



(12)发明专利

(10)授权公告号 CN 104798054 B

(45)授权公告日 2018.03.30

(21)申请号 201380060662.1

R・勒斯列-赫德 C・V・罗扎斯

(22)申请日 2013.06.24

U・R・萨瓦高恩卡

(65)同一申请的已公布的文献号

V・R・斯卡拉塔 V・尚伯格

申请公布号 CN 104798054 A

W・H・史密斯 I・安奈蒂

(43)申请公布日 2015.07.22

I・埃里克山德洛维奇 A・贝伦宗

G・尼格

(30)优先权数据

(74)专利代理机构 上海专利商标事务所有限公

13/729,277 2012.12.28 US

司 31100

(85)PCT国际申请进入国家阶段日

代理人 姬利永

2015.05.20

(51)Int.Cl.

G06F 12/14(2006.01)

(86)PCT国际申请的申请数据

(56)对比文件

PCT/US2013/047322 2013.06.24

CN 102473224 A, 2012.05.23, 权利要求2, 说明书第[0039],[0065]-[0069],[0244]段, 附图6.

(87)PCT国际申请的公布数据

US 2011/0307651 A1, 2011.12.15, 全文.

W02014/105159 EN 2014.07.03

US 2012/0158184 A1, 2012.06.21, 全文.

(73)专利权人 英特尔公司

审查员 曾鹏飞

地址 美国加利福尼亚州

权利要求书2页 说明书4页 附图3页

(72)发明人 F・X・麦克金 M・A・戈德史密斯

B・E・亨特利 S・P・约翰逊

(54)发明名称

安全区域内的分页

(57)摘要

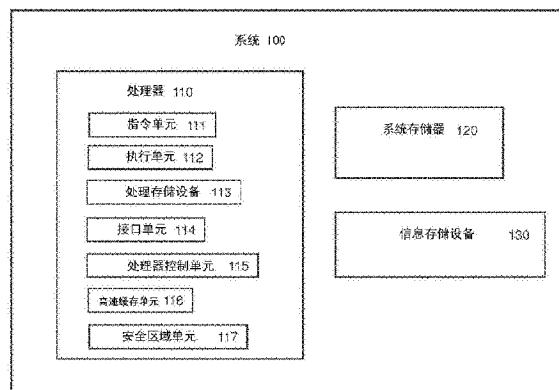
公开了用于安全区域内的分页的本发明的

实施例。在一个实施例中,处理器包括指令单元

和执行单元。该指令单元用于接收第一指令。该

执行单元用于执行该第一指令,其中该第一指令

的执行包括从区域页高速缓存中逐出第一页。



1. 一种处理器,包括:

指令单元,用于接收第一指令和第三指令;以及

执行单元,用于执行所述第一指令和第三指令,其中所述第一指令的执行包括从区域页高速缓存中逐出第一页并且所述第三指令的执行包括分配所述区域页高速缓存中的第二页作为版本阵列页,其中相关于所述第一指令的执行,在所述版本阵列页中存储所述第一页的版本号。

2. 如权利要求1所述的处理器,其中,所述第一指令的执行还包括加密所述第一页的内容以便生成经加密的页。

3. 如权利要求2所述的处理器,其中,所述第一指令的执行还包括在存储器中存储所述经加密的页。

4. 如权利要求3所述的处理器,其中,所述第一指令的执行还包括在所述存储器中存储所述经加密的页的完整性检查元数据。

5. 如权利要求4所述的处理器,其中,所述指令单元还用于接收第二指令并且所述执行单元还用于执行所述第二指令,其中所述第二指令的执行包括将所述第一页重新加载到所述区域页高速缓存中。

6. 如权利要求5所述的处理器,其中,所述第二指令的执行还包括解密所述经加密的页。

7. 如权利要求6所述的处理器,其中,所述第二指令的执行还包括验证所述版本号。

8. 一种用于安全区域内的分页的方法,包括:

接收第三指令;

响应于接收所述第三指令,分配区域页高速缓存中的第二页作为其中用于存储多个版本号的版本阵列页,所述多个版本号中的每一个对应于从区域页高速缓存逐出的页;

