



[12] 发明专利说明书

专利号 ZL 200310117072.6

[45] 授权公告日 2008 年 3 月 12 日

[11] 授权公告号 CN 100374977C

[22] 申请日 2003.12.3

[21] 申请号 200310117072.6

[30] 优先权

[32] 2002.12.31 [33] US [31] 10/334, 954

[73] 专利权人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 大卫·I·波伊斯尼尔

[56] 参考文献

EP1229424A2 2002.8.7

US6148082A 2000.11.14

US6393126B1 2002.5.21

审查员 马晓亚

[74] 专利代理机构 永新专利商标代理有限公司

代理人 王英

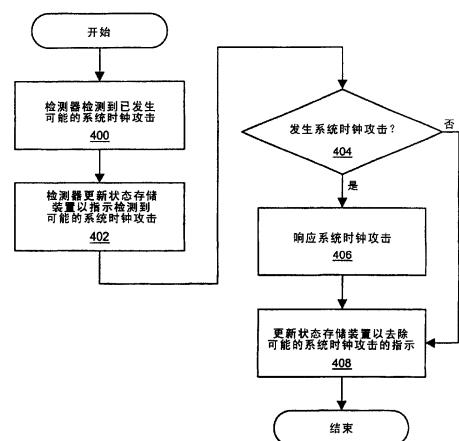
权利要求书 5 页 说明书 13 页 附图 4 页

[54] 发明名称

受信系统时钟

[57] 摘要

本发明描述了一种尝试增加由系统时钟提供的系统时间的受信度的方法和装置。在一些实施例中，检测器检测可能与对系统时钟的攻击相关的活动。基于检测器是否检测到对系统时钟的可能的攻击，计算设备可以确定是否信任由系统时钟提供的系统时间。



1. 一种和保持系统时间的系统时钟一起使用，以指示出对所述系统时钟的攻击的方法，包括

存储一个指示，用于指示出有对系统时间的更新等待解决，

基于在所存储的指示指示出对所述系统时间的更新仍等待解决的同时接收到系统定时器中断，检测对所述系统时钟的攻击，以及更新状态存储装置，以指示出对所述系统时钟的攻击。

2. 如权利要求 1 所述的方法，还包括响应于确定了系统时钟以不适当速率被更新，检测对所述系统时钟的攻击。

3. 如权利要求 1 所述的方法，还包括

响应于系统定时器中断，更新所述系统时间，和

响应于检测到改变所述系统定时器中断产生的速率的企图，检测对所述系统时钟的攻击。

4. 如权利要求 1 所述的方法，还包括

响应于系统定时器中断，更新所述系统时间，和

响应于检测到可能改变所述系统定时器发出所述系统定时器中断的速率的、对所述系统定时器的接口的一个或多个访问，检测对所述系统时钟的攻击。

5. 如权利要求 1 所述的方法，还包括

响应于由系统定时器发送的系统定时器中断，更新所述系统时间，和

响应于检测到与所述系统定时器相关的振荡器的频率具有对预定值域的预定关系，检测对所述实时时钟的攻击。

6. 如权利要求 1 所述的方法，还包括

响应于检测到对所述系统时钟的攻击，将所述状态存储装置的一个位激活，和

防止非受信软件禁止所述状态存储装置的所述位。

7. 如权利要求 1 所述的方法，还包括

响应于检测到对所述系统时钟的攻击，更新所述状态存储装置的计数

器的计数，以及

防止非受信软件变更所述计数器的计数。

8. 如权利要求 1 所述的方法，还包括

响应于由系统定时器发送的系统定时器中断，更新所述系统时间，和

响应于确定了对所述系统定时器发送所述系统定时器中断的速率的调整具有对预定值域的预定关系，确定未发生攻击。

9. 如权利要求 1 所述的方法，还包括

响应于由系统定时器发送的系统定时器中断，更新所述系统时间，和

响应于确定了已对所述系统定时器发送所述系统定时器中断的速率进行了超过预定次数的调整，确定发生了攻击。

10. 一种用于指示出对系统时钟的攻击的芯片组，包括

状态存储装置，以指示是否检测到对系统时钟的攻击，和

检测器，以检测对所述系统时钟的攻击，并基于是否检测到对所述系统时钟的攻击来更新所述状态存储装置，以及

更新存储装置，以存储一个指示，用于指示出是否有对所述系统时钟的更新等待解决，其中所述检测器基于如下情况的发生来检测对所述系统时钟的攻击：在接收到用于更新所述系统时钟的系统定时器中断时，所述更新存储装置所存储的指示指示出有对所述系统时钟的更新等待解决。

11. 如权利要求 10 所述的芯片组，还包括系统定时器以产生中断，其中所述检测器响应于确定了所述系统时钟正以不适当速率被更新，检测到对所述系统时钟的攻击。

12. 如权利要求 10 所述的芯片组，其中所述更新存储装置位于安全性增强空间中，所述安全性增强空间防止非受信代码更新所述更新存储装置。

13. 如权利要求 10 所述的芯片组，其中

所述状态存储装置包括一个位，防止非受信代码禁止所述位，而允许安全性增强环境的受信代码禁止所述位，并且

响应于检测到对所述系统时钟的攻击，所述检测器激活所述状态存储装置的所述位。

14. 如权利要求 10 所述的芯片组，其中

所述状态存储装置包括计数器，防止非受信代码更新所述定时器，而
允许安全性增强环境的受信代码禁止所述计数器，并且

响应于检测到对所述系统时钟的攻击，所述检测器更新所述定时器的
计数。

15. 如权利要求 10 所述的芯片组，还包括系统定时器锁，响应于被激
活，所述系统定时器锁防止所述系统定时器产生所述系统定时器事件的速
率被变更。

16. 如权利要求 15 所述的芯片组，其中所述系统定时器锁位于安全性
增强空间中，所述安全性增强空间防止非受信代码变更所述系统定时器锁
的状态。

17. 一种用于指示出对系统时钟的攻击的计算设备，包括
存储器，以存储用于系统定时器中断的中断服务例程，
系统定时器，以产生引发所述中断服务例程的执行的系统定时器中
断，

