

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200610163400.X

[51] Int. Cl.

G06F 17/00 (2006.01)

G06F 17/50 (2006.01)

G06F 21/00 (2006.01)

[43] 公开日 2007 年 6 月 20 日

[11] 公开号 CN 1983245A

[22] 申请日 2006.12.6

[21] 申请号 200610163400.X

[30] 优先权

[32] 2005.12.14 [33] US [31] 11/302,842

[71] 申请人 戴尔产品有限公司

地址 美国得克萨斯州

[72] 发明人 W·F·绍贝尔 G·D·休伯

[74] 专利代理机构 北京纪凯知识产权代理有限公司

代理人 程伟 王锦阳

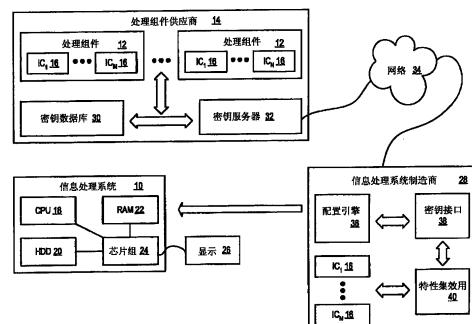
权利要求书 4 页 说明书 8 页 附图 5 页

[54] 发明名称

用于配置信息处理系统集成电路的系统和方法

[57] 摘要

用于制造信息处理系统的处理组件，包括位于信息处理系统制造地点、按单定制的集成电路，该集成电路包括可被有选择地有效的特性。例如，集成在集成电路内的熔丝，可以在信息处理系统制造地点被有选择地熔断，以便永久性地使各特性无效，这样，该处理组件便拥有了所期望的配置。作为另一例子，特性集的有效或无效状态被编程进包含在该集成电路内的闪速存储器，而该闪速存储器随后可被无效，以便永久性地设置特性，这样，该处理组件便拥有了所期望的配置。用由处理组件制造商提供的密钥来设置特性，以便跟踪信息处理系统制造商的特性使用。



1. 一种由多个处理组件制造信息处理系统的方法，该方法包括：

在信息处理系统制造地点接收多个处理组件，至少一个处理组件包含至少一个集成电路，该集成电路包含多种特性；

接收信息处理系统配置，该配置包含至少部分特性被选中、部分特性被取消选中的所述处理组件；

修改所述集成电路，以便永久性地使被选中的特性有效和永久性地使被取消选中的特性无效；

制造所述信息处理系统，以便包含所述处理组件；以及

将有关被有效或被无效的各特性的信息提供给集成电路制造商。

2. 根据权利要求 1 所述的方法，进一步包括：

在信息处理系统制造地点接收密钥，该密钥包含用于修改具有被选中和被取消选中的各特性的所述集成电路的授权；

应用该密钥以允许对所述集成电路的修改；以及

跟踪对该密钥的应用，以便跟踪被选中和被取消选中的各特性。

3. 根据权利要求 1 所述的方法，其中，修改所述集成电路进一步包括熔断包含在所述集成电路内、与将被取消选中的各特性的无效相关联的熔丝。

4. 根据权利要求 1 所述的方法，其中，所述处理组件包括包含多个集成电路的芯片组，该方法进一步包括：

接收包含所述芯片组的信息处理系统配置，所述芯片组包含所述多个集成电路中的每个集成电路的至少部分特性被选中和至少部分特性被取消选中；以及

修改所述集成电路，以便永久性地使被选中的特性有效和永久性地使被取消选中的特性无效。

5. 根据权利要求 1 所述的方法，其中：

接收所述处理组件进一步包括至少一个具有多个特性被无效的所述处理组件；以及

修改所述集成电路进一步包括：

改变集成在所述集成电路的闪速存储器内的特性表，以便使被选中的特性有效；以及

永久性地限制对所述特性表的访问。

6. 根据权利要求 5 所述的方法，其中，所述修改进一步包括输入密钥以访问所述特性表。

7. 根据权利要求 1 所述的方法，其中，所述处理组件包括 CPU，所述多个特性包括浮点支持。

8. 根据权利要求 1 所述的方法，其中，所述处理组件包括存储器，所述多个特性包括可变存储器容量。

9. 一种信息处理系统处理组件，包括：

具有多个可被有选择地有效的特性的至少一个集成电路；

包含在所述集成电路内的特性选择器，可操作于永久性地使多个可被有选择地有效的特性中被选中的特性有效或无效；以及

10. 根据权利要求 9 所述的信息处理系统处理组件，其中，所述特性选择器包括与所述多个可被有选择地有效的特性中的每个相关联的熔丝，所述熔丝可操作于激活永久性地防止对相关联的可被有选择地有效的特性的访问。

