(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101772863 A
(43)申请公布日 2010.07.07

(21)申请号 200880100401.7

(22)申请日 2008.05.21

(30)优先权数据
11/828319 2007.07.25 US

(85)PCT申请进入国家阶段日
2010.01.25

(86)PCT申请的申请数据
PCT/US2008/006575 2008.05.21

(87)PCT申请的公布数据
WO2009/014574 EN 2009.01.29

(71)申请人 惠普开发有限公司
地址 美国德克萨斯州

(72)发明人 V·阮 C·V·华 M·H·阮
E·D·诺伊菲尔德

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李娜 王洪斌

(51)Int.Cl.
H01R 13/639(2006.01)

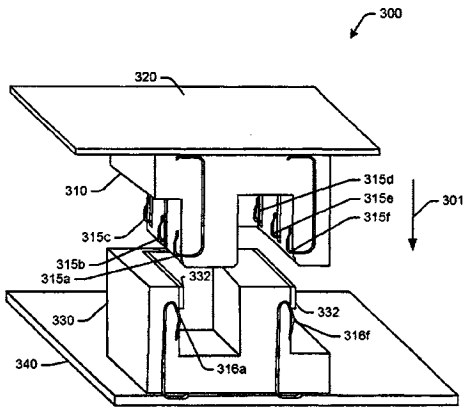
权利要求书 2 页 说明书 4 页 附图 4 页

(54)发明名称

显窃启连接器

(57)摘要

公开了一种任选地可以用在可信计算环境中的显窃启连接器(200或300)的实施例。在示例性实施例中,显窃启连接包括设有第一部件(320)的一次性匹配接合组件(310),所述一次性匹配接合组件(310)包括可折叠部(315a)。所述显窃启连接还包括设有第二部件(340)的容纳室(330),所述一次性匹配接合组件(310)装配在所述容纳室(330)中以将所述第一部件(320)物理地固定到所述第二部件(340),所述一次性匹配接合组件(310)的可折叠部(315a)在将所述一次性匹配接合组件(310)从所述容纳室(330)中移除的期间展开,从而当已经从所述第二部件(340)移除了所述第一部件(320)时提供窃启的证据。任选地,第一部件是可信平台模块(TPM)(165),并且第二部件是系统板(105)。



CN 101772863 A

1. 一种显窃启连接器 (300)，包括：

设有第一部件 (320) 的一次性匹配接合组件 (310)，所述一次性匹配接合组件 (310) 包括可折叠部 (315a)；以及

设有第二部件 (340) 的容纳室 (330)，所述一次性匹配接合组件 (310) 装配在所述容纳室 (330) 中以将所述第一部件 (320) 物理地固定到所述第二部件 (340)，所述一次性匹配接合组件 (310) 的可折叠部 (315a) 在将所述一次性匹配接合组件 (310) 从所述容纳室 (330) 中移除的期间展开，从而当已经从所述第二部件 (340) 移除了所述第一部件 (320) 时提供窃启的证据。

2. 根据权利要求 1 所述的显窃启连接器 (300)，其中在移除一次性匹配接合组件 (310) 后所述容纳室 (330) 能够重新与不同的一次性匹配接合组件 (310) 一起使用。

3. 根据权利要求 1 所述的显窃启连接器 (300)，其中在从所述容纳室 (330) 中移除所述一次性匹配接合组件 (310) 后所述一次性匹配接合组件 (310) 不能与任何容纳室 (330) 一起使用。

4. 根据权利要求 1 所述的显窃启连接器 (300)，其中在将一次性匹配接合组件 (310) 从容纳室 (330) 中移除之后所述一次性匹配接合组件 (310) 呈现出物理损坏。

5. 一种显窃启连接器 (300)，包括：

设有第一部件 (320) 的凸形块体结构 (310)，所述凸形块体结构 (310) 包括至少一个可折叠销 (315a)；

设有第二部件 (340) 的凹形块体结构 (330)，所述凹形块体结构 (330) 包括突出部 (332)；以及

其中所述凸形块体结构 (310) 装配在所述凹形块体结构 (330) 中从而将所述第一部件 (320) 物理地固定到所述第二部件 (340)，所述凸形块体结构 (310) 的该至少一个可折叠销 (315a) 接触所述凹形块体结构 (330) 的突出部 (332) 以使得所述可折叠销 (315a) 在将所述凸形块体结构 (310) 从所述凹形块体结构 (330) 移除的期间展开，从而当已经从所述第二部件 (340) 移除了所述第一部件 (320) 时提供窃启的可见证据。

