(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 107771324 A
(43)申请公布日 2018.03.06

(21)申请号 201580079000.8

(22)申请日 2015.09.17

(85)PCT国际申请进入国家阶段日
2017.10.19

(86)PCT国际申请的申请数据
PCT/US2015/050632 2015.09.17

(87)PCT国际申请的公布数据
WO2017/048256 EN 2017.03.23

(71)申请人 慧与发展有限责任合伙企业
地址 美国德克萨斯州

(72)发明人 W·G·霍恩 A·J·阿瓦德
P·K·马纳达它

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
G06F 12/14(2006.01)
H04L 9/06(2006.01)

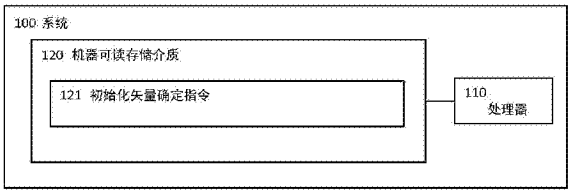
权利要求书3页 说明书7页 附图2页

(54)发明名称

有效地存储初始化矢量

(57)摘要

示例涉及在系统中的初始化矢量的有效存储。一个示例便于确定用于在对存储器的第一页面的第一高速缓存行加密时使用的初始化矢量，其中确定初始化矢量包括：级联页面级计数器与第一组分级计数器。第一组分级计数器包括：与第一高速缓存行相关联的第一计数器；与高速缓存行的第一分组相关联的第一分组计数器，高速缓存行的第一分组包括第一高速缓存行；以及与高速缓存行分组的第一群集相关联的第一群集计数器，第一群集包括高速缓存行的第一分组。



CN 107771324 A

1.一种用于初始化矢量的有效存储的系统，所述系统包括：实现存储在非暂时性机器可读存储介质上的机器可读指令的物理处理器，所述机器可读指令使所述系统用于：

确定用于在对存储器的第一页面的第一高速缓存行加密时使用的初始化矢量，其中，确定所述初始化矢量包括：

级联页面级计数器与第一组分级计数器，所述第一组分级计数器包括：

与所述第一高速缓存行相关联的第一计数器；

与高速缓存行的第一分组相关联的第一分组计数器，所述高速缓存行的第一分组包括所述第一高速缓存行；以及

与高速缓存行分组的第一群集相关联的第一群集计数器，所述第一群集包括所述高速缓存行的第一分组。

2.如权利要求1所述的系统，其中，所述第一页面的每个高速缓存行与以下相关联：相对应的计数器、与包括所述高速缓存行的相对应的分组相关联的相对应的分组计数器，以及与包括所述相对应的分组的相对应的群集相关联的相对应的群集计数器。

3.如权利要求1所述的系统，其中，所述物理处理器实现机器可读指令，所述机器可读指令使所述系统用于：

响应于新数据被写到所述第一高速缓存行而使所述第一计数器递增；

更新所述初始化矢量以包括递增的第一计数器；以及

使用更新的初始化矢量来对所述第一高速缓存行加密。

4.如权利要求3所述的系统，其中，所述物理处理器实现机器可读指令，所述机器可读指令使所述系统用于：

响应于所述第一计数器上溢而使所述第一分组计数器递增；以及

初始化与所述第一分组计数器相关联的第一组计数器。

5.如权利要求4所述的系统，其中，所述物理处理器实现机器可读指令，所述机器可读指令使所述系统用于：

响应于所述第一分组计数器上溢而使所述第一群集计数器递增；以及

初始化与所述第一群集计数器相关联的所述第一组分组计数器；以及

响应于初始化所述第一分组计数器而初始化与所述第一分组计数器相关联的所述第一组计数器。

6.如权利要求5所述的系统，其中，所述物理处理器实现机器可读指令，所述机器可读指令使所述系统用于：

响应于初始化所述第一分组计数器而初始化与所述第一分组计数器相关联的所述第一组计数器。

7.如权利要求6所述的系统，其中，所述物理处理器实现机器可读指令，所述机器可读指令使所述系统用于：

响应于将第二数据写到所述第一高速缓存行，通过以下来确定用于对所述第一高速缓存行的数据加密的第二初始化矢量：

级联递增的第一群集计数器、递增的第一分组计数器和递增的第一计数器。

8.一种用于将初始化矢量有效地存储在包括实现计算机可读指令的物理处理器的系统中的方法，所述方法包括：

将数据写到存储器的第一页面的第一高速缓存行；

确定用于在对所述第一高速缓存行加密时使用的初始化矢量；

使用确定的初始化矢量来对所述第一高速缓存行加密，其中，确定所述初始化矢量包括：

级联页面级计数器与第一组分级计数器，所述第一组分级计数器包括：

与所述第一高速缓存行相关联的第一计数器；

与高速缓存行的第一分组相关联的第一分组计数器，所述高速缓存行的第一分组包括所述第一高速缓存行；以及

与高速缓存行分组的第一群集相关联的第一群集计数器，所述第一群集包括所述高速缓存行的第一分组。

9.如权利要求8所述的方法，其中，所述第一页面的每个高速缓存行与以下相关联：相对应的计数器、与包括所述高速缓存行的相对应的分组相关联的相对应的分组计数器，以及与包括所述相对应的分组的相对应的群集相关联的相对应的群集计数器。

