(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108140094 B
(45)授权公告日 2022.05.13

(21)申请号 201680042518.9
(22)申请日 2016.06.20
(65)同一申请的已公布的文献号
申请公布号 CN 108140094 A
(43)申请公布日 2018.06.08
(30)优先权数据
62/194,763 2015.07.20 US
62/195,148 2015.07.21 US
62/198,201 2015.07.29 US
14/974,944 2015.12.18 US
(85)PCT国际申请进入国家阶段日
2018.01.19
(86)PCT国际申请的申请数据
PCT/US2016/038394 2016.06.20
(87)PCT国际申请的公布数据
WO2017/014887 EN 2017.01.26

(73)专利权人 英特尔公司
地址 美国加利福尼亚
(72)发明人 幸滨 P·M·帕帕占 S·查伯拉 R·拉尔 S·B·麦高恩
(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 刘瑜 王英

(51)Int.Cl.
G06F 21/60(2006.01)
G06F 13/28(2006.01)
(56)对比文件
CN 101281577 A,2008.10.08
CN 103793662 A,2014.05.14
CN 103250401 A,2013.08.14
CN 1604066 A,2005.04.06
审查员 石蒙蒙

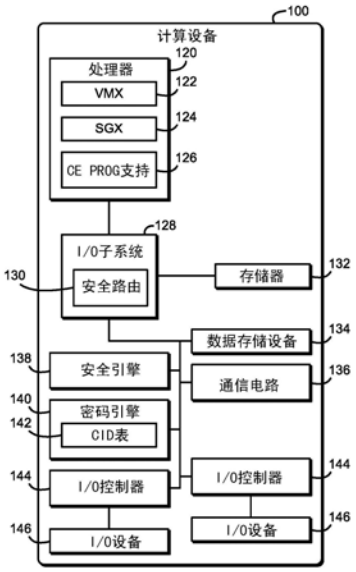
权利要求书4页 说明书14页 附图4页

(54)发明名称

用于安全可信I/O访问控制的技术

(57)摘要

用于可信I/O(TIO)的技术包括具有密码引擎和一个或多个I/O控制器的计算设备。该计算设备执行TIO核心服务,TIO核心服务具有由操作系统授予的密码引擎编程特权。TIO核心服务接收来自应用的保护DMA通道的请求。TIO核心服务请求操作系统保护DMA通道,并且作为响应,操作系统对TIO核心服务的密码引擎编程特权进行验证。响应于验证TIO核心服务的密码引擎编程特权,操作系统对密码引擎进行编程以保护DMA通道。如果特许委托确定用户已经确认对DMA通道的保护终止,则TIO核心服务可以对DMA通道解除保护。描述并要求保护其他实施例。



CN 108140094 B

1.一种用于可信I/O访问控制的计算设备,所述计算设备包括:

公共信任模块,其用于(i)执行可信I/O核心服务,其中,所述可信I/O核心服务具有由所述计算设备的操作系统授予的密码引擎编程特权,以及(ii)接收来自应用的保护与所述计算设备的I/O设备相关联的DMA通道的请求,其中,所述应用不具有所述密码引擎编程特权;

访问控制模块,其用于(i)响应于对来自所述应用的保护所述DMA通道的请求的接收,由所述操作系统接收来自所述可信I/O核心服务的保护所述DMA通道的请求,以及(ii)响应于对保护所述DMA通道的请求的接收,由所述操作系统验证所述可信I/O核心服务的所述密码引擎编程特权;以及

编程模块,其用于响应于对所述可信I/O核心服务的所述密码引擎编程特权的验证,对所述计算设备的密码引擎进行编程以保护所述DMA通道。

2.根据权利要求1所述的计算设备,还包括具有安全隔离区支持的处理器,其中,所述应用包括利用所述处理器的安全隔离区支持而建立的安全隔离区。

3.根据权利要求1所述的计算设备,其中,所述公共信任模块还用于:

响应于对所述密码引擎进行编程以保护所述DMA通道,由所述可信I/O核心服务从所述操作系统接收对所述DMA通道解除保护的请求;

响应于对所述DMA通道解除保护的请求的接收,由与所述DMA通道相关联的特许委托确定所述计算设备的用户是否已经确认对所述DMA通道的保护终止,其中,所述特许委托是由所述可信I/O核心服务建立的;以及

响应于所述用户已经确认对所述DMA通道的保护终止的确定,由所述可信I/O核心服务对所述DMA通道解除保护。

4.根据权利要求3所述的计算设备,其中,确定所述计算设备的用户是否已经确认对所述DMA通道的保护终止包括经由所述计算设备的受保护的DMA通道来接收受保护的用户输入。

5.根据权利要求4所述的计算设备,其中,经由所述受保护的DMA通道来接收所述受保护的用户输入包括经由第二DMA通道来接收所述受保护的用户输入,其中,所述第二DMA通道与对所述DMA通道解除保护的请求中的所述DMA通道不同。

6.根据权利要求3所述的计算设备,还包括具有安全隔离区支持的处理器,其中,所述特许委托包括利用所述处理器的安全隔离区支持而建立的安全隔离区。

7.根据权利要求3所述的计算设备,其中,所述访问控制模块还用于:

响应于对所述密码引擎进行编程以保护所述DMA通道,由所述操作系统确定是否对所述DMA通道解除保护;以及

响应于对所述DMA通道解除保护的确定,由所述操作系统请求所述可信I/O核心服务对所述DMA通道解除保护。

8.根据权利要求7所述的计算设备,其中,确定是否对所述DMA通道解除保护包括确定所述应用是否已经终止。

9.根据权利要求1所述的计算设备,其中:

所述公共信任模块还用于:(i)响应于对保护所述DMA通道的请求的接收,由所述可信I/O核心服务建立的密码引擎隔离区CEE生成通道加密密钥,以及(ii)由所述CEE对所述通

道加密密钥进行打包以生成经打包的编程信息;并且

接收来自所述可信I/O核心服务的保护所述DMA通道的请求包括接收来自所述可信I/O核心服务的所述经打包的编程信息。

10.根据权利要求9所述的计算设备,其中,对所述通道加密密钥进行打包包括:调用所述计算设备的处理器中的处理器指令,以生成所述经打包的编程信息。

11.根据权利要求9所述的计算设备,其中:

所述编程模块还用于:响应于对所述经打包的编程信息的接收,由所述操作系统对所述经打包的编程信息进行解包,以生成经解包的编程信息;并且

对所述密码引擎进行编程包括:响应于对所述经打包的编程信息的解包,利用所述经解包的编程信息对所述密码引擎进行编程以保护所述DMA通道。

12.根据权利要求11所述的计算设备,其中,对所述经打包的编程信息进行解包包括调用所述计算设备的处理器中的处理器指令,以生成所述经解包的编程信息。

13.一种用于可信I/O访问控制的方法,所述方法包括:

由计算设备执行可信I/O核心服务,其中,所述可信I/O核心服务具有由所述计算设备的操作系统授予的密码引擎编程特权;

由所述可信I/O核心服务接收来自应用的保护与所述计算设备的I/O设备相关联的DMA通道的请求,其中,所述应用不具有所述密码引擎编程特权;

响应于接收到来自所述应用的保护所述DMA通道的请求,由所述操作系统接收来自所述可信I/O核心服务的保护所述DMA通道的请求;

响应于接收到保护所述DMA通道的请求,由操作系统验证所述可信I/O核心服务的所述密码引擎编程特权;以及

响应于验证所述可信I/O核心服务的所述密码引擎编程特权,由所述操作系统对所述计算设备的密码引擎进行编程以保护所述DMA通道。

14.根据权利要求13所述的方法,其中,所述应用包括利用所述计算设备的处理器的安全隔离区支持而建立的安全隔离区。

15.根据权利要求13所述的方法,还包括:

响应于对所述密码引擎进行编程以保护所述DMA通道,由所述可信I/O核心服务从所述操作系统接收对所述DMA通道解除保护的请求;

响应于接收到对所述DMA通道解除保护的请求,由与所述DMA通道相关联的特许委托确定所述计算设备的用户是否已经确认对所述DMA通道的保护终止,其中,所述特许委托是由所述可信I/O核心服务建立的;以及

响应于确定所述用户已经确认对所述DMA通道的保护终止,由所述可信I/O核心服务对所述DMA通道解除保护。

16.根据权利要求15所述的方法,其中,确定所述计算设备的用户是否已经确认对所述DMA通道的保护终止包括经由所述计算设备的受保护的DMA通道来接收受保护的用户输入。

17.根据权利要求15所述的方法,还包括:

响应于对所述密码引擎进行编程以保护所述DMA通道,由所述操作系统确定是否对所述DMA通道解除保护;以及

响应于确定对所述DMA通道解除保护,由所述操作系统请求所述可信I/O核心服务对所

述DMA通道解除保护。

18.根据权利要求13所述的方法,还包括:

响应于接收到保护所述DMA通道的请求,由所述可信I/O核心服务建立的密码引擎隔离区CEE生成通道加密密钥;以及

由所述CEE对所述通道加密密钥进行打包以生成经打包的编程信息;