接收第一指令;以及

响应于接收所述第一指令,从所述区域页高速缓存中逐出第一页并且将所述第一页的版本号存储在版本阵列页中。

9. 如权利要求8所述的方法,进一步包括响应于接收所述第一指令,加密所述第一页的内容以便生成经加密的页。

10. 如权利要求9所述的方法,进一步包括响应于接收所述第一指令,将所述经加密的页存储在存储器中。

11. 如权利要求10所述的方法,进一步包括响应于接收所述第一指令,将所述经加密的页的完整性检查元数据存储在所述存储器中。

12. 如权利要求11所述的方法,进一步包括:

接收第二指令;以及

响应于接收所述第二指令,将所述第一页重新加载到所述区域页高速缓存中。

13. 如权利要求12所述的方法,进一步包括响应于接收所述第二指令,解密所述经加密的页。

14. 如权利要求13所述的方法,进一步包括响应于接收所述第二指令,验证所述版本号。

15. 一种信息处理系统,包括:

存储器；以及
处理器，所述处理器包括：
指令单元，用于接收第一指令和第三指令；以及
执行单元，用于执行所述第一指令和第三指令，其中所述第一指令的执行包括从区域页高速缓存中逐出第一页并且所述第三指令的执行包括分配所述区域页高速缓存中的第二页作为版本阵列页，其中相关于所述第一指令的执行，在所述版本阵列页中存储所述第一页的版本号。

16. 如权利要求15所述的系统，其中，所述指令的执行还包括加密所述第一页的内容以便生成经加密的页并且将所述经加密的页存储在所述存储器内。

17. 一种机器可读介质，其上存储有指令，所述指令在被执行时致使机器执行如权利要求8-14中任一项所述的方法。

18. 一种用于安全区域内的分页的设备，包括多个装置，每个装置用于执行如权利要求8-14中任一项所述的方法的相应步骤。

安全区域内的分页

- [0001] 背景
- [0002] 1. 领域
- [0003] 本公开涉及信息处理领域，并且更具体地涉及信息处理系统中的安全性领域。
- [0004] 2. 相关技术描述
- [0005] 机密信息由许多信息处理系统存储、传输和使用。因此，已经开发了提供机密信息的安全处理和存储的技术。这些技术包括用于在信息处理系统内创建和维护安全、受保护或隔离分区或环境的各种方法。
- [0006] 附图简要说明
- [0007] 通过举例而非限制在附图中示出本发明。
- [0008] 图1示出根据本发明的实施例的包括安全区域内的分页的系统。
- [0009] 图2示出根据本发明的实施例的安全区域单元。
- [0010] 图3示出根据本发明实施例的用于安全区域内的分页的方法。
- [0011] 详细描述
- [0012] 描述了用于安全区域 (secure enclave) 内的分页的本发明的实施例。在本描述中，可列出众多特定细节(诸如组件和系统配置)，以便提供本发明的更透彻理解。然而，本领域普通技术人员将认识到可在没有这些特定细节的情况下实践本发明。此外，未详细示出某些公知的结构、电路和其他特征，以便避免不必要的混淆本发明。
- [0013] 在以下描述中，对“一个实施例”、“实施例”、“示例实施例”、“各实施例”等等的引用指示如此描述的本发明的实施例可包括具体特征、结构、或特性，然而多个实施例可以包括但不是每个实施例都需要包括该具体特征、结构、或特性。进一步地，某些实施例可具有针对其他实施例所描述的特征中的某些、全部或没有。
- [0014] 如在权利要求书中所使用的，除非以其他方式指明，用于描述元件的顺序形容词“第一”、“第二”、“第三”等等的使用仅指示元件的具体实例或者类似元件的不同实例并且不旨在暗示这些如此描述的元件必须按特定顺序(或者按时间、按空间排序或者以任何其他方式)。
- [0015] 如在背景部分中所描述的，已经开发了用于在信息处理系统内创建和维护安全、受保护或隔离分区或环境的各种方法。一种这种方法涉及如在于2012年6月19日提交的序列号为13/527,547标题为“提供安全应用执行的方法和装置 (Method and Apparatus to Provide Secure Application Execution)”的共同未决的美国专利申请所描述的安全区域，该申请通过引用作为安全区域的至少一个实施例的示例并入在此。然而，并入的引用不旨在以任何方式限制本发明的实施例的范围并且可使用其他实施例同时仍保留在本发明的精神和范围内。
- [0016] 图1示出系统100，即根据本发明的实施例的包括安全区域内的分页的信息处理系统。系统100可表示任何类型的信息处理系统，诸如服务器、桌上计算机、便携式计算机、机顶盒、手持式设备、或嵌入式控制系统。系统100包括处理器110、系统存储器120和信息存储设备130。体现本发明的系统可包括任何数量的这些组件中的每一个组件以及任何其他组