10.如权利要求8所述的方法，还包括：

响应于新数据被写到所述第一高速缓存行而使所述第一计数器递增；

响应于所述第一计数器上溢而使所述第一分组计数器递增；以及

初始化与所述第一分组计数器相关联的第一组计数器。

11.如权利要求10所述的方法，还包括：

响应于所述第一分组计数器上溢而使所述第一群集计数器递增；以及

初始化与所述第一群集计数器相关联的所述第一组分组计数器；以及

响应于初始化所述第一分组计数器而初始化与所述第一分组计数器相关联的所述第一组计数器。

12.如权利要求11所述的方法，还包括：

响应于初始化所述第一分组计数器而初始化与所述第一分组计数器相关联的所述第一组计数器。

13.如权利要求12所述的方法，还包括：

响应于将第二数据写到所述第一高速缓存行，通过以下来确定用于对所述第一高速缓存行的数据加密的第二初始化矢量：

级联递增的第一群集计数器、递增的第一分组计数器和递增的第一计数器。

14.一种包括用于有效地存储初始化矢量的指令的非暂时性机器可读存储介质，所述指令能够由系统的物理处理器执行以用于：

对于存储器的页面的每个高速缓存行，确定用于在对所述高速缓存行加密时使用的相对应的初始化矢量，其中，确定所述相对应的初始化矢量包括：

级联页面级计数器与相对应的一组分级计数器，所述相对应的一组分级计数器包括：

与相对应的高速缓存行相关联的相对应的计数器；

与高速缓存行的相对应的分组相关联的相对应的分组计数器，高速缓存行的第一分组包括所述相对应的高速缓存行；以及

与高速缓存行分组的相对应的群集相关联的相对应的群集计数器，所述相对应的群集包括所述高速缓存行的相对应的分组。

15.如权利要求14所述的非暂时性机器可读存储介质，还包括指令，所述指令能够由所述系统的物理处理器执行以用于：

响应于新数据被写到相对应的高速缓存行而使计数器递增；

更新所述初始化矢量以包括递增的计数器；以及

使用更新的初始化矢量来对所述相对应的高速缓存行加密。

有效地存储初始化矢量

背景技术

[0001] 在安全处理系统中，数据必须被保护而避开内部和外部对手。存储在安全处理系统中的数据常常被加密。该数据可在数据存储到系统内时由预先生成的加密填充加密。可基于初始化矢量和加密密钥来生成这些预先生成的加密填充。

附图说明

[0002] 下面的详细描述参考附图，其中：

[0003] 图1是用于初始化矢量的有效存储的示例系统的方框图；

[0004] 图3是用于初始化矢量的有效存储的用于存储初始化矢量的高速缓存树的示例描绘；

[0005] 图3是用于初始化矢量的有效存储的示例系统的方框图；

[0006] 图4是用于初始化矢量的有效存储的示例方法的流程图；以及

[0007] 图5是用于初始化矢量的有效存储的示例方法的流程图。

具体实施方式

[0008] 下面的详细描述引用附图。在可能的情形下，相同的附图标记在附图和下面的描述中用于指代相同或相似的部件。虽然在这个文档中描述了几个示例，但是修改、改编和其它实现是可能的。相应地，下面的详细描述并不限制所公开的示例。替代地，所公开的示例的正确范围可由所附权利要求限定。

[0009] 如上面提到的，在安全处理系统中，数据必须被保护而避开内部和外部对手。存储在安全处理系统中的数据常常被加密。该数据可在数据存储到系统内时由预先生成的加密填充加密。可基于初始化矢量和加密密钥来生成这些预先生成的加密填充。可在高速缓存行被传送时生成这些预先生成的加密填充。一旦高速缓存行被传送时，可以在加密填充和数据之间(例如，如在AES-Ctr模式加密中的)执行低时延操作(例如XOR)以生成加密数据。如果相同的初始化矢量值与相同的加密密钥一起被使用，则加密方案可能被破坏。因此，相同的初始化矢量值不能再次与相同的加密密钥一起被使用。

[0010] 为了处理这个问题，安全处理系统将初始化矢量部分地实现为计数器，并且每当数据使用相同的加密密钥被加密时使初始化矢量递增。特别是，初始化矢量常常包括128位值，64位用于高速缓存行地址，而64位用于计数器。因此，如在本文使用的术语“使初始化矢量递增”可以是使初始化矢量的计数器部分递增，且初始化矢量值可以是初始化矢量的计数器的值。类似地，确定初始化矢量可以是确定初始化矢量的计数器的值。

[0011] 初始化矢量的递增引起它自己的一组技术挑战。因为每当使用相同的加密密钥对数据加密时，不同的初始化矢量被使用，最新的初始化矢量值需要被存储，以便能够对所存储的数据解密。如果每个高速缓存行存储它自己的初始化矢量，则每个64字节高速缓存行将引起12.5％存储开销，导致存储和效率问题。这些存储和效率问题由于在高速缓存行中的初始化矢量上溢的潜在后果而恶化。因此，其中每个高速缓存行存储它自己的初始化矢