其中,接收来自所述可信I/O核心服务的保护所述DMA通道的请求包括接收来自所述可信I/O核心服务的所述经打包的编程信息。

19.一种用于可信I/O访问控制的计算设备,所述计算设备包括:

用于执行可信I/O核心服务的模块,其中,所述可信I/O核心服务具有由所述计算设备的操作系统授予的密码引擎编程特权;

用于由所述可信I/O核心服务接收来自应用的保护与所述计算设备的I/O设备相关联的DMA通道的请求的模块,其中,所述应用不具有所述密码引擎编程特权;

用于响应于接收到来自所述应用的保护所述DMA通道的请求而由所述操作系统接收来自所述可信I/O核心服务的保护所述DMA通道的请求的模块;

用于响应于接收到保护所述DMA通道的请求而由操作系统验证所述可信I/O核心服务的所述密码引擎编程特权的模块;以及

用于响应于验证所述可信I/O核心服务的所述密码引擎编程特权而由所述操作系统对所述计算设备的密码引擎进行编程以保护所述DMA通道的模块。

20.根据权利要求19所述的计算设备,其中,所述应用包括利用所述计算设备的处理器的安全隔离区支持而建立的安全隔离区。

21.根据权利要求19所述的计算设备,还包括:

用于响应于对所述密码引擎进行编程以保护所述DMA通道而由所述可信I/O核心服务从所述操作系统接收对所述DMA通道解除保护的请求的模块;

用于响应于接收到对所述DMA通道解除保护的请求而由与所述DMA通道相关联的特许委托确定所述计算设备的用户是否已经确认对所述DMA通道的保护终止的模块,其中,所述特许委托是由所述可信I/O核心服务建立的;以及

用于响应于确定所述用户已经确认对所述DMA通道的保护终止而由所述可信I/O核心服务对所述DMA通道解除保护的模块。

22.根据权利要求21所述的计算设备,其中,用于确定所述计算设备的用户是否已经确认对所述DMA通道的保护终止的模块包括用于经由所述计算设备的受保护的DMA通道来接收受保护的用户输入的模块。

23.根据权利要求21所述的计算设备,还包括:

用于响应于对所述密码引擎进行编程以保护所述DMA通道而由所述操作系统确定是否对所述DMA通道解除保护的模块;以及

用于响应于确定对所述DMA通道解除保护而由所述操作系统请求所述可信I/O核心服务对所述DMA通道解除保护的模块。

24.根据权利要求19所述的计算设备,还包括:

用于响应于接收到保护所述DMA通道的请求而由所述可信I/O核心服务建立的密码引擎隔离区CEE生成通道加密密钥的模块;以及

用于由所述CEE对所述通道加密密钥进行打包以生成经打包的编程信息的模块；

其中，用于接收来自所述可信I/O核心服务的保护所述DMA通道的请求的模块包括用于接收来自所述可信I/O核心服务的所述经打包的编程信息的模块。

用于安全可信I/O访问控制的技术

[0001] 相关申请的交叉引用

[0002] 本申请要求享有于2015年12月18日提交的、题为“TECHNOLOGIES FOR SECURE TRUSTED I/O ACCESS CONTROL”的美国实用专利申请序号14/974,944的优先权，该申请根据35U.S.C.§119(e)要求享有于2015年7月20日提交的、题为“CRYPTOGRAPHIC PROTECTION OF I/O DATA FOR DMA CAPABLE I/O CONTROLLERS”的美国临时专利申请序号62/194,763的优先权，要求享有于2015年7月21日提交的、题为“CRYPTOGRAPHIC PROTECTION OF I/O DATA FOR DMA CAPABLE I/O CONTROLLERS”的美国临时专利申请序号62/195,148的优先权，并且要求享有于2015年7月29日提交的、题为“SECURE I/O DEVICE MANAGEMENT FOR HARDWARE CRYPTOGRAPHY TRUSTED I/O”的美国临时专利申请序号62/198,201的优先权。

背景技术

[0003] 为了安全性，典型的计算设备可以依靠软件代理(例如，防恶意软件代理)。然而，赶上用户设备上越来越多的恶意软件攻击是很困难的。为了对抗恶意软件威胁，存在通过在可信执行环境(TEE)内运行安全敏感的软件来保护安全敏感的软件的趋势。TEE提供了即使当系统的其他部分受到损害时也可以保护秘密的无菌环境。TEE的示例包括Intel®软件防护扩展(Intel®SGX)、安全虚拟机(VM)以及融合安全引擎(CSE)。TEE虽然对于保护TEE内的秘密很有用，但是不能保护传送到安全“容器”内和/或传送到安全“容器”外的诸如用户和传感器数据的I/O数据。对于可信I/O的安全要求根据使用情况和设备而变化，并且涉及保密性、完整性、活性以及重放保护的风格和组合。

[0004] 在个人计算机平台上，保护I/O具有若干复杂性。为了保护用于给定用途的I/O，可能需要保护许多输入设备，因为平台通常具有经由不同I/O控制器连接的多个相同类别的设备，并且用户可能在使用期间动态地选择所连接的设备中的任一个。例如，当输入文本时，用户可以选择使用嵌入式键盘、USB键盘、或蓝牙(BT)键盘。用户还可以使用触摸屏来输入数据。这意味着所有键盘和触摸输入可能都需要被保护，以用于要求安全的文本输入的用途。另外，I/O设备可以由安全应用以及由常规应用使用，这意味着可能要求这些设备从受保护动态地切换到未加密(in-the-clear)，并且反之亦然。

[0005] 硬件密码可信I/O(TIO)提供硬件架构来保护用于诸如SGX安全隔离区(enclave)、虚拟机监视器(VMM)以及其他TEE的TEE的I/O数据。硬件密码TIO提供了这样的机制：在I/O设备与存储器之间的直接存储器存取(DMA)路径中使用中央密码引擎(CE)来保护I/O数据，从而在I/O数据移入或移出封装时保护该I/O数据。

附图说明

[0006] 本文描述的概念在附图中通过示例的方式而非通过限制的方式示出。为了简单且清楚地说明，图中所示的元素不一定按比例绘制。在认为适当的地方，附图标记在图中重复以指示对应或类似的元素。

[0007] 图1是用于可信I/O访问控制的计算设备的至少一个实施例的简化框图；

[0008] 图2是可以由图1的计算设备建立的环境的至少一个实施例的简化框图；

[0009] 图3是可以由图1-图2的计算设备建立的系统架构的至少一个实施例的简化框图；以及

[0010] 图4是可以由图1-图3的计算设备执行的用于可信I/O访问控制的方法的至少一个实施例的简化流程图。

具体实施方式

[0011] 虽然本公开的概念易受各种修改和替代形式影响，但是其特定实施例已经通过附图中的示例示出，并且将在本文中详述。然而，应该理解的是，并非旨在将本公开的概念限制到所公开的特定形式，而是相反，旨在覆盖与本公开和所附权利要求一致的所有修改、等同物以及替代物。

[0012] 在说明书中提及“一个实施例”、“实施例”、“说明性实施例”等指示所描述的实施例可以包括特定特征、结构或特性，但是每个实施例可以必须或可以不一定包括该特定特征、结构或特性。此外，这种短语不一定指代相同的实施例。此外，当结合实施例描述特定特征、结构或特性时，认为结合无论是否明确描述的其他实施例来实现这样的特征、结构或特性是在本领域技术人员的知识范围内的。另外，应该认识到，包括在“A、B以及C中的至少一个”形式的列表中的项目可以表示(A)；(B)；(C)；(A和B)；(A和C)；(B和C)；或(A、B以及C)。类似地，以“A、B、或C中的至少一个”形式列出的项目可以表示(A)；(B)；(C)；(A和B)；(A和C)；(B和C)；或(A、B以及C)。

[0013] 所公开的实施例在一些情况下可以以硬件、固件、软件、或其任何组合来实现。所公开的实施例还可以被实现为由一个或多个暂时性或非暂时性机器可读(例如，计算机可读)存储介质携带或存储的指令，其可以由一个或多个处理器读取并执行。机器可读存储介质可以体现为用于存储或传输机器可读形式的信息的任何存储设备、机制、或其他物理结构(例如，易失性或非易失性存储器、媒体盘、或其他介质设备)。

[0014] 在附图中，可以以特定的布置和/或排序来示出一些结构或方法特征。然而，应该认识到，可以不需要这样的特定布置和/或排序。而是，在一些实施例中，这样的特征可以以不同于说明性的图中所示的方式和/或次序来布置。另外，在特定的图中包括结构或方法特征并不意味着暗示在所有实施例中都需要这样的特征，并且在一些实施例中，可以不包括这些特征或者这些特征可以与其他特征组合。

