[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
G06F 12/14

[12] 发明专利说明书

[21] ZL 专利号 97199904.X

[45] 授权公告日 2004 年 12 月 29 日

[11] 授权公告号 CN 1182678C

[22] 申请日 1997.7.30 [21] 申请号 97199904.X
[30] 优先权
[32] 1996.9.30 [33] US [31] 08/722298
[86] 国际申请 PCT/US1997/013518 1997.7.30
[87] 国际公布 WO1998/015086 英 1998.4.9
[85] 进入国家阶段日期 1999.5.19
[71] 专利权人 英特尔公司
地址 美国加利福尼亚州
[72] 发明人 D·L·达维斯
审查员 李 卉

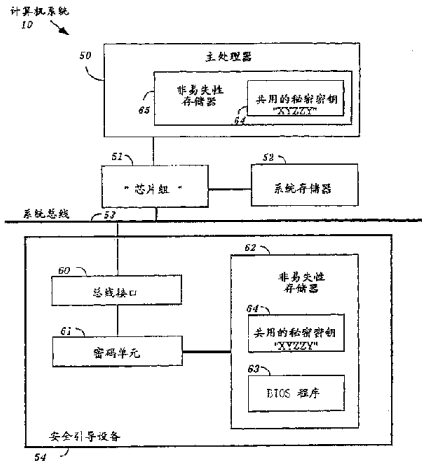
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王 勇 王 岳

权利要求书 3 页 说明书 5 页 附图 2 页

[54] 发明名称 安全引导

[57] 摘要

本发明揭示了一个用于防止对实现在一个可修改非易失性存储器(比如快速存储器)(620)中的引导固件(例如 BIOS(63))进行非法替换的子系统。该固件设备包含在一个响应该主处理器(50)的安全引导设备(54)中。 该安全保护是通过使用一个由该安全引导设备(54)和该主处理器(50)共用的秘密密钥(64)加密和解密该引导指令而建立的。



ISSN1008-4274

1.一个用于防止对包含可执行代码的存储装置进行非法替换的系统，包括:

第一密码装置，用于在加电序列期间响应一个访问请求，根据一个秘密密钥对所述可执行代码进行加密以产生一个加密的代码，所述第一密码装置与所述存储装置相连;

第二密码装置，用于根据所述秘密密钥对所述加密的代码进行解密，产生解密的代码，所述第二密码装置与所述第一密码装置相连，并且如果所述解密的代码与所述可执行代码一致则能够执行所述解密的代码，所述第二密码装置产生所述访问请求；以及

通讯装置，用于使所述第一密码装置与所述第二密码装置通过交换所述加密的代码和解密的代码进行通讯。

2.根据权利要求 1 的系统，其特征在于所述第一密码装置包括一个安全的引导装置。

3.根据权利要求 1 的系统，其特征在于所述第二密码装置包括一个主处理器。

4.根据权利要求 1 的系统，其特征在于所述通讯装置包括一个连接一条总线的接口，允许所述第一密码装置响应来自所述第二密码装置的所述访问请求。

5.根据权利要求 1 的系统，其特征在于所述秘密密钥可由所述第一密码装置和所述第二密码装置取得。

6.根据权利要求 1 的系统，其特征在于所述可执行代码是一操作系统。

7.根据权利要求 1 的系统，其特征在于所述可执行代码是一基本输入和输出系统。

8.根据权利要求 1 的系统，其特征在于所述存储装置是一可修改非易失性存储装置。

9.根据权利要求 8 的系统，其特征在于所述可修改非易失性存储装置是一快速存储器。

10.一个用于防止对可执行代码进行非法替换的系统，包括:

第一处理器，用于在加电序列期间响应一个访问请求，根据一个秘密密钥对所述可执行代码进行加密，产生一个加密的代码，所述第一处理器与所述可执行代码相连；

第二处理器，用于根据所述秘密密钥对所述加密的代码进行解密，产生解密的代码，所述第二处理器与所述第一处理器相连，并且如果所述解密的代码与所述可执行代码一致则能够执行所述解密的代码，所述第二处理器产生所述访问请求；以及

一个通讯路径，用于使所述第一处理器与所述第二处理器通过交换所述加密的代码和解密的代码进行通讯。

11. 根据权利要求 10 的系统，其特征在于所述第一处理器是一个安全的引导装置。

12. 根据权利要求 10 的系统，其特征在于所述第二处理器是一个主处理器。

13. 根据权利要求 10 的系统，其特征在于所述通讯路径包括一个连接一条总线的接口，允许所述第一处理器响应来自所述第二处理器的所述访问请求。

14. 根据权利要求 10 的系统，其特征在于所述秘密密钥可由所述第一处理器和所述第二处理器取得。

15. 根据权利要求 10 的系统，其特征在于所述可执行代码是一操作系统。

16. 根据权利要求 10 的系统，其特征在于所述可执行代码是一基本输入和输出系统。

17. 根据权利要求 10 的系统，其特征在于所述存储装置是一可修改非易失性存储装置。

18. 根据权利要求 17 的系统，其特征在于所述可修改非易失性存储装置是一快速存储器。

19. 一种用于防止对包含在存储装置中、主处理器可访问的可执行代码进行非法替换的方法，包括下列步骤：

提供一个与所述存储装置相连的安全处理器，所述安全处理器响应所述主处理器；

在加电序列期间对所述安全处理器产生一个访问请求；

响应所述访问请求，根据一个秘密密钥对所述可执行代码进行加密，产生加密的代码；

根据所述秘密密钥对所述加密的代码进行解密，产生解密的代码；

如果所述解密的代码与所述可执行代码一致则执行所述解密的代码；以及

在所述主处理器和所述安全处理器之间建立一个通讯路径，允许所述主处理器与所述安全处理器进行通讯。

20.根据权利要求 19 的方法，其特征在于所述通讯路径包括一个连接到一条总线的接口，允许所述安全处理器响应来自所述主处理器的所述访问请求。

21.根据权利要求 19 的方法，其特征在于所述秘密密钥可由所述主处理器和所述安全处理器取得。

22.根据权利要求 19 的方法，其特征在于所述可执行代码是一操作系统。

23.根据权利要求 19 的方法，其特征在于所述可执行代码是一基本输入和输出系统。

24.根据权利要求 19 的方法，其特征在于所述存储装置是一可修改非易失性存储装置。

25.根据权利要求 19 的方法，其特征在于所述安全处理器是一个安全的引导设备。

26.根据权利要求 19 的方法，其特征在于所述加密的步骤由所述安全处理器执行，所述解密的步骤由所述主处理器执行。

27.根据权利要求 24 的方法，其特征在于所述可修改非易失性存储装置是一快速存储器。

安全引导

相关申请的交叉引用

本申请的发明人已于 1995 年 12 月 4 日提交了一份名称为“用于加密的伴随压印的装置和方法”的美国专利申请，申请号为 08/566910. 该申请由本申请的同一受让人所有.

本发明的背景技术

1. 发明领域

本发明涉及计算机固件的安全的领域，尤其涉及在通用计算机系统，特别是个人计算机中包括操作系统(OS)和基本输入输出系统(BIOS)的引导(boot-up)固件的领域.

2. 相关技术描述

计算机系统中的一个十分关键的单元是引导固件. 该引导固件可以是一个操作系统(OS)，该 OS 的一部分，或者是基本输入输出系统(BIOS). 该引导固件实际上是通常存储在某些类型的非易失性存储器中的机器代码，以允许中央处理单元（CPU）执行诸如初始化，诊断，从大容量存储器中装载操作系统以及常规的输入/输出(I/O)功能.

在通过一个加电序列对 CPU 供电时，CPU 通过取出驻留在引导固件中的指令代码而启动. 传统上，该引导固件是以可擦除可编程只读存储器(EPROM)实现的. 然而，半导体技术的最新进展已经允许可以以快速存储器实现引导固件，从而增加了引导固件受到非法入侵的可能性.

由于引导固件在计算机系统中的关键作用，应当好好对之保护以免受到入侵攻击. 一种入侵是入侵者直接接近计算机，物理地去除包括引导固件(例如快速存储器，包含存储器的印刷线路板)的引导设备，用另一引导设备代替该引导设备. 在某些情况下，入侵者可能是该计算机系统的合法拥有者或用户，他在试图欺骗第三方服务提供者.

当前所用的机械安全机制，尤其是便携式计算机所使用的防止擦除重要信息的机制(如果该膝上形计算机的外壳没有授权而被打开的话)对于防止这些入侵没有任何效果. 目前还没有一个设计好的电子安全机制对连接主处理器和引导设备的路径提供安全保护.

因此，希望提供一种安全机制，能防止入侵者通过替换引导设备，诸如加密的协处理器或比如快速存储设备，成功地欺骗他人。它可以通过将该物理引导设备“绑定”到主处理器上而实现，从而在该主处理器和该引导固件之间提供了一个安全的路径。由于主处理器不能执行由特定的加密协处理器事先未加密的引导指令(该指令相对于该协处理器已经打上标记)，因此这一方案能防止入侵者简单地替换该特定的加密协处理器。

发明概述

本发明描述了一种安全子系统以防止对包含引导可执行代码的存储设备的非法替换，它是通过基于电子密钥机制在一个安全引导设备和一个主处理器之间建立一个安全的路径而实现的。

该安全引导设备连接到该存储设备，并且基于一个秘密的密钥对该可执行代码进行加密生成一个加密的代码。主处理器然后基于该同一个秘密的密钥对该加密的代码进行解密，以生成一个解密的代码。只有在该解密的代码与该可执行代码一致时，该主处理器才执行该解密的代码。在该安全引导设备和该主处理器之间建立的安全路径允许该两个处理器通过这种加密的消息进行安全的通信。

附图的简要描述

从下面对本发明的详细描述中可以更清楚地明白本发明的特征及其优点。其中

图 1 示出在主处理器和安全引导设备之间具有安全路径的本发明，这种安全路径使得能够安全地引导该系统。

图 2 是本发明在主处理器对引导程序进行正常的读取访问期间进行操作的流程图。

较佳实施例的描述

通过在主处理器和安全的引导设备之间建立一个安全的通信协议，本发明在该主处理器和包含一个引导程序的存储器设备之间提供一个安全的路径。在以下的描述中，使用一些术语来讨论某些密码特征。比如，“密钥”是常规的加密算法所用的编码和/或解码参数，这些加密算法比如 Rivest, Shamir 和 Adleman(RSA)，在数据加密标准(DES)中规定的数据加密算法(DEA)等等。“秘密密钥”是有限数目的访问该密钥的电子设备用于加密和解密的密钥。

如下所述，安全引导设备通过使用与主处理器共用的秘密密钥加密引导程序中的指令代码而响应主处理器访问该引导程序的请求(主请求)．主处理器使用该同一个秘密密钥对加密的指令代码进行解密．由于秘密密钥只为该主处理器和该安全引导设备所知，任何试图替换包含该引导程序的安全引导设备都会产生不正常解密的代码，使得系统不能工作．

参见图 1，其示出了一个利用本发明的计算机系统的实施例．计算机系统 10 包括一个芯片组 51，该芯片组作为一个接口工作，以支持主处理器 50，系统存储器 52 和连接到系统总线 53 上的设备之间的通信．更具体地说，主处理器 50 包括一个逻辑电路(未示出)以及一个用来存储密钥信息的小容量的内部非易失性存储器 65．系统存储器 52 可以包括常规的存储器，诸如各种类型的随机存取存储器(RAM)，如 DRAM，VRAM，SRAM 等以及存储器映射的 I/O 设备，但并不限于这些设备．系统总线 53 可以以包含外围部件互连（PCI）和通用串行总线（USB）等的总线结构中的一种实现．

一个可连接到系统总线 53 上的设备包括一个安全引导设备 54．安全引导设备 54 包括总线接口 60，密码单元 61 和本地非易失性存储器 62．使用总线接口 60 建立到系统总线 53 的电连接．引导程序 63 存储在非易失性存储器 62 中．

仍然参见图 1，其中将主处理器 50 和安全引导设备 54 配置成在它们各自的非易失性存储器 65 和 62 中包括一个共用的秘密密钥 64．这一秘密密钥由生产该主处理器和安全引导设备的原始设备制造商或其他系统提供者初始化期间在制造厂建立的，由安全引导设备 54 和主处理器 50 用于加密和解密．该加密和解密可以通过多种技术进行，其中包括采用专门的硬件电路，硬件和软件的组合，或者专门的加速器．在图 2 中描述了在系统加电(引导)序列期间主处理器 50 和安全引导设备 54 用于引导访问所执行的序列．

现在参见图 2，其中示出了与系统的引导阶段相关的步骤．首先，在步骤 110，主处理器对相应于引导程序的一个地址发出一个读请求．安全引导设备通过将其地址空间映射到该相应的引导程序检测这一引导地址(步骤 112)．在检测到该读请求时，安全引导设备使用该共用的秘密密钥加密该相应的引导指令(步骤 114)．在步骤 116，安全引导设备

以该加密的引导指令响应该主请求．在步骤 118，在接收到该加密的引导指令时，主处理器使用该共用的秘密密钥解密该加密的引导指令．在步骤 120，所得到的解密的引导指令可能与正确的指令一致，也可能不一致，这取决于该系统是否被篡改．如果该系统已被篡改，所解密的引导指令是一个不正确的或不合法的指令(步骤 130)．由于多种原因，该系统很可能停机，诸如总线错误，不能识别的操作码，无限循环等．因此，该引导序列造成系统失败．在步骤 140，所解密的引导指令是该引导程序中的一个有效的或正确的指令．该主处理器执行该指令，以及处理下一引导指令，直到完成整个引导序列．

只有该安全引导设备和该主处理器才知道该共用秘密密钥，因此试图通过用另一安全引导设备来代替该安全引导设备而改变该系统是徒劳的．其原因是该替代设备不能与该主处理器通讯．入侵者不知道该共用的秘密密钥就不能复制该加密的子系统．因此可以保护该引导固件不会受到引导设备的物理替换．

尽管上述讨论是针对主处理器和专用的安全引导设备之间的安全路径，但很容易就可认识到可以在任意数目的子系统，处理器或设备，以及其组合之间建立该安全路径．一个典型的安全路径涉及由所有设备/处理器共用的秘密密钥，以及由任一硬件、固件或软件或其任一组合实现的加密/解密算法．

在本发明的另一实施例中(未示出)，一个具有安全引导设备功能的芯片组(其包含一些引导代码)与该主处理器相连接．该引导代码可以是一个可执行指令序列．使用由该芯片组和该主处理器共用的秘密密钥来加密和解密该引导代码．从而建立上述的安全路径．

又一实施例(未示出)涉及一个包含引导程序或一些可执行代码或信息代码的印刷电路板(PCB)或诸如 PCMCIA 的“智能卡”．该 PCB 或智能卡可以插入系统主板上的任一扩展槽中，或者在任一底板接口总线上．一个安全引导设备连接到这样一个 PCB 或智能卡上，响应主请求，使用该板/卡和主处理器共用的一个秘密密钥加密该引导代码．主处理器使用该同一秘密密钥解密该加密的代码．该安全引导设备可以驻留在同一个 PCB 或智能卡上，或在系统中的其他地方，诸如另一单独的 PCB 或智能卡．只要该安全引导设备能够与该主处理器通过交换加密的或解密的

引导代码进行通讯，任何试图移走该 PCB 或智能卡以及用另一没有该秘密密钥的 PCB 或智能卡来替换将造成系统不能工作。

尽管已经参照示意性实施例描述了本发明，但是这些描述并不局限于此。对于本领域的普通技术人员来说，可以对该较佳实施例进行各种改变，而且可以给出其他实施例，但是所有这些修改都被认为落在本发明的精神与范围之内。

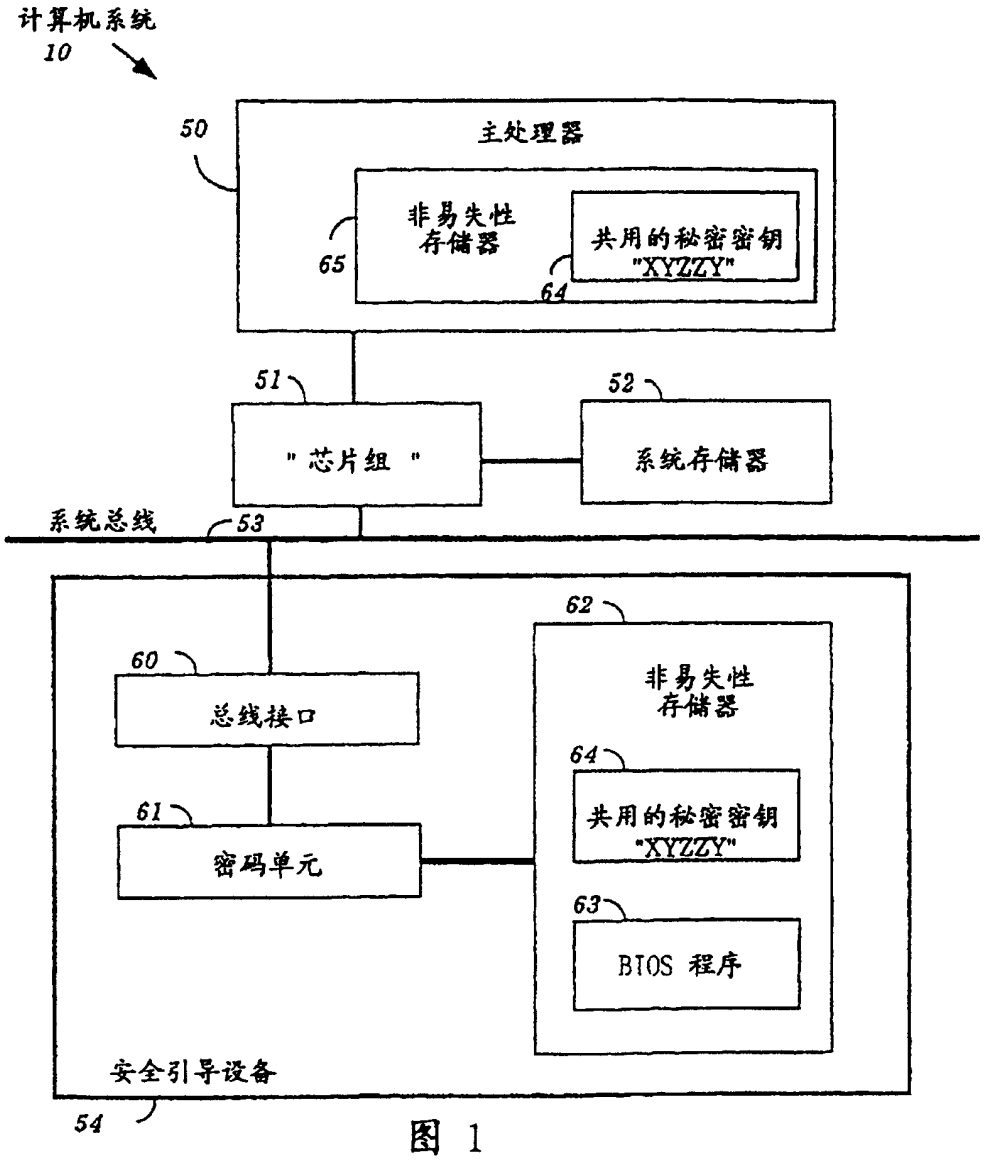

计算机系统
10
50
主处理器
非易失性
存储器
65
共用的秘密密钥
"XYZZY"
64
51
"芯片组"
52
系统存储器
系统总线
53
62
60
总线接口
非易失性
存储器
64
61
密码单元
共用的秘密密钥
"XYZZY"
63
BIOS 程序
安全引导设备
54

图 1

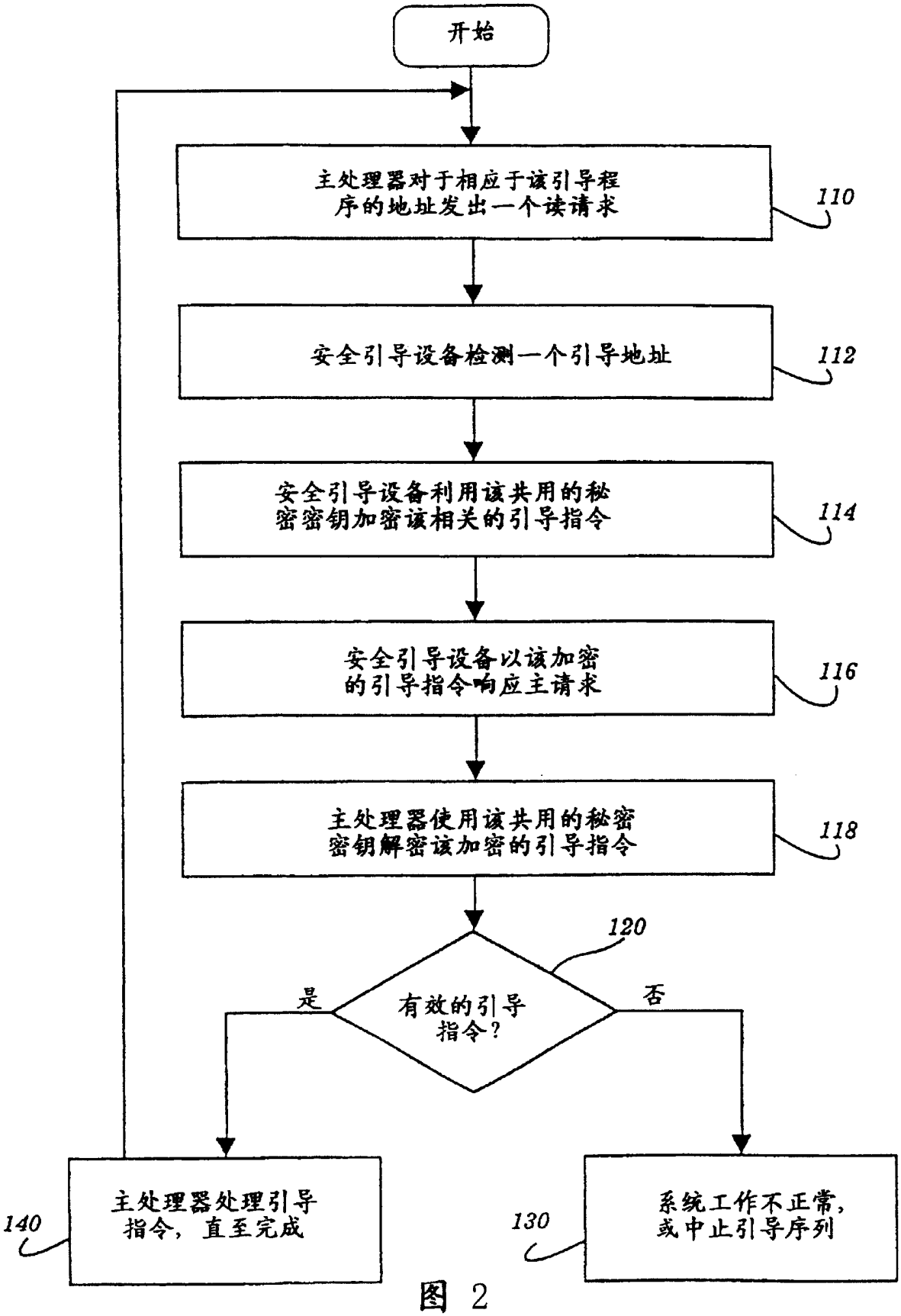

开始
主处理器对于相应于该引导程序的地址发出一个读请求
110
安全引导设备检测一个引导地址
112
安全引导设备利用该共用的秘密密钥加密该相关的引导指令
114
安全引导设备以该加密的引导指令响应主请求
116
主处理器使用该共用的秘密密钥解密该加密的引导指令
118
120
有效的引导指令?
是
否
主处理器处理引导指令，直至完成
140
系统工作不正常，或中止引导序列
130

图 2