量的解决方案可能对于大规模地在存储器系统中实现是在技术上有挑战性的。

[0012] 对这个技术挑战的新技术解决方案涉及初始化矢量的有效存储。特别是，示例安全处理系统通过使用一组分级计数器来有效地存储初始化矢量，以用于将存储器中的数据的高速缓存行加密。在存储器中的每个高速缓存行可与相对应的高速缓存行计数器相关联。每组n个高速缓存行可共享单个分组计数器。每组的m组计时器可共享单个群集计数器，等等，直到高速缓存行的p个级别的树形成为止，其中m、n和p是大于或等于2的正整数。树的根可以是直接分级地连接到计数器的最高级别的页面级计数器。可然后通过级联与那个高速缓存行相关联的这分组计数器(例如第一计数器的数据、第一分组计数器的数据、第一群集计数器的数据等)来确定特定的高速缓存行的初始化矢量。

[0013] 每当高速缓存行写入出现时，相对应的高速缓存行计时器将递增。如果高速缓存行计数器上溢，则与高速缓存行计数器相关联的分组计数器将递增，且与分组计数器相关联的所有高速缓存行计数器将被初始化。响应于上溢、分组计数器的递增和高速缓存行计时器的初始化，相对应的高速缓存行的数据将被重新加密。类似地，如果分组计数器上溢，则群集计数器将递增，且该组中的所有高速缓存行将再次被加密。这个模式将重复，直到最高级计数器递增到上溢为止。响应于最高级计数器上溢，页面计数器将递增，且在该页面中的所有高速缓存行将再次被加密。

[0014] 实现初始化矢量的有效存储的示例计算机系统可使用在计数器的分级结构中的3个级别的计数器(例如，高速缓存行计数器、与高速缓存行的第一分组计数器相关联的分组计数器和与一组分组计数器相关联的群集计数器)。在这个示例中，系统可确定用于在对存储器的第一页面的第一高速缓存行加密时使用的初始化矢量。确定初始化矢量可包括将页面级计数器与和第一高速缓存行相关联的第一组分级计数器级联。第一组分级计数器可包括例如与第一高速缓存行相关联的第一计数器、与高速缓存行的第一分组相关联的第一分组计数器(其中高速缓存行的第一分组包括第一高速缓存行)以及与高速缓存行分组的第一群集相关联的第一群集计数器，其中第一群集包括高速缓存行的第一分组。如下面进一步讨论的，在计数器的分级结构中的3个级别的使用仅仅是示例，且不限于可被使用的级别的量。

[0015] 现在参考附图，图1是用于初始化矢量的有效存储的示例系统100的方框图。在图1中描绘的示例中，系统100包括非暂时性机器可读存储介质120和处理器110。

[0016] 现在参考附图，图1是用于初始化矢量的有效存储的示例系统100的方框图。系统100可包括服务器、大型计算机、笔记本计算机、桌上型计算机、平板计算机、工作站、移动设备、基于云的设备和/或适合于执行下面所述的功能的任何其它设备。在图1的实施例中，系统100包括非暂时性机器可读存储介质120和处理器110。

[0017] 处理器110可以是一个或多个中央处理单元(CPU)、微处理器和/或适合于取回和执行存储在机器可读存储介质120中的指令的其它硬件设备。处理器110可取出、解码和执行程序指令121和/或其它指令以使初始化矢量的有效存储成为可能，如下所述。作为可替代的或除了取回和执行指令以外，处理器110可包括一个或多个电子电路，其包括用于执行一个或多个指令121和/或其它指令的功能的多个电子部件。

[0018] 在一个示例中，程序指令121和/或其它指令可以是可由处理器110执行来实现在本文所述的功能的安装封装的部分。在这种情况下，存储器120可以是由计算设备维持的便

携式介质，例如CD、DVD或闪存驱动器或存储器，安装封装可从便携式介质被下载和安装。在另一示例中，程序指令可以是已经安装在系统100上的一个或多个应用的部分。

[0019] 非暂时性机器可读存储介质120可以是用于维持系统100可访问的数据的任何硬件存储设备。例如，机器可读存储介质120可包括一个或多个硬盘驱动器、固态驱动器、磁带驱动器、存储器结构和/或任何其它存储设备。存储设备可位于系统100中，可越过不同的地理上分布设备和/或在与系统100通信的另一设备中被定位。例如，机器可读存储介质120可以是存储可执行指令的任何电子、磁性、光学或其它物理存储设备。因此，机器可读存储介质120可以是例如随机存取存储器(RAM)、电可擦除可编程只读存储器(EEPROM)、存储驱动器、光盘、通用存储器等。如下面更详细描述的，可以使用用于初始化矢量的有效存储的可执行指令来对机器可读存储介质120编码。如下面详述的，存储介质120可维持和/或存储在本文描述的数据和信息。

[0020] 例如，存储介质120可维持和/或存储与初始化矢量的有效存储有关的数据和信息。存储介质120可例如将存储器的每个页面的一组分级计数器存储在存储介质120中。