[0015] 现在参考图1，在说明性实施例中，用于安全I/O编程访问控制的计算设备100除了其他组件之外包括处理器120、主存储器132、硬件密码引擎140以及与一个或多个I/O设备146通信的一个或多个I/O控制器144。在使用中，密码引擎140提供对经由直接存储器存取(DMA)事务在I/O控制器144与存储器132之间传送的数据的即时(on-the-fly)加密和解密。每个DMA事务被标记有通道ID(CID)，其表示与特定I/O设备146或I/O设备146的集合相关联的数据流。密码引擎140使用CID来可靠地识别必须受到保护的事务，取回对应的加密密钥，并对DMA数据执行适当的密码操作。计算设备100建立两个独立的信任域：操作系统(和/或VMM)以及基于安全隔离区的TIO堆栈。基于安全隔离区的TIO堆栈的组件可以使用安全隔离区证明而彼此信任。然而，操作系统和基于安全隔离区的TIO堆栈可以不彼此信任；例如，操作系统可以不对已加密的I/O数据进行解密，并且TIO堆栈可以不对I/O设备146进行完全控

制。特许TIO核心服务受操作系统和基于安全隔离区的TIO堆栈两者信任。在使用中，如下面进一步描述的，安全应用隔离区可以请求TIO核心服务对DMA通道进行加密，并且作为响应，TIO核心服务向操作系统提交请求以保护DMA通道。在一些实施例中，该请求可以指定特许委托由TIO核心服务托管，这可以确定用户是否已经确认安全TIO会话已经终止。

[0016] 因此，计算设备100允许TIO核心服务代表安全应用来保护I/O设备146，同时还防止拒绝服务(DoS)攻击，例如，通过防止恶意安全隔离区拒绝释放已加密的I/O设备146。另外，即使原始安全应用崩溃，计算设备100也可以保护用户输入，同时仍允许操作系统回收已加密的设备。此外，计算设备100可以通过仅要求有限数量的模块(例如，由TIO核心服务托管的安全隔离区)受操作系统信任，而不是要求大量的模块被列入白名单或以其他方式受信任(例如，不要求计算设备100的每个安全隔离区、可信应用、可信设备驱动程序、和/或其他可信执行环境都受信任)来提供灵活的安全性。

[0017] 计算设备100可以体现为能够执行本文描述的功能的任何类型的计算或计算机设备，包括但不限于计算机、台式计算机、工作站、服务器、膝上型计算机、笔记本计算机、平板计算机、移动计算设备、可穿戴计算设备、网络器具、web器具、分布式计算系统、基于处理器的系统、和/或消费者电子设备。如图1所示，计算设备100说明性地包括处理器120、输入/输出子系统128、存储器132、数据存储设备134以及通信电路136。当然，在其他实施例中，计算设备100可以包括其他或附加组件，例如，在台式计算机中常见地发现的那些组件(例如，各种输入/输出设备)。另外，在一些实施例中，说明性组件中的一个或多个组件可以并入另一组件，或以其他方式形成另一组件的一部分。例如，在一些实施例中，存储器132或其部分可以并入处理器120中。

[0018] 处理器120可以体现为能够执行本文描述的功能的任何类型的处理器。处理器120可以体现为单核或多核处理器、数字信号处理器、微控制器、或者其他处理器或处理/控制电路。如所示出的，处理器120可以包括硬件虚拟化支持122、安全隔离区(enclave)支持124以及密码引擎编程支持126。

[0019] 硬件虚拟化支持122支持计算设备100对操作系统、应用以及其他软件的虚拟化执行。硬件虚拟化支持122可以通过提供以下两种执行模式来包括虚拟机扩展(VMX)支持：VMX根模式和VMX非根模式。VMX根模式允许执行软件对计算设备100及其硬件资源具有广泛的控制。相反地，管理程序、虚拟机监视器(VMM)、或主机操作系统(OS)可以在VMX根模式下执行。VMX非根模式限制对特定硬件指令的存取，同时仍然实现处理器120的普通环/特权系统。一个或多个客体OS可以在VMX非根模式下执行。这些客体OS可以在环零中执行，类似于不进行虚拟化地执行。硬件虚拟化支持122还可以支持扩展页表(EPT)，其可以体现为硬件辅助的第二级页面地址转换。硬件虚拟化支持122可以体现为例如Intel®VT-x技术。

[0020] 安全隔离区支持124允许处理器120建立被称为安全隔离区的可信执行环境，其中执行代码可以被测量、验证和/或以其他方式确定为是可信的。另外，可以对包括在安全隔离区中的代码和数据进行加密，或以其他方式保护其免于被在安全隔离区之外执行的代码存取。例如，包括在安全隔离区中的代码和数据可以在被执行时或者在被存储于处理器120的某个受保护的高速缓存存储器中时由处理器120的硬件保护机制进行保护。包括在安全隔离区中的代码和数据可以在存储于共享高速缓存或主存储器132中时被加密。安全隔离区支持124可以体现为允许处理器120在存储器132中建立一个或多个安全隔离区的一组处

理器指令扩展。例如，安全隔离区支持124可以体现为Intel®软件防护扩展(SGX)技术。

[0021] 密码引擎编程支持126允许处理器120对密码引擎140编程以提供对I/O数据的密码保护。特别地，处理器120可以启用或禁用某些I/O通道的加密，并且可以将加密密钥安全地提供给密码引擎140。密码引擎编程支持126可以体现为一个或多个专用处理器指令(例如，指令EBINDTIO、UNWRAP、或其他指令)和相关联的硬件、伪代码、固件或处理器120的其他组件。处理器120的密码引擎编程支持126可以允许受信任的软件对密码引擎140进行编程，同时防止不可信软件对密码引擎140进行编程。

[0022] 存储器132可以体现为能够执行本文描述的功能的任何类型的易失性或非易失性存储器或数据存储装置。在操作中，存储器132可以存储在计算设备100的操作期间使用的各种数据和软件，例如，操作系统、应用、程序、库以及驱动程序。存储器132经由I/O子系统128可通信地耦合到处理器120，I/O子系统128可以体现为用于促进与处理器120、存储器132以及计算设备100的其他组件的输入/输出操作的电路和/或组件。例如，I/O子系统128可以体现为或以其他方式包括存储器控制器中心、输入/输出控制中心、平台控制器中心、集成控制电路、固件设备、通信链路(即，点对点链路、总线链路、电线、电缆、光导、印刷电路板迹线等)和/或用于促进输入/输出操作的其他组件和子系统。I/O子系统128还可以包括安全路由支持130。安全路由支持130包括硬件支持，用于确保在流氓软件的影响下I/O数据无法在结构128中误传。安全路由支持130可以与密码引擎140一起用于提供对I/O数据的密码保护。在一些实施例中，I/O子系统128可以形成片上系统(SoC)的一部分，并且与处理器120、存储器132以及计算设备100的其他组件一起并入到单个集成电路芯片上。

[0023] 数据存储设备134可以体现为被配置用于短期或长期存储数据的任何类型的设备或多个设备，例如，存储器设备和电路、存储器卡、硬盘驱动器、固态驱动器、或其他数据存储设备。在一些实施例中，数据存储设备134可以用于存储一个或多个安全隔离区的内容。安全隔离区的内容在由数据存储设备134存储时可以被加密以防止未经授权的存取。

[0024] 计算设备100的通信电路136可以体现为能够通过网络实现计算设备100与其他远程设备之间的通信的任何通信电路、设备、或其集合。通信电路136可以被配置为使用任何一种或多种通信技术(例如，有线或无线通信)和相关联的协议(例如，以太网、蓝牙®、Wi-Fi®、WiMAX等)来实现这种通信。

[0025] 在一些实施例中，计算设备100可以包括安全引擎138，该安全引擎138可以体现为能够向计算设备100提供安全相关的服务的任何(多个)硬件组件或电路。特别地，安全引擎138可以包括能够独立且安全地从处理器120执行固件和/或其他代码的微处理器、微控制器、或其他嵌入式控制器。因此，安全引擎138可以用于建立与由处理器120执行的代码分离的可信执行环境。安全引擎138可以通过诸如主机嵌入式控制器接口(HECI)的专用总线与处理器120和/或计算设备100的其他组件进行通信。安全引擎138还可以提供对计算设备100的远程配置、控制、或管理。在说明性实施例中，安全引擎138体现为并入计算设备100的片上系统(SoC)中的融合安全和管理性引擎(CSME)。在一些实施例中，安全引擎138可以体现为管理性引擎、带外处理器、可信平台模块(TPM)、或者其他安全引擎设备或设备集合。此外，在一些实施例中，安全引擎138还能够独立于计算设备100的状态(例如，独立于主处理器120的状态)使用通信电路136或专用通信电路进行通信，也被称为“带外”通信。

[0026] 密码引擎140可以体现为能够执行本文描述的功能的任何微控制器、微处理器、功

能块、逻辑、或者其他电路或电路集合。密码引擎140可以在对存储器132进行的一个或多个直接存储器存取(DMA)操作中加密和/或解密由I/O控制器144读取或写入的I/O数据。密码引擎140包括内部通道标识符(CID)表142，密码引擎140使用该表来动态地识别要保护的(多个)DMA通道。CID表142可以由受信任的软件来控制和/或编程，例如，使用处理器120的密码引擎编程支持126。CID表142的加密密钥和/或其他秘密信息不可用于不可信软件。在一些实施例中，密码引擎140可以与I/O子系统128和/或处理器120一起并入计算设备100的片上系统(SoC)中。