6. 根据权利要求 5 所述的显窃启连接器 (300)，其中在将凸形块体结构 (320) 装配到凹形块体结构 (330) 的期间，该至少一个可折叠销 (315a) 滑过凹形块体结构 (330) 的突出部 (332)。

7. 根据权利要求 5 所述的显窃启连接器 (300)，其中该至少一个可折叠销 (315a) 嵌在凸形块体结构 (310) 中。

8. 根据权利要求 5 所述的显窃启连接器 (300)，其中该至少一个可折叠销 (315a) 是导电的并且与凹形块体结构 (330) 中的至少一个销 (316a) 形成电连接，以及其中所述电连接提供了第一部件 (320) 和第二部件 (340) 之间的通信管道以用于传输安全信息。

9. 一种显窃启连接器 (200)，包括：

销，所述销具有头部 (210) 和本体部 (214)，所述本体部 (214) 滑动通过第一部件 (240) 直到被邻接所述第一部件 (240) 的头部 (210) 所阻止；

外壳构件 (220)，所述外壳构件 (220) 具有室部 (222) 和可膨胀部 (224)，所述销的本体部 (214) 装配在第二部件 (245) 中；以及

其中所述销的本体部 (214) 滑动通过所述室部 (222) 并且滑入所述外壳构件 (220) 的

可膨胀部(224),所述销使所述可膨胀部(224)膨胀以将所述第一部件(240)物理地固定到所述第二部件(245),所述外壳构件(220)的可膨胀部(224)分裂开以便将所述销从所述外壳构件(220)中释放出来,从而当已经从所述第二部件(245)移除了所述第一部件(240)时提供窃启的可见证据。

10. 一种用在安全计算环境中的显窃启连接器(200或300),包括:

用于TPM(165)的一次性匹配接合组件;以及

用于系统板(105)的容纳室,所述一次性匹配接合组件装配在所述容纳室中以将所述TPM(165)物理地固定到所述系统板(105);以及

可破部,如果从所述系统板(105)移除了所述TPM(165)则所述可破部提供窃启的可见证据。

显窃启连接器

背景技术

[0001] 在不安全的计算机环境中，计算机应用可以访问任意可用的计算资源而很少考虑或者不考虑这些资源是否是安全的。然而存在很多理由使得希望控制对计算资源的访问。

[0002] 形成了可信计算组 (TCG)，其采用工业标准规范来增强计算环境的安全性。目标是提供基于增强的硬件和操作系统 (OS) 的可信计算平台 (TCP) 以供客户运行他们的应用。至于硬件方面的考虑，引入了可信平台模块 (TPM)，其包括存储安全信息的微控制器。TPM 是信任的根源，用以创建使得操作系统和应用能够对抗软件攻击的安全环境。TCG 要求 TPM 识别是唯一的并且物理绑定到特定平台以便其不能被容易地移除或者转移到另一平台。此外，在检查后 TPM 必须显示出物理窃启 (tampering) 的证据。

[0003] 制造具有 TPM 的平台提高了制造成本。另外，一些国家（例如俄罗斯和中国）不允许产品带有诸如 TPM 的安全装置。因此，没有 TPM 的单独平台需要被制造和跟踪（例如使用唯一的 SKU 号）以在这些市场出售，从而进一步提高了成本。

附图说明

[0004] 图 1 是示例性可信计算平台 (TCP) 的高级图示。

[0005] 图 2 是可以在 TCP 中实施的示例性显窃启 (tamper-evident) 连接器的透视图。

[0006] 图 2a 是示出为安装到 TCP 中的系统板的图 2 中示例性显窃启连接器的透视图。

[0007] 图 2b 是从系统板移除之后图 2 中的示例性显窃启连接器的透视图。

[0008] 图 3 是可以在 TCP 中实施的另一示例性显窃启连接器的透视图。

[0009] 图 3a 是示出为安装到 TCP 中的系统板的图 3 中示例性显窃启连接器的透视图。

[0010] 图 3b 是从系统板移除之后图 3 中的示例性显窃启连接器的透视图。

具体实施方式

[0011] 简要地，公开了显窃启连接器的实施例。这种设计使得 TPM 能够作为任选部件而被单独地制造，从而减少了为不同市场制造单独的系统板的成本，同时仍满足 TCG 物理绑定要求（也就是，如果 TPM 被移除的话则存在窃启的可见证据）。在移除之后，如果 TPM 已经被损坏，残缺 (malformed) 的 TPM 很可能不能在另一系统中被重新使用（或者很难重新使用），从而维持了可信软件环境 (TSE) 的完整性。然而，该移除过程不影响系统板，从而允许被授权的管理员在需要时更换系统板上的 TPM 模块。