[0021] 初始化矢量确定指令121当由处理器110执行时可便于初始化矢量的有效存储，以用于在对数据的高速缓存行加密时使用。对于存储器的每个页面，初始化矢量确定指令121当由处理器110执行时可确定存储器的那个页面的每个高速缓存行的初始化矢量。每个页面可与页面级计数器和用于存储初始化矢量的高速缓存树相关联。页面级计数器和高速缓存树可被存储为页面的部分，可连同与页面的相关联性(例如指针、链路等)一起存储在存储介质120中，和/或以由处理器可访问的另一方式。在一些示例中，页面级计数器也可以是高速缓存树的部分。

[0022] 初始化矢量确定指令121当由处理器110执行时可经由高速缓存存储器将数据写到页面并取回数据。对于取回的或存储在高速缓存存储器中的每个高速缓存行，初始化矢量确定指令121当由处理器110执行时可根据需要对数据加密或解密。如上面提到的，初始化矢量确定指令121当由处理器110执行时可使用加密密钥(例如存储数据或从页面取回数据的用户的加密密钥)和初始化矢量对数据加密。也如上面提到的，每个高速缓存行与它自己的初始化矢量相关联。

[0023] 当数据经由高速缓存存储器被写到页面并从页面取回时，初始化矢量确定指令121当由处理器110执行时可通过使用页面级计数器和高速缓存树来确定被写入的高速缓存树的适当的初始化矢量。高速缓存树可包括至少三个级别的分级计数器，包括页面级计数器。初始化矢量确定指令121当由处理器110执行时可通过将与待加密(或解密)的高速缓存行相关联的每个级别的高速缓存树的计数器进行级联来确定适当的初始化矢量。

[0024] 在如上面提到的一些示例中，初始化矢量的计数器部分是64位。相应地，高速缓存树的所级联的计数器也具有64位的尺寸。在一些示例中，页面级计数器包括8位值或16位，使得在高速缓存树中的计数器的其余部分具有包括位的剩余数字的总值。所级联的计数器的尺寸应等于或稍微刻板地对应于初始化矢量的计数器部分的尺寸。

[0025] 在图2中描绘了高速缓存树的示例。如图2所示，每个高速缓存行具有它自己的计数器(例如第一计数器221)。与相对应的高速缓存树相关联的一分组计数器(例如第一计数器221、…、第n计数器222)可在第一分组计数器220A下被分组。分组计数器的每组(例如220A、….、220M)可被分组为第一群集计数器210A。为了确定与第一计数器221相关联的高

速缓存行的初始化矢量，初始化矢量确定指令121当由处理器110执行时可级联页面级计数器200、第一群集计数器210A、第一分组计数器220A和第一计数器221。类似地，为了确定与第n计数器234相关联的高速缓存行的初始化矢量，初始化矢量确定指令121当由处理器110执行时可级联页面级计数器200与p级群集计数器210N、第m分组计数器230N和第n计数器234。

[0026] 高速缓存树中的级别的数量和在每个级别的节点的数量不限于在图2中描绘的示例。多于3个级别的计数器可以在高速缓存树中可用，且在每个级别的节点的数量可在级别当中不同。在一些示例中，初始化矢量的尺寸、页面级计数器的尺寸、高速缓存树的级别的数量和/或在页面的高速缓存树的每个级别的节点的数量可取决于数据的类型、应用、用户和/或与存储在那个页面中的数据相关联的其它特性。

[0027] 实现初始化矢量的有效存储的示例计算机系统可使用在计数器的分级结构中的3个级别的计数器(例如高速缓存级计数器、与高速缓存行的第一分组计数器相关联的分组计数器和与一组分组的高速缓存行相关联的群集计数器)。在这个示例中，初始化矢量确定指令121当由处理器110执行时可确定用于在对存储器的第一页面的第一高速缓存行加密时使用的初始化矢量。初始化矢量确定指令121当由处理器110执行时可通过级联页面级计数器与和第一高速缓存行相关联的第一组分级计数器来确定初始化矢量。第一组分级计数器可包括例如与第一高速缓存行相关联的第一计数器、与高速缓存行的第一分组相关联的第一分组计数器(其中高速缓存行的第一分组包括第一高速缓存行)以及与高速缓存行分组的第一群集相关联的第一群集计数器，其中第一群集包括高速缓存行的第一分组。在一些示例中，第一组分级计数器可包括与每个级别的分级计数器的第一高速缓存行相关联的计数器。例如，使用图2的高速缓存树，初始化矢量确定指令121当由处理器110执行时可级联页面级计数器200、第一群集计数器210A、第一分组计数器220A和第一计数器221以确定在对第一高速缓存行加密时使用的初始化矢量。

[0028] 初始化矢量确定指令121当由处理器110执行时也可管理用于对存储在页面中的数据加密和解密的高速缓存树和初始化指令。例如，初始化矢量确定指令121当由处理器110执行时可管理其中高速缓存树中的计数器上溢的过程。