[0027] 类似地，I/O控制器144可以体现为能够执行本文描述的功能的任何嵌入式控制器、微控制器、微处理器、功能块、逻辑、或者其他电路或电路集合。在一些实施例中，I/O控制器144中的一个或多个可以嵌入到计算设备100的另一组件中，例如，I/O子系统128和/或处理器120。另外或可替代地，I/O控制器144中的一个或多个可以经由诸如PCI快速(PCIe)或其他I/O连接的扩展总线连接到I/O子系统128和/或处理器120。如下面进一步描述的，I/O控制器144例如通过外围通信总线(例如，USB、蓝牙等)与一个或多个I/O设备146进行通信。I/O设备146可以体现为任何I/O设备，例如，人机接口设备、键盘、鼠标、触摸屏、麦克风、照相机以及其他输入设备，以及显示器和其他输出设备。如上面描述的，使用被称为通道标识符(CID)的标识符来唯一地标识I/O控制器144和相关联的DMA通道。每个I/O控制器144可以用每个DMA事务断言适当的CID(例如，作为事务层分组(TLP)前缀的一部分)，以唯一地识别DMA事务的源并提供活性保护。CID还实现I/O与不同的设备146的隔离。

[0028] 在使用中，密码引擎140可以探查由I/O控制器144生成的针对存储器132的所有DMA事务。对于去往或来自能够参与可信I/O的设备146的每个事务，密码引擎140参考CID表142以在CID表142中找到对应于DMA通道的CID。匹配指示通道当前受到保护，并且密码引擎140应该使用与该通道相关联的通道密钥来保护写入存储器132的数据和/或从存储器132读取的数据(取决于通道的方向)。

[0029] 现在参照图2，在说明性实施例中，计算设备100在操作期间建立环境200。说明性环境200包括公共信任模块202、访问控制模块204以及编程模块206。环境200的各种模块可以体现为硬件、固件、微代码、软件或其组合。因此，在一些实施例中，环境200的模块中的一个或多个模块可以体现为电路或电子设备的集合(例如，公共信任电路202、访问控制电路204、和/或编程电路206)。应当意识到，在这样的实施例中，公共信任电路202、访问控制电路204、和/或编程电路206中的一个或多个可以形成处理器120、I/O子系统128、密码引擎140、和/或计算设备100的其他组件中的一个或多个的一部分。另外，在一些实施例中，说明性模块中的一个或多个可以形成另一模块的一部分，和/或说明性模块中的一个或多个可以彼此独立。

[0030] 公共信任模块202被配置为执行可信I/O核心服务。可信I/O核心服务具有由计算设备100的操作系统授予的密码引擎编程特权。公共信任模块202还被配置为接收来自应用的保护与I/O设备146相关联的DMA通道的请求。应用不具有密码引擎编程特权。在一些实施例中，公共信任模块202还可以被配置为由可信I/O核心服务从操作系统接收对DMA通道解除保护的请求，以由与DMA通道相关联的特许委托确定计算设备100的用户是否已经确认对DMA通道的保护终止，并且如果用户确认终止，则由可信I/O核心服务对DMA通道解除保护。特许委托由可信I/O核心服务建立。公共信任模块202还被配置为响应于接收到保护DMA通

道的请求，由密码引擎隔离区(CEE)生成通道加密密钥。CEE由可信I/O核心服务建立并且使用处理器120的安全隔离区支持124来保护。公共信任模块202还可以被配置为由CEE对通道加密密钥进行打包以生成经打包的编程信息，例如，通过执行处理器120的EBINDTIO指令。

[0031] 访问控制模块204被配置为响应于可信I/O核心服务接收到来自应用的请求，由操作系统接收来自可信I/O核心服务的保护DMA通道的请求。访问控制模块204还被配置为响应于接收到保护DMA通道的请求，由操作系统验证可信I/O核心服务的密码引擎编程特权。在一些实施例中，访问控制模块204还可以被配置为由操作系统确定是否对DMA解除保护，并请求可信I/O核心服务对DMA通道解除保护。

[0032] 编程模块206被配置为响应于验证可信I/O核心服务的密码引擎编程特权而对密码引擎140进行编程以保护DMA通道。编程模块206还可以被配置为由操作系统对经打包的编程信息进行解包，以生成经解包的编程信息。编程模块206可以被配置为对经打包的编程信息进行解包，并且将经解包的编程信息编程到密码引擎140，例如，通过执行处理器120的UNWRAP指令。

[0033] 现在参照图3，示出了可以由计算设备100建立的系统架构图300。该系统架构包括可信I/O(TIO)核心服务302，其可以体现为应用、服务器、守护进程、或计算设备100的其他用户级进程。如下面进一步描述的，TIO核心服务302具有由操作系统316识别的密码引擎编程特权，并且因此被允许控制密码引擎140。在允许通过指示内核模式驱动程序(例如，密码引擎驱动程序(CED)318)对密码引擎140进行编程来对密码引擎140进行编程的意义上而言，TIO核心服务302可以体现为特许进程。在说明性实施例中，TIO核心服务302托管继承TIO核心服务302的特权的若干安全隔离区。这些安全隔离区中的每一个可以体现为受处理器120的安全隔离区支持124保护的用户级代码(例如，环3代码)。特别地，TIO核心服务302建立密码引擎隔离区(CEE)304、一个或多个特许设备驱动程序隔离区(DDE)306以及一个或多个特许委托308。

[0034] CEE 304生成、维护与一个或多个DMA通道相关联的加密密钥，或以其他方式具有对该加密密钥的访问权。CEE 304使用处理器120的密码引擎编程支持126利用通道加密密钥对密码引擎140进行编程。例如，CEE 304可以执行诸如EBINDTIO的一个或多个专用处理器指令，以准备二进制数据，该二进制数据包括经打包的通道编程信息，其包括可以用于对密码引擎140进行编程的经打包的加密密钥。特许DDE 306中的每一个可以体现为管理特定I/O设备146或特定类的I/O设备146的安全隔离区，类似于不可信的设备驱动程序。例如，在一些实施例中，HID DDE 306可以解析人机接口设备(HID)报告。如下面进一步描述的，特许委托308中的每一个可以体现为特许DDE 306，其被授权代表另一软件组件来确定对特定DMA通道解除保护是否安全。在一些实施例中，TIO核心服务302还可以建立用于对计算设备100的I/O设备146进行枚举、证明以及验证的附加安全隔离区，例如，平台枚举器隔离区和/或一个或多个安全总线枚举器。如上面描述的，TIO核心服务302及其组件(例如，CEE 304、特许DDE 306、和/或委托308)受计算设备100的操作系统316信任，并且例如可以由操作系统316的供应商提供或以其他方式验证。

[0035] 系统架构还可以包括一个或多个非特许应用310和相关联的应用隔离区312，以及一个或多个非特许DDE 314。非特许应用隔离区312和/或非特许DDE 314不被准许对密码引擎140进行编程或以其他方式直接访问CED 318。相反，非特许应用隔离区312和/或非特许

DDE 314可以请求TIO核心服务302建立可以用于安全I/O与相关联的I/O设备146的一个或多个安全DMA通道。如下面进一步描述的，当请求对DMA通道进行加密时，非特许应用隔离区312和/或非特许DDE 314可以被要求指定特许委托308。相比之下，由TIO核心服务302(包括委托308本身)建立的特许DDE 306被允许对DMA通道进行加密而无需指定委托308。

[0036] 系统架构还包括操作系统316和密码引擎驱动程序(CED)318。操作系统316建立与计算设备100的可信I/O组件分离的信任域。例如，操作系统316可以不能访问受安全隔离区支持124保护的安全隔离区(例如，CEE304、特许DDE 306、委托308、应用隔离区312、和/或非特许DDE 314)的安全内部状态。CED 318可以体现为计算设备100的内核模块、内核进程、或其他内核模式代码(例如，环0代码)。CED 318将经打包的编程信息提供给解包引擎320，解包引擎320可以对编程信息进行解包和验证，并且如果得到验证，则将通道编程信息编程到密码引擎140。CED 318可以限制对解包引擎320的访问，例如，通过验证对经打包的编程信息进行解包的请求源自TIO核心服务302或计算设备100的其他特许组件。在说明性实施例中，解包引擎320体现为处理器120的硬件和/或微代码资源。为了访问解包引擎320，CED 318可以调用处理器120的一个或多个专用的、内核级的处理器指令，例如，UNWRAP指令。在一些实施例中，解包引擎320的功能可以由密码引擎140和/或计算设备100的其他组件来执行。

[0037] 说明性实施例公开了使用基于安全隔离区的可信执行环境(TEE)的硬件密码TIO，例如，与基于VMM的TEE相比。应该理解，虽然说明性实施例描述了基于安全隔离区的TIO实施例，但是本公开也适用于其中两个或更多个信任域共存但不彼此信任或者没有足够的信息来代表彼此进行行动(例如，Microsoft®的VTIO和/或VSM)的实施例。