处理器，以响应于执行所述中断服务例程，更新系统时钟的系统时
间，

更新存储装置，以存储一个指示，用于指示出是否有对所述系统时钟
的更新等待解决，和

检测器，以基于如下情况的发生来检测对所述系统时钟的攻击：在接
收到系统定时器中断时，所述更新存储装置所存储的指示指示出有对所述
系统时钟的更新等待解决。

18. 如权利要求 17 所述的计算设备，还包括状态存储装置，以指示出
是否检测到对所述系统时钟的攻击，其中

所述检测器更新所述状态存储装置，以指示出对所述系统时钟的攻
击。

19. 如权利要求 17 所述的计算设备，还包括一个位，以指示出是否检
测到对所述系统时钟的攻击，其中

所述检测器将所述位激活，以指示出对所述系统时钟的攻击。

20. 如权利要求 19 所述的计算设备，其中所述位位于安全性增强空间中，所述安全性增强空间防止非受信代码变更所述位的内容。

21. 如权利要求 17 所述的计算设备，还包括外部振荡器，以向所述系统定时器提供振荡信号，其中

所述系统定时器以第一速率产生所述系统定时器事件，所述第一速率基于所述振荡信号的频率，并且

所述检测器响应于确定了所述振荡信号的频率具有对预定值域的预定关系，检测到对所述系统时钟的攻击。

22. 如权利要求 17 所述的计算设备，还包括系统定时器锁，响应于被激活，所述系统定时器锁防止所述系统定时器产生所述系统定时器事件的速率被变更。

23. 如权利要求 22 所述的计算设备，其中所述系统定时器锁位于安全性增强空间中，所述安全性增强空间防止非受信代码变更所述系统定时器锁的状态。

24. 如权利要求 17 所述的计算设备，其中所述中断服务例程包括系统时钟块，其引发一个或多个系统时钟的更新。

25. 一种用于指示出对系统时钟的攻击的装置，包括

更新存储装置，以存储一个指示，用于指示出是否有对系统时钟的更新等待解决，和

检测逻辑，以基于所述更新存储装置所存储的指示和一个或多个用于引发所述系统时钟的更新的系统定时器中断，检测对所述系统时钟的攻击，

其中如果在所述更新存储装置所存储的指示指示出有对所述系统时钟的更新等待解决的同时接收到系统定时器中断，则所述检测逻辑确定已发生对所述系统时钟的攻击。

26. 如权利要求 25 所述的装置，其中

所述更新存储装置包括一个位，所述位可以被激活以指示有更新等待解决，并且所述位可以被禁止以指示没有更新等待解决，以及

如果当所述更新存储装置的所述位是激活的同时接收到系统定时器中

断，所述检测逻辑确定已发生对所述系统时钟的攻击。

27. 如权利要求 26 所述的装置，其中所述更新存储装置位于安全性增强空间中，所述安全性增强空间防止非受信代码变更所述更新存储装置的内容并允许受信代码变更所述更新存储装置的内容。

28. 如权利要求 25 所述的装置，其中

所述更新存储装置包括计数值，所述计数值表明等待解决的更新的数目，以及

如果所述计数值具有对预定值的预定关系，所述检测逻辑确定已发生对所述系统时钟的攻击。

29. 如权利要求 28 所述的装置，其中所述更新存储装置位于安全性增强空间中，所述安全性增强空间防止非受信代码变更所述更新存储装置的内容并允许受信代码变更所述更新存储装置的内容。

受信系统时钟

技术领域

本发明一般地涉及系统时钟。更具体而言，本发明涉及操作系统中的可以保持正确时间的受信系统时钟。

背景技术

操作系统可以包括系统时钟，以提供用于测量小的时间增量（例如 1 毫秒的增量）的系统时间。系统时钟可以响应于某个系统定时器所产生的周期性的中断而更新系统时钟，所述系统定时器例如是 Intel 8254 事件定时器、Intel 高性能事件定时器（HPET）或实时时钟事件定时器。操作系统可以使用系统时间来给文件打上时间戳，产生周期性中断，产生基于时间的单触发（one-shot）中断，以及调度进程等等。一般而言，系统时钟可以在计算设备运行的同时保持系统时间，但是一旦将计算设备断电或置于睡眠状态，则一般不能保持系统时间。因此，操作系统可以使用参考时钟来在系统启动或系统苏醒时将系统时钟的系统时间初始化。此外，系统时钟容易漂移离开正确的时间。因此，操作系统可以使用参考时钟来周期性地更新系统时钟的系统时间。

一种这样的参考时钟是硬件实时时钟（RTC）。计算设备一般包括 RTC 和当计算设备处于低功耗（power down）状态时给 RTC 供电的电池。由于电池的电源，即使将计算设备断电或置于睡眠状态，RTC 也能够维持实际时间（real time）或壁钟时间（wall time），并且一般能比系统时钟更精确地保持时间。除了设有用于获得壁钟时间的接口以外，RTC 还设有一个接口，例如可以用来设置或改变 RTC 时间的一个或多个寄存器。如本领域技术人员所知，壁钟时间指的是真正的实际时间（例如，2002 年 12 月 4 日，星期五，下午 12 : 01），该时间可以包括例如当前的秒、分、小时、星期几、日、月和年。壁钟时间的名字来源于挂在墙上的传统时钟

所提供的时问，并且通常用于与 CPU 时问相区分，所述 CPU 时问代表了处理器执行处理所花费的秒数。由于多任务和多处理器系统，执行一个处理的 CPU 时问可能大大不同于执行该处理的壁钟时间。

计算设备可以使用系统时钟和/或 RTC 时钟来实施用于时间敏感数据的策略。具体而言，计算设备可以在数据上设置基于时间的访问限制。例如，计算设备可以在从发送起经过了一段时间（例如一个月）之后禁止读取电子邮件消息。计算设备还可以防止读取托管维护的源代码，直到特定日期的到来。作为另一个例子，计算设备可以防止给财务事务指定早于当前日期和/或时间的日期和/或时间。但是，为了使这些基于时间的访问限制有效，计算设备必须相信，系统时钟能抵抗为对攻击者有利而可能变更系统时间的攻击。

发明内容

本发明的一个目的在于提供一种用于指示出对系统时钟的攻击的方法和装置。

根据本发明的第一方面，提供了一种和保持系统时间的系统时钟一起使用以指示出对所述系统时钟的攻击的方法，包括存储一个指示，用于指示出有对系统时间的更新等待解决，基于在所存储的指示指示出仍有对系统时间的更新等待解决的同时接收到系统定时器中断而检测对所述系统时钟的攻击，以及更新状态存储装置，以指示出对所述系统时钟的攻击。

根据本发明的第二方面，提供了一种用于指示出对系统时钟的攻击的芯片组，包括：状态存储装置，以指示是否检测到对系统时钟的攻击；检测器，以检测对所述系统时钟的攻击，并基于是否检测到对所述系统时钟的攻击来更新所述状态存储装置；以及更新存储装置，以存储一个指示，用于指示出是否有对系统时钟的更新等待解决，其中所述检测器基于如下情况的发生来检测对系统时钟的攻击：在接收到用于更新所述系统时钟的系统定时器中断时，所述更新存储装置所存储的指示指示出有对系统时钟的更新等待解决。