[0029] 下面是使用图2的高速缓存树的示例。响应于新数据被写到第一高速缓存行(与第一计数器221相关联)，初始化矢量确定指令121当由处理器110执行时可以使第一计数器221递增。响应于使第一计数器221递增，初始化矢量确定指令121当由处理器110执行时可更新初始化矢量以包括递增的第一计数器221并使用所更新的初始化矢量来对第一高速缓存行加密。初始化矢量确定指令121当由处理器110执行时可然后使第一高速缓存行的加密数据被写到存储介质120。

[0030] 在一些示例中，响应于第一计数器221递增，第一计数器221可上溢。响应于第一计数器221上溢，初始化矢量确定指令121当由处理器110执行时可使第一分组计数器220A递增。初始化矢量确定指令121当由处理器110执行时可响应于第一分组计数器220A递增而初始化第一分组计数器221、…、222。初始化矢量确定指令121当由处理器110执行时可通过将第一分组计数器置零来初始化第一分组计数器221、…、222和/或以另外方式初始化第一分组计数器221、…、222。响应于第一分组计数器221、…、222被初始化，初始化矢量确定指令121当由处理器110执行时可将与第一分组计数器221、…、222相关联的高速缓存行的数据

重新加密。

[0031] 在一些示例中，响应于第一分组计数器220A递增，第一分组计数器220A可上溢。响应于第一分组计数器220A上溢，初始化矢量确定指令121当由处理器110执行时可使第一群集计数器210A递增。初始化矢量确定指令121当由处理器110执行时可响应于第一群集计数器210A递增而初始化第一组分组计数器220A、…、220N。初始化矢量确定指令121当由处理器110执行时可通过将第一组分组计数器220A、…、220N置零来初始化第一组分组计数器220A、…、220N和/或以另外方式初始化第一组分组计数器220A、…、220N。响应于第一组分组计数器220A、…、220N被初始化，初始化矢量确定指令121当由处理器110执行时可初始化与在第一组分组计数器220A、…、220N中的每个分组计数器相关联的每分组计数器221、…、222、…223、…224。初始化矢量确定指令121当由处理器110执行时然后可将与初始化的计数器221、…、222、…223、…224相关联的高速缓存行的数据重新加密。

[0032] 在一些示例中，响应于第一群集计数器210A递增，第一群集计数器210A可上溢。响应于第一群集计数器210A上溢，初始化矢量确定指令121当由处理器110执行时可使页面级计数器递增。响应于页面级计数器递增，初始化矢量确定指令121当由处理器110执行时可初始化每组群集计数器210A、…、210N。初始化矢量确定指令121当由处理器110执行时也可以用与在这个示例中在上面所述的方式相同或类似的方式初始化分组计数器和与每个高速缓存行相关联的计数器，并可对页面中的每个高速缓存行重新加密。

[0033] 每当数据被请求、存储和/或以另外方式处理时，系统100可执行这个功能。

[0034] 图3是用于初始化矢量的有效存储的示例系统300的方框图。如图系统100一样，系统300可包括服务器、大型计算机、笔记本计算机、桌上型计算机、平板计算机、工作站、移动设备、基于云的设备和/或适合于执行下面所述的功能的任何其它设备。如图1的系统100一样，处理器310可以是一个或多个CPU、微处理器和/或适合于指令的取回和执行的其它硬件设备。图3的非暂时性机器可读存储装置可与图1的存储介质120相同或类似。图3的非暂时性机器可读存储介质可存储与和在非暂时性机器可读存储介质中的存储器的每个页面相关联的初始化矢量有关的信息。在一些示例中，由非暂时性机器可读存储介质存储的信息可与由非暂时性机器可读存储介质120存储的信息相同或类似。

[0035] 如下详述的，系统300可包括用于初始化矢量的有效存储的一系列引擎300。每个引擎可通常代表硬件和编程的任何组合。例如，引擎的编程可以是存储在非暂时性机器可读存储介质上的处理器可执行指令，且引擎的硬件可包括系统300的至少一个处理器以执行那些指令。此外或作为可选方案，每个引擎可包括一个或多个硬件设备，其包括用于实现下面所述的功能的电子电路。

[0036] 初始化矢量确定引擎320可便于系统300的初始化矢量的有效存储。例如，在使用计数器的分级结构中的3个级别的计数器(例如高速缓存级别计数器、与高速缓存行的第一分组相关联的分组计数器和与一组分组的高速缓存行相关联的群集计数器)的系统300中，初始化矢量确定引擎320可确定用于在对存储器的第一页面的第一高速缓存行加密时使用的初始化矢量。初始化矢量确定引擎320可通过级联页面级计数器与和第一高速缓存行相关联的第一组分级计数器来确定初始化矢量。第一组分级计数器可包括例如与第一高速缓存行相关联的第一计数器、与高速缓存行的第一分组相关联的第一分组计数器(其中高速缓存行的第一分组包括第一高速缓存行)以及与高速缓存行分组的第一群集相关联的第一

群集计数器，其中第一群集包括高速缓存行的第一分组。在一些示例中，第一组分级计数器可包括与在每个级别的分级计数器的第一高速缓存行相关联的计数器。

[0037] 在一些示例中，初始化矢量确定引擎320可以用与系统100的初始化矢量确定指令121的方式相同或类似的方式来便于初始化矢量的有效存储。在上面关于图1的初始化矢量确定指令121来提供关于初始化矢量确定引擎320的示例实现的另外的细节。