件或其他元件，诸如信息存储设备、外围设备和输入/输出设备。本系统实施例或任何系统实施例中的任何或全部组件或其他元件可通过任何数量的总线、点到点、或其他有线或无线接口或连接而连接、耦合、或以其他方式与彼此通信。

[0017] 系统存储器120可以是动态随机存取存储器或者处理器10可读的任何其他类型的介质。信息存储设备130可包括任何类型的永久或非易失性存储器或存储设备，诸如闪存和/或固态驱动、磁驱动或光盘驱动。

[0018] 处理器110可表示集成在单个衬底上或者封装在单个封装中的一个或多个处理器，每个处理器可包括呈任何组合的多个线程和/或多个执行核。被表示为处理器110的每个处理器可以是任何类型的处理器，包括通用微处理器，诸如英特尔®酷睿®处理器族、英特尔®凌动®处理器族中的处理器、或来自英特尔®公司的其他处理器族或来自另一家公司的另一个处理器或专用处理器或微控制器。处理器110可包括指令单元111、执行单元112、处理存储设备113、接口单元114、处理器控制单元115、高速缓存单元116以及安全区域单元117。处理器110还可包括未在图1中示出的任何其他电路、结构、或逻辑和/或在图1中的其他地方示出或描述的任何电路、结构、或逻辑。

[0019] 指令单元111可表示用于取出、接收、解码、和/或调度指令的任何电路、结构或其他硬件，诸如指令解码器。可在本发明的范围内使用任何指令格式；例如，指令可包括操作码和一个或多个操作数，其中该操作码可被解码为一个或多个微指令或微操作以便由执行单元112执行。

[0020] 执行单元112可包括用于处理数据并执行指令、微指令、和/或微操作的任何电路、结构、或其他硬件，诸如算术单元、逻辑单元、浮点单元、移位器等等。

[0021] 处理存储设备113可表示可用于处理器110内的任何目的的任何类型的存储设备，例如，其可包括任何数量的数据寄存器、指令寄存器、状态寄存器、配置寄存器、控制寄存器、其他可编程或硬编码寄存器或寄存器组、或任何其他存储结构。

[0022] 接口单元114可表示任何电路、结构、或其他硬件（诸如总线单元、消息传送单元、或任何其他单元、端口、或接口），以便允许处理器110通过任何类型的总线、点到点、或其他连接直接或通过任何其他组件（诸如存储器控制器或总线桥）与系统100内的其他组件通信。

[0023] 处理器控制单元115可包括任何逻辑、微代码、电路、或其他硬件以便控制处理器110的这些单元和其他元件的操作以及在处理器110之内、向内、以及向外的数据传送。处理器控制单元115可通过致使处理器110执行由指令单元111接收的指令和从由指令单元111接收的指令导出的微指令或微操作，来致使处理器110执行或参与执行本发明的方法实施例，诸如以下描述的方法实施例。

[0024] 高速缓存单元116可表示信息处理系统110的存储器层次内的用静态随机存取存储器或任何其他存储器技术实现的一个或多个高速缓存存储器级别。高速缓存单元116可包括根据用于信息处理系统内的高速缓存的任何已知的方法专用于或者在处理器110内的任何一个或多个执行核或处理器之间共享的高速缓存存储器的任何组合。

[0025] 安全区域单元117可表示用于创建和维护安全、受保护或隔离环境的任何逻辑、电路、硬件或其他结构，该环境诸如在此描述的安全区域，应用或其他软件可在该安全区域内运行、执行、加载或以其他方式在信息处理系统（诸如系统100）中存在。出于本描述的目的，

这种环境的每个实例可被称为安全区域,尽管本发明的实施例不限于在一个实施例中将安全区域用作安全、受保护或隔离环境的那些实施例,可使用英特尔®酷睿®处理器族或来自英特尔®公司的其他处理器族的处理器的指令集内的指令创建并维护安全区域。