[0012] 虽然本文描述的系统和方法有助于为运行可信软件和访问可信资源实现安全措施，但是应当注意显窃启连接器的应用并不限于计算机安全性。在熟悉了文中的教导之后显窃启连接器的其它应用对于本领域普通技术人员来说将是显而易见的。

[0013] 图 1 是示例性可信计算平台 (TCP)100 的高级图示。示例性 TCP 100 可以包括一个或多个处理器或者处理单元 110，以及系统存储器 120，诸如例如系统板 105 上的只读存储器 (ROM) 和随机存取存储器 (RAM)。也可提供其它存储器（例如本地的和 / 或远程的，固定的和 / 或可移动的，磁和 / 或光介质）。所述存储器提供对计算机可读指令，数据结构，程

序模块和用于计算平台 100 的其它数据的存储。

[0014] 要注意，计算平台 100 可以作为独立设备进行操作和 / 或可以使用到一个或多个远程资源（未示出）的逻辑连接在连网计算环境中操作。所述逻辑连接可以包括局域网 (LAN) 和 / 或广域网 (WAN)。示例性远程资源包括，但是不限于个人计算机，服务器，路由器，网络 PC，以及对等设备或者其它网络节点。远程资源可以包括对于计算平台 100 所描述的要素中的许多要素或者所有要素，诸如例如处理能力和存储器。

[0015] 计算平台 100 还可以包括一个或多个资源 130a-c。如文中所使用的，术语“资源”包括多种不同类型的设备（例如 PCIe 设备）和 / 或（例如由该设备提供的）功能中的任一种。在示例性实施例中，资源 130a-c 可以经由一个或多个实施高速 PCI (PCIe) 规范的外围部件互连 (PCI) 链接 140a-b 通信地耦合到计算平台 100。在这样的实施例中，资源 130a-c 可以经由一个或多个 PCIe 卡 145a-c 直接连接到根联合体 (root complex) 150。

[0016] 主桥和存储器控制器集线器（通常也称为根联合体 150）将各个系统部件耦合到处理单元 110。根联合体 150 是检测和初始化资源 130a-c，并且管理链接 140a-c 从而使得处理器 110 可以向资源 130a-c 进行读 / 写和 / 或以其他方式控制资源 130a-c 的子系统。

[0017] 计算平台 100 可以在受保护或可信操作环境中操作。可信操作环境是用于运行可信软件和访问可信设备的受保护的或安全的环境。可信软件是具有可靠建立的标识概念（例如指示该软件来自可信源）的软件。可信设备是可经由可信配置访问机构 (TCAM) 160 访问的设备。要注意对于每个计算平台 100（或者对于计算平台上的每个分区）可以存在单个或多个 TCAM。

[0018] 在被提供用于标准配置空间的增强配置访问机构 (ECAM)（例如图 3 中的 ECAM 340）之后图案化 (pattern) TCAM 160，所述标准配置空间由 PCIe 规范定义。类似于 ECAM，TCAM 160 也包括存储器映射区域，每总线号 1 兆字节 (MB)，基地址和总线号范围由固件报告。然而，与 ECAM 不同，TCAM 160 仅能由可信软件使用，任选地仅当由硬件（例如可信平台模块 (TPM) 165）启用时才能使用。TPM 165 提供了受保护存储，受保护功能，计算平台 100 的验证，平台完整性的测量，以及平台完整性的认证 (attestation)。TPM 165 可以被实施为只有当 / 仅当平台完整性已被认证时才使得启用 TCAM 160 以供使用的硬件信号有效 (assert)。PCIe 规范定义了 TCAM，TCAM 然后允许经由例如存储器 120 中的存储器映射地址空间来访问可信配置寄存器。