[0038] 图4是用于由计算设备执行的用于初始化矢量的有效存储的示例方法的流程图。

[0039] 虽然下面所述的方法的执行参考图1的系统100和/或图3的系统300，用于执行这种方法的其它适当的设备将对本领域中的技术人员而言是显而易见的。图4和其它附图中描述的方法可以以存储在机器可读存储介质例如存储介质120中的可执行指令的形式由本文所述的一个或多个引擎和/或以电子电路的形式实现。

[0040] 在操作400中，可将数据写到存储器的第一页面的第一高速缓存行。例如，系统100(和/或初始化矢量确定指令121、初始化矢量确定引擎320或系统100的其它资源)可将数据写到第一高速缓存行。系统100可以用与上面关于初始化矢量确定指令121的执行、初始化矢量确定引擎320或系统100的其它资源所述的方式类似或相同的方式将数据写到第一高速缓存行。

[0041] 在操作410中，可确定用于在对第一高速缓存行加密时使用的初始化矢量，其中初始化矢量可通过级联页面级计数器与第一组分级计数器来确定。例如，系统100(和/或初始化矢量确定指令121、初始化矢量确定引擎320或系统100的其它资源)可确定初始化矢量。系统100可以用与上面关于初始化矢量确定指令121的执行、初始化矢量确定引擎320或系统100的其它资源所述的方式类似或相同的方式确定初始化矢量。

[0042] 在操作420中，可使用所确定的初始化矢量来对第一高速缓存行加密。例如，系统100(和/或初始化矢量确定指令121、初始化矢量确定引擎320或系统100的其它资源)可对第一高速缓存行加密。系统100可以用与上面关于初始化矢量确定指令121的执行、初始化矢量确定引擎320或系统100的其它资源所述的方式类似或相同的方式对第一高速缓存行加密。

[0043] 图5是用于由计算设备执行的用于初始化矢量的有效存储的示例方法的流程图。

[0044] 在操作500中，第一计数器可响应于新数据被写到第一高速缓存行而递增。例如，系统100(和/或初始化矢量确定指令121、初始化矢量确定引擎320或系统100的其它资源)可使第一计数器递增。系统100可以用与上面关于初始化矢量确定指令121的执行、初始化矢量确定引擎320或系统100的其它资源所述的方式类似或相同的方式使第一计数器递增。

[0045] 在操作510中，第一分组计数器可响应于第一计数器上溢而递增。例如，系统100(和/或初始化矢量确定指令121、初始化矢量确定引擎320或系统100的其它资源)可使第一分组计数器递增。系统100可以用与上面关于初始化矢量确定指令121的执行、初始化矢量确定引擎320或系统100的其它资源所述的方式类似或相同的方式使第一分组计数器递增。

[0046] 在操作520中，第一群集计数器可响应于第一分组计数器上溢而递增。例如，系统100(和/或初始化矢量确定指令121、初始化矢量确定引擎320或系统100的其它资源)可使第一群集计数器递增。系统100可以用与上面关于初始化矢量确定指令121的执行、初始化矢量确定引擎320或系统100的其它资源所述的方式类似或相同的方式使第一群集计数器递增。

[0047] 在操作530中，第一组分组计数器可响应于使第一群集计数器递增而被初始化。例如，系统100(和/或初始化矢量确定指令121、初始化矢量确定引擎320或系统100的其它资源)可初始化第一组分组计数器。系统100可以用与上面关于初始化矢量确定指令121的执行、初始化矢量确定引擎320或系统100的其它资源所述的方式类似或相同的方式初始化第一组分组计数器。

[0048] 在操作540中，高速缓存行的第一分组计数器可响应于第一计数器递增或上溢而被初始化。例如，系统100(和/或初始化矢量确定指令121、初始化矢量确定引擎320或系统100的其它资源)可初始化高速缓存行的第一分组计数器。系统100可以用与上面关于初始化矢量确定指令121的执行、初始化矢量确定引擎320或系统100的其它资源所述的方式类似或相同的方式初始化高速缓存行的第一分组计数器。

[0049] 前述公开描述了用于初始化矢量的有效存储的多个示例实施方式。所公开的示例可包括用于初始化矢量的有效存储的系统、设备、计算机可读存储介质和方法。为了解释的目的，参考图1-5所示的部件描述了某些示例。然而，所示部件的功能可重叠，并可存在于更少或更大数量的元件和部件中。此外，所示元件的全部或部分功能可共同存在或分布在几个地理上分散的位置当中。而且，所公开的示例可在各种环境中实现，且不限于所示示例。

[0050] 此外，关于图1-5所述的操作的顺序是示例，且不是要进行限制。额外的或更少的操作或操作的组合可以使用或可改变而不偏离所公开的示例的范围。此外，与所公开的示例一致的实现不需要以任何特定的顺序执行操作的序列。因此，本公开仅仅阐述实现的可能示例，且可对所述示例做出很多变化和修改。所有这样的修改和变化被规定为被包括在本公开的范围内并被下面的权利要求保护。