[0026] 图2示出安全区域单元200,其实施例可用作系统100内的安全区域单元117。安全区域单元200的全部或部分可被包括在处理器110的任何一个或多个其他单元内,诸如指令单元111、执行单元112、处理器存储设备113、处理器控制单元115和高速缓存单元116。

[0027] 安全区域单元200可包括加密单元,该加密单元可包括用于执行任何一个或多个加密算法和相应的解密算法的任何逻辑、电路或其他硬件并且可包括与处理器110内的另一个加密单元共享的逻辑、电路或其他硬件。安全区域单元200还可包括完整性保护单元212,该完整性保护单元可包括用于实现用于完整性和/或重放攻击保护的任何方法的任何逻辑、电路或其他硬件,诸如通过生成用于有待保护的数据的单调计数器值、随机数、完整性检查值和/或任何其他元数据。

[0028] 安全区域单元200还可包括区域页高速缓存(EPC)220。在一个实施例中,EPC 220可以是高速缓存单元116的专用部分,诸如末级高速缓存的部分。其他实施例是可能的,包括其中EPC 220的全部或部分可位于处理器110外部的实施例。EPC 220可用于为一个或多个安全区域存储未经加密的代码和数据。访问控制逻辑214、范围寄存器216和EPC映射(EPCM)218可用于防止访问EPC 220内的页,除非由该页所分配给的安全区域内在处理器110上运行的应用访问。

[0029] 安全区域单元200还可包括EPC分页单元230。EPC分页单元230可包括用于提供根据本发明的实施例将页移出和移入EPC 220的任何逻辑、电路或其他硬件。EPC分页单元230可包括用于解码和执行EWB指令231、ELD指令232和EPA指令233的微代码、逻辑、电路和/或其他硬件。

[0030] 这些指令可由操作系统或其他软件用于管理EPC 220以及提供虚拟存储器空间以便由比EPC 220的尺寸更大的一个或多个安全区域使用。EWB指令231可用于将页(诸如页222)从EPC 220逐出到系统存储器120。ELD指令232可用于将页从系统存储器120加载到EPC 220。EPA指令233可用于分配特殊EPC页,诸如版本阵列页224,其上存储用于逐出页的版本信息。

[0031] EWB指令231的参数可包括指向有待被分页出的EPC页的指针,指向其中存储有待被分页出的页的版本号的版本阵列页内的空槽(slot)的指针,以及指向其中存储有经加密的页、完整性检查值、安全区域控制结构(SECS)信息和该页的任何其他元数据的EPC页外部的存储器位置的指针。EPC中的任何页(包括版本阵列页和SECS页)可被分页出,根版本阵列页除外。

[0032] ELD指令232的参数可包括指向有待被分页回的经加密的页及其相关联的元数据的指针、指向其中加载该页的EPC中的空闲页位置的指针、指向该页所分配给的安全区域的SECS的指针、以及指向其中存储该页的版本号的版本阵列页内的槽的指针。

[0033] 图3示出根据本发明实施例的用于安全区域内的分页的方法300。尽管本发明的方法实施例在此方面不受限制,可参考图1和图2的元素以便帮助描述图3的方法实施例。

[0034] 在框310中,创建安全区域。在框312中,EPC 220内的页(包括页222)可被分配给该安全区域。

[0035] 在框320中,EPA指令233的执行开始。在框322中,在EPC 130中创建有待用于存储所逐出页的版本信息的版本阵列页(例如,版本阵列页224)。可在本发明的范围内创建多于一个版本阵列页,并且版本阵列页还可被分页出,只要所逐出版本阵列页的版本信息存储在存在于EPC 220内的另一个版本阵列页中,并且只要被分页出的任何版本阵列页在被其版本信息存储在该版本阵列页内的任何页内分页回之前被分页回。任何页布局和/或任何类型的数据结构可用于将版本号和/或其他信息存储在版本阵列页中以及创建版本阵列页的层次。

[0036] 在框340中,EWB指令231的执行开始。在框342中,有待从EPC 220逐出的页(例如,页222)的内容由加密单元110加密以便生成经加密的页。可在本发明的范围内使用任何加密算法或技术。在框344中,由完整性保护单元212为该页和/或经加密的页生成完整性检查值、防重放值和/或其他元数据。可在本发明的范围内使用用于完整性检查、防重放保护和/或其他验证或认证的任何方法。在框346中,在版本阵列页(例如,版本阵列页224)内的槽中存储该页的唯一版本号。在框348中,将经加密的页、元数据和该页的EPCM信息写入系统存储器120。

