


图 2

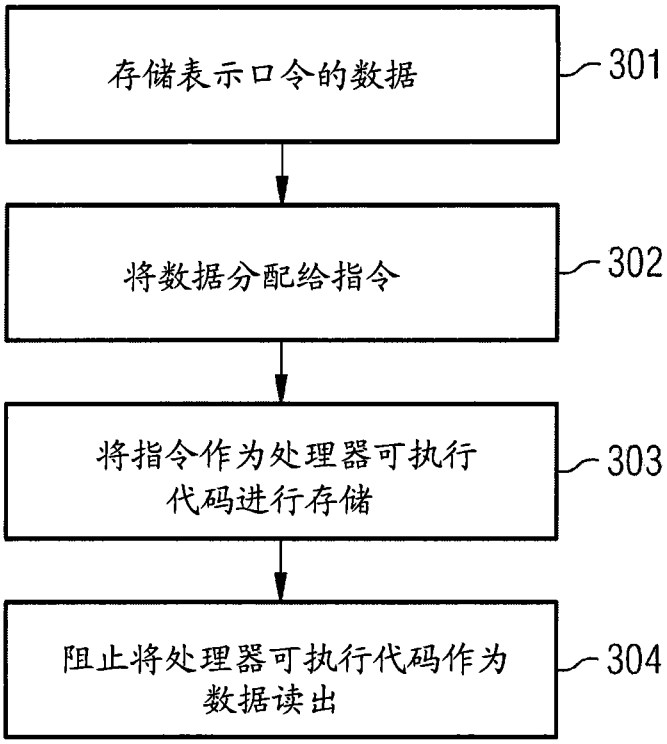

存储表示口令的数据
301
将数据分配给指令
302
将指令作为处理器可执行代码进行存储
303
阻止将处理器可执行代码作为数据读出
304

图 3

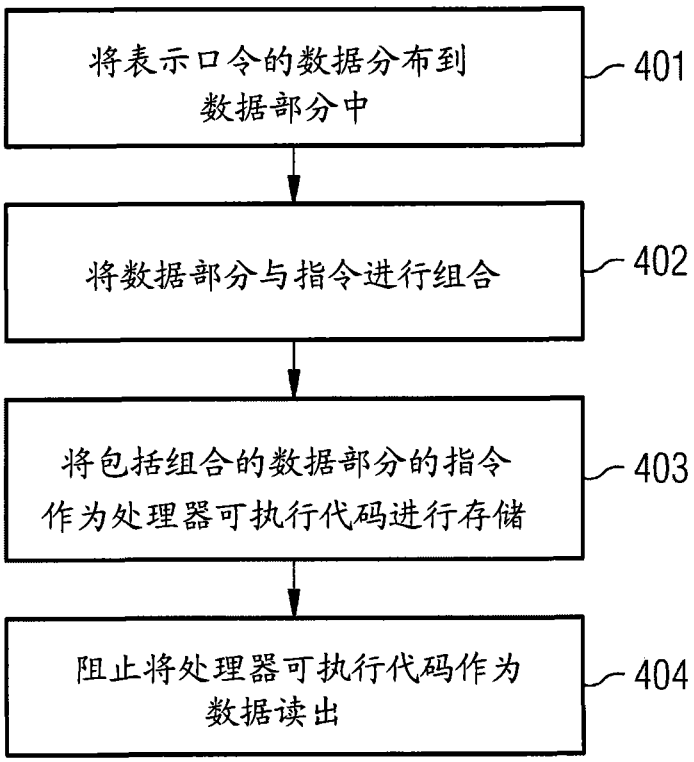

将表示口令的数据分布到数据部分中
401
将数据部分与指令进行组合
402
将包括组合的数据部分的指令作为处理器可执行代码进行存储
403
阻止将处理器可执行代码作为数据读出
404

图 4