根据本发明的第三方面，提供了一种用于指示出对系统时钟的攻击的

计算设备，包括：存储器，以存储用于系统定时器中断的中断服务例程；系统定时器，以产生引发所述中断服务例程的执行的系统定时器中断；处理器，以响应于执行所述中断服务例程，更新系统时钟的系统时间；更新存储装置，以存储一个指示，用于指示出是否有对系统时钟的更新等待解决；和检测器，以基于如下情况的发生来检测对所述系统时钟的攻击：在接收到系统定时器中断时，所述更新存储装置所存储的指示指示出有对系统时钟的更新等待解决。

根据本发明的第四方面，提供了一种用于指示出对系统时钟的攻击的装置，包括：更新存储装置，以存储一个指示，用于指示出是否有对系统时钟的更新等待解决；和检测逻辑，以基于所述更新存储装置所存储的指示和一个或多个用于引发所述系统时钟的更新的系统定时器中断，检测对所述系统时钟的攻击，其中如果在所述更新存储装置指示出有对系统时钟的更新等待解决的同时接收到系统定时器中断，则所述检测逻辑确定已发生对系统时钟的攻击。

附图说明

在附图中，以举例而非限制的方式示出了本文中所描述的本发明。为图示简单和清楚起见，图中所示的元件不一定按比例绘制。例如，为清楚起见，可能将一些元件的尺寸相对于其它元件进行扩大。此外，在认为合适的地方，在图形之间用重复的标号来指示相应的或相似的元件。

图 1 图示了计算设备的实施例；

图 2 图示了图 1 中的计算设备的检测器的实施例，其检测对系统时钟可能的攻击；

图 3 图示了可以由图 1 的计算设备建立的安全性增强（SE）环境的实施例；

图 4 图示了系统时钟响应可能的攻击的方法的示例实施例。

具体实施方式

以下说明描述了多种技术，用于保护系统时钟的系统时间免于为了获

得对时间敏感数据的未授权访问和/或执行未授权的时间敏感操作而被改变。为了更彻底地理解本发明，在以下说明中阐明了许多具体细节，如逻辑实现、操作码（opcode）、指定操作数的方式、资源划分/共享/复制的实现、系统组件的类型和相互关系以及逻辑划分/集成选择。但是，本领域技术人员应该认识到，没有这些具体细节也可以实施本发明。在其它情况下，未详细示出一些控制结构、门级电路和完整的指令序列，以免混淆本发明。利用所包括的说明，本领域普通技术人员将无需过多的实验就能够实现适当的功能。

在本说明书中，提到“一个实施例”、“实施例”、“示例实施例”等，指示所描述的实施例可能包括特定的特征、结构或特性，但每个实施例可能不一定包括该特定的特征、结构或特性。此外，这样的词语不一定指相同的实施例。另外，当结合实施例描述了特定的特征、结构或特性时，无论是否明示，都认为结合其它实施例对这种特定的特征、结构或特性的实现是在本领域技术人员的知识范围之内。

在图 1 中，示出了计算设备 100 的示例实施例。计算设备 100 可以包括经由处理器总线 106 耦合到芯片组 104 上的一个或多个处理器 102。芯片组 104 可以包括以下部件：将处理器 102 耦合到系统存储器 108 的一个或多个集成电路封装或芯片、令牌（token）110、固件 112 和/或计算设备 100 的其它 I/O 设备 114（例如，鼠标、键盘、磁盘驱动器、视频控制器等）。

处理器 102 可以支持安全进入（SENTER）指令的执行，以开始创建安全性增强（SE）环境，例如图 3 的示例 SE 环境。处理器 102 还可以支持安全退出（SEXIT）指令，以开始解除 SE 环境。在一个实施例中，处理器 102 可以在处理器总线 106 上发出与 SENTER、SEXIT 及其它指令的执行相关联的总线消息。在其它实施例中，处理器 102 还可以包括存储器控制器（未示出），以访问系统存储器 108。

处理器 102 还可以支持一个或多个操作模式，例如，实模式、保护模式、虚拟实模式和虚拟机扩展模式（VMX 模式）。此外，处理器 102 在所支持的每一个操作模式中都可以支持一个或多个优先级或环（ring）。

一般而言，处理器 102 的操作模式和优先级限定了可用于执行的指令和执行这样的指令的效果。更具体而言，仅当处理器 102 处于适当的模式和/或优先级中时，才可以允许处理器 102 执行具有一定优先权的指令。

固件 112 可以包括基本输入/输出系统例程（BIOS）。BIOS 可以提供低级例程，在系统启动期间，处理器 102 可以执行所述低级例程，以启动计算设备 100 的多个组件，从而开始执行操作系统。令牌 110 可以包括一个或多个加密密钥和用来记录和报告度量值的一个或多个平台配置寄存器（PCR 寄存器）。令牌 110 可以支持 PCR 引用（quote）操作，该引用操作返回已标识的 PCR 寄存器的引用或内容。令牌 110 还可以支持 PCR 扩展操作，该扩展操作将接收到的度量值记录在已标识的 PCR 寄存器中。在一个实施例中，令牌 110 可以包括受信平台模块（Trusted Platform Module, TPM），该模块在 2001 年 12 月的 Trusted Computing Platform Alliance (TCPA) Main Specification 1.1a 版或其他版本中有详细描述。

芯片组 104 可以包括将处理器 102 接口到计算设备 100 的组件的一个或多个芯片或集成电路封装，所述组件例如是计算设备 100 的系统存储器 108、令牌 110 和其它 I/O 设备 114。在一个实施例中，芯片组 104 包括存储器控制器 116。但是，在其它实施例中，处理器 102 可以包括存储器控制器 116 的全部或部分。存储器控制器 116 可以为计算设备 100 的其它组件提供访问系统存储器 108 的接口。此外，芯片组 104 的存储器控制器 116 和/或处理器 102 可以将存储器 108 的某些区域定义为安全性增强（SE）存储器 118。

在一个实施例中，处理器 102 在处于适当的操作模式（例如保护模式）和优先级（例如 0P）的时候只能访问 SE 存储器 118。而且，SE 存储器 118 可以包括受信系统时钟 120 以保持系统时间。受信系统时钟 120 可以包括响应系统定时器中断而由处理器 102 执行的中断服务例程。中断服务例程可能基于系统定时器中断产生的速率来增加受信系统时钟 120 的系统时间。例如，如果以每毫秒一个系统定时器中断的速率来产生系统定时器中断，中断服务例程可能以每产生一个系统定时器中断就增加一毫秒来增加受信系统时钟 120 的系统时间。计算设备 100 可以使用受信系统时钟