[0019] TPM 165 可以通过显窃启连接器而物理地附接到系统板 105。（例如根据 TCG 物理绑定要求）如果从系统板 105 移除了 TPM 165 则显窃启连接器提供窃启的可见证据。通过以下参考图 2-3 提供的显窃启连接器的示例性实施例的描述，将更好地理解这些以及其它特征。

[0020] 图 2 是可以在 TCP 中实施的示例性显窃启连接器的透视图。在这个实施例中，显窃启连接器被实施为机械结合铆钉 (binding rivet) 200。机械结合铆钉 200（或者简称为“铆钉 200”）可以包括具有头部 212 和本体部 214 的销 (pin) 210。铆钉 200 还可以包括具有室部 222 和可膨胀 (expandable) 部 224 的外壳构件 220。

[0021] 当在安全计算环境中使用铆钉 200 时，电连接器 230 可以邻近销 210 安装在第一部件（例如 TPM 240）上，并且第二电连接器 235 可以邻近壳构件 220 安装在第二部件（例如系统板 250）上。在示例性实施例中，第一电连接器 230 和第二电连接器 235 可以是商业

上可得到的 20 管脚（或者任何数量的管脚 (pin)）匹配电连接器。在任何情况下，电连接器 230 和 235 可以被推到一起以形成 TPM240 和系统板 250 之间的电连接，例如用于将安全信息从 TPM 240 传输到系统板 250。

[0022] 在继续之前，要注意虽然是作为分开的部件示出，但是销 210 和壳构件 220 可以被制造为具有销 210 和壳构件 220 两者的功能的单一部件。例如，可以将铆钉 200 制造成使得其可以在销 210 松散地连接到壳构件 220 的情况下被装运从而使得这些部件不太可能被放错地方或另外丢失。此外，电连接器 230 和 235 也可以集成到铆钉 200 中而不必单独提供。

[0023] 图 2a 是示出为安装到 TCP 中的系统板的图 2 中示例性显窃启连接器的透视图。在使用中，销 210 的本体部 214 可以滑动通过在 TPM 240 中形成的开口直到头部 212 邻接 TPM 240 的表面。销 210 的头部 212 用于阻止该销整个滑动通过 TPM 240。

[0024] 壳构件 220 可以装配到形成在系统板 250 中的开口 252 中。例如，当挤压壳构件 220 以装配穿过开口 252 时，壳构件 220 的可膨胀部 224 中的槽 226 使得壳构件 220 能够在尺寸上有所减小（例如具有更小的直径）。弹簧动作自然地将可膨胀部 224 在开口 252 内返回到展宽状态从而至少部分地将壳构件 220 保持在系统板 250 中。

[0025] 当销 210 的本体部 214 滑入壳构件 220 的可膨胀部 224 中时，销 210 的存在迫使壳构件 210 的可膨胀部 224 在开口 252 内进一步展宽。任选地，销 210 可以在端部更宽（或者可以包括“翼片”或者其它设备）从而增强迫使可膨胀部 224 张开。这种展宽动作物理地并且不可逆地将 TPM 240 固定到系统板 250。

[0026] 图 2b 是在从系统板移除后图 2 中的示例性显窃启连接器的透视图。一旦被连接，在不将 TPM 240 从系统板 250 移除的情况下就不能断开电连接器 230 和 235 之间的电连接。然而，为了将 TPM 240 从系统板 250 移除，外壳构件的可膨胀部必须被分裂开以将销从壳构件中释放出来，从而当已经从系统板 250 移除了 TPM 240 时提供窃启的可见证据。

[0027] 图 3 是可以在 TCP 中实施的另一示例性显窃启连接器的透视图。在这个实施例中，显窃启连接器被实施为“插头 (plug) 型”连接器 300。插头型连接器（或者简称为“插头 300”）可以包括用于第一部件（例如 TPM 320）的凸形块体结构 310 以及用于第二部件（例如系统板 340）的凹形块体结构 330。

[0028] 凸形块体结构 310 包括至少一个可折叠销（并且图 3 示出了多个可折叠销 315a-c），以及凹形块体结构 330 包括突出 (ledge) 部 332。在示例性实施例中，（一个或多个）可折叠销 315a-c 基本上是钩形或者 J 形的，使得当凸形块体结构 310 被装配到凹形块体结构 330 中时可折叠销接触突出部 332 从而物理地将 TPM 310 固定到系统板 340。