[0038] 现在参考图4，在使用中，计算设备100可以执行用于对密码引擎140进行安全访问控制的方法400。方法400开始于框402，其中计算设备100使TIO核心服务302安装有一个或多个操作系统316特权。特别地，TIO核心服务302安装有访问CED 318或者以其他方式控制密码引擎140的编程的特权。例如，TIO核心服务302可以体现为具有基于角色的特权的操作系统316进程，该基于角色的特权可以被由TIO核心服务302托管的任何安全隔离区继承。与TIO核心服务302相关联的特权可以在安装时由系统管理员(对于Microsoft®Windows™操作系统316)、由根用户(对于Linux®操作系统316)、或由另一管理角色来分配。与TIO核心服务302相关联的特权可以体现为特定用户和/或特定组中的成员资格。例如，在基于Linux的操作系统316上，在安装TIO核心服务302期间，可以创建特殊的组(例如，“sgxio_核心”)和该组中的用户(例如，具有相同名称“sgxio_核心”)。CED 318可以创建一个或多个设备节点以接收系统调用(例如，IOCTL)，并且可以在每个设备节点上设置权限以要求相关联的组中的成员资格。例如，可以创建设备节点“/dev/sgxio_核心”，将所有权设置为用户“根”和组“sgxio_核心”，以及将权限设置为“rw-rw----”(用户和组可读取/可写入)，这仅允许根和“sgxio_核心”组的成员发送IOCTL到CED 318。

[0039] 在框404中，计算设备100利用相关联的操作系统316特权来执行TIO核心服务302。例如，如上面描述的，计算设备100可以执行要在组“sgxio_核心”中的用户账户“sgxio_核心”中运行的TIO核心服务302进程。如上面描述的，在被执行时，TIO核心服务302可以创建或以其他方式托管一个或多个安全隔离区，例如，CEE 304、一个或多个特许DDE 306、和/或

一个或多个特许委托308,其各自继承TIO核心服务302的一个或多个操作系统316特权。例如,安全隔离区中的每一个也可以在如上面描述的用户账户“sgxio_核心”中执行。

[0040] 在框406中,诸如应用隔离区312和/或DDE 314的非特许软件向TIO核心服务302请求与I/O设备146或一类I/O设备146相关联的已加密的DMA通道。例如,应用隔离区312可以请求来自计算设备100的一个或多个键盘146的安全键盘输入。非特许软件可能不具有访问CED 318或以其他方式控制密码引擎140的编程所要求的特权。例如,非特许应用隔离区312可以在普通用户账户中执行,该普通用户账户未包括在“sgxio_核心”组中,并且因此不具有将IOCTL发送到CED 318的能力。

[0041] 在一些实施例中,在框408中,请求可以指定特许委托308。如下面进一步描述的,每个特许委托308可以安全地确定用户是否已经确认TIO会话的终止(即,确认对DMA通道的保护将被终止)。每个特许委托308由TIO核心服务302托管,并且由此继承TIO核心服务302的密码引擎140编程特权。因此,每个特许委托308受TIO堆栈(例如,受TIO核心服务302和相关组件)信任而不会不恰当地对DMA通道解除保护,以便有意地使机密的用户输入未加密。在一些实施例中,计算设备100可以使用默认特许委托308和/或用于所有应用的系统范围的特许委托308。例如,计算设备100可以使用监测特定安全键盘输入的委托308(例如,传统PC系统上的CTRL-ALT-DEL)。因此,在一些实施例中,对安全I/O的请求可能不明确地识别委托308。

[0042] 在框410中,在接收到对已加密的DMA通道的请求之后,CEE 304生成通道加密密钥以保护所请求的DMA通道。例如,可以使用具有随机种子值(即,EGETKEY的“KEY ID”参数)的处理器指令(例如,EGETKEY)来导出加密密钥,该处理器指令将导出的密钥与CEE 304的身份联系起来。CEE 304被信任永不会将加密密钥给予除请求隔离区(例如,应用隔离区312和/或非特许DDE 314)以外的任何其他软件实体。在一些实施例中,在框412中,CEE 304可以将随机种子值提供给不可信软件(即,从TIO堆栈的角度来看是不可信的)以用于备份目的。例如,CEE 304可以将随机种子值提供给应用隔离区312、操作系统316、或另一不可信实体。如果CEE 304崩溃,则在重新启动时,CEE 304可以使用随机种子值来安全地重新生成通道加密密钥。

[0043] 在框414中,CEE 304将通道编程信息打包并调用CED 318来保护DMA通道。通道编程信息可以包括如在框410中确定的加密密钥以及其他编程信息,例如,要被编程的DMA通道的通道标识符(CID)、编程命令、可以用于认证和重放保护的随机一次使用数(random nonce)以及其他编程信息。通道编程信息可以以存储在诸如BIND_STRUCT结构的二进制结构中。CEE 304可以调用诸如EBINDTIO的处理器120的处理器指令来生成经打包的编程信息。经打包的编程信息可以包括利用解包引擎320已知的密钥进行加密的通道编程密钥。如上面描述的,CEE 304可以例如通过调用一个或多个系统调用(例如,IOCTL)或计算设备100的其他特许功能来将经打包的编程信息提供给CED 318。

[0044] 在框416中,CED 318验证TIO核心服务302的密码引擎140编程特权,并且如果成功,则对密码引擎140进行编程。如上面描述的,CED 318可以通过要求特定组成员资格或其他基于角色的特权访问CED 318的系统调用接口来验证TIO核心服务302的特权。例如,与CED 318相关联的设备节点的权限可能要求“sgxio_核心”组中的成员资格。为了对密码引擎140进行编程,CED 318可以调用处理器120的处理器指令(例如,UNWRAP),以对编程信息

进行解包并对DMA通道安全地进行编程。UNWRAP指令可以使处理器120的解包引擎320对经打包的通道编程密钥进行解密，验证通道编程信息，并且将经解包的通道编程信息复制到密码引擎140。

[0045] 在框418中，密码引擎140保护非特许软件与I/O设备146之间的通道通信。例如，密码引擎140可以拦截直接存储器存取(DMA)事务，并对I/O设备146与非特许应用隔离区312和/或非特许DDE 314之间交换的I/O数据进行加密。

[0046] 在框420中，计算设备100确定是否回收与受保护的DMA通道相关联的I/O设备146。例如，如果相关联的非特许软件(例如，应用隔离区312和/或非特许DDE 314)崩溃或以其他方式终止，则操作系统316可以确定回收I/O设备146。如果在这种情形下I/O设备146未被回收，则该I/O设备146的DMA事务可以保持被加密，直到计算设备100重置为止，使得I/O设备146对于其他应用不可用并且因此导致拒绝服务。如果计算设备100确定不回收I/O设备146，则方法400循环回到框418，并且密码引擎140继续保护DMA通道。如果计算设备100确定回收I/O设备146，则方法400前进到框422。

[0047] 在框422中，操作系统316请求TIO核心服务302对与要回收的I/O设备146相关联的DMA通道解除保护。操作系统316可以例如使用进程间通信设施向TIO核心服务302发送消息，或者以其他方式调用TIO核心服务302。

[0048] 在框424中，响应于对DMA通道解除保护的请求，与该DMA通道相关联的特许委托308提示用户确认TIO会话的终止。在一些实施例中，操作系统316可以代表委托308提示用户。委托308可以使用任何适当的技术来安全地(即，不通过DMA通道接收未受保护的用户输入)确认与用户的终止。因此，委托308可以决定在不了解关于崩溃的应用隔离区312和/或DDE 314的任何信息的情况下对I/O设备146解除保护是否是安全的。假定去往/来自受保护的I/O设备146的所有经过的DMA业务被加密，只要没有更多的机密数据被馈送到输入设备146，就可以认为对I/O设备146解除保护是“安全的”。因此，只要人类用户已经确认没有应用正在处理他或她的机密输入，并且I/O设备146将要受保护，则可以认为对I/O设备146解除保护是安全的。接收来自人类用户的确认的安全技术可以是通过不同的已加密I/O设备146来接收确认。例如，特许委托308和/或操作系统316可以向用户显示消息，并且然后特许委托308可以通过另一已加密的输入设备146来接收确认用户输入，例如通过经由不同的DMA通道接收受保护的用户输入。继续该示例，具有键盘146的计算设备100可以接收如密钥的特殊组合的确认，使得当人类用户按下该密钥组合时(例如，类似于按下CTRL+ALT+DEL来打开图形登录界面)对DMA通道解除保护被认为是“安全的”。

[0049] 在框426中，特许委托308确定用户是否已经确认TIO会话被终止。委托308可以认为在接收到来自人类用户的确认之后对I/O设备146解除保护是安全的，该人类用户被认为在做出确认之前已经停止将敏感输入数据馈送到I/O设备146。如果用户尚未确认，则方法400循环回到框424以继续对用户确认进行监测。在对用户确认进行监测的同时，DMA通道和相关的输入数据仍然受到保护。如果用户已经确认TIO会话被终止，则方法400前进到框428。

[0050] 在框428中，CEE 304对与要回收I/O设备146相关联的DMA通道解除保护。为了对DMA通道解除保护，CEE 304可以执行类似于上文结合框414到416所描述的保护DMA通道的请求的操作。例如，CEE 304可以生成经打包的编程信息并将经打包的编程信息提交给CED