120 的系统时间来给文件打上时间戳，产生周期性中断，产生基于时间的单触发中断，以及调度进程等。此外，计算设备可以使用受信系统时钟来实施用于时间敏感数据的策略。具体地说，计算设备可以对数据实施基于时间的访问限制。例如，计算设备可以在从发送起经过了一段时间（例如一个月）之后禁止读取电子邮件消息。计算设备还可以防止读取托管维护的源代码，直到某特定日期到来。作为另一个例子，计算设备可以防止向财务事务指定早于当前日期和/或时间的日期和/或时间。然而，为了让这些基于时间的访问限制有效，计算设备必须相信系统时钟能抵抗为对攻击者有利而可能变更系统时间的攻击。

芯片组 104 还可以支持 I/O 总线上的标准 I/O 操作，所述 I/O 总线例如是外围组件互连（PCI）、加速图形端口（AGP）、通用串行总线（USB）、低引脚数（LPC）总线或任何其它种类的 I/O 总线（未示出）。令牌接口 122 可以用来将芯片组 104 与包括一个或多个平台配置寄存器（PCR）的令牌 110 相连接。在一个实施例中，令牌接口 122 可以是 LPC 总线（Low Pin Count (LPC) Interface Specification, 英特尔公司, 修订版 1.0, 1997 年 12 月 29 日）。

芯片组 104 还可以包括实时时钟（RTC）124 以保持壁钟时间，所述壁钟时间包括例如秒、分钟、小时、星期几、日、月和年。RTC 124 还可以从电池 126 接收电源以使得即使当计算设备 100 处于低功耗状态（例如断电、睡眠状态等）时 RTC 124 也可以保持壁钟时间。RTC 124 还可以基于由外部振荡器 128 提供的振荡信号来每秒一次地频率更新其壁钟时间。例如，振荡器 128 可以提供具有 32.768 千赫兹频率的振荡信号，而 RTC 124 可以将此振荡信号分频以获得具有 1 赫兹频率的更新信号，用来更新 RTC 124 的壁钟时间。

芯片组 104 还可以包括系统定时器 103，其以可编程的速率产生用来驱动受信系统时钟 120 的系统定时器中断。为此，系统定时器 130 可以包括可被编程来以特定速率产生系统定时器中断的英特尔 8254 事件定时器、英特尔高性能事件定时器（HPET）或者实时时钟事件定时器。在一个实施例中，系统定时器 130 可以包括可能用计数值编程的计数器，并且

系统定时器 130 可以在按振荡器 132 提供的振荡信号的每个周期来更新（例如减二）该计数值。此外，在每次当计数值具有对预定值（例如 0）的预定关系（例如相等）时，系统定时器 130 可以使系统定时器中断（例如 IRQ0）在激活状态和禁止状态之间转换。系统定时器 130 还可以在转换系统定时器中断后重新装入计数值。因此，系统定时器 130 可以产生一种周期性系统定时器中断，其具有由计数值和振荡器 132 的频率定义的速率或频率。系统定时器 130 还可以包括接口 134，以对系统定时器中断的速率编程并获得系统定时器中断的速率。在一个实施例中，接口 134 可以包括一个或多个寄存器，为了获得计数值以及由此获得系统定时器中断的速率，处理器 102 可以从所述寄存器中读取数据，并且为了设置系统定时器中断的速率，处理器 102 可以向所述寄存器中写入计数值。在另一个实施例中，处理器 102 可以通过处理器总线 106 向接口 134 提供命令或消息以获得系统定时器中断的速率和/或对系统定时器中断的速率编程。

芯片组 104 还可以包括系统定时器锁 136。当被激活时，系统定时器锁 136 可以防止系统定时器 130 的速率被变更。例如，系统定时器锁 136 可以防止可能改变速率的写入、命令和/或消息到达接口 134，或者使得接口 134 忽略这些写入、命令和/或消息。锁 136 可以位于芯片组 104 的安全增强（SE）空间（未示出）中。在一个实施例中，处理器 102 只可以通过执行一个或多个特权指令来改变 SE 空间的内容。因此，SE 环境可以防止处理器 102 通过非受信代码来变更锁 136 的内容，其中处理器 102 是通过将非受信代码分配到不能成功执行此类特权指令的处理器环中来试图变更锁 136 的内容的。

状态存储装置 138 可以包括一个位或多个位，可用来存储是否检测到可能的系统时钟攻击的指示。例如，状态存储装置 138 可以包括单个的位，所述单个的位可以被激活以指示检测到对系统时钟的可能的攻击，也可以被禁止以指示没有检测到可能的系统时钟攻击。在另一个实施例中，状态存储装置 138 可以包括具有多个位（例如 32 位）的计数器来存储计数。计数值的改变可以用来指示可能的系统时钟攻击。在另一个实施例中，状态存储装置 138 可以包括多个位或者多个计数器，它们用来不但确

定检测到可能的系统时钟的攻击，还可以指示所检测到的系统时钟攻击的类型。状态存储装置 138 还可以位于芯片组 104 的 SE 空间中，以防止非受信代码变更状态存储装置 138 的内容。

芯片组 104 的检测器 140 可以检测攻击者对受信系统时钟 120 发起攻击的一个或多个方式，并可以报告是否发生了可能的系统时钟攻击。攻击者可能攻击受信系统时钟 120 的一个方式是通过接口 134 改变系统定时器 130 产生系统定时器中断的速率。尽管一个实施例包括锁 136 以防止非受信代码改变系统定时器 130 的速率，但是检测器 140 仍可以检测通过接口 134 改变速率的企图。例如，响应于检测到数据被写入到用来对系统定时器 130 的速率编程的系统定时器接口 134 的寄存器中，寄存器 140 可以更新状态存储装置 138，以指示已发生可能的系统时钟攻击。类似地，响应于检测到接口 134 接收到可能使系统定时器 130 改变其发出系统定时器中断的速率的一个或多个命令或消息，寄存器 140 可以更新状态存储装置 138，以指示可能的系统时钟攻击。在另一实施例中，如果锁 136 被禁止，检测器 140 可以确定对接口 134 的此类访问不是系统时钟攻击，因此让接口 134 不被锁定。