[0029] 图 3a 是示出为安装到 TCP 中的系统板的图 3 中示例性显窃启连接器的透视图。当在安全计算环境中使用插头 300 时，可折叠销 315a-c 用作电连接器，与凹形块体结构 330 中的销 335 相匹配。可替代地，可以提供分开的电连接（例如集成的或邻近的凸形和凹形块体结构）。当凸形和凹形块体结构 310 和 330 相互连接时，在 TPM 320 和系统板 340 之间形成了电连接，例如用于将安全信息从 TPM 320 传输到系统板 340。

[0030] 图 3b 是图 3 中的示例性显窃启连接器的透视图。一旦被连接，在不将 TPM320 从系统板 340 移除的情况下就不可能断开电连接。然而，为了将 TPM 320 从系统板 340 移除，由突出部 332 拉动可折叠销 315a-c 并且在将凸形块体结构 310 拉动远离凹形块体结构 330

的期间可折叠销 315a-c 展开。这样当已经从系统板 340 移除了 TPM 320 时提供窃启的可见证据。

[0031] 要注意关于上面描述的显窃启连接器的任意实施例，可以在客户场所或者在原始设计制造商 (ODM) 的制造期间由系统集成者执行 TPM 安装（初始结合过程）。对于初始结合过程来说不需要使用工具，使得显窃启连接器易于使用。

[0032] 移除之后，如果 TPM 已经被损坏，很可能不能在另一系统中重新使用（或者很难重新使用）残缺的 TPM，从而保持了可信软件环境 (TSE) 的完整性。然而，移除过程并不影响系统板，从而允许被授权的管理员在有需要时更换系统板上的 TPM 模块，例如用于维修或者更换。

[0033] 要注意提供图中所示出以及上面讨论的示例性实施例是为了说明的目的。除了文中明确陈述的特定实施例之外，考虑本文公开的说明书，其它方面和实施例对于本领域技术人员将是显而易见的。说明书和示出的实施例仅仅打算被作为示例来考虑。