318,CED 318可以将编程信息解包并且对密码引擎140进行编程以对DMA通道解除保护。在许多实施例中,可能需要用于保护DMA通道的加密密钥来生成经打包的编程信息,以对DMA通道解除保护。因此,CEE 304和/或TIO堆栈的其他组件(例如,特许委托308)可以保留加密密钥的副本,或者以其他方式对与每个DMA通道相关联的加密密钥进行访问。在对DMA通道解除保护之后,I/O数据可以在I/O设备146与存储器132之间未加密地传送,并且方法400循环回到框406,以对保护DMA通道的附加请求进行监测。

[0051] 应该理解,在一些实施例中,方法400可以体现为存储在计算机可读介质上的各种指令,其可以由处理器120和/或计算设备100的其他组件执行以使得计算设备100执行对应的方法400。计算机可读介质可以体现为能够由计算设备100读取的任何类型的介质,包括但不限于存储器132、数据存储设备134、计算设备100的其他存储器或数据存储设备、计算设备100的外围设备可读的便携式介质、和/或其他介质。

[0052] 示例

[0053] 下面提供了本文公开的技术的说明性示例。这些技术的实施例可以包括下面描述的示例中的任何一个或多个以及其任何组合。

[0054] 示例1包括一种用于可信I/O访问控制的计算设备,该计算设备包括:公共信任模块,其用于(i)执行可信I/O核心服务,其中,可信I/O核心服务具有由计算设备的操作系统授予的密码引擎编程特权,以及(ii)接收来自应用的保护与计算设备的I/O设备相关联的DMA通道的请求,其中,应用不具有密码引擎编程特权;访问控制模块,其用于(i)响应于对来自应用的保护DMA通道的请求的接收,由操作系统接收来自可信I/O核心服务的保护DMA通道的请求,以及(ii)响应于对保护DMA通道的请求的接收,由操作系统验证可信I/O核心服务的密码引擎编程特权;以及编程模块,其用于响应于对可信I/O核心服务的密码引擎编程特权的验证,对计算设备的密码引擎进行编程以保护DMA通道。

[0055] 示例2包括示例1的主题,并且还包括具有安全隔离区支持的处理器,其中,应用包括利用处理器的安全隔离区支持而建立的安全隔离区。

[0056] 示例3包括示例1和2中任一个的主题,并且其中,操作系统包括密码引擎驱动程序。

[0057] 示例4包括示例1-3中任一个的主题,并且其中,公共信任模块还用于:响应于对密码引擎进行编程以保护DMA通道,由可信I/O核心服务从操作系统接收对DMA通道解除保护的请求;响应于对DMA通道解除保护的请求的接收,由与DMA通道相关联的特许委托确定计算设备的用户是否已经确认对DMA通道的保护终止,其中,特许委托是由可信I/O核心服务建立的;以及响应于用户已经确认对DMA通道的保护终止的确定,由可信I/O核心服务对DMA通道解除保护。

[0058] 示例5包括示例1-4中任一个的主题,并且其中,确定计算设备的用户是否已经确认对DMA通道的保护终止包括经由计算设备的受保护的DMA通道来接收受保护的用户输入。

[0059] 示例6包括示例1-5中任一个的主题,并且其中,经由受保护的DMA通道来接收受保护的用户输入包括经由第二DMA通道来接收受保护的用户输入,其中,第二DMA通道与对DMA通道解除保护的请求中的DMA通道不同。

[0060] 示例7包括示例1-6中任一个的主题,并且其中,接收保护DMA通道的请求包括接收识别特许委托的请求。

[0061] 示例8包括示例1-7中任一个的主题，并且还包括具有安全隔离区支持的处理器，其中，特许委托包括利用处理器的安全隔离区支持而建立的安全隔离区。

[0062] 示例9包括示例1-8中任一个的主题，并且其中，访问控制模块还用于：响应于对密码引擎进行编程以保护DMA通道，由操作系统确定是否对DMA通道解除保护；以及响应于对DMA通道解除保护的确定，由操作系统请求可信I/O核心服务对DMA通道解除保护。

[0063] 示例10包括示例1-9中任一个的主题，并且其中，确定是否对DMA通道解除保护包括确定应用是否已经终止。

[0064] 示例11包括示例1-10中任一个的主题，并且其中，公共信任模块还用于：(i)响应于对保护DMA通道的请求的接收，由可信I/O核心服务建立的密码引擎隔离区(CEE)生成通道加密密钥，以及(ii)由CEE对通道加密密钥进行打包以生成经打包的编程信息；并且接收来自可信I/O核心服务的保护DMA通道的请求包括接收来自可信I/O核心服务的经打包的编程信息。

[0065] 示例12包括示例1-11中任一个的主题，并且其中，对通道加密密钥进行打包包括：调用计算设备的处理器中的处理器指令，以生成经打包的编程信息。

[0066] 示例13包括示例1-12中任一个的主题，并且其中，生成通道加密密钥包括：生成用于生成通道加密密钥的随机种子；以及将随机种子提供给计算设备的不可信软件。

[0067] 示例14包括示例1-13中任一个的主题，并且其中：编程模块还用于响应于对经打包的编程信息的接收，由操作系统对经打包的编程信息进行解包，以生成经解包的编程信息；并且对密码引擎进行编程包括：响应于对经打包的编程信息的解包，利用经解包的编程信息对密码引擎进行编程以保护DMA通道。

[0068] 示例15包括示例1-14中任一个的主题，并且其中，对经打包的编程信息进行解包包括调用计算设备的处理器中的处理器指令，以生成经解包的编程信息。

[0069] 示例16包括一种用于可信I/O访问控制的方法，该方法包括：由计算设备执行可信I/O核心服务，其中，可信I/O核心服务具有由计算设备的操作系统授予的密码引擎编程特权；由可信I/O核心服务接收来自应用的保护与计算设备的I/O设备相关联的DMA通道的请求，其中，应用不具有密码引擎编程特权；响应于接收到来自应用的保护DMA通道的请求，由操作系统接收来自可信I/O核心服务的保护DMA通道的请求；响应于接收到保护DMA通道的请求，由操作系统验证可信I/O核心服务的密码引擎编程特权；以及响应于验证可信I/O核心服务的密码引擎编程特权，由操作系统对计算设备的密码引擎进行编程以保护DMA通道。

[0070] 示例17包括示例16的主题，并且其中，应用包括利用计算设备的处理器的安全隔离区支持而建立的安全隔离区。

[0071] 示例18包括示例16和17中任一个的主题，并且其中，操作系统包括密码引擎驱动程序。

[0072] 示例19包括示例16-18中任一个的主题，并且还包括：响应于对密码引擎进行编程以保护DMA通道，由可信I/O核心服务从操作系统接收对DMA通道解除保护的请求；响应于接收到对DMA通道解除保护的请求，由与DMA通道相关联的特许委托确定计算设备的用户是否已经确认对DMA通道的保护终止，其中，特许委托是由可信I/O核心服务建立的；以及响应于确定用户已经确认对DMA通道的保护终止，由可信I/O核心服务对DMA通道解除保护。

[0073] 示例20包括示例16-19中任一个的主题，并且其中，确定计算设备的用户是否已经

确认对DMA通道的保护终止包括经由计算设备的受保护的DMA通道来接收受保护的用户输入。

[0074] 示例21包括示例16-20中任一个的主题，并且其中，经由受保护的DMA通道来接收受保护的用户输入包括经由第二DMA通道来接收受保护的用户输入，其中，第二DMA通道于对DMA通道解除保护的请求中的DMA通道不同。

[0075] 示例22包括示例16-21中任一个的主题，并且其中，接收保护DMA通道的请求包括接收识别特许委托的请求。

[0076] 示例23包括示例16-22中任一个的主题，并且其中，特许委托包括利用计算设备的处理器的安全隔离区支持而建立的安全隔离区。

[0077] 示例24包括示例16-23中任一个的主题，并且还包括：响应于对密码引擎进行编程以保护DMA通道，由操作系统确定是否对DMA通道解除保护；以及响应于确定对DMA通道解除保护，由操作系统请求可信I/O核心服务对DMA通道解除保护。

[0078] 示例25包括示例16-24中任一个的主题，并且其中，确定是否对DMA通道解除保护包括确定应用是否已经终止。

[0079] 示例26包括示例16-25中任一个的主题，并且还包括：响应于接收到保护DMA通道的请求，由可信I/O核心服务建立的密码引擎隔离区(CEE)生成通道加密密钥；以及由CEE对通道加密密钥进行打包以生成经打包的编程信息；其中，接收来自可信I/O核心服务的保护DMA通道的请求包括接收来自可信I/O核心服务的经打包的编程信息。

[0080] 示例27包括示例16-26中任一个的主题，并且其中，对通道加密密钥进行打包包括调用计算设备的处理器中的处理器指令，以生成经打包的编程信息。

[0081] 示例28包括示例16-27中任一个的主题，并且其中，生成通道加密密钥包括：生成用于生成通道加密密钥的随机种子；以及将随机种子提供给计算设备的不可信软件。