攻击者可能攻击受信系统时钟 120 的另一个方式是增大或减小振荡器 132 的振荡信号的频率或者从系统定时器 130 去除振荡信号。攻击者可以增大振荡信号的频率，以使得受信系统时钟 120 走快并指示出超前于正确的壁钟时间的系统时间。类似地，攻击者可以减小振荡信号的频率，以使得受信系统时钟 120 走慢并指示出滞后于正确的壁钟时间的系统时间。此外，攻击者可以去除振荡信号或者将振荡信号减小至零赫兹，以使得系统时钟 120 停止更新其系统时间。在一个实施例中，响应于检测到振荡器 132 的振荡信号不存在，检测器 140 可以更新状态存储装置 138，以指示可能的系统时钟攻击。在另一个实施例中，响应于检测到振荡信号的频率具有对预定值域的预定关系（例如小于一个值、大于一个值和/或不在两个值之间），检测器 140 可以更新状态存储装置 138，以指示可能的系统时钟攻击。为此，检测器 140 可以包括提供参考振荡信号的自由运行的振荡器，检测器 140 可以从所述参考振荡信号来确定由振荡器 132 提供的振荡

信号的频率是否具有对预定值域的预定关系。

攻击者可能攻击受信系统时钟 120 的另一个方式是防止处理器 102 响应每个系统定时器中断而更新受信系统时钟 120 的系统时间，由此有效地使得受信系统时钟 120 走慢或者停止。为此，检测器 140 可以包括检测受信系统时钟 120 是否响应每个系统定时器中断而更新的逻辑。此逻辑的实施例如图 2 中所示。如图所示，检测器 140 可以包括更新存储装置 200 以指示是否有受信系统时钟 120 的更新等待处理。此外，更新存储装置 200 可以位于芯片组 104 的 SE 空间中，以允许受信代码改变更新存储装置 200 的状态，并防止非受信代码改变更新存储装置 200 的状态。检测器 140 还可以包括检测逻辑 202，以基于更新存储装置 200 和产生的系统定时器中断来检测可能的系统时钟攻击。

在一个实施例中，更新存储装置 200 可以包括单个的位，所述单个的位可以被激活以指示有更新等待解决，并且所述位可以被禁止以指示没有更新等待解决。检测器 140 可以响应于每个产生的系统定时器中断而激活更新存储装置 200，以指示有受信系统时钟 120 的更新等待解决。此外，在更新受信系统时钟 120 的系统时间后，受信系统时钟 120 的中断服务例程可以禁止更新存储装置 200 以指示更新完成。然后，当更新存储装置 200 指示更新仍然等待解决时，检测逻辑 202 可以响应于所发出的系统定时器中断而确定已发生可能的系统时钟攻击。

在另一个实施例中，更新存储装置 200 可以包括具有计数值的计数器，所述计数值指示从上次更新系统时钟 120 起已经产生的系统定时器中断的数目。响应于每个所产生的系统定时器中断，检测器 140 可以增大更新存储装置 200 的计数器的值，以指示等待解决的系统时钟更新的数目。此外，受信系统时钟 120 的中断服务例程可以响应于系统定时器中断而从更新存储装置 200 获得计数值，并且可以基于所获得的计数值来更新受信系统时钟 120 的系统时间。在更新受信系统时钟 120 后，中断服务例程还可以相应地更新计数值。例如，中断服务例程可以按照受信系统时钟 120 的更新所服务的系统定时器中断的数目来减小计数器的值。然后，当更新存储装置 200 的计数值具有对预定的等待解决的系统时钟更新的数目（例

如 5) 的预定关系 (例如超出) 时, 响应于所发出的系统定时器中断, 检测逻辑 202 可以确定已发生可能的系统时钟攻击。

图 3 示出了 SE 环境 300 的实施例。可以响应于各种事件来启动 SE 环境 300, 所述事件例如是系统启动、应用程序请求、操作系统请求等。如图所示, SE 环境 300 可以包括以下部件: 受信虚拟机内核或监控器 302、一个或多个标准虚拟机 (标准 VM) 304 和一个或多个受信虚拟机 (受信 VM) 306。在一个实施例中, 操作环境 300 的监控器 302 在最优先的处理器环 (例如 0P) 的保护模式中执行, 以管理安全性并在虚拟机 304、306 之间设置屏障。

标准 VM 304 可以包括操作系统 308, 该操作系统在 VMX 模式的最优先的处理器环 (例如 0D) 中执行, 标准 VM 304 还包括一个或多个应用程序 310, 所述应用程序在 VMX 模式的较低优先级的处理器环 (例如 3D) 中执行。由于监控器 302 在其中执行的处理器环比操作系统 308 在其中执行的处理器环更为优先, 所以操作系统 308 不能自由地控制计算设备 100, 而是受到监控器 302 的控制和约束。具体而言, 监控器 302 可以防止诸如操作系统 308 和应用程序 310 之类的非受信代码对 SE 存储器 118 和令牌 110 进行直接访问。此外, 监控器 302 可以防止非受信代码直接变更系统定时器 130 的速率, 还可以防止非受信代码变更状态存储装置 138 和更新存储装置 200。

监控器 302 可以对受信内核 312 进行一个或多个测量, 例如内核代码的加密哈希散列 (例如消息摘要 5 (Message Digest 5, MD 5)、安全哈希散列算法 1 (Secure Hash Algorithm 1, SHA-1) 等), 以获取一个或多个度量值, 可以使令牌 110 用内核 312 的度量值来扩展 PCR 寄存器, 并且可以将所述度量值记录在存储于 SE 存储器 118 中的关联 PCR 日志中。此外, 监控器 302 可以在 SE 存储器 118 中建立受信 VM 306, 并在所建立的受信 VM 306 中启动受信内核 312。

类似地, 受信内核 312 可以对小应用程序 (applet) 或应用程序 314 进行一个或多个测量, 例如小应用程序代码的加密哈希散列, 以获取一个或多个度量值。然后, 受信内核 312 可以经由监控器 302 来使令牌 110 用小

应用程序 314 的度量值来扩展 PCR 寄存器。受信内核 312 还可以将所述度量值记录在存储于 SE 存储器 118 中的关联 PCR 日志中。此外，受信内核 312 可以在 SE 存储器 118 的所建立的受信 VM 306 中启动受信小应用程序 314。

受信内核 312 还可以包括受信系统时钟 120。如上所述，受信系统时钟 120 可以包括响应于系统定时器中断而由处理器 102 执行的中断服务例程。受信系统时钟 120 可以增大其系统时间，增大量基于系统定时器 130 周期性地产生系统定时器中断的速率。应当了解到，受信系统时钟 120 可以位于 SE 环境 300 的另一受信模块中。例如，监控器 302 可以包括受信系统时钟 120。在另一个实施例中，受信系统时钟 120 可以包括位于监控器 302 中的系统时钟块 (system clock nub) 316。处理器 102 可以响应于系统定时器中断而执行系统时钟块 316。此外，系统时钟块 316 可以产生一个或多个中断、信号和/或消息，所述一个或多个中断、信号和/或消息使得处理器 102 执行受信内核 312 更新受信系统时钟 120 的系统时间的代码。系统时钟块 316 的所述一个或多个中断、信号和/或消息还可以使得处理器 102 执行操作系统 308 的代码，所述代码更新非受信操作系统 308 的非受信系统时钟 318。