[0037] 在框350中,由页222的逐出所释放的页位置可由相同的安全区域或由不同的安全区域使用。

[0038] 在框360中,ELD指令232的执行开始。在框362中,有待重新加载到EPC 220中的页(例如,页222)的经加密的内容由加密单元210解密。在框364中,由完整性保护单元212检查完整性检查值、防重放值和/或该页的其他元数据以便验证该页的完整性,包括检查该版本是否是与上次写出的相同版本。如果验证通过,方法300在框366中继续。如果未通过,方法300在可选地用信号通知错误或故障之后结束。

[0039] 在框366中,将未经加密的页重新加载到EPC 220中并且将EPCM信息恢复到EPCM 218。

[0040] 在本发明的各实施例中,可用不同的顺序执行在图3中示出的方法,组合或省略所展示的框、添加附加的框、或者重新排序、组合、省略、或者附加框的组合。此外,许多其他方法实施例在本发明的范围内是可能的。

[0041] 如以上所描述的,本发明的实施例的各实施例或各部分可存储在任何形式的机器可读介质上。例如,方法300的全部或部分可体现在存储在处理器110可读的介质上的软件或固件指令中,当由处理器110执行时,这些指令导致处理器110执行本发明的实施例。同样,本发明的各方面可体现在存储在机器可读介质上的数据中,其中,该数据表示可用于促成处理器110的全部或部分的设计或其他信息。

[0042] 因此,已经描述了用于安全区域内的分页的本发明的实施例。尽管已经描述了并且在附图中展示了某些实施例,应当理解的是这种实施例仅仅展示而非限制宽泛的发明,并且本发明不应被限制为所展示和描述的特定的构造和安排,因为当学习本公开时,本领域普通技术人员将认识到各种其他修改。在诸如这种技术领域中,其中成长很快并且不能轻易地预见进一步的进步,可在不背离本公开的原理或所附权利要求书的范围的情况下容易地对所公开的实施例做出安排和细节上的修改,正如通过使能技术进步所促进的。