[0082] 示例29包括示例16-28中任一个的主题，并且还包括：响应于接收到经打包的编程信息，由操作系统对经打包的编程信息进行解包，以生成经解包的编程信息；其中，对密码引擎进行编程包括：响应于对经打包的编程信息进行解包，利用经解包的编程信息对密码引擎进行编程以保护DMA通道。

[0083] 示例30包括示例16-29中任一个的主题，并且其中，对经打包的编程信息进行解包包括调用计算设备的处理器中的处理器指令，以生成经解包的编程信息。

[0084] 示例31包括一种计算设备，其包括：处理器；以及其中存储有多个指令的存储器，该指令在由处理器执行时使得计算设备执行示例16-30中任一个的方法。

[0085] 示例32包括一种或多种机器可读存储介质，包括存储在其上的多个指令，该指令响应于被执行而使得计算设备执行示例16-30中任一个的方法。

[0086] 示例33包括一种计算设备，其包括用于执行示例16-30中任一个的方法的模块。

[0087] 示例34包括用于可信I/O访问控制的计算设备，该计算设备包括：用于执行可信I/O核心服务的模块，其中，可信I/O核心服务具有由计算设备的操作系统授予的密码引擎编程特权；用于由可信I/O核心服务接收来自应用的保护与计算设备的I/O设备相关联的DMA通道的请求的模块，其中，应用不具有密码引擎编程特权；用于响应于接收到来自应用的保护DMA通道的请求而由操作系统接收来自可信I/O核心服务的保护DMA通道的请求的模块；用于响应于接收到保护DMA通道的请求而由操作系统验证可信I/O核心服务的密码引擎编

程特权的模块;以及用于响应于验证可信I/O核心服务的密码引擎编程特权而由操作系统对计算设备的密码引擎进行编程以保护DMA通道的模块。

[0088] 示例35包括示例34的主题,并且其中,应用包括利用计算设备的处理器的安全隔离区支持而建立的安全隔离区。

[0089] 示例36包括示例34和35中任一个的主题,并且其中,操作系统包括密码引擎驱动程序。

[0090] 示例37包括示例34-36中任一个的主题,并且还包括:用于响应于对密码引擎进行编程以保护DMA通道而由可信I/O核心服务从操作系统接收对DMA通道解除保护的请求的模块;用于响应于接收到对DMA通道解除保护的请求而由与DMA通道相关联的特许委托确定计算设备的用户是否已经确认对DMA通道的保护终止的模块,其中,特许委托是由可信I/O核心服务建立的;以及用于响应于确定用户已经确认对DMA通道的保护终止而由可信I/O核心服务对DMA通道解除保护的模块。

[0091] 示例38包括示例34-37中任一个的主题,并且其中,用于确定计算设备的用户是否已经确认对DMA通道的保护终止的模块包括用于经由计算设备的受保护的DMA通道来接收受保护的用户输入的模块。

[0092] 示例39包括示例34-38中任一个的主题,并且其中,用于经由受保护的DMA通道来接收受保护的用户输入的模块包括用于经由第二DMA通道来接收受保护的用户输入的模块,其中,第二DMA通道于对DMA通道解除保护的请求中的DMA通道不同。

[0093] 示例40包括示例34-39中任一个的主题,并且其中,用于接收保护DMA通道的请求的模块包括用于接收识别特许委托的请求的模块。

[0094] 示例41包括示例34-40中任一个的主题,并且其中,特许委托包括利用计算设备的处理器的安全隔离区支持而建立的安全隔离区。

[0095] 示例42包括示例34-41中任一个的主题,并且还包括:用于响应于对密码引擎进行编程以保护DMA通道而由操作系统确定是否对DMA通道解除保护的模块;以及用于响应于确定对DMA通道解除保护而由操作系统请求可信I/O核心服务对DMA通道解除保护的模块。

[0096] 示例43包括示例34-42中任一个的主题,并且其中,用于确定是否对DMA通道解除保护的模块包括用于确定应用是否已经终止的模块。

[0097] 示例44包括示例34-43中任一个的主题,并且还包括:用于响应于接收到保护DMA通道的请求而由可信I/O核心服务建立的密码引擎隔离区(CEE)生成通道加密密钥的模块;以及用于由CEE对通道加密密钥进行打包以生成经打包的编程信息的模块;其中,用于接收来自可信I/O核心服务的保护DMA通道的请求的模块包括用于接收来自可信I/O核心服务的经打包的编程信息的模块。

[0098] 示例45包括示例34-44中任一个的主题,并且其中,用于对通道加密密钥进行打包的模块包括用于调用计算设备的处理器中的处理器指令以生成经打包的编程信息的模块。

[0099] 示例46包括示例34-45中任一个的主题,并且其中,用于生成通道加密密钥的模块包括:用于生成随机种子的模块,该随机种子用于生成通道加密密钥;以及用于将随机种子提供给计算设备的不可信软件的模块。

[0100] 示例47包括示例34-46中任一个的主题,并且还包括:用于响应于接收到经打包的编程信息而由操作系统对经打包的编程信息进行解包以生成经解包的编程信息的模块;其

中,用于对密码引擎进行编程的模块包括用于响应于对经打包的编程信息进行解包而利用经解包的编程信息对密码引擎进行编程以保护DMA通道的模块。

[0101] 示例48包括示例34-47中任一个的主题,并且其中,用于对经打包的编程信息进行解包的模块包括用于调用计算设备的处理器中的处理器指令以生成经解包的编程信息的模块。

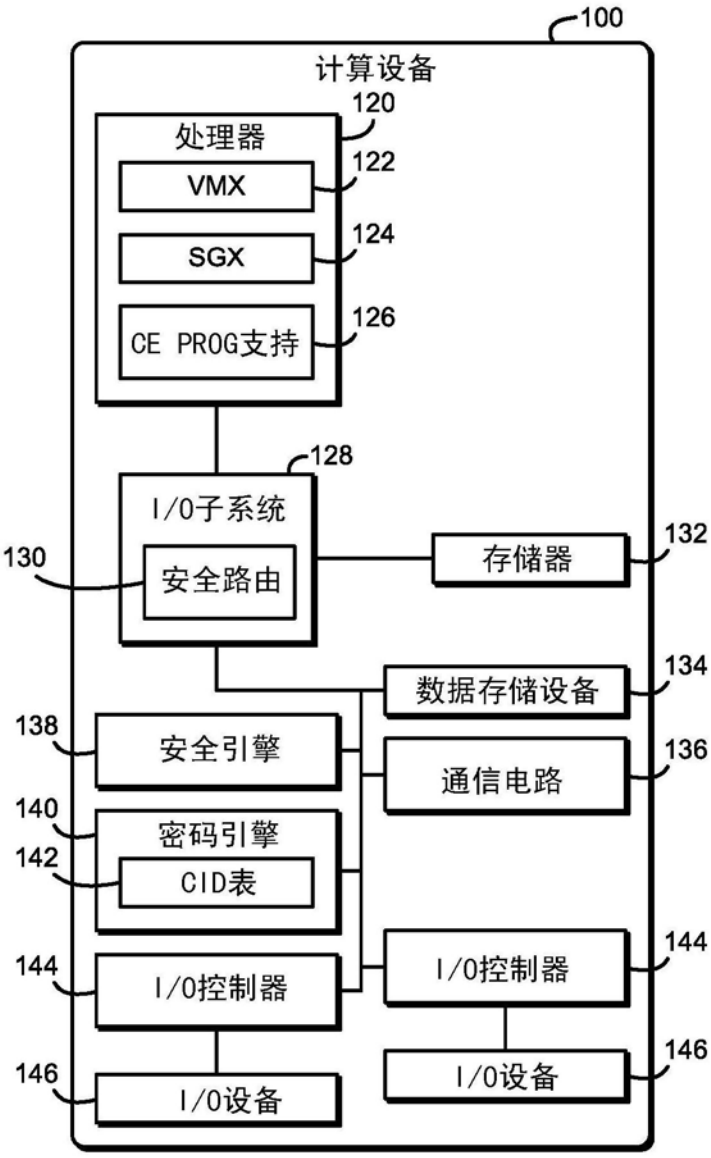

100
计算设备
120
处理器
122
VMX
124
SGX
126
CE PROG支持
128
I/O子系统
130
安全路由
132
存储器
134
数据存储设备
138
安全引擎
136
通信电路
140
密码引擎
142
CID表
144
I/O控制器
144
I/O控制器
146
I/O设备
146
I/O设备