响应于图 3 的 SE 环境 300 的启动，计算设备 100 还将监控器 302 和计算设备 100 的硬件组件的度量值记录在令牌 110 的 PCR 寄存器中。例如，处理器 102 可以获取硬件标识符，例如处理器 102、芯片组 104 和令牌 110 的处理器系列、处理器版本、处理器微代码版本、芯片组版本和令牌版本。然后，处理器 102 可以将所获取的硬件标识符记录在一个或多个 PCR 寄存器中。

在图 4 中，示出了响应对受信系统时钟 120 可能的攻击的示例方法。在方框 400 中，检测器 140 可以检测到发生了可能的系统时钟攻击。例如，响应于确定了振荡器 132 的频率与预定范围具有预定关系、以可能已改变了系统定时器 130 发送系统定时器中断的速率的方式访问了系统定时器接口 134、和/或对受信系统时钟 120 的等待解决的更新数目与等待解决更新的预定数目具有预定关系，检测器 140 可以确定发生了可能的系统时

钟攻击。在方框 402 中，检测器 140 可以更新状态存储装置 138，以指示发生了可能的系统时钟攻击。在一个实施例中，检测器 140 可以通过将状态存储装置 138 的一个位激活来指示可能的系统时钟攻击。在另一个实施例中，检测器 140 可以通过更新（例如，增大、减小、设置、重置）状态存储装置 138 的计数值来指示可能的系统时钟攻击。

在方框 404 中，监控器 302 可以基于状态存储装置 138 来确定是否发生了系统时钟攻击。在一个实施例中，监控器 302 可以响应于状态存储装置 138 的一个位的激活而确定发生了系统时钟攻击。在另一个实施例中，监控器 302 可以响应于状态存储装置 138 的计数值与期望计数值具有预定关系（例如相等），确定发生了系统时钟攻击。例如，监控器 302 可以保持在系统复位、系统低功耗或 SE 环境关闭期间也被保持的期望计数值。监控器 302 可以将状态存储装置 138 的计数值与期望计数值相比较，以确定自监控器 302 上次更新其期望计数值以来，检测器 140 是否检测到了一次或多次可能的系统时钟攻击。

除了状态存储装置 138 之外，监控器 302 还可以基于信任策略来确定是否发生了系统时钟攻击。信任策略可以允许对受信系统时钟 120 的系统时间的某种调整或改变，否则所述调整或改变会被检测器 140 标记为可能的系统时钟攻击。例如，状态存储装置 138 可以指示系统定时器 130 的速率经由接口 134 而被改变了。但是，信任策略可以允许处理器 102 不超过预定量地增加或减小系统定时器 130 的速率，而不将其定义为系统时钟攻击。虽然信任策略可以允许改变系统定时器 130 的速率，但是如果在预定时间段内（例如每天、每周、每次系统复位/低功耗）经由接口 134 进行了超过预定次数（例如 1 次、2 次）的改变，则信任策略可以将这样的改变定义为系统时钟攻击。

在方框 406 中，监控器 302 可以响应所检测到的系统时钟攻击。在一个实施例中，监控器 302 可以基于信任策略进行响应。在一个实施例中，信任策略可以指示 SE 环境 300 不包含时间敏感数据和/或当前未在进行时间敏感操作。因此，监控器 302 可以简单地忽略可能的系统时钟攻击。在另一个实施例中，策略可以指示出监控器 302 要响应于检测到某些类型的

系统时钟攻击而将计算设备 100 复位或关闭 SE 环境 300，所述某些类型的系统时钟攻击例如是检测到振荡信号的频率具有对预定值域的预定关系，或系统定时器 130 的速率具有对预定值域的预定关系。在另一个实施例中，监控器 302 可以给感兴趣的一方提供验证和/或改变受信系统时钟 120 的系统时间的机会。例如，监控器 302 可以将受信系统时钟 120 的系统时间提供给计算设备 100 的用户和/或时间敏感数据的所有者，并且可以让所述的用户和/或所有者来验证系统时间是正确的和/或将系统时间更新为正确的壁钟时间。

在方框 408 中，监控器 302 可以更新状态存储装置 138，以去除可能的系统状态攻击的指示。在一个实施例中，监控器 302 可以禁止状态存储装置 138 的一个位，以清除可能的 RTC 攻击的指示。在另一个实施例中，监控器 302 可以更新其期望计数值和/或状态存储装置 138 的计数值，以使得所述的期望计数值和状态存储装置 138 的计数值具有指示未检测到系统时钟攻击的关系。

计算设备 100 可以响应于机器可读介质的执行指令来执行图 4 的示例方法的全部或其子集，所述介质例如是只读存储器（ROM）；随机访问存储器（RAM）；磁盘存储介质；光学存储介质；闪存设备；和/或电、光、声或其它形式的传播信号，例如载波、红外线信号、数字信号、模拟信号。此外，虽然将图 4 的示例方法图示为操作序列，但是一些实施例中的计算设备 100 可以并行地或以不同的顺序执行所述方法的各种所图示的操作。

虽然已经参考示例实施例对本发明的某些特征进行了描述，但是以上说明不应被解释为具有限制意义。那些对本领域技术人员是显而易见的对所述的示例实施例的各种修改，以及本发明的其它实施例都被认为落入本发明的精神和范围之内。