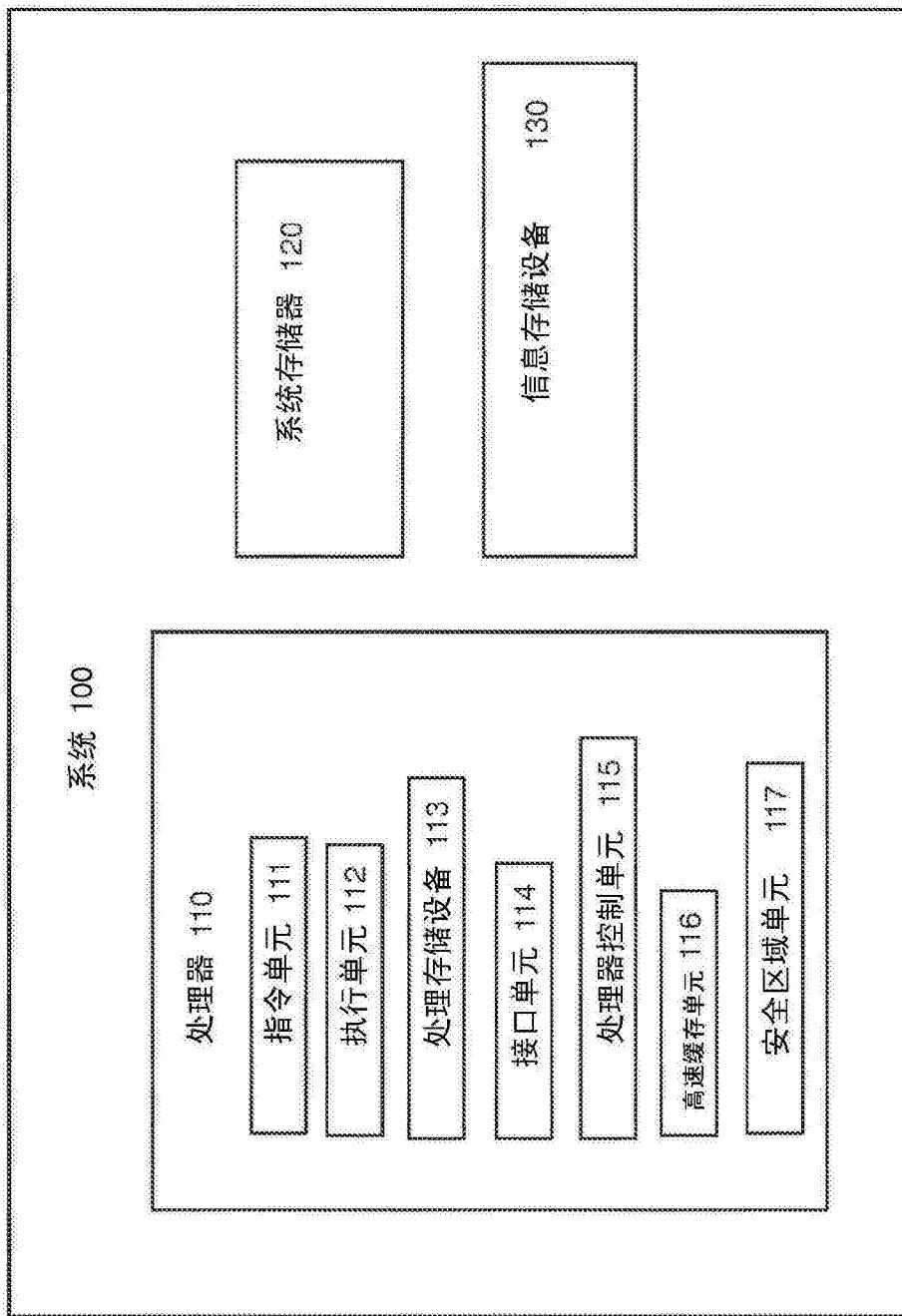


图 1

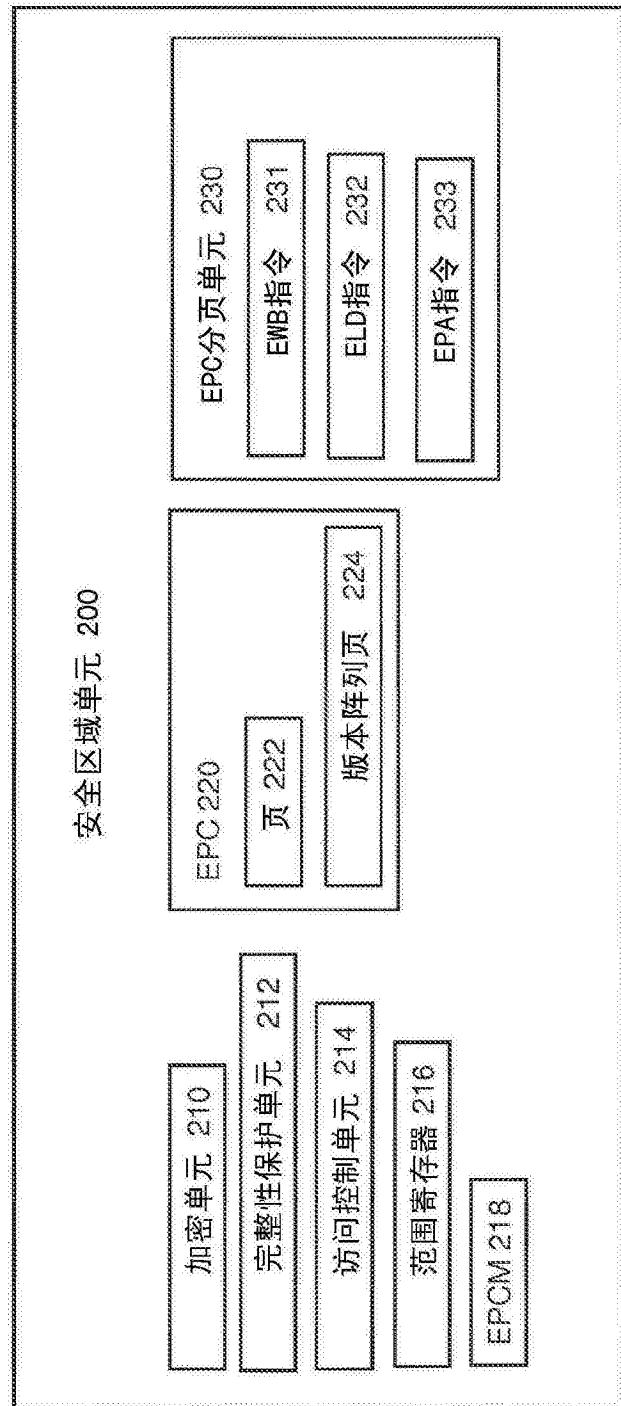