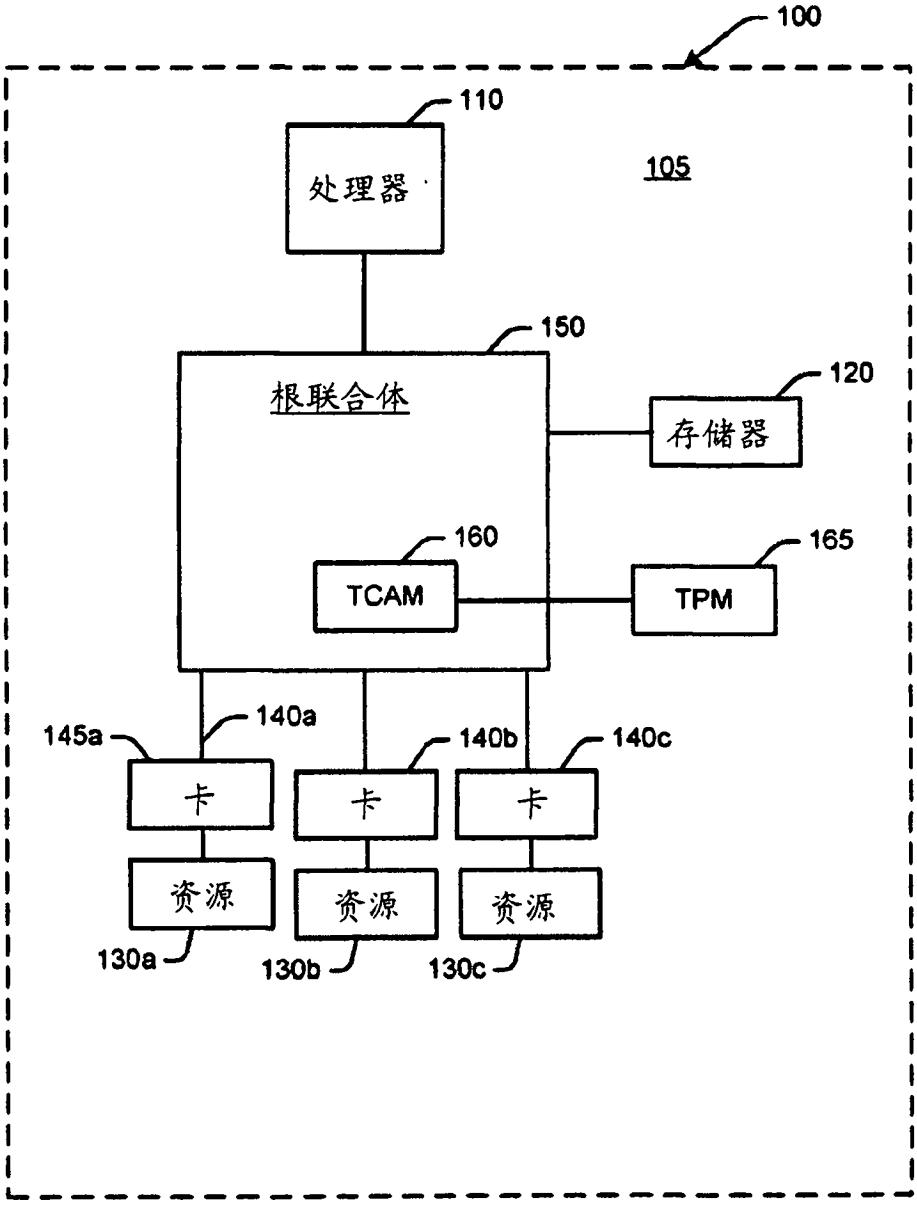

100
110
处理器
105
150
根联合体
120
存储器
160
TCAM
165
TPM
145a
140a
140b
140c
卡
卡
卡
资源
资源
资源
130a
130b
130c