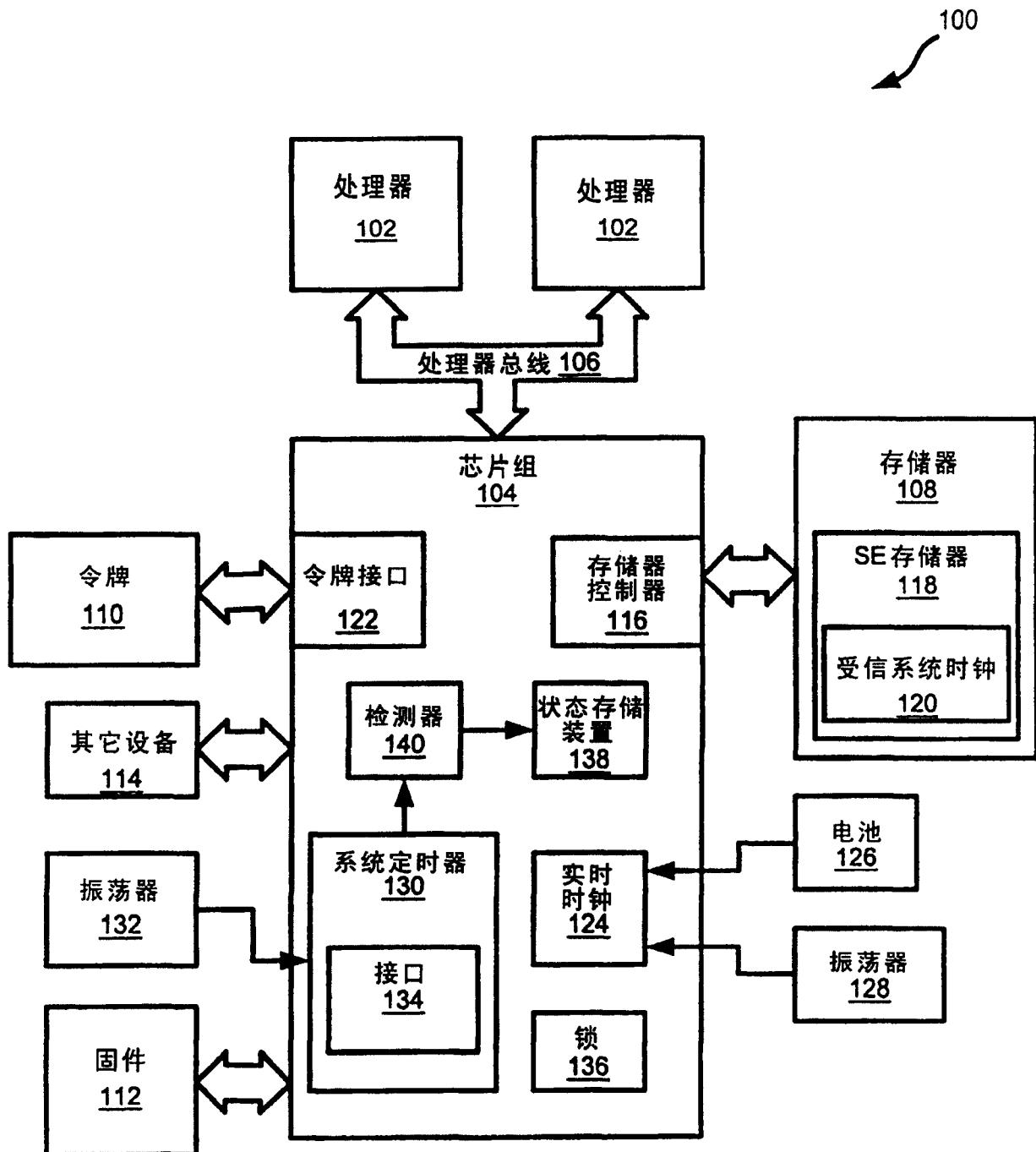


图1

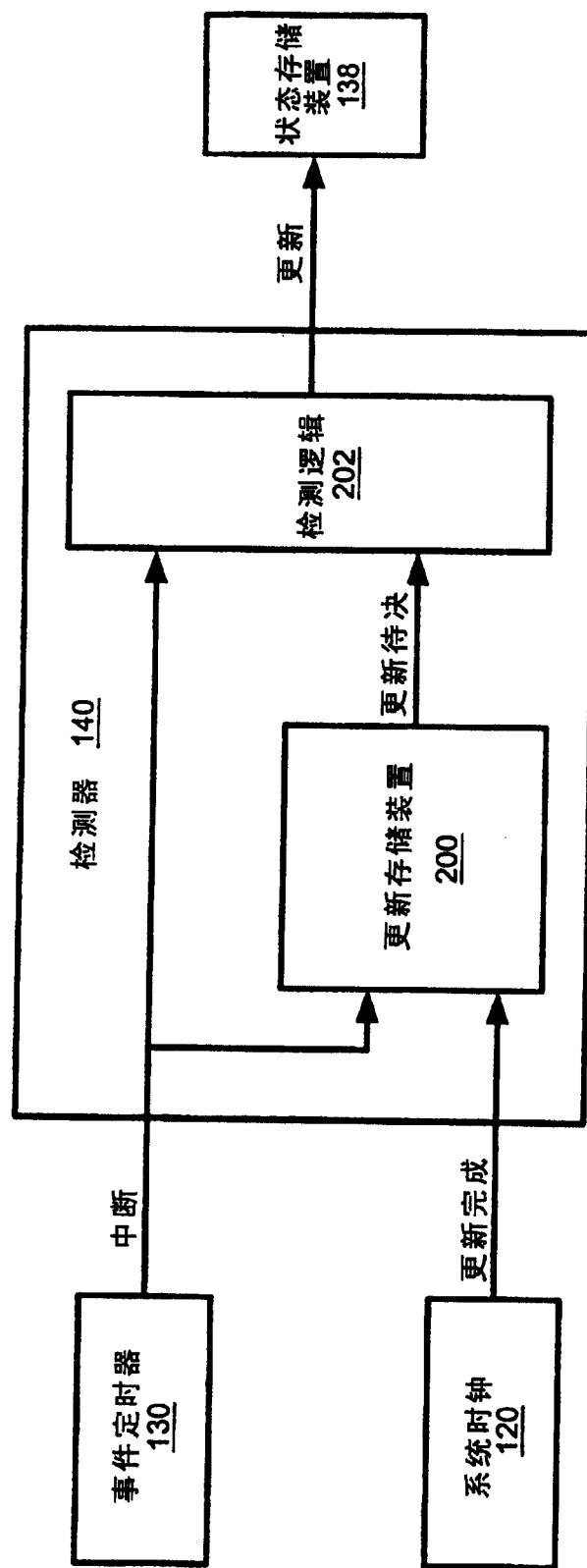


图2