图2

方法 300

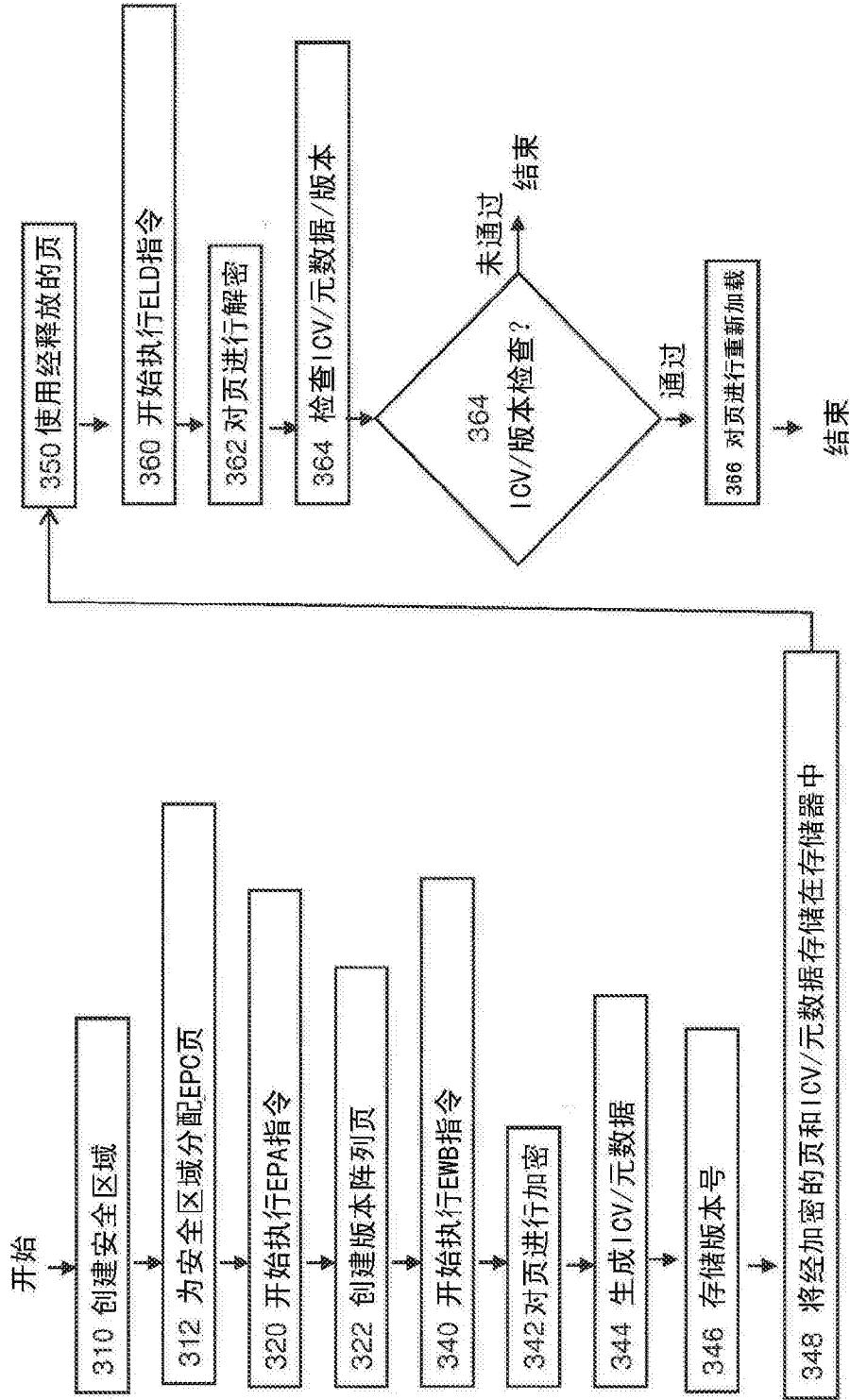


图3