图1

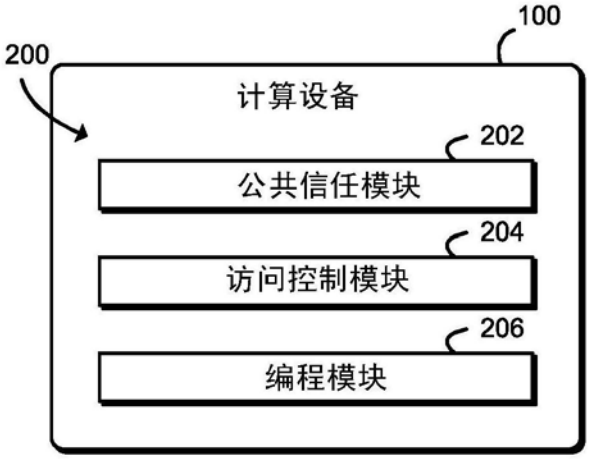


图2

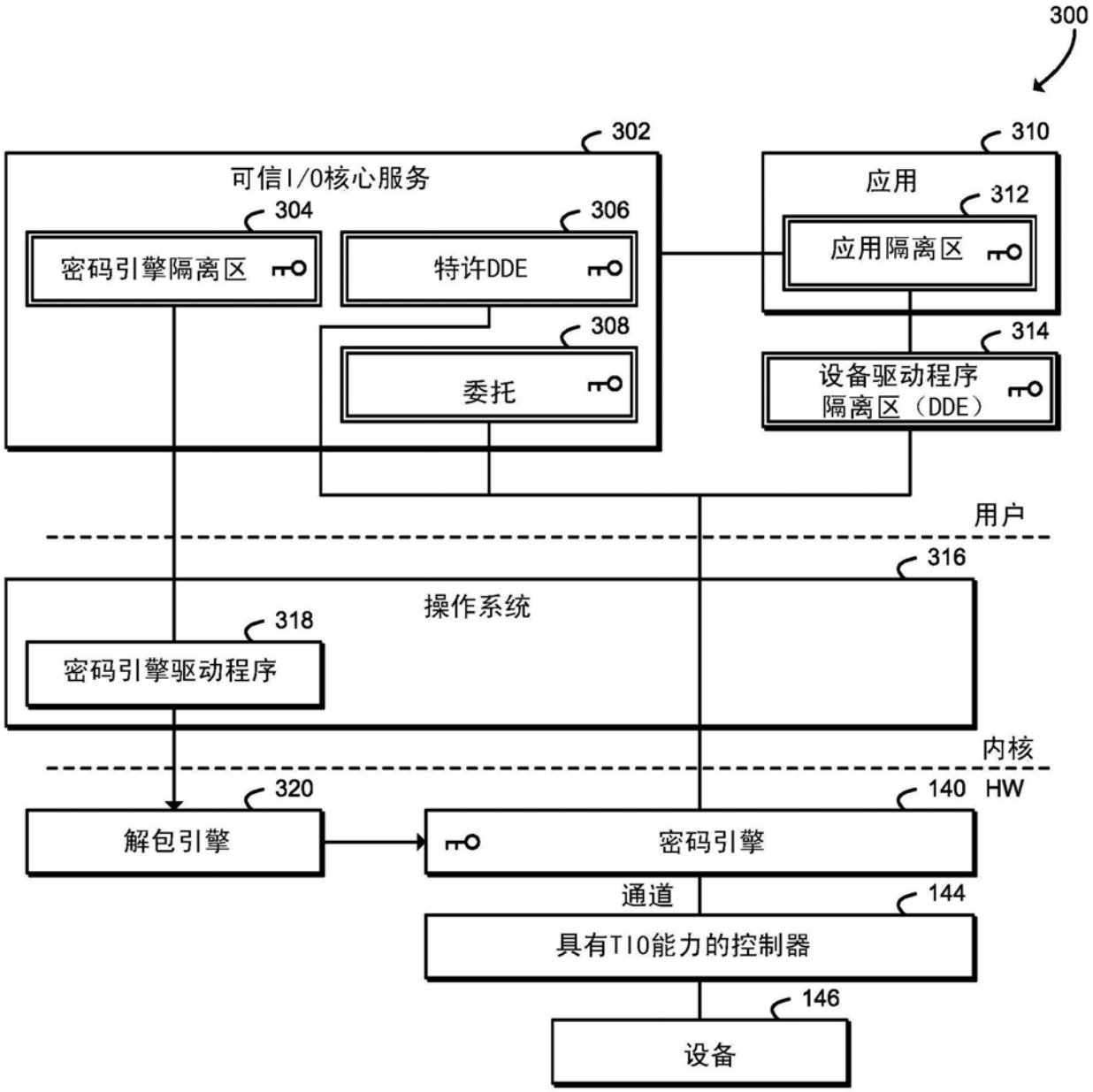

300
302
可信I/O核心服务
304
密码引擎隔离区
306
特许DDE
308
委托
310
应用
312
应用隔离区
314
设备驱动程序
隔离区（DDE）
用户
316
操作系统
318
密码引擎驱动程序
内核
320
解包引擎
140
HW
密码引擎
通道
144
具有TIO能力的控制器
146
设备

图3

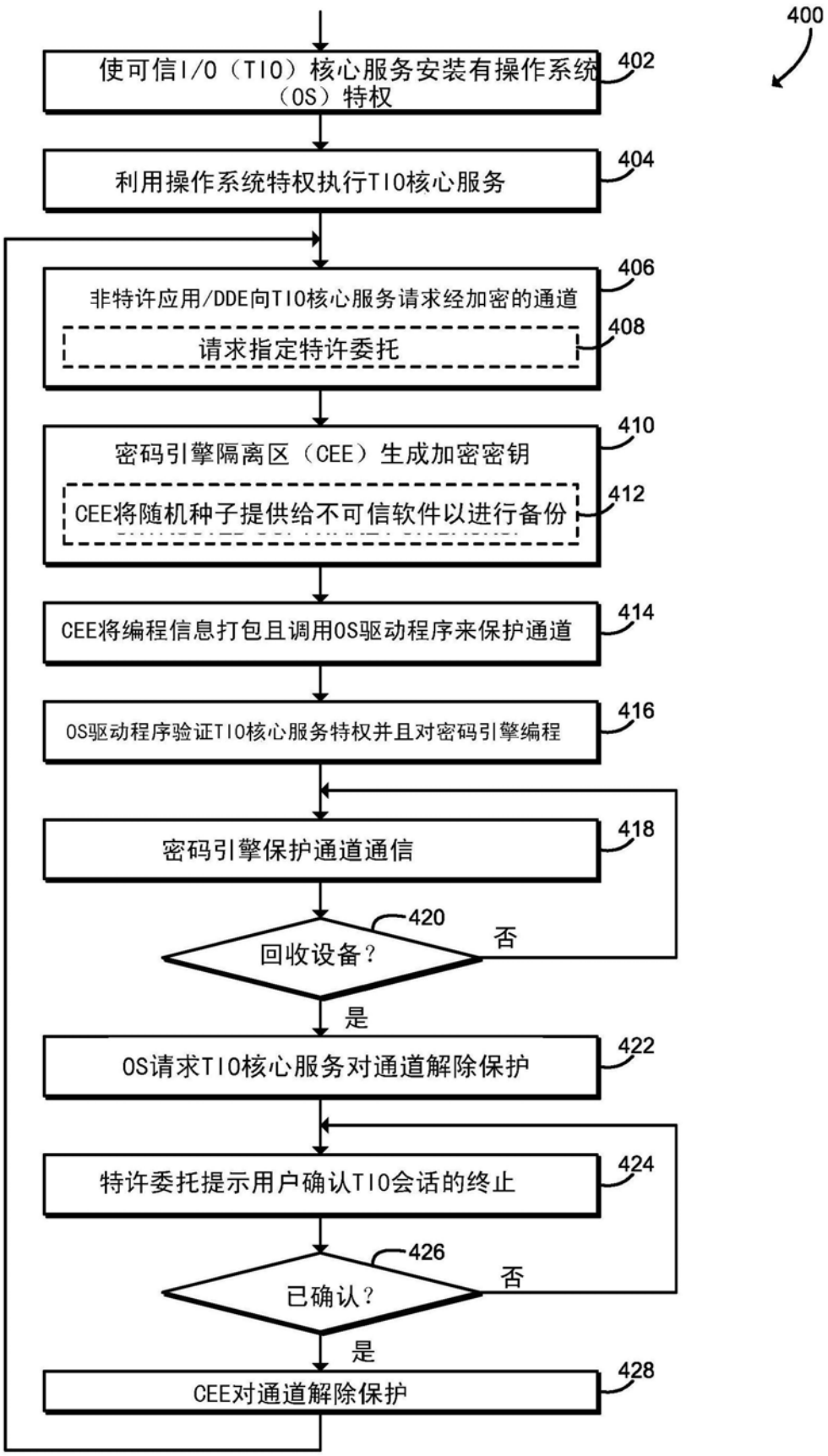

400
使可信I/O（TIO）核心服务安装有操作系统（OS）特权
402
利用操作系统特权执行TIO核心服务
404
非特许应用/DDE向TIO核心服务请求经加密的通道
406
请求指定特许委托
408
密码引擎隔离区（CEE）生成加密密钥
410
CEE将随机种子提供给不可信软件以进行备份
412
CEE将编程信息打包且调用OS驱动程序来保护通道
414
OS驱动程序验证TIO核心服务特权并且对密码引擎编程
416
密码引擎保护通道通信
418
回收设备？
420
否
是
OS请求TIO核心服务对通道解除保护
422
特许委托提示用户确认TIO会话的终止
424
已确认？
426
否
是
CEE对通道解除保护
428

图4