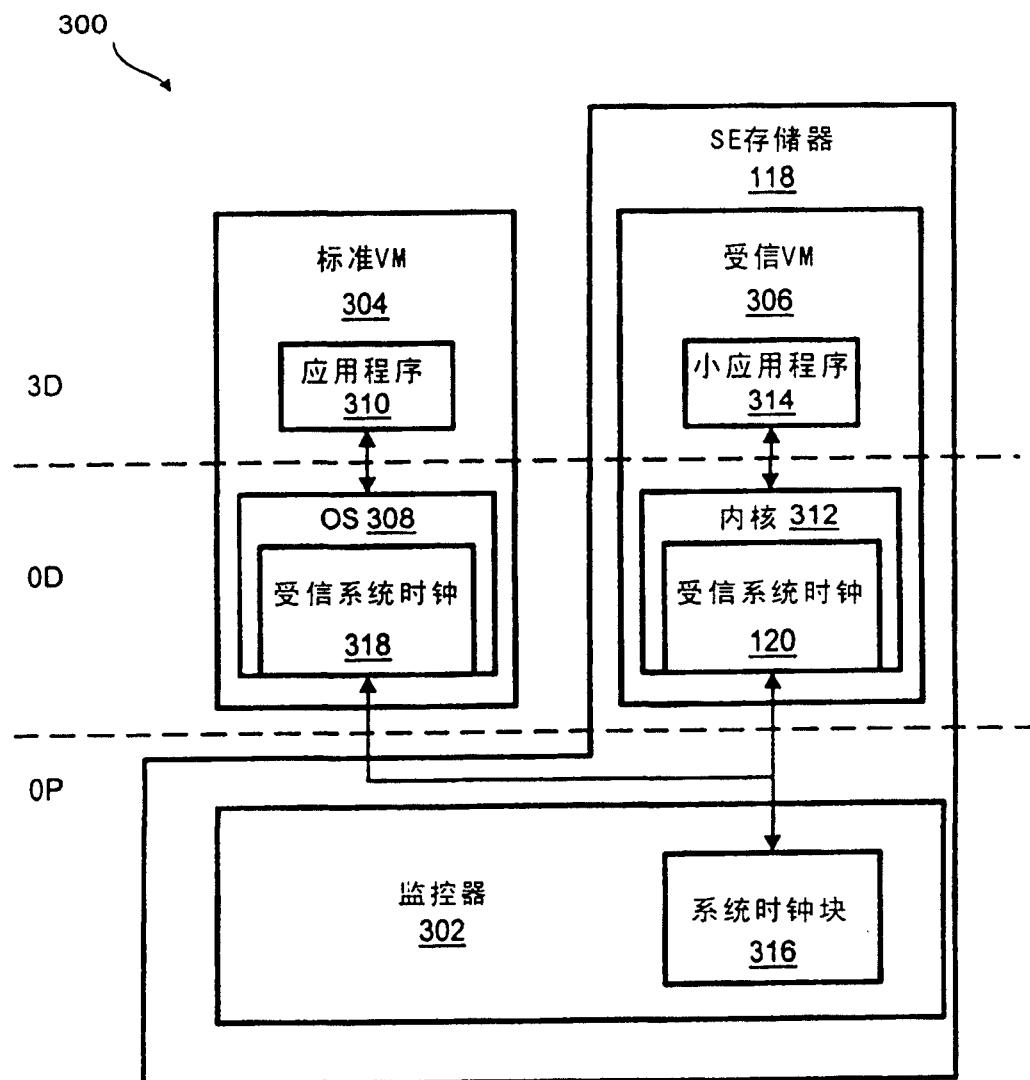


图3

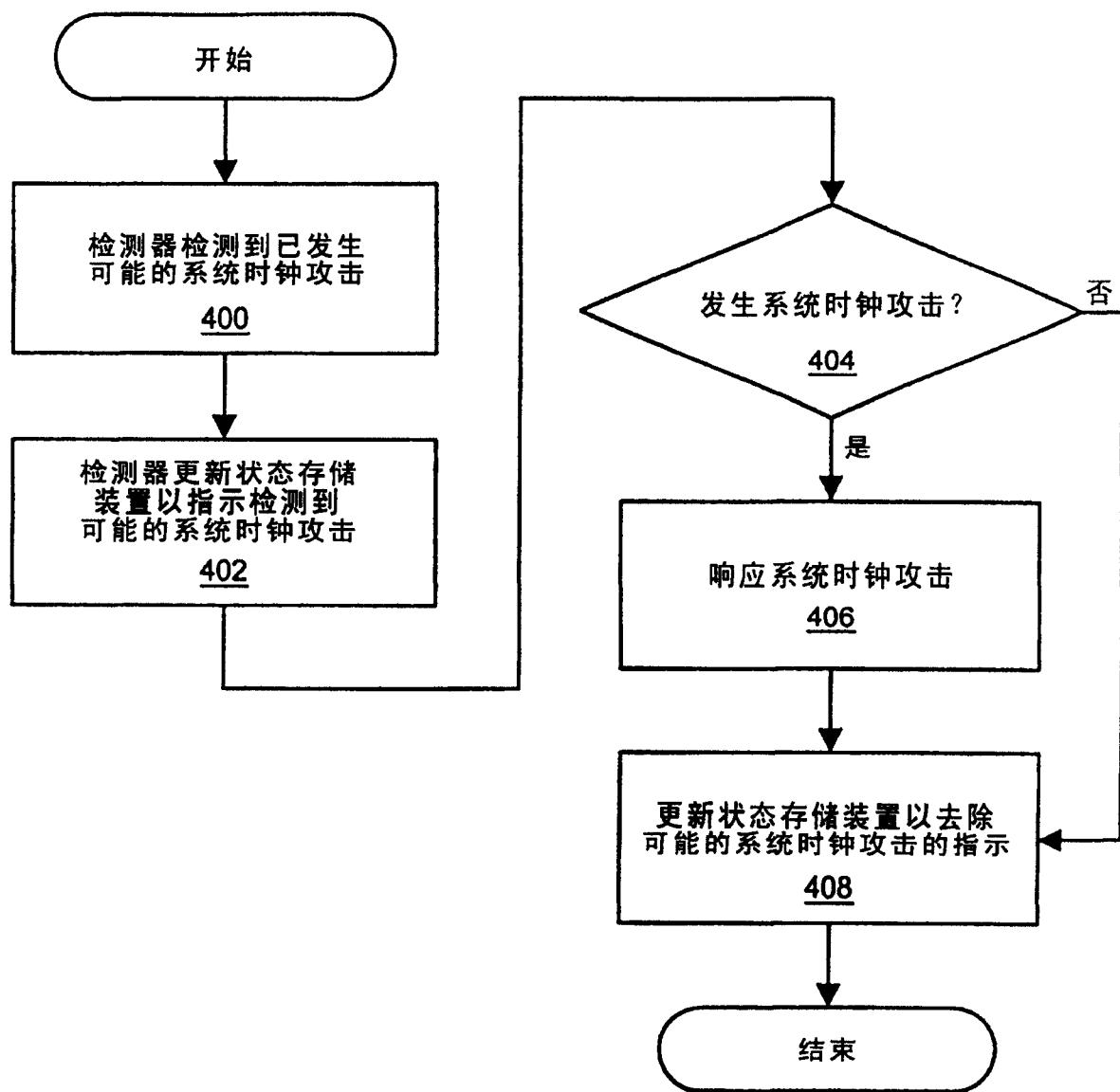


图4