图 1

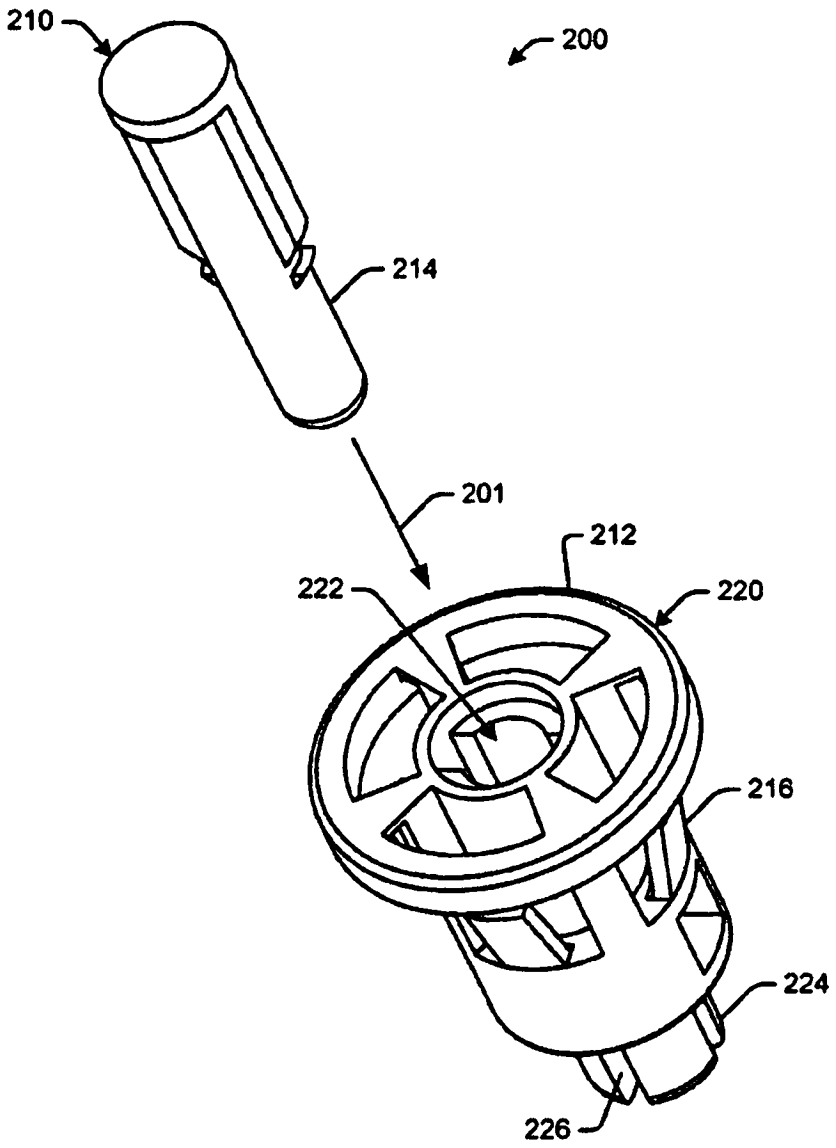

210
200
214
201
212
222
220
216
224
226

图 2

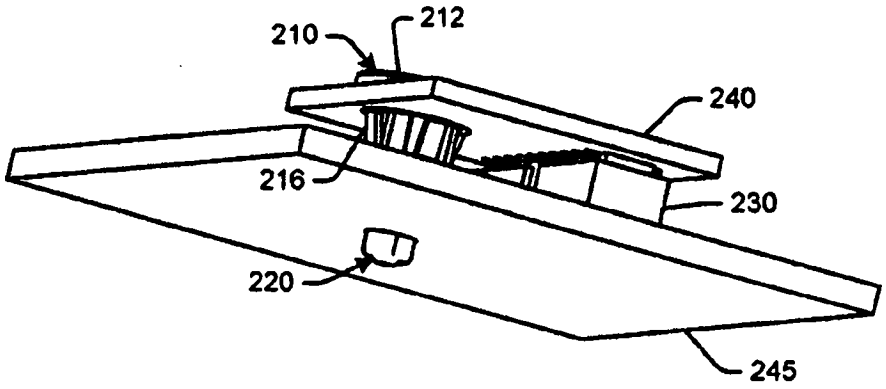

210
212
240
216
230
220
245

图 2a

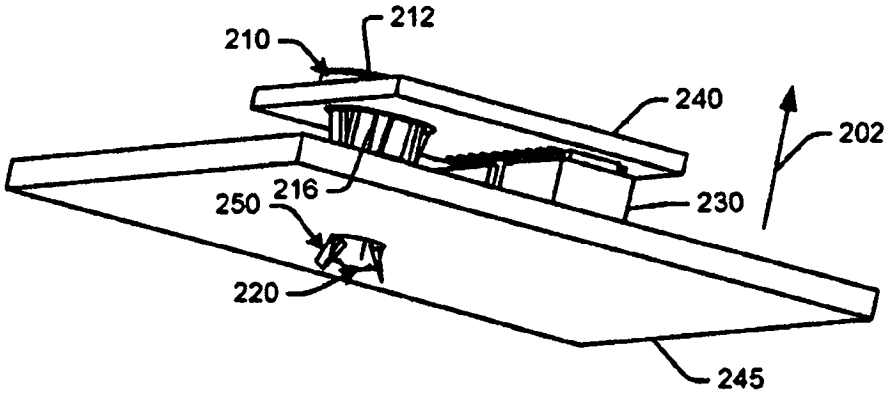

210
212
240
202
216
250
230
220
245

图 2b

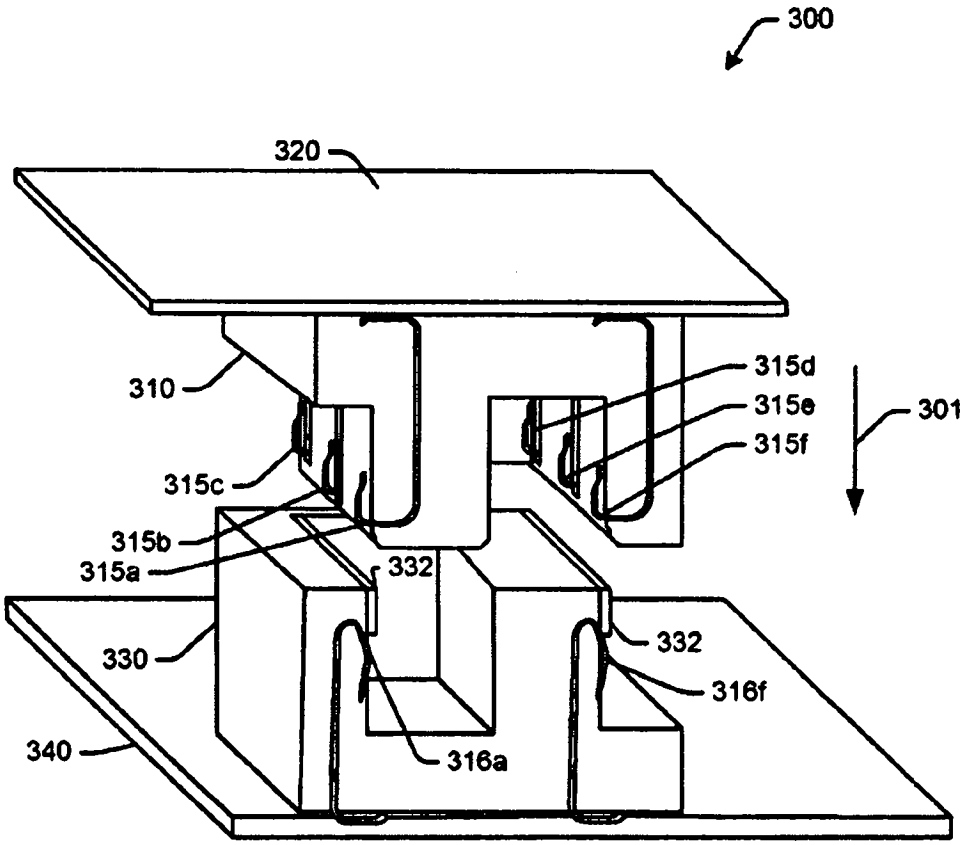