100 系统
120 机器可读存储介质
121 初始化矢量确定指令
110
处理器

图1

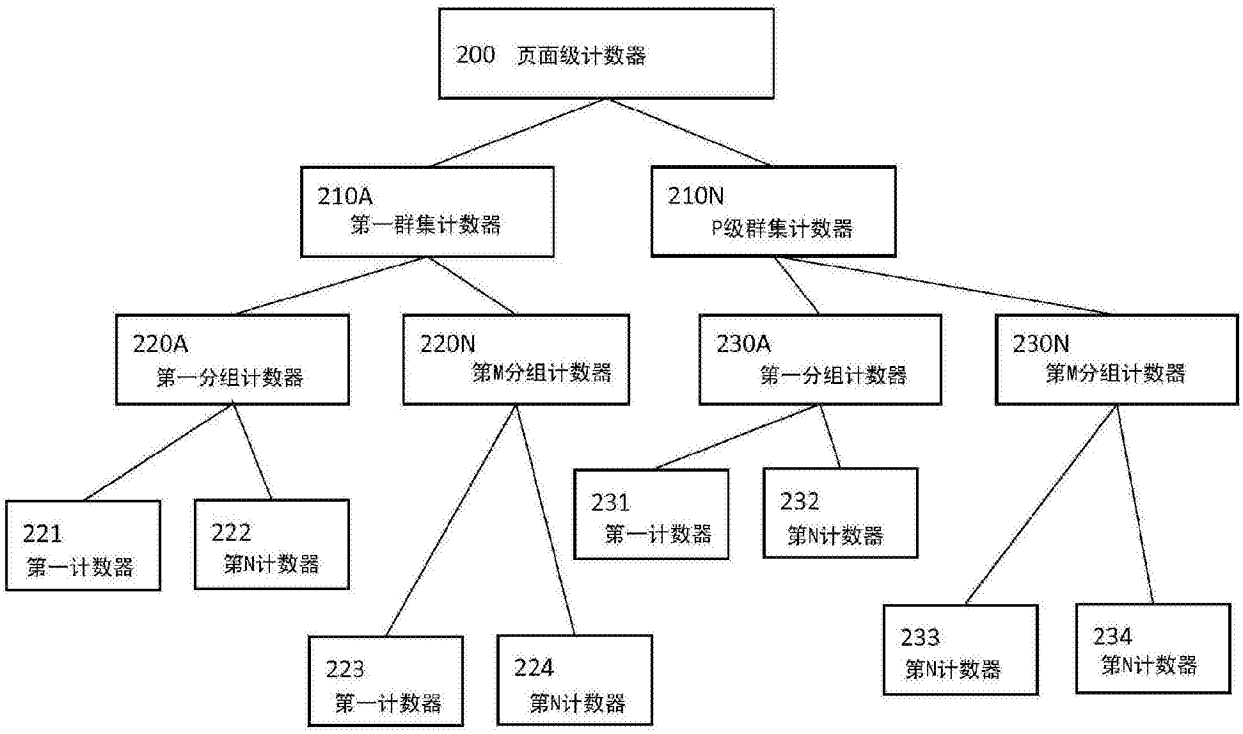

200 页面级计数器
210A
第一群集计数器
210N
P级群集计数器
220A
第一分组计数器
220N
第M分组计数器
230A
第一分组计数器
230N
第M分组计数器
221
第一计数器
222
第N计数器
223
第一计数器
224
第N计数器
231
第一计数器
232
第N计数器
233
第N计数器
234
第N计数器