11. 根据权利要求 9 所述的信息处理系统处理组件，其中，所述特性选择器包括：

保存所述多个可被有选择地有效的特性中的每个被有效或被无效的状态的闪速存储器，所述闪速存储器可编程于改变所述特性的状态；以及

特性安全模块，可操作于永久性地使所述闪速存储器的可编程性无效。

12. 根据权利要求 9 所述的信息处理系统处理组件，其中，所述密钥包括保存在所述集成电路上的模式，如果给所述集成电路的输入与保存在所述集成电路上的所述模式相匹配，则所述特性选择器为可访问。

13. 根据权利要求 9 所述的信息处理系统处理组件，其中，所述集成电路包括双核处理器，所述各特性包括具有一个活动的核以及具有两个活动的核。

14. 根据权利要求 9 所述的信息处理系统处理组件，其中，所述集成电路包括显示控制器。

15. 一种在制造地点由从处理组件供应商处收到的多个处理组件而制造信息处理系统的系统，所述系统包括：

位于制造地点的配置引擎，可操作于由多个处理组件来确定信息处理系统配置，至少一个所述处理组件包含集成电路，所述集成电路包含多个可被有选择地有效的特性，所述信息处理系统配置包含被有效或被无效的所述可被有选择地有效的特性；

位于制造地点的特性集效用，与所述配置引擎接口连接，而且可操作于根据所述配置，永久性地使所述处理组件的所述可被有选择地有效的特性有效或无效；以及

与所述特性集效用相关联的密钥接口，可操作于应用密钥，以允许所述特性集效用永久性地使集成电路的各特性有效或无效，以便提供由所述配置引擎所确定的处理组件。

16. 根据权利要求 15 所述的系统，进一步包括位于处理组件供应商处的密钥服务器，可操作于给所述密钥接口提供密钥以及通过这些密钥跟踪位于所述集成电路上的被有效的各特性。

17. 根据权利要求 15 所述的系统，其中，所述密钥包括给所述集成电路的低引脚数目插头的代码输入。

18. 根据权利要求 15 所述的系统，其中，所述密钥包括代码，所述密钥接口包含所述代码的多个拷贝，所述密钥接口进一步可操作于在每个拷贝允许所示特性集效用的操作之后，销毁每个拷贝。

19. 根据权利要求 15 所述的系统，其中，所述处理组件的所述可被有选择地有效的特性，初始具有被无效的状态，所述特性集效用使包括在配置中的特性有效。

20. 根据权利要求 15 所述的系统，其中，所述处理组件的所述可被有选择地有效的特性，初始具有被有效的状态，所述特性集效用使不包括在配置中的特性无效。

用于配置信息处理系统集成电路的系统和方法

技术领域

本发明涉及信息处理系统集成电路，具体地说，涉及用于配置信息处理系统集成电路的系统和方法。

背景技术

随着信息的价值和应用持续地增长，个人和商业机构寻求额外的方式来处理和保存信息。这些用户可选择的一个选项是信息处理系统。一般而言，出于商业的、个人的或其他目的，信息处理系统处理、编辑、保存和/或传递信息或数据，从而允许这些用户充分利用这些信息的价值。因为对技术和信息处理的需要和要求随不同用户或应用而改变，信息处理系统随所处理信息的不同类型，处理信息的方法，所处理、保存或所传递信息的总量，信息处理、保存或传递的速度和效率等因素而改变。信息处理系统中的各种变化，允许各种信息处理系统，既可以是普遍性的，或者，也可以为特定用户或如金融交易处理、航空票务预定、公司数据保存或全球通信等特定应用而配置。此外，信息处理系统可以包括配置为处理、保存和传递信息的不同硬件和软件组件，也可以包括一个或多个计算机系统、数据存储系统和网络系统。

典型地，信息处理系统由多个处理组件在物理空间（housing）中组装而成，并且，通过称为主板（motherboard）的主印刷电路板以及多个称为子板（daughter board）的二级印刷电路板接口连接。多个处理组件是独立集成电路，例如 CPU，而其他处理组件包括集成电路以提供智能来执行功能，例如，硬磁盘驱动器上微处理器和微控制器，光驱，芯片组，网络接口卡，总线控制器，图形卡，存储器和显示器。通常地，集成电路也称为半导体设备，因为使用如与铜线相连的硅晶体管等由半导体材料制成的电路执行逻辑功能。典型地，集成电路的大部分成本来自其设计和制造流程，而不是用于制造物理电路的材料。换言之，电路设计和用于创建电路设计的资本设备之后的工程代表了

集成电路的大部分费用。因为这个原因，制造商通常将多种功能合并在一个特定集成电路中，即使并不是所有的功能都为所有的终端用户所使用，甚至是所期望。因为制造更少类型的集成电路只需要更少的电路设计和制造流程，这种多特性集成电路的制造成本得到缩减。

制造和销售多特性集成电路的一个困难是，购买商会为是否为特定信息处理系统所不需要的功能付款而犹豫。例如，芯片组里的 RAID 功能通常并不为基本桌上型系统需要，但有时作为一项功能包括进来以便同一个芯片组能用于基本和先进系统。但是，集成电路制造商通常为所有包括的功能收费，否则，购买商可以只订购和支付有限的几个功能，却在集成电路制造商不知情的情况下，使用额外功能。为解决这个困难，通过基于定价或市场划分购买该设备，来无效或限制速度的功能，选择性地区分单个集成电路设备类型。典型地，通过在制造流程期间激活熔断（fusing）选项，来实现区分单个设备类型。例如，熔断（blow）内建于集成电路的熔丝（fuse），具有使与该熔丝相关联的电路部分不可访问的效果。通过在制造期间熔断熔丝来缩减功能，还具有降低测试成本的优点，因为不需要测试失效的功能。可是，用熔断来区分集成电路导致系统集成师必须定义多个类型的印刷电路板来容纳各种熔断选项，从而导致平台断裂和终端用户成本升高。

发明内容

因此，出现了对允许集成电路系统集成师配置完整功能的集成电路的灵活性的系统和方法的需求，这里，系统集成师通过选择所期望的功能来进行配置。

根据本发明，提供系统和方法，其能极大地降低与此前用于配置信息处理系统组件集成电路的功能的方法和系统相关联的缺点和问题。在依照订单制造信息处理系统的时候，在信息处理系统的制造时选择性地有效特性集（feature set），以便按单制造处理组件。通过选择性地有效或无效处理组件中集成电路的功能，来配置处理组件以便具有与信息处理系统配置相关联的特性集。在信息处理系统的制造地点执行集成电路功能的永久设置，以获得信息处理系统制造流程中改善的灵活性。

更具体地说，将包含具备预定特性集与组合特性选择器的集成电路的处理组件发送到信息处理系统的制造地点。例如，在一个实施例中，将集成电路特性集以完全有效的形式发送出去，而在信息处理系统制造地点有选择地熔断的熔丝，以便无效相关的功能。或者，可选地，将集成电路特性集通过包含在集成电路内的特性集表至少部分地无效的形式发送出去，该特性集表允许特性集功能状态在关与开之间变化。由配置引擎确定适合于信息处理系统配置的特性集，以便特性集效用与特性选择器互动，永久地设置集成电路的功能，来支持该信息处理系统配置。密钥接口提供密钥给特性集效用来授权所期望的特性集，并且，通过信息处理系统制造商使用的各功能的处理组件制造来允许进行跟踪。例如，可以从与处理组件制造相关联的密钥服务器处下载密钥，并在特性集效用使用之后销毁该密钥。

本发明提供多个重要的技术优点。重要技术优点的一个例子是，发送给信息处理系统制造商的处理组件集成电路具有可选择性地有效的功能，这允许为信息处理系统配置按单定制处理组件。密钥保护了到集成电路的特性选择器的访问，以防止未经授权的功能的使用，并且，支持对有效后的功能的跟踪。例如，CPU 的浮点支持功能可以有选择地被有效或无效，以满足信息处理系统配置。另一个例子，CPU 的双核可以有选择地被有效或无效，芯片组具有选中的存储器和 I/O 集线器集成电路功能，通过功能选择选中 RAM 的存储容量和访问速度，以及，通过其自己的微控制器选择性地有效可以提供电视功能的显示能力。通过在处理组件内“按单定制的硅”来降低制造成本，这由信息处理系统制造商来进行有效或无效。当使用更少的设计和制造流程时，处理组件制造商可以保护各功能的知识产权价值。在信息处理系统制造流程中，信息处理系统制造商获得部分使用中的获得提高的灵活性。

附图说明

参考以下的附图，对本发明可以获得更完整的理解，其目标、特征和优点对本领域的技术人员更加明显。各附图中，同样的附图标记指示了相似或类似的元件。

图 1 是说明根据信息处理系统配置来设置信息处理系统处理组件集成电路各特性的系统的块图；

图 2 是说明根据信息处理系统配置来设置集成电路各特性的流程的流程图；

图 3 是说明响应外部输入而由集成电路逻辑设置各特性的流程图；

图 4 是说明集成电路熔丝安排的电路图；以及

图 5 说明通过集成的闪速存储器而包含带可被有选择地有效的特性集的集成电路的处理组件。

具体实施方式

信息处理系统处理组件集成电路的按单定制，在将处理组件装配进信息处理系统的装配线，为配置集成电路的特性集提供灵活性。出于本发明的目的，一个信息处理系统可以包括一种手段或多种手段的集合，这些手段均可操作于计算、分类、处理、传输、接收、重新获得、产生、交换、保存、显示、展示、检测、记录、复制、操作或使用用于商业、科学、控制或其他目的的任意形式的信息、情报或数据。例如，一个信息处理系统可以是一台个人电脑，一台网络存储设备或任意其他合适的设备，也可以在尺寸、形状、性能、功能和价格上各有不同。该信息处理系统可以包括随机存取存储器（RAM），一个或多个如中央处理器（CPU）、硬件或软件控制逻辑等的处理资源，ROM，和/或其他类型的非易失性存储器。该信息处理系统的其他组件包括一个或多个磁盘驱动器，一个或多个用于与外部设备通信的网络接口，以及诸如键盘、鼠标和视频显示器等的各类输入输出（I/O）设备。该信息处理系统还可以包括一个或多个总线，均可操作于在各种硬件组件之间传送消息。

参考图 1，这是说明根据信息处理系统配置来设置信息处理系统处理组件集成电路功能的块图。信息处理系统 10 由从处理组件供应商地点 14 提供的处理组件 12 制造而成。处理组件 12 包括一个集成电路 16，如处理器，或多个集成电路 16，如核逻辑芯片组，每个集成电路均具有执行每个处理组件的功能的多个特性。例如，处理组件包括 CPU 18，硬磁盘驱动器 20，RAM 22，芯片组 24 和显示器 26 或其他如打印机等

的外设。每个处理组件有一个或多个集成电路，每个均具有执行多个功能的结构。例如，具有多种特性的 CPU 18 处理的消息，比如多核或浮点支持电路，RAM 22 在已定义地址范围以由芯片组 24 限制的已定义访问速度保存预定总量的信息，芯片组 24 具有各个集成电路来提供存储器集线器，I/O 集线器，图形和网络，以及通过如 DVI、VGA 和电视输入等多种输入信号而连接的显示器 26。制造集成电路 16 来为每个处理组件提供多个功能，并包括允许在特定集成电路上的特性集的特性选择器，该特性集在永久性的基础上有选择地被有效或无效。例如，熔断包含在集成电路中的熔丝，以便将与每个熔丝相关联的特性变为不可访问。或者，可选地，包含在每个集成电路中的闪速存储器为该集成电路的各特性定义开/关状态，通过终结该闪速存储器的可编程性永久地设置各特性（状态）。

在处理组件供应商 14 处，用带有设为预定状态的集成电路 16 来制造处理组件 12。如果集成电路 16 使用熔丝来有选择地无效掉各特性，当将处理组件 12 发送到信息处理系统制造地点 28 时，集成电路 16 典型地将所有特性设为有效。如果集成电路 16 使用所包含的闪速存储器来设置各特性，各特性或者可以被全部有效，或者被全部无效，或者部分有效、部分无效。与特性集相关联的密钥保存在密钥数据库 30 中，通过以如互联网的网络 34 连接的密钥服务器 32 而可获得。将带有处于预定状态的集成电路特性集的处理组件 12，从处理组件供应商地点 14 发送到信息处理系统制造商地点 28。为该信息处理系统制造商提供到密钥数据库 30 的访问，以便一旦在地点 28 处理组件可为装配所获得时，能如所期望地设置被有选择地有效的各个特性。密钥数据库 30 的密钥可以防止未经授权的对集成电路特性集的改变，而且，允许被信息处理系统制造商有效的特性集的跟踪。例如，密钥数据库 30 的密钥可以独立地从处理组件 12 购买，并且被信息处理系统制造商如其所期望地应用于配置处理组件集成电路特性集。在一个实施例中，同时需要单次使用密钥和主密钥，以改变集成电路特性集。密钥可以通过模式匹配或以内建于集成电路的更高层次的安全验证逻辑，来保护特性集。每个密钥可以关联到单个特性，或者，可选地，多个密钥可以关联到多个结合到 SKU 的特性，例如在处理组件内用于如存储器

和芯片组 24 的 I/O 集线器等多个集成电路的特性。在另一实施例中，信息处理系统制造地点 28 地理上分散，例如，通过子组件在各个地点的制造并被发送到最终装配地点。在另一实施例中，在信息处理系统制造地点 28，以转发到处理组件供应商地点 14 的计费信息，来维护密钥服务器 32 和数据库 30。

在信息处理系统制造地点 28，根据由配置引擎 36 提供如按单定制的配置，将处理组件 12 装配进信息处理系统 10。配置引擎 36 将加载到处理组件 12 的集成电路 16 各特性的预设状态，与制造配置进行比较，以便确定需要对其特性集进行改变的集成电路 16。例如，要求不带浮点支持的信息处理系统配置，会产生从配置引擎 36 到密钥接口 38 的请求，请求无效掉所发送的具有这项特性的 CPU 的浮点支持。密钥接口 38 通过网络 34 从密钥服务器 32 获得密钥，并且提供该密钥给特性集效用 40。特性集效用 40 应用该密钥来访问 CPU 的特性选择器，并无效掉其浮点支持，例如通过熔断与浮点支持相关联的熔丝，然后，销毁该密钥。特性集效用 40 通过密钥接口 38 将密钥使用报告给密钥服务器 32，以便跟踪用于已装配进信息处理系统 10 里的集成电路 16 的特性集。特性集效用 40 以多种方式应用这些密钥，例如，通过操作员的手动输入，文件下载，USB 闪速存储器设备，位于插入 LPC（低引脚数目）插头的闪速设备上的单个密钥，或通过如 JTAG 端口的其他设备接口。可以在集成电路自身执行密钥验证效用的全部或部分。

参考图 2，这是说明根据信息处理系统配置来设置集成电路特性流程的流程图。在步骤 42，该流程由从与该信息处理系统的配置相关联的制造指令读取设备类型开始，前进到在步骤 44 从密钥数据库读取密钥类型。在步骤 46，对密钥和设备类型进行比较以确保匹配，否则，在步骤 48 发布错误消息。在步骤 50，从密钥数据库读取该密钥，以便初始该设备的特性设置。在步骤 52，检查该密钥的有效性，如果密钥无效，则在步骤 54 发布错误消息。如果密钥是有效的，在步骤 56 它被写到该设备，以便允许通过有效或无效掉已被有选择地有效的特性，对设备特性集的改变。在步骤 58，查询该设备以确保该密钥作为有效密钥为该设备所接收，而如果密钥无效则在步骤 60 发布错误消息。如果该设备接收该密钥为有效，该流程前进到步骤 62，对该设备编程，

例如，通过预备熔断熔丝或改变该设备闪速存储器中或为有效、或为无效的特性状态。在步骤 64，查询该设备以确保合适的编程，而如果特性设置不正确，则在步骤 66 发布错误消息。如果特性集编程正确完成，则在步骤 68 设置编程后的特性，例如，通过熔断合适的设备熔丝或者更新设备闪速存储器特性集表。在步骤 70，销毁用于编程和设置特性的该密钥，以确保对所选特性的正确跟踪。

参考图 3，这是说明集成电路操作流程的流程图。该流程从步骤 72 开始，确定该设备是否被编程，如果是，在步骤 74，允许正常设备操作，而且，该流程在步骤 76 结束。如果在步骤 72 中该设备没有被编程，该流程前进到步骤 78，检查密钥是否存在，如果没有密钥，则在步骤 80 发布错误消息。如果在步骤 78 中存在密钥，该流程前进到步骤 82，确定该密钥是否是有效的编程密钥。如果存在有效编程密钥，该流程前进到步骤 84，使编程有效，而一旦设置了特性，该流程在步骤 86 结束。如果在步骤 82，确定该密钥不是有效的编程密钥，该流程前进到步骤 88，确定该密钥是否是有效测试密钥。如果存在有效测试密钥，该流程前进到步骤 90，使所有功能对测试有效，并前进到步骤 92，测试特性。如果在步骤 88，确定该密钥不是有效的测试密钥，该流程前进到步骤 94，确定该密钥是无效的，并在步骤 96 发布错误消息。注意，该测试密钥的范围部分取决于该处理组件交货时各特性的预设状态。在发货之前，可以测试所有特性均为有效的处理组件，可是，所发送的部分特性为无效的处理组件必须测试那些随后将被设为有效的特性。

参考图 4，这是说明集成电路熔丝安排 98 的电路图，该安排为每个特性集组合提供单个熔丝 100。基于由特性集电压 102 熔断的熔丝 100，有选择地使功能 A 到功能 D 有效。熔断熔丝 100 将与相该熔丝关联的功能，从该集成电路的其他功能断开。相比之下，参考图 5，处理组件 12 具有包含可选择地被有效的特性 104 集的集成电路 16，特性 104 集通过集成闪速存储器结构实现。特性表 108 定义每个特性 104 的状态，并且，通过闪存编程和测试模块 110 而为可编程。由要求合适密钥的特性安全模块 112，管理特性表 108 通过模块 110 的可编程性。一旦各特性的状态编程入特性表 108，特性安全模块 112 永久地使闪存

编程和测试模块 110 无效，以便根据由该密钥授权的内容来确定特性集，例如通过设置闪存编程内的编程位。在正常操作期间，可以将特性位从闪存编程传递到使设备特性有效或无效的寄存器。将特性表 108 集成进集成电路 16 为特性设置提供了安全性，并为处理组件制造商在处理组件发货时提供特性初始状态的附加的灵活性。

尽管已经很详细地描述了本发明，但仍可以创造出各类改变、替换和变化而不必脱离权利要求中所述的本发明的精神和范围。

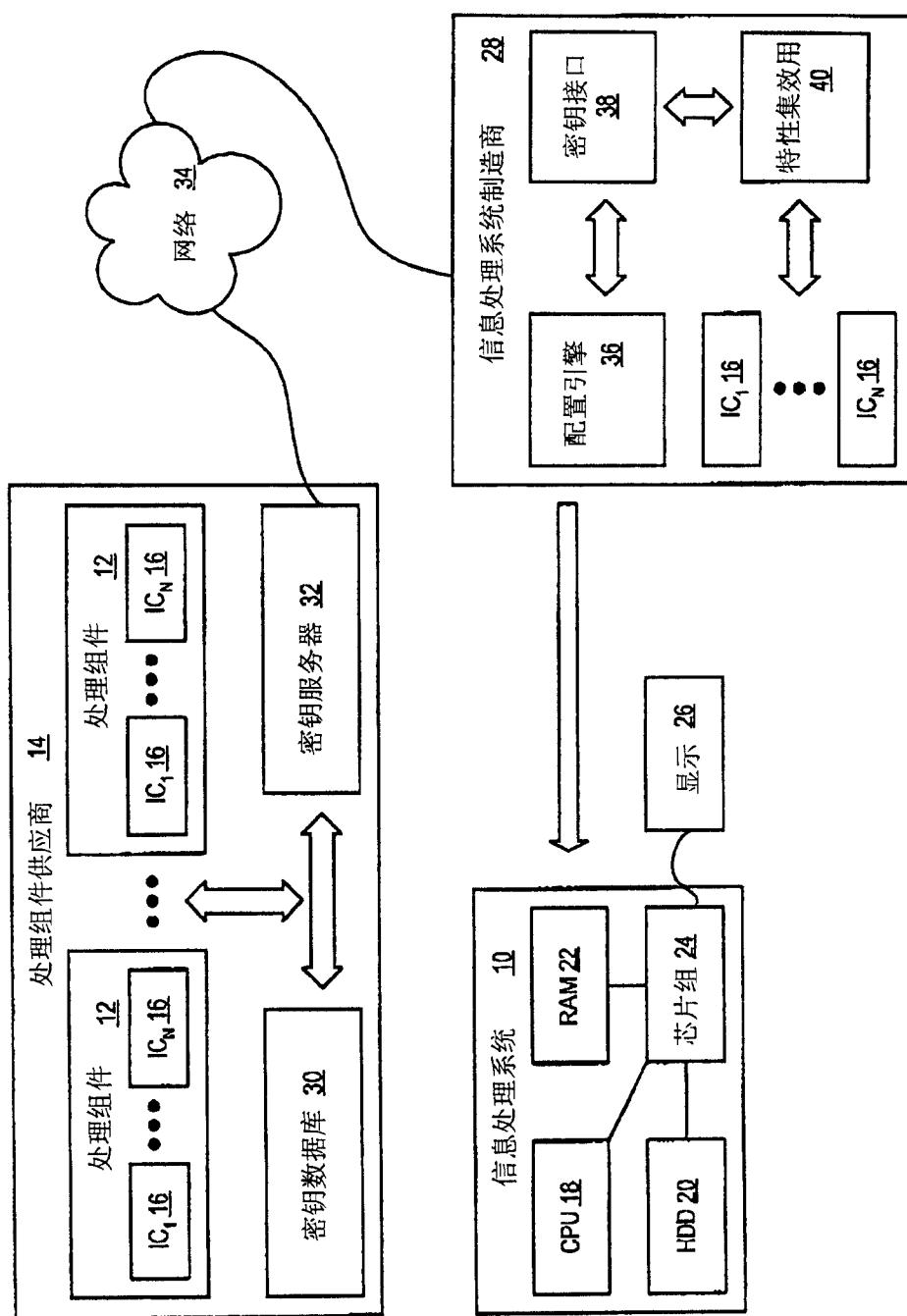


图 1

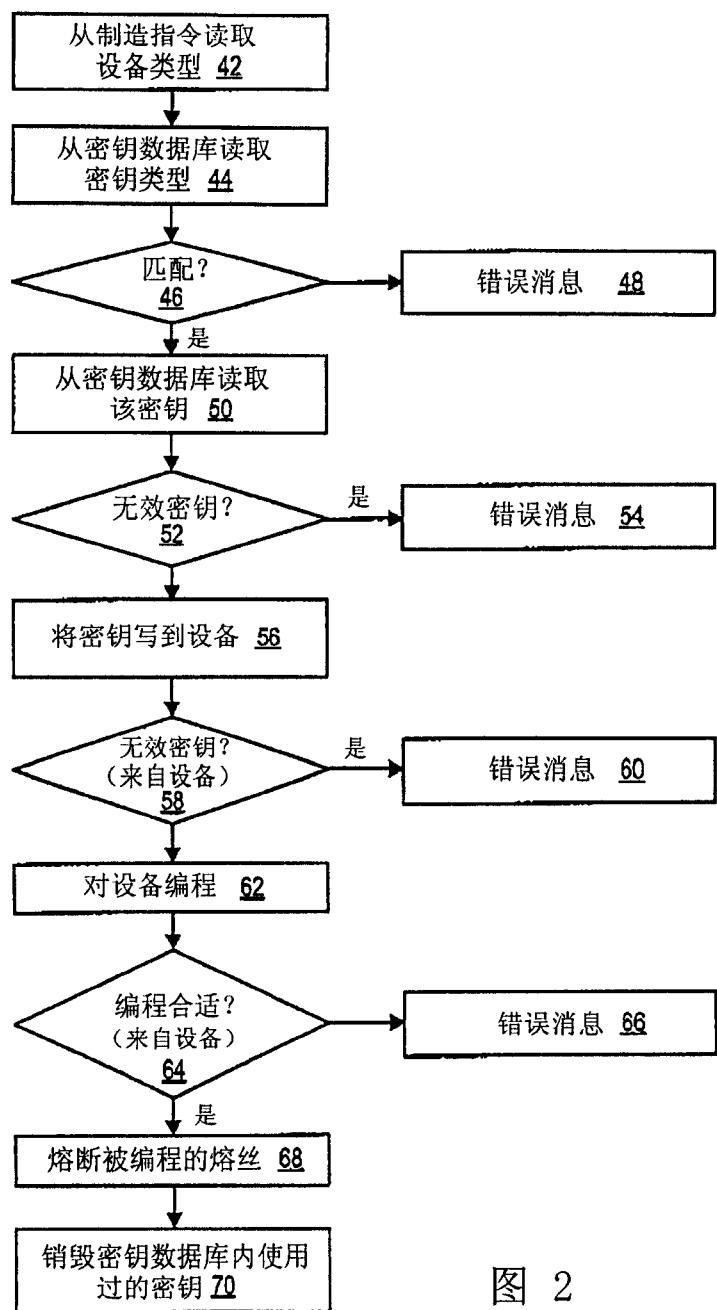


图 2

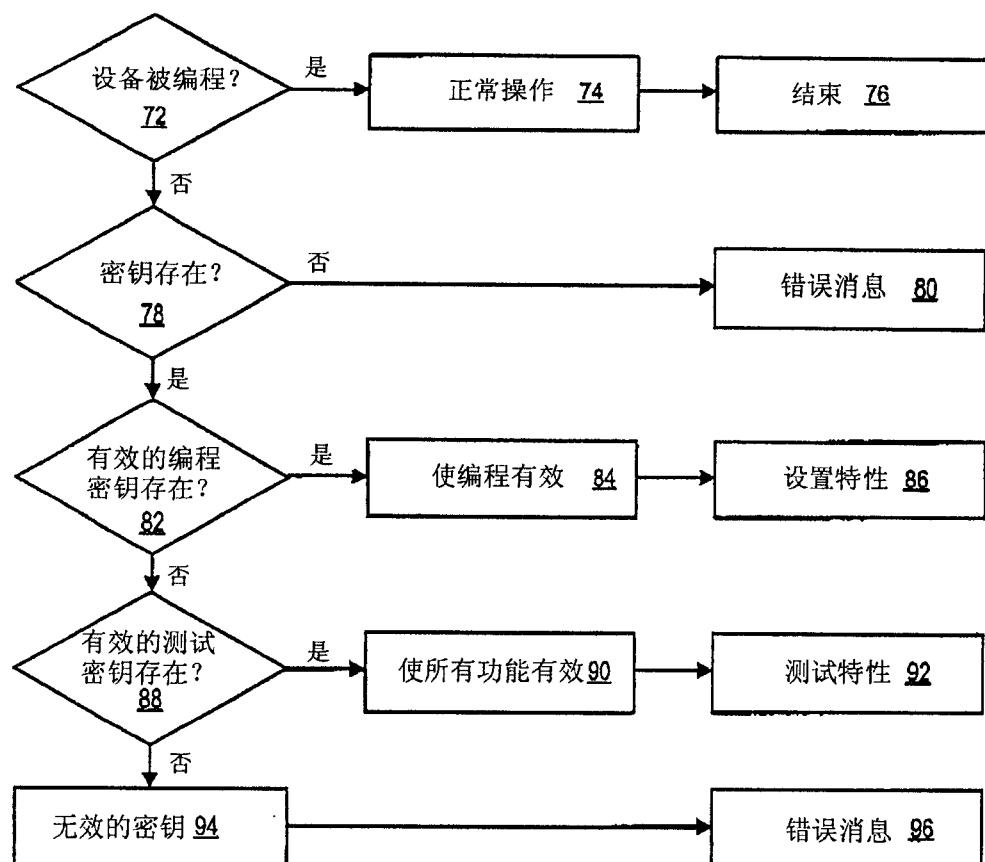


图 3

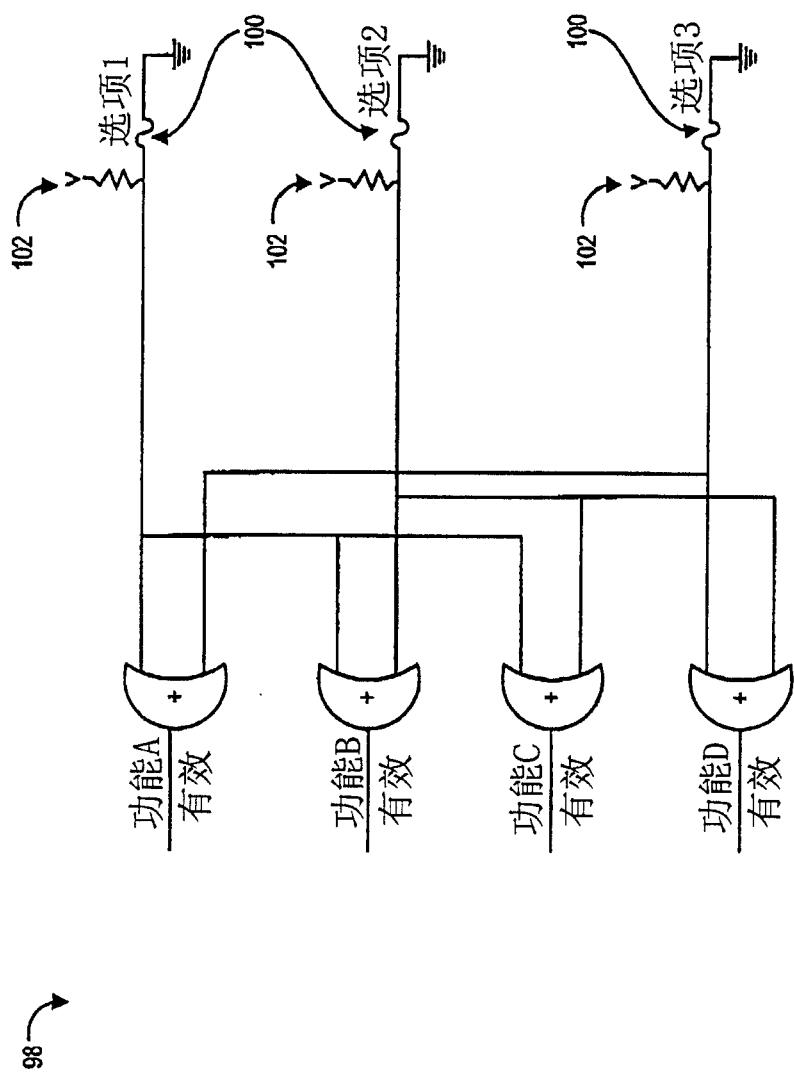


图 4

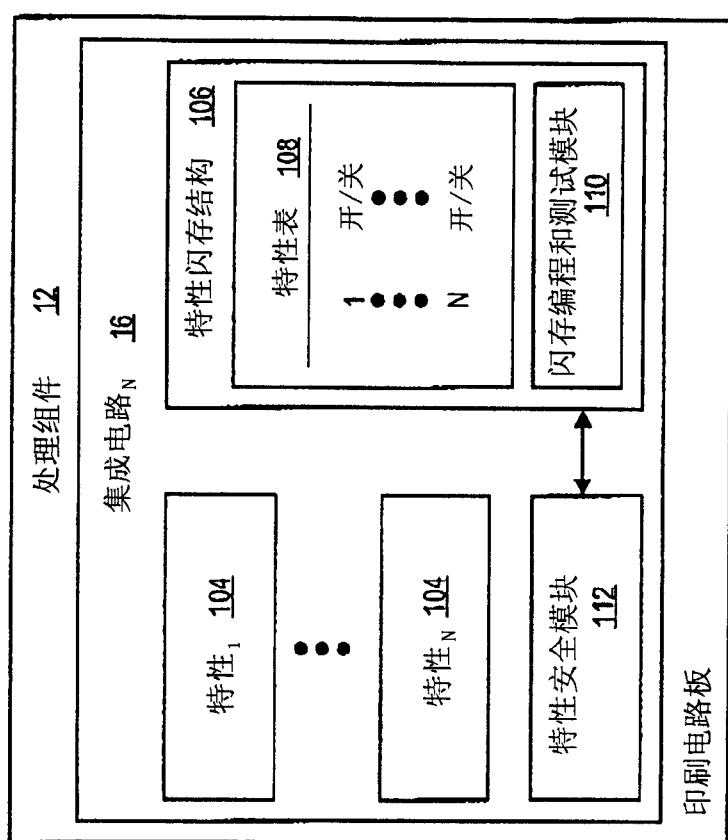


图 5