300
320
310
315d
315e
315f
301
315c
315b
315a
332
330
332
316f
340
316a

图 3

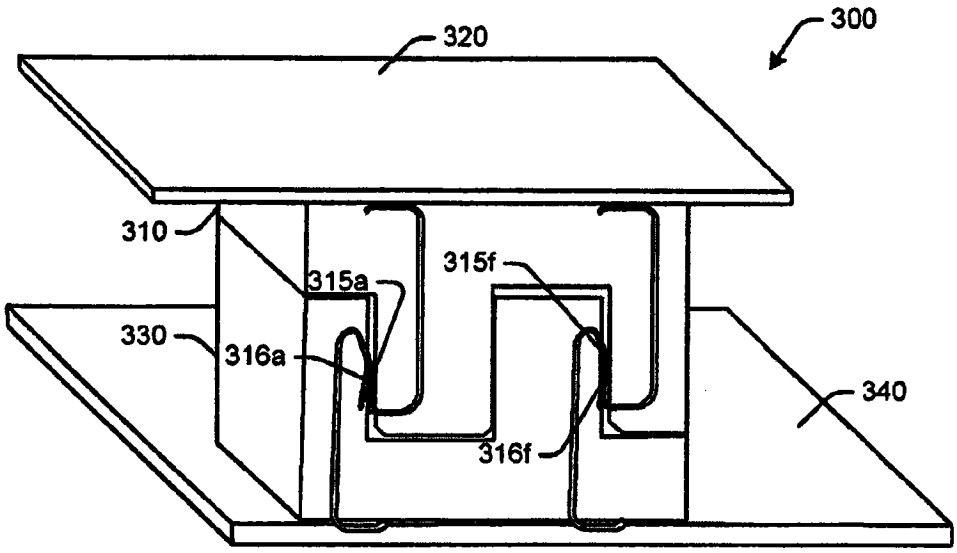

300
320
310
315a
315f
330
316a
340
316f

图 3a

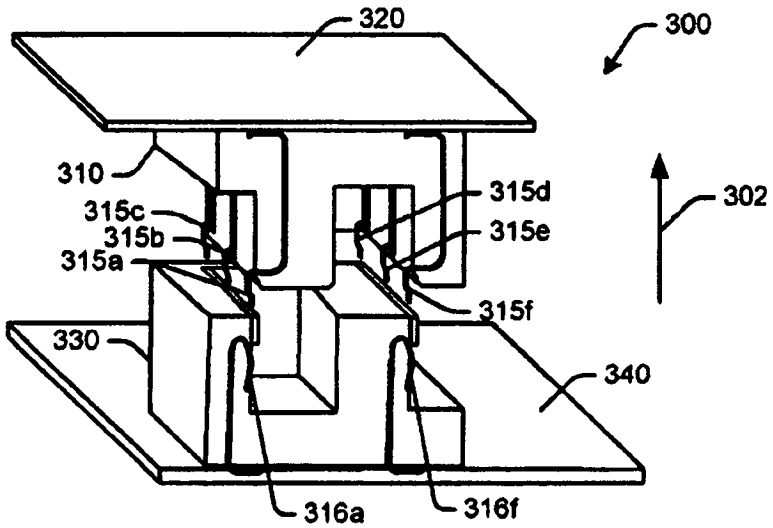

320
300
310
315c
315b
315a
315d
315e
315f
302
330
340
316a
316f

图 3b