(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108475237 B
(45)授权公告日 2021.07.13

(21)申请号 201680078576.7
(22)申请日 2016.09.21
(65)同一申请的已公布的文献号
申请公布号 CN 108475237 A
(43)申请公布日 2018.08.31
(30)优先权数据
14/993,455 2016.01.12 US
(85)PCT国际申请进入国家阶段日
2018.07.11
(86)PCT国际申请的申请数据
PCT/US2016/052839 2016.09.21
(87)PCT国际申请的公布数据
WO2017/123285 EN 2017.07.20

(73)专利权人 超威半导体公司
地址 美国加利福尼亚州
(72)发明人 努万·贾亚塞纳 张东平
(74)专利代理机构 上海胜康律师事务所 31263
代理人 樊英如 邱晓敏

(51)Int.Cl.
G06F 12/14(2006.01)
(56)对比文件
US 2013022201 A1,2013.01.24
CN 1242120 A,2000.01.19
CN 104298937 A,2015.01.21
US 2013145177 A1,2013.06.06
US 8234505 B2,2012.07.31
审查员 庄湧

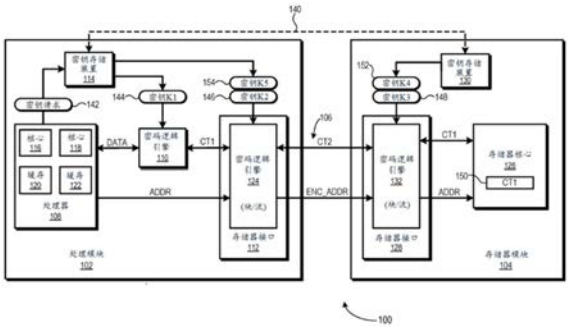
权利要求书4页 说明书10页 附图5页

(54)发明名称

存储器操作加密

(57)摘要

一种处理系统包括处理模块,该处理模块具有能耦合到互连的第一接口。该第一接口包括第一密码逻辑引擎,该第一密码逻辑引擎用于使用第一密钥和第一基于反馈的密码逻辑过程来加密存储操作的存储数据的表示和存储器地址,以产生第一经加密的数据和经加密的存储器地址。所述存储器地址对应于存储器模块的存储器位置,所述存储器模块包括多个存储器位置;并且其中所述第一接口将经由所述互连将所述第一经加密的数据和所述经加密的存储器地址传输到所述存储器模块。



CN 108475237 B

1.一种在电子装置中的方法,所述电子装置包括经由专用互连而耦合到存储器模块的处理模块,所述方法包括:

响应于存储操作的起始:

在所述处理模块处到所述互连的第一接口处,基于所述存储操作的属性从多个密钥中选择第一密钥;

在所述第一接口处使用所述第一密钥和第一基于反馈的密码逻辑过程来加密所述存储操作的存储数据的表示以产生第一经加密的数据;

在所述第一接口处使用所述第一密钥和所述第一基于反馈的密码逻辑过程来加密所述存储操作的存储器地址以产生经加密的存储器地址,所述存储器地址对应于所述存储器模块的存储器位置,所述存储器模块包括多个存储器位置;以及

经由所述互连将所述第一经加密的数据和所述经加密的存储器地址传输到所述存储器模块,

进一步包括:

经由所述互连将所述属性的表示从所述第一接口传送到第二接口;

在所述第二接口处基于所述属性的所述表示而从多个密钥选择第二密钥;

在所述第二接口处使用所述第二密钥和第二基于反馈的密码逻辑过程来解密所述第一经加密的数据以获得所述存储数据的所述表示的副本;

在所述第二接口处使用所述第二密钥和所述第二基于反馈的密码逻辑过程来解密所述经加密的存储器地址以获得所述存储器地址的副本;

基于所述存储器地址的所述副本将所述存储数据的所述表示的所述副本存储到存储器位置。

2.如权利要求1所述的方法,其中所述属性包括以下各者中的至少一者:发出所述存储操作的处理器核心的识别符;发出所述存储操作的进程的识别符;发出所述存储操作的线程的识别符;以及与所述存储操作相关联的地址空间的识别符。

3.如权利要求1所述的方法,其中所述第一密钥和所述第二密钥是相同的密钥。

4.如权利要求1所述的方法,进一步包括:

在所述第一接口处使用所述存储器地址和所述存储数据的所述表示来执行密码逻辑散列以产生第一散列值;

在所述第一接口处加密所述第一散列值以产生经加密的散列值;

经由所述互连将所述经加密的散列值从所述第一接口传输到所述第二接口;

在所述第二接口处解密所述经加密的散列值以产生所述第一散列值的副本;

在所述第二接口处使用所述存储器地址的所述副本和所述存储数据的所述表示的所述副本来执行密码逻辑散列以产生第二散列值;并且

其中基于所述存储器地址的所述副本将所述存储数据的所述表示的所述副本存储到所述存储器位置包括:响应于所述第二散列值与所述第一散列值的所述副本的比较的结果而将所述存储数据的所述表示的所述副本存储到所述存储器位置。

5.如权利要求1所述的方法,进一步包括:

在所述第一接口处确定序列号序列中的下一个序列号;

在所述第一接口处加密所述下一个序列号以产生经加密的序列号;

经由所述互连将所述经加密的序列号从所述第一接口传输到所述第二接口；

在所述第二接口处解密所述经加密的序列号以产生所述下一个序列号的副本；并且

其中基于所述存储器地址的所述副本将所述存储数据的所述表示的所述副本存储到所述存储器位置包括：响应于所述下一个序列号的所述副本与预期的下一个序列号的比较的结果而将所述存储数据的所述表示的所述副本存储到所述存储器位置。

6.如权利要求1所述的方法，其中所述第一基于反馈的密码逻辑过程包括块链接密码逻辑过程和流密码密码逻辑过程中的至少一者。

7.如权利要求1所述的方法，进一步包括：

在所述处理模块处使用第二密钥来加密所述存储数据以产生第二经加密的数据，其中所述存储数据的所述表示包括所述第二经加密的数据。

8.如权利要求1所述的方法，进一步包括：

在所述第一接口处使用所述存储器地址和所述第一经加密的数据来执行密码逻辑散列以产生第一散列值；以及

经由所述互连将所述第一散列值从所述第一接口传输到所述存储器模块。

9.一种在电子装置中的方法，所述电子装置包括经由专用互连而耦合到存储器模块的处理模块，所述方法包括：

响应于加载操作的起始：

在所述处理模块处到所述互连的第一接口处基于所述加载操作的属性而从多个密钥选择第一密钥；

在所述第一接口处使用所述第一密钥和第一基于反馈的密码逻辑过程来加密与所述加载操作相关联的存储器地址以产生经加密的存储器地址，所述存储器地址对应于所述存储器模块的存储器位置，所述存储器模块包括多个存储器位置；

经由所述互连将所述经加密的存储器地址传输到所述存储器模块；

经由所述互连将所述属性的表示从所述第一接口传送到第二接口；

在所述存储器模块处到所述互连的第二接口处基于所述属性的所述表示而从多个密钥选择第二密钥；在所述第二接口处使用所述第二密钥来解密所述经加密的存储器地址以获得所述存储器地址的副本；

在所述第二接口处基于所述存储器地址的所述副本而从所述存储器模块的存储器位置存取第一经加密的数据；

在所述第二接口处使用第三密钥和第二基于反馈的密码逻辑过程来加密所述第一经加密的数据以产生第二经加密的数据；

经由所述互连将所述第二经加密的数据从所述第二接口传输到所述第一接口；以及

在所述第一接口处使用第四密钥和第三基于反馈的密码逻辑过程来解密所述第二经加密的数据以获得所述第一经加密的数据的副本。

10.如权利要求9所述的方法，进一步包括：

在所述第一接口处使用第五密钥来解密所述第一经加密的数据的所述副本以获得用于所述加载操作的加载数据的副本。

11.如权利要求10所述的方法，其中：

所述第一密钥和所述第二密钥包括相同密钥；并且

所述第三密钥和所述第四密钥包括相同密钥。

12.如权利要求9所述的方法,其中:

所述第一、第二和第三基于反馈的密码逻辑过程中的每一个包括块链接密码逻辑过程或流密码密码逻辑过程中的一个。

13.一种处理系统,所述处理系统包括:

处理模块,所述处理模块包括:

至少一个处理器核心;

第一接口,所述第一接口耦合到所述至少一个处理器核心并且能够耦合到互连,所述第一接口包括:

第一密码逻辑引擎,所述第一密码逻辑引擎用于使用第一密钥和第一基于反馈的密码逻辑过程来加密存储操作的存储数据的表示和与所述存储数据相关联的存储器地址以产生第一经加密的数据和经加密的存储器地址,所述存储器地址对应于存储器模块的存储器位置,所述存储器模块包括多个存储器位置;并且

其中所述第一接口将经由所述互连将所述第一经加密的数据和所述经加密的存储器地址传输到所述存储器模块,

第二密码逻辑引擎,所述第二密码逻辑引擎用于使用第二密钥加密所述存储数据以产生第二经加密的数据,其中所述存储数据的所述表示包括所述第二经加密的数据,

其中所述处理模块进一步包括第一密钥存储装置,所述第一密钥存储装置用于基于所述存储操作的属性而从多个密钥选择所述第一密钥,

所述存储器模块进一步包括第二密钥存储装置,所述第二密钥存储装置用于基于经由所述互连所接收的所述属性的表示而从多个密钥选择所述第二密钥。

14.如权利要求13所述的处理系统,进一步包括:

所述存储器模块,所述存储器模块包括:

存储器核心;以及

第二接口,所述第二接口耦合到所述互连和所述存储器核心,所述第二接口包括第二密码逻辑引擎,所述第二密码逻辑引擎使用第二密钥和第二基于反馈的密码逻辑过程来解密所述第一经加密的数据和所述经加密的存储器地址以产生所述存储数据的所述表示的副本和所述存储器地址的副本;并且

其中所述第二接口将基于所述存储器地址的所述副本而将所述存储数据的所述表示的所述副本存储到所述存储器核心的存储器位置。

15.如权利要求14所述的处理系统,其中:

所述第一和第二基于反馈的密码逻辑过程中的每一个包括块链接密码逻辑过程或流密码密码逻辑过程中的一个。

16.如权利要求14所述的处理系统,其中:

所述第一接口包括第一密码逻辑散列模块,所述第一密码逻辑散列模块用于使用所述存储器地址和所述存储数据的所述表示来执行密码逻辑散列以产生第一散列值,并且所述第一接口将把所述第一散列值的表示传输到所述存储器模块;并且

所述第二接口包括:

第二密码逻辑散列模块,所述第二密码逻辑散列模块用于使用所述存储器地址的所述

副本和所述存储数据的所述表示的所述副本来执行密码逻辑散列以产生第二散列值;以及

散列比较逻辑,所述散列比较逻辑用于响应于所述第二散列值与所述第一散列值的比较的结果而授权将所述第一经加密的数据的所述副本存储到所述存储器位置。

存储器操作加密

[0001] 背景

[0002] 本公开的领域

[0003] 本公开大体上涉及利用存储器用于数据存储的处理系统，并且更具体来说，涉及利用经加密的存储器的处理系统。

[0004] 相关技术的描述

[0005] 已经提出使用经加密的存储器(即，其中存储器的内容经过加密)作为在数据拥有者对用于执行的硬件不具有物理控制的环境下增强安全性的一种方式。然而，经加密存储器的常规方法容易遭受基本的攻击技术，这是因为鉴于存储器存取的不可预知性以及典型的处理器-存储器架构的约束条件，需要个别地并且分开地加密缓存线。

[0006] 常规的经加密存储器实现方式通常依赖于基于电子码簿(ECB)的加密方案，其中仅依据将要存储在存储器中的数据和将要使用的加密密钥来加密所述数据。此方法具有若干弱点，例如以下事实：具有相同明文的任何两个缓存线会产生相同的密文，这可能会向经加密数据的观察者泄漏关于数据的信息。此类信息使得ECB容易遭受“字典”攻击，其中可以使用数据的统计性质来推断出关于经加密数据的信息，并且有可能甚至破译用于加密数据的加密密钥。常规的基于ECB的经加密存储器实现方式的另一弱点是，它们容易遭受数据“注入”攻击，其中攻击者将业务注入到处理器与存储器之间的互连上，这可能会破坏或覆写经加密数据。为了阻止此类攻击，常规的经加密存储器系统常常依赖于在存储器的整个内容上产生基于树的结构，并且因此需要许多存储器存取来认证每个加载操作或存储操作。

[0007] 附图简述

[0008] 通过参考附图，可以更好地理解本公开，并且使其众多特征和优势对于本领域技术人员显而易见。在不同图式中使用相同的参考符号会指示类似或等同的项目。

[0009] 图1是根据一些实施方案的采用经加密存储器的处理系统的框图。

[0010] 图2是说明根据一些实施方案的用于在图1的处理系统中执行安全存储器存取操作的方法的流程图。

[0011] 图3是说明根据一些实施方案的利用密码逻辑散列和序列号中的一者或两者来用于认证的成对存储器接口的示例性实现方式的框图。

[0012] 图4是说明根据一些实施方案的基于块链接的密码逻辑引擎的框图。

[0013] 图5是说明根据一些实施方案的图1的处理系统的示例性堆叠式处理器-存储器内(PIM)实现方式的图。

[0014] 详细描述

[0015] 图1至图5说明用于在处理系统中采用增强的经加密存储器的示例性方法和系统。在至少一个实施方案中，处理系统包括经由存储器总线或其他互连而耦合到存储器模块的处理模块。对于存储类型的存储器存取操作(即，“存储操作”)，所述处理模块使用第一密钥来加密缓存线或将要存储的其他数据以产生第一密文。所述处理模块的密码逻辑引擎随后使用第二密钥来加密所述第一密文以产生第二密文。所述密码逻辑引擎还使用所述第二密

钥或另一密钥来加密与存储操作相关联的存储器地址以产生经加密的存储器地址。经由互连将所述第二经加密的数据和所述经加密的存储器地址传输到存储器模块。存储器模块分别解密所述经加密的存储器地址和所述第二经加密的密文以获得存储器地址的副本和第一经加密的密文的副本。存储器模块随后将所述第一经加密的密文的所述副本存储在由存储器地址的副本寻址的存储器位置处。

[0016] 对于加载类型的存储器存取操作(即,“加载操作”),处理模块使用第二密钥或另一密钥来加密与加载操作相关联的存储器地址以产生经加密的存储器地址,并且经由互连将此经加密的存储器地址传输到存储器模块。存储器模块解密所述经加密的存储器地址以获得存储器地址的副本,并且存取在由存储器地址的副本寻址的存储器位置处存储的第一密文。存储器模块随后进一步加密所述第一密文以产生第二密文,经由接口将所述第二密文传输到处理模块。在所述处理模块处解密所述第二密文以产生第一密文的副本,并且解密第一密文的副本以产生由加载操作寻找的加载数据的副本。

[0017] 在至少一个实施方案中,每个存储器模块与每个处理模块之间的连接是由互连的单独、专用的例子以及所述互连的两侧处的对应的密码逻辑引擎服务。此配置产生以下情形:存储器模块处的密码逻辑引擎与处理模块处的密码逻辑引擎观察到相同的数据存取序列。因此,与常规的经加密的存储器实现方式相比,密码逻辑引擎可以利用密码逻辑过程,所述密码逻辑过程不仅随着正被加密的当前缓存线或其他数据而变,而且随着先前加密的一个或多个先前缓存线或其他数据而变。此类型的密码逻辑过程在本文被称作“基于反馈的密码逻辑过程”。反馈相依的密码逻辑过程的实例包括例如密码块链接(CBC)和密码反馈(CFB)算法等块链接密码逻辑过程,以及例如CryptMT和Rabbit算法等流密码。基于反馈的密码逻辑过程通常提供与仅随着正被加密的当前缓存线/数据而变的密码逻辑过程相比之下的增强的密码逻辑安全性,并且因此采用基于反馈的密码逻辑过程的能力提供了对未授权的观察者例如通过使用字典类型攻击或分析存储器存取模式来存取明文数据的未授权意图的提高的抵抗性。

[0018] 图1说明根据本公开的至少一个实施方案的采用安全数据存储的处理系统100。处理系统100可以表示(例如)其中存储在其中的数据的拥有者不具有对存储和处理所述数据的硬件的物理控制(例如,在“云”服务器情景下)的系统。在所描绘的实例中,处理系统100包括经由互连106而耦合到存储器模块104的至少一个处理模块102。

[0019] 处理模块102包括一个或多个处理器108、硬件密码逻辑引擎110、存储器接口112,并且进一步可以包括密钥存储装置114。处理器108可以包括(例如)中央处理单元(CPU)、图形处理单元(GPU)或其组合,并且可以包括一个或多个处理器核心,(例如,处理器核心116、118)以及一个或多个缓存(例如,缓存120、122)。存储器接口112耦合到处理器108、密码逻辑引擎110、密钥存储装置114和互连106,并且包括密码逻辑引擎124。

[0020] 存储器模块104作为用于处理模块102的经加密存储器而操作。为此,存储器模块104包括存储器核心126、存储器接口128,并且可以包括密钥存储装置130。存储器核心126包括多个存储器位置(未示出)或条目,每个存储器位置或条目经由对应的存储器地址(例如,物理存储器地址)进行存取。可以使用多种随机存取存储器(RAM)架构中的任一者来实施存储器核心126,所述架构例如为静态RAM(SRAM)架构、动态RAM(DRAM)架构、非易失性RAM(NVRAM)架构、快闪存储器架构等。存储器接口128耦合到存储器核心126、密钥存储装置130

和互连106，并且包括密码逻辑引擎132。

[0021] 互连106包括总线或充当处理模块102与存储器模块104之间的双向接口的其他类型的互连。互连106包括用于执行用于在模块102、104之间执行的存储器存取操作的信令的多个信号路径，包括用于传输存储器地址信息的信号路径、用于传输数据信息的信号路径、用于传输控制信息的信号路径等。在其中多个处理模块102连接到同一存储器模块104的实现方式中，在一个实施方案中，每个处理模块102具有与存储器模块104的单独、专用的互连106，并且存储器模块104随后将针对每个处理模块102/互连106实施单独的存储器接口128。类似地，在一些实施方式中，处理模块102可以连接到多个存储器模块104，在那种情况下，处理模块102将针对将处理模块102连接到对应的存储器模块104的每个互连106实施单独的存储器接口112。在此布置下，连接特定配对的处理模块102和存储器模块104的互连106的相对侧处的接口112、128都会观察到相同的加载操作和存储操作序列，并且因此可以实施基于反馈的密码逻辑过程。

[0022] 如在下文参考图5更详细地描述，在典型的实现方式中，将把处理模块102和存储器模块104实施为单独的装置或封装，并且因此将把互连106实施为横越中介物或上面实施有两个模块102、104的电路板或横越连接所述两个模块102、104的电缆的一组导电迹线。因此，互连106尤其可能容易遭受呈连接到导电迹线的物理分接头的形式的未授权的存取。未授权方随后可能会使用此类物理分接头以试图例如经由字典类型攻击来获得对存储在存储器模块104中或者另外在模块102、104之间传输的数据的明文版本的存取。

[0023] 鉴于互连106的脆弱性，处理系统100采用密码逻辑技术的组合来增强数据安全性。如在下文参考图2更详细地描述，模块102、104针对在互连106上传输(和存储在存储器核心126中)的数据采用基于反馈的密码逻辑过程，以便阻挠通过使用字典式攻击或分析所述互连上的数据流的统计性质的其他试图来试图存取呈明文形式的数据。此外，为了防止泄漏关于存储器存取模式的信息，模块102、104针对在互连106上传输的存储器地址采用加密方案。另外，如在下文参考图3和图4更详细地描述，处理系统100可以利用基于密码逻辑散列的认证过程或基于序列号的认证过程中的一者或两者来进一步增强处理系统100中的数据安全性。

[0024] 图2说明根据本公开的至少一个实施方案的用于执行安全存储器存取操作的处理系统100的操作的方法200。一般可以将存储器存取操作广泛地分类为存储类型存储器存取操作(“存储操作”)或加载类型存储器存取操作(“加载操作”)。对于存储操作，由处理模块102提供数据，用于存储在存储器模块104的存储器核心126中的对应位置处。相反，对于加载操作，从存储器核心126的对应位置存取数据并且将所述数据传输到处理模块102，因此将加载数据存储在处理器108的一个或多个缓存或寄存器中以供随后使用。通常，以缓存线的形式或大小完成数据存储或加载，因此本文参考以缓存线为示例性基础的数据的存储和存取，但在一些实施方案中，数据的大小可以被设计成小于或大于缓存线。

[0025] 在通电复位(POR)或其他初始化/重新初始化事件之后，并且在处理存储器存取操作之前，在框202处，处理系统100执行初始化过程，所述初始化过程通常包括处理模块102的存储器接口112与存储器模块104的存储器接口128之间的密钥交换140(图1)或其他密钥初始化。在一些实施方案中，处理系统100采用公开私密密钥方案。对于此方案，处理模块102的存储器接口112例如通过从预先识别的存储器位置读取公开密钥而向存储器接口128

询问存储器接口128的公开密钥，并且随后在密码逻辑引擎124处使用所述公开密钥来加密将要共享的密钥，并且将经加密的密钥传输到存储器模块104的存储器接口128。通过使用存储器接口128的对应的私密密钥来解密经加密的密钥，并且随后将所得的经解密的密钥存储在存储器模块104的密钥存储装置130中。

[0026] 替代地，存储器模块104可以产生将要由存储器接口112、128使用的密钥，并且将存储器接口112将要使用的密钥传送到处理模块102，因此，将所述密钥存储在处理模块102的密钥存储装置114中。这可以通过(例如)以下方式实现：存储器接口128产生密钥(例如，响应于来自处理模块102的命令)；使用由处理模块102提供的公开密钥来加密所述密钥；以及随后将经加密的密钥存储在存储器核心126中的已知位置，因此，处理模块102可以存取所述经加密的密钥，使用对应的私密密钥来解密所述经加密的密钥，并且将所述经解密的密钥存储在密钥存储装置130中。

[0027] 处理系统100的一些使用可以导致多个数据拥有者同时利用处理模块102和存储器模块104。因此，为了进一步确保数据的安全性，在此类实现方式中，可以实施多个密钥组。为了说明，可以基于每个物理请求者(例如，每个核心)、每个线程、每个过程、每个地址空间等来实施不同的密钥组。在这些情况下，在密钥存储装置114、130内基于请求者识别符(ID)或其他存储器存取属性(例如，核心ID、线程ID、过程ID或地址空间ID)将不同的密钥组编制索引，随后在起始存储器存取操作时参考所述请求者识别符或其他存储器存取属性来存取适当的密钥组，如下文论述。

[0028] 在使用适当的密钥起始存储器接口112、128和密钥存储装置114、130的情况下，处理系统100准备好执行存储器存取操作。因此，在框204处，处理模块102处的请求者起始存储器存取操作，如上文所述，所述存储器存取操作一般采取将数据存储到存储器模块104的存储操作或从存储器模块104存取数据的加载操作的形式。在多个密钥组在使用中的情况下，在框206处，存储器接口112、128分别从密钥存储装置114、130存取适当的密钥组。为了说明，当在框204处起始存储器存取操作时，或者当请求者从先前的请求者取得对处理模块102的资源的控制权时，在框206处，处理器108可以向密钥存储装置114发出密钥请求142(图1)，其中所述密钥请求142可以包括相关的存储器存取属性的表示，例如请求存储器存取操作或与存储器存取操作相关的地址空间的ID的核心、线程、进程的ID。此外，存储器接口112向存储器接口128提供此相同信息，使得可以从存储器模块104的密钥存储装置130存取适当的密钥组。

[0029] 在一些实施方案中，存储器接口112将存储器存取属性信息或某一其他代表性索引作为互连106上的单独通信(所述通信可以经由预先识别的公开-私密密钥进行加密)或者在传输对应的存储器存取请求之前经由单独的边频带连接将存储器存取属性信息或某一其他代表性索引提供给存储器接口132。在另一实施方案中，存储器接口112可以包括存储器存取属性或其他代表性索引作为针对存储器存取请求而提供的信令的部分(例如，在控制信令内)。从相应的密钥存储装置114、130存取对应的密钥(在下文描述)并且将所述密钥临时存储在密码逻辑引擎110、124、132的对应的缓冲器或寄存器中。

[0030] 在初始化密码逻辑引擎110、124、132的情况下，处理系统100准备好开始存储器存取操作，所述存储器存取操作可以包括存储操作或加载操作。图2的流路径208说明针对存储操作而执行的过程，并且图2的流路径210说明针对加载操作而执行的过程。

[0031] 在流路径208的框212处起始存储操作，因此，将要存储在存储器核心126的对应的寻址位置(例如，从缓存120、122中的一者逐出的缓存线)处的明文存储数据(在图1中表示为“DATA”)被提供给密码逻辑引擎110，因此，密码逻辑引擎110使用仅处理模块102知晓的密钥K1(密钥144，图1)来加密所述明文数据，从而产生第一经加密的数据或密文(在本文表示为密文“CT1”)。可以使用多种加密算法中的任一者来加密所述明文数据，所述加密算法例如为AES(高级加密标准)、DES(数据加密标准)、3DES(三重DES)、PGP(优良隐私)、Blowfish等。随后将第一密文CT1和数据将要被存储到的存储器地址(表示为“ADDR”)提供给存储器接口112，其中，在框214处，密码逻辑引擎124根据基于反馈的密码逻辑过程(例如，CFB或流密码)使用不同的密钥K2(密钥146，图1)来分别加密第一密文CT1和存储器地址ADDR，以产生第二经加密的数据(表示为密文“CT2”)和经加密的存储器地址(表示为“EN_ADDR”)。虽然图1说明借以在跨越互连106传输数据之前将所述数据加密两次的实现方式，但在一些实施方案中，省略了密码逻辑引擎110的第一加密，在那种情况下，将明文数据DATA提供给密码逻辑引擎110来取代密文CT1，用于加密为密文CT2。

[0032] 在一个实施方案中，分开地(但并行地)加密第一密文CT1和存储器地址ADDR以产生单独的经加密值。然而，在其他实施方案中，可以例如通过在加密之前将第一密文CT1和存储器地址串接成单个值而将第一密文CT1和存储器地址ADDR一起加密，从而产生单个经加密值。在框216处，存储器接口112经由在互连106上执行的信令而将存储请求传输到存储器模块104，其中所述信令包括第二密文CT2和经加密的存储器地址EN_ADDR。

[0033] 存储器接口128接收表示所述存储请求的信令，并且在框218处，密码逻辑引擎132使用密钥K3(密钥148，图1)来解密第二密文CT2和经加密的存储器地址EN_ADDR，以产生第一密文CT1的副本和存储器地址ADDR的明文副本。密码逻辑引擎124、132可以采用对称密钥加密过程(例如，AES、DES)，在那种情况下，密钥K2和K3是相同密钥。在地址被解密的情况下，在框220处，存储器接口128将第一密文CT1存储在由在框218处获得的存储器地址ADDR寻址或者另外与所述存储器地址相关联的存储器核心126的存储器位置150(图1)处。

[0034] 可以采用多种加密算法中的任一者来加密和解密第一密文CT1和存储器地址ADDR，例如上述加密算法中的任一者。具体来说，因为每个互连106特定于特定的处理模块/存储器模块配对，所以处理模块102的存储器接口112和存储器模块104的存储器接口128都会看到相同的缓存线或其他数据序列。因此，密码逻辑引擎124、132各自可以采用基于反馈的加密技术，其中相同的明文项目分别在加密过程和解密过程期间的重现不会产生相同的密文，例如流密码或块链接密码，如下文参考图4详细描述。

[0035] 如流路径208所演示，在存储操作期间，存储数据在于互连106上传输之前会经由块链接或流密码进行加密，这通常避免了每次对给定明文值的加密会产生相同的经加密值的情形。因此，系统100抵抗住通过分析在互连106上传输的数据而进行的字典式攻击。此外，在其中利用密码逻辑引擎110的实施方案中，数据在存储于存储器核心126中时保持经加密的形式(作为密文CT1)，因此阻挠了在未授权实体突破了存储器核心126的情况下获得对数据的明文版本的存取的试图。另外，用于存储操作的存储器地址ADDR在传输之前经过加密，从而防止泄漏可以用作对处理系统100的数据的攻击的基础的存储器存取模式或其他存储器存取信息。

[0036] 返回到框206，在存储器存取操作是加载操作的情况下，将用于加载操作的存储器

地址(表示为“ADDR”)从处理器108提供给存储器接口112,因此在框222处,密码逻辑引擎124使用密钥K2(密钥146,图1)和块链接或流密码算法来加密存储器地址以产生经加密的存储器地址(表示为“EN_ADDR”)。用于加载操作的密钥K2可以是用于存储操作的同一密钥K2,或者可以是不同的密钥。在框224处,存储器接口112经由在互连106上执行的信令而将加载请求传输到存储器模块104,其中所述信令包括经加密的存储器地址EN_ADDR。

[0037] 存储器接口128接收表示所述加载请求的信令,并且在框226处,密码逻辑引擎132使用密钥K3(密钥148,图1)和对应的块链接或流密码算法来解密经加密的存储器地址EN_ADDR,以产生存储器地址ADDR的明文副本。用于加载操作的密钥K3可以是用于存储操作的同一密钥K3,或者可以是不同的密钥。在框228处,存储器接口128从由存储器地址ADDR的所获得的副本参考的存储器核心126的存储器位置(例如,位置150,图1)存取所请求的数据。如上文阐释,在存储操作期间,将所述数据作为经加密的数据或密文存储在存储器核心126中,并且因此所存取的数据在本文被称作第一密文CT1。

[0038] 在从存储器核心126获得所请求的数据的情况下,在框230处,密码逻辑引擎132使用密钥K4(密钥152,图1)进一步加密经加密的密文CT1以产生第二密文CT2。在对称密钥加密实现方式中,密钥K4可以是与由密码逻辑引擎124使用的密钥K2相同的密钥,或者在共享密钥实现方式中,密钥K4可以是公开密钥-私密密钥对的公开密钥。在框232处,存储器接口128经由互连106使用表示加载结果或对存储器接口112的加载回复的信令将第二密文CT2传输到处理模块102。

[0039] 在于存储器接口112处接收到第二密文CT2的情况下,在框234处,密码逻辑引擎124使用密钥K5(密钥154,图5)解密第二密文CT2以产生存储在存储器核心126中的第一密文CT1的副本。在密码逻辑引擎124、132采用对称密钥加密的情况下,密钥K5可以是与密钥K2相同的密钥,并且可以是与密钥K4相同的密钥。替代地,如果采用公开密钥/私密密钥方案,那么密钥K5将是所述密钥对的私密密钥,其中密钥K4是公开密钥,如上文所述。在框236处,密码逻辑引擎110使用密钥K1来解密第一密文CT1的所获得的副本,以获得由第一密文CT1表示的明文加载数据的副本。随后可以将此明文加载数据存储在缓存线或核心116、118中的对应一者的其他临时存储位置处,以供加载操作的请求者存取。

[0040] 如流路径210所演示,在加载操作期间,在将加载数据于互连106上从存储器模块104传输到处理模块102之前使用基于反馈的密码逻辑过程来加密所述加载数据,并且用于所述加载操作的存储器地址ADDR在传输之前经过加密,这两种操作提供增强的数据安全性,与上文参考流路径208所述类似。

[0041] 因为互连106可以相对容易地被存取和物理分接,所以攻击者可能会试图使用互连106来注入假的存储操作,以便覆写存储在存储器模块104处的经加密的数据并且因此破坏存储在其中的数据。因此,为了防止此类攻击,在至少一个实施方案中,处理系统100可以采用各种认证过程来验证存储操作实际上是来自经授权的请求者的有效存储操作。此类认证过程可以包括(例如)密码逻辑散列认证过程或基于序列号的认证过程。

[0042] 图3说明根据至少一个实施方案的用于实施这些认证过程中的一者或两者的示例性硬件实现方式。在所描绘的实施方案中,存储器接口112的密码逻辑引擎124包括密码逻辑散列模块302、加密/解密模块304和序列号产生器305。类似地,存储器接口128的密码逻辑引擎132包括加密/解密模块306、密码逻辑散列模块308、散列比较逻辑310和序列号比较

逻辑312。

[0043] 对于基于散列的认证操作，将第一密文CT1和存储器地址ADDR输入到密码逻辑散列模块302，所述密码逻辑散列模块使用散列密钥X来执行第一密文CT1和存储器地址ADDR的密码逻辑散列以产生散列值(表示为“H1”)。随后将所述散列值H1输入到加密/解密模块304，因此，加密/解密模块304使用对应的密钥K(例如，密钥K2，图1)来分别加密所述散列值H1、第一密文CT1和存储器地址ADDR，以产生经加密的散列值(表示为“H2”)、第二密文CT2和经加密的存储器地址EN_ADDR。随后将经加密的散列值H2与第二密文CT2和经加密的存储器地址EN_ADDR一起作为用于存储操作的信令的部分进行传输，如上文描述。在于存储器接口128处接收到此信令的情况下，加密/解密模块306使用对应的密钥K(例如，密钥K3，图1)解密经加密的散列值H2、第二密码文本CT2和经加密的存储器地址EN_ADDR，以产生散列值H1和存储器地址ADDR的明文副本并且产生第一密文CT1的副本。

[0044] 为了验证所接收的存储操作是正当的，密码逻辑散列模块308使用散列值H1、存储器地址ADDR和第一密文CT1的所获得的副本来执行由密码逻辑散列模块302执行的相同或对称的散列操作，从而产生散列值(表示为“H3”)。散列比较逻辑310随后将散列值H1的所获得的副本与所产生的散列值H3进行比较。在比较结果揭露两个散列值匹配的情况下，散列比较逻辑310将存储操作识别为经过授权，并且因此提供“VALID”信号，存储器接口128响应于所述信号而继续处理所述存储操作。然而，因为攻击者不太可能具有用于密码逻辑散列模块302、308的密钥X的副本，所以攻击者注入欺诈性存储操作的试图将导致所获得的散列值H1与所产生的散列值H3之间的失配。在此情况下，散列比较逻辑310提供“NOP”信号，存储器接口128响应于所述信号而停止对存储操作的任何进一步处理，并且将所述存储操作视为“无操作”或“NOP”。

[0045] 对于基于序列号的认证操作，序列号产生器305产生序列号序列(例如，递增或递减序列)中的下一个序列号，并且将此序列号作为值SN提供到加密/解密模块304，所述加密/解密模块使用对应的密钥K(例如，密钥K2，图1)来分别加密所述序列号SN、第一密文CT1和存储器ADDR以产生经加密的序列号(表示为“EN_SN”)、第二密文CT2和经加密的存储器地址EN_ADDR。随后将这些值作为用于存储操作的信令的部分进行传输，如上文描述。在于存储器接口128处接收到此信令的情况下，加密/解密模块306使用对应的密钥K(例如，密钥K3，图1)来解密经加密的序列号EN_SN、第二密码文本CT2和经加密的存储器地址EN_ADDR，以产生序列号SN和存储器地址ADDR的明文副本并且产生第一密文CT1的副本。

[0046] 为了验证所接收的存储操作是正当的，序列号比较逻辑312使来自寄存器314或其他存储组件中的序列的当前序列号维持在使用中。这可以通过递增或递减所尝试的每个存储器存取操作的当前序列号的本地副本或者通过把将要认证的最后一个存储器存取操作的序列号存储在寄存器314中来实现。将序列号SN的经解密的副本从加密/解密模块306提供到序列号比较逻辑312，所述序列号比较逻辑随后将此序列号SN与当前序列号进行比较。如果所述比较指示所接收的序列号SN正确地是所述序列中的预期的下一个序列号，那么序列号比较逻辑312将存储操作识别为经过授权，并且因此提供“VALID”信号，存储器接口128响应于所述信号而继续处理所述存储操作。然而，因为攻击者不太可能知晓序列中的下一个序列号，所以攻击者使用虚构的序列号来注入欺诈性存储操作的试图将导致序列号SN的经解密的副本与所述序列中的预期的下一个序列号之间的失配。在此情况下，序列号比较

逻辑312提供“NOP”信号，存储器接口128响应于所述信号而停止对存储操作的任何进一步处理，并且将所述存储操作视为“无操作”或“NOP”。

[0047] 在一些实施方案中，可以并行地利用两个认证过程，在那种情况下，可以使用AND逻辑以在散列比较逻辑310和序列号比较逻辑312都发出“VALID”信号时提供“VALID”信号，并且在散列比较逻辑310和序列号比较逻辑312中的任一者发出“NOP”信号时提供“NOP”信号。

[0048] 在每个处理模块/存储器模块配对实施互连106和存储器接口112、128的单独实现方式时，给定处理模块102的存储器接口112观察到与互连106的另一侧上的对应的存储器接口128相同的存储器存取操作序列，并且反之亦然。因此，与常规系统相比，处理系统100可以采用流密码或块密码的链接模式作为在密码逻辑引擎124、132处执行的加密/解密过程的部分。在典型的链接模式或流密码中，缓存线或其他数据的加密(或者解密)不仅随着当前的缓存线/数据和加密密钥而变，而且随着在当前缓存线之前经加密的一个或多个先前加载操作或存储操作的缓存线/数据而变。然而，将此类反馈相依的密码逻辑过程实施于经加密的存储器系统中可能会在时序关键的存储器存取路径中引入第二加密过程，并且因此冒着增加存储器等待时间的风险。

[0049] 图4说明采用密码反馈(CFB)模式的密码逻辑引擎124、132的示例性硬件实现方式400，所述密码反馈模式通过在存储器存取关键路径之外产生密钥材料来减少对存储器存取等待时间的影响。在所描绘的实施方案中，硬件实现方式400表示可以由密码逻辑引擎124、132两者实施的加密路径硬件。可以通过相同的方式实施解密路径硬件。

[0050] 硬件实现方式400包括块密码逻辑404和“异或”逻辑406，所述逻辑在被识别为阶段401、402、403的三个连续加密阶段在逻辑上是重复的。块密码逻辑404具有两个输入端：用于接收密钥(在图4中表示为“KEY”)的一个输入端，和用于从前一阶段接收经加密输出的输入端，不同之处在于，第一阶段401替代地接收初始化向量(IV)。IV通常是如上文描述在初始化过程期间在处理模块102与存储器模块104之间交换的共享密钥信息的部分。在给定阶段，块密码逻辑404使用所述两个输入端来执行密码过程(加密或解密)，并且将结果输出到同一阶段的“异或”逻辑406的对应输入端。“异或”逻辑406具有用于接收与那个阶段相关联的对应数据的第二输入端。每个数据可以包括来自对存储器模块104的存储器存取操作序列的对应缓存线。每个数据可以包括来自对存储器模块104的存储器存取操作序列的对应存储器地址。在由图4说明的CFB模式中，从存储器存取关键路径移除几乎两个“异或”操作(在每个存储器接口处一个)，因此使对存储器等待时间的影响最小化，同时采用了由密码块链接技术给予的增强的安全性。

[0051] 如上文阐释，存储器模块104实施具有密码逻辑引擎132的存储器接口128。此布置尤其良好地适合于处理-存储器内(PIM)实现方式，所述实现方式利用紧密地耦合到对应的存储器电路的额外的逻辑。图5说明可以有利地利用本文描述的技术的示例性基于PIM的系统500。

[0052] 在所描绘的实例中，系统500包括主机处理器502(处理模块102的一个实施方案)和安置在中介物501(其可以包括电路板或裸片)上的一组一个或多个存储器堆叠(存储器模块104的一个实施方案)，例如存储器堆叠504、505、506、507。每个存储器堆叠包括裸片堆叠，所述裸片堆叠包括逻辑裸片508和一组存储器裸片509、510、511、512。逻辑裸片508实施

存储器接口128，并且存储器裸片实施存储器核心126。存储器堆叠的裸片通过穿硅通孔(TSV)(未示出)进行耦合，并且因此相对难以物理地分接。将主机处理器502连接到存储器堆叠504-507的中介物501的导电迹线(未示出)以及将所述导电迹线连接到对应组件的引脚(未示出)形成主机处理器502与存储器堆叠504-507之间的对应互连106(图1)。然而，与存储器堆叠的TSV不同，导电迹线和引脚是相对容易物理分接的，并且因此未授权实体相对容易接近，从而试图获得在这些互连上传输的数据的存取权。因此，基于PIM的系统500可以采用上文描述的双重加密、存储器地址加密、密码逻辑散列验证或基于链的加密技术中的一者或多者以确保互连和在其中传输的数据的完整性。

[0053] 在一些实施方案中，上文所描述的技术实施于包括一个或多个集成电路(IC)装置(还被称作集成电路封装或微芯片)(例如，上文参考图1至图5所描述的模块102、104)的系统中。可以在这些IC装置的设计和制造中使用电子设计自动化(EDA)和计算机辅助设计(CAD)软件工具。这些设计工具通常表示为一个或多个软件程序。所述一个或多个软件程序包括可以由计算机系统执行以便进行以下操作的代码：操纵计算机系统对表示一个或多个IC装置的电路的代码进行操作，以便执行用于设计或调适制造系统来制造电路的过程的至少一部分。此代码可以包括指令、数据或指令与数据的组合。表示设计工具或制造工具的软件指令通常存储在计算系统可存取的计算机可读存储介质中。同样，表示IC装置的设计或制造的一个或多个阶段的代码可以存储在同一计算机可读存储介质或不同计算机可读存储介质中并且从所述同一计算机可读存储介质或不同的计算机可读存储介质进行存取。

[0054] 在一些实施方案中，上文所描述的技术的某些方面可以由执行软件的处理系统的一个或多个处理器实施。所述软件包括存储在或另外有形地体现在非暂时性计算机可读存储介质上的一组或多组可执行指令。所述软件可以包括指令和某些数据，所述指令和某些数据当由一个或多个处理器执行时会操纵所述一个或多个处理器执行上文所描述的技术的一个或多个方面。非暂时性计算机可读存储介质可以包括可以由计算机系统在使用期间存取以将指令和/或数据提供给计算机系统的任何非暂时性存储介质，或非暂时性存储介质的组合。此类存储介质可以包括(但不限于)光学介质(例如，压缩光盘(CD)、数字多功能光盘(DVD)、蓝光光盘)、磁性介质(例如，软盘、磁带或磁性硬盘驱动器)、易失性存储器(例如，随机存取存储器(RAM)或缓存)、非易失性存储器(例如，只读存储器(ROM)或快闪存储器)，或基于微机电系统(MEMS)的存储介质。计算机可读存储介质可以嵌入计算系统(例如，系统RAM或ROM)中、固定地附接到计算系统(例如，磁性硬盘驱动器)、可移除地附接到计算系统(例如，光盘或基于通用串行总线(USB)的快闪存储器)，或经由有线或无线网络耦合到计算机系统(例如，网络可存取存储装置(NAS))。存储在非暂时性计算机可读存储介质上的可执行指令可以呈由一个或多个处理器解译或可以通过其他方式执行的源代码、汇编语言代码、目标代码，或其他指令格式。

[0055] 应注意，不需要上文在一般描述中所描述的所有活动或要素、可能不需要特定活动或装置的一部分，并且可以执行一个或多个其他活动，或者包括除了所描述的要素之外的要素。此外，列举活动的次序不一定是执行活动的次序。而且，已经参考特定实施方案描述了概念。然而，本领域技术人员应了解，可以在不脱离所附权利要求书中所陈述的本公开的范围的情况下作出各种修改和改变。因此，可以在说明性意义而不是限制性意义上对待说明书和图，并且希望所有此类修改包括在本公开的范围内。

[0056] 上文已关于特定实施方案描述了益处、其他优势和问题的解决方案。然而，这些益处、优势、问题的解决方案以及可以致使任何益处、优势或解决方案发生或变得更加突出的任何特征不应被解释为任何或所有权利要求的关键、所需或实质特征。另外，上文公开的特定实施方案仅是说明性的，因为所公开的标的可以按受益于本文教导的益处的本领域技术人员显而易见的不同但等效的方式加以修改和实践。除了所附权利要求书中所描述的内容之外，不希望对本文示出的构造或设计的细节进行限制。因此显然的是，可以更改或修改上文所公开的特定实施方案，并且所有此类变化都被视为在所公开的标的的范围内。因此，本文寻求的保护在所附权利要求书中予以陈述。

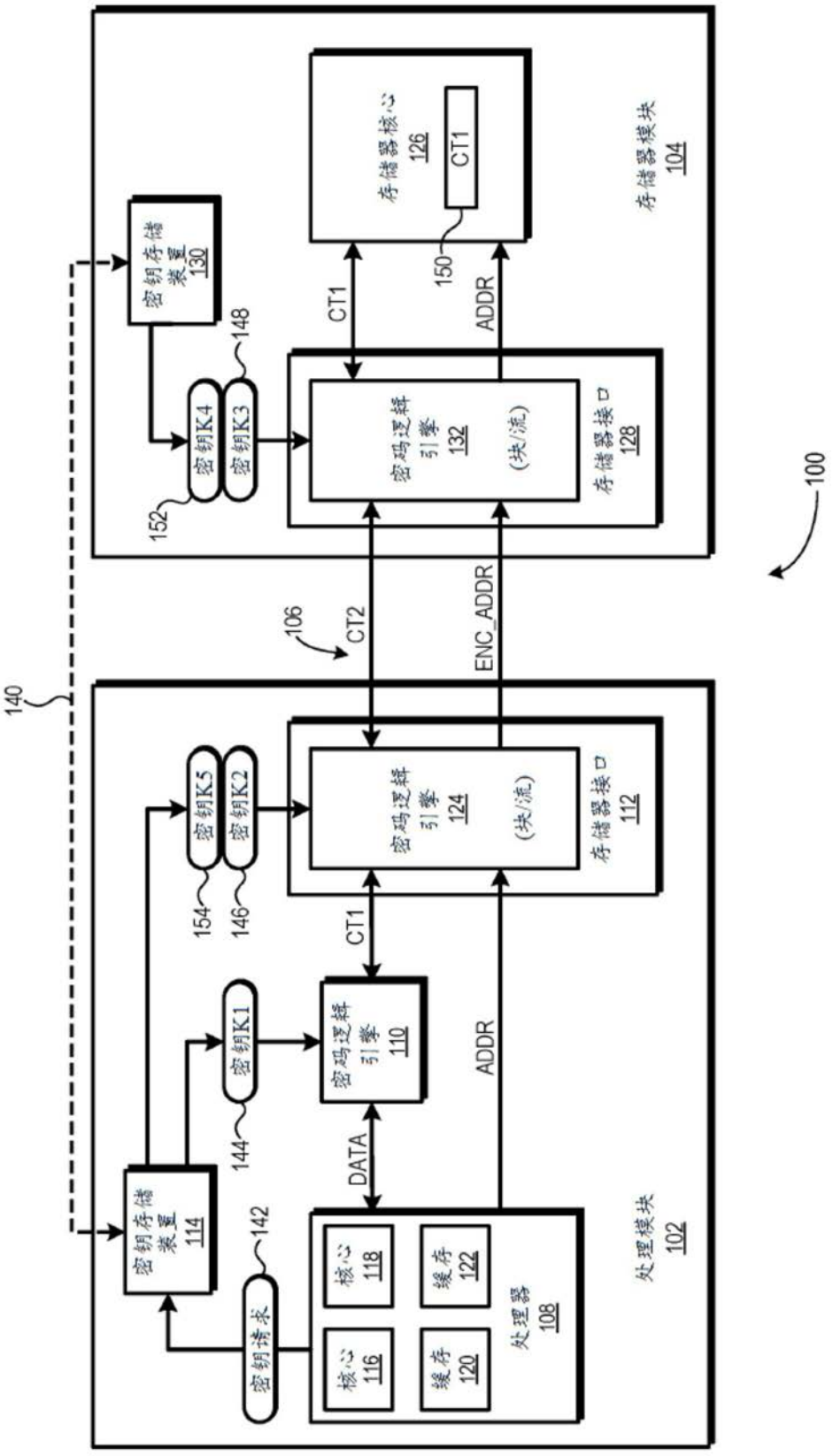

100
140
处理模块
102
存储器模块
104
106
CT2
ENC_ADDR
CT1
ADDR
DATA
密钥存储装置
114
密钥存储装置
130
密钥请求
142
密钥K1
144
密钥K2
146
密钥K3
148
密钥K4
152
密钥K5
154
密码逻辑引擎
110
密码逻辑引擎
124
(块/流)
密码逻辑引擎
132
(块/流)
存储器接口
112
存储器接口
128
存储器核心
126
CT1
150
处理器
108
核心
116
核心
118
缓存
120
缓存
122

图1