图2

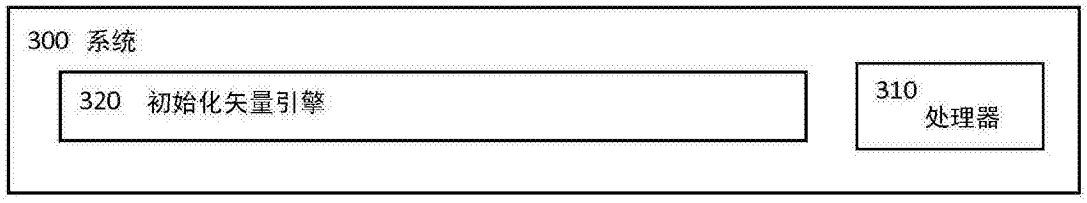

300 系统
320 初始化矢量引擎
310
处理器

图3

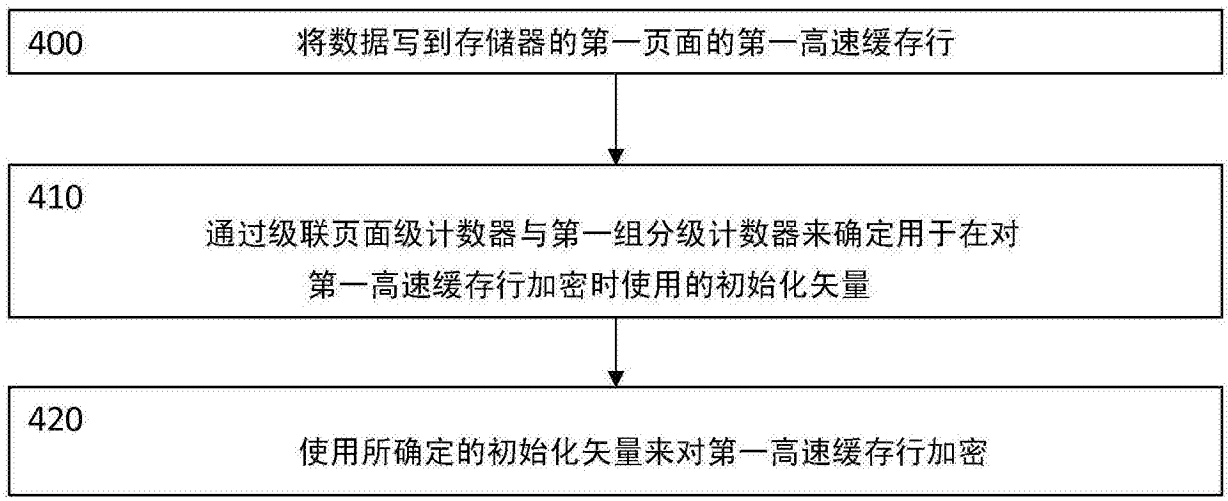

400
将数据写到存储器的第一页面的第一高速缓存行
410
通过级联页面级计数器与第一组分级计数器来确定用于在对第一高速缓存行加密时使用的初始化矢量
420
使用所确定的初始化矢量来对第一高速缓存行加密

图4

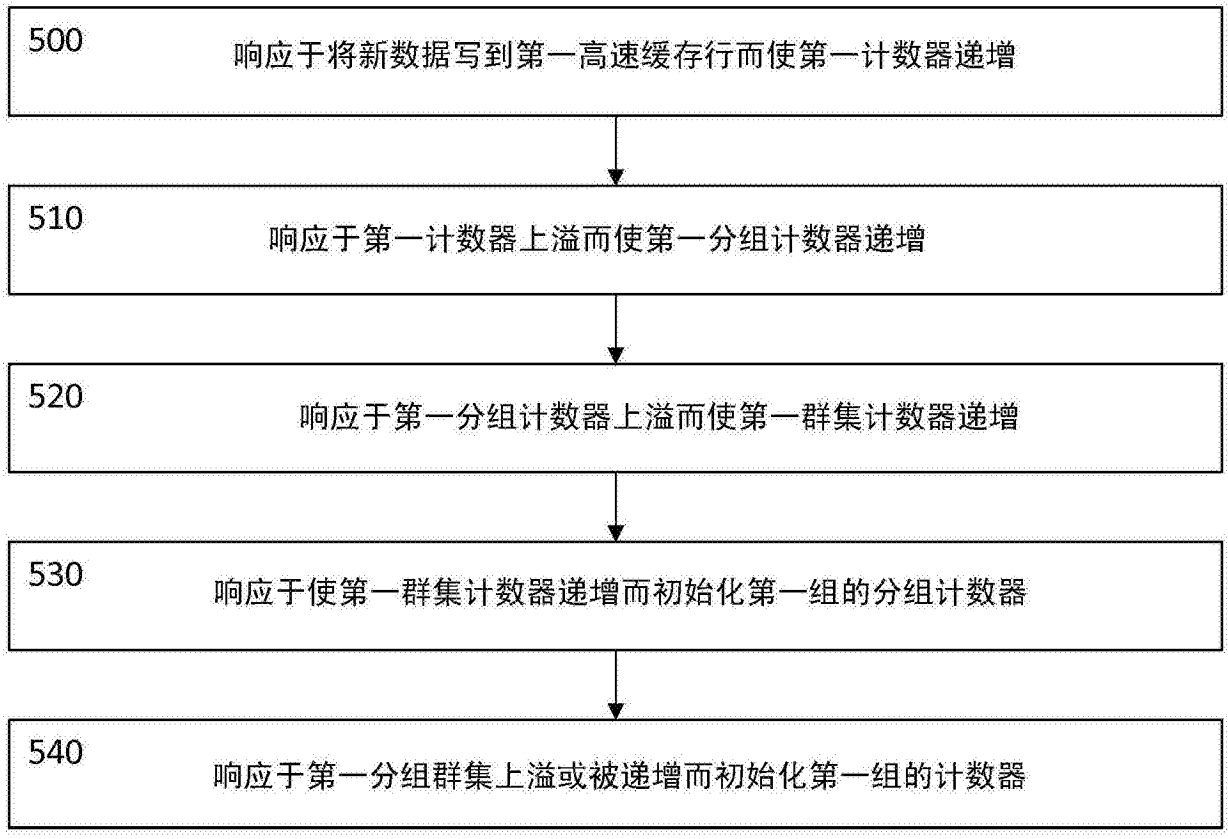

500
响应于将新数据写到第一高速缓存行而使第一计数器递增
510
响应于第一计数器上溢而使第一分组计数器递增
520
响应于第一分组计数器上溢而使第一群集计数器递增
530
响应于使第一群集计数器递增而初始化第一组的分组计数器
540
响应于第一分组群集上溢或被递增而初始化第一组的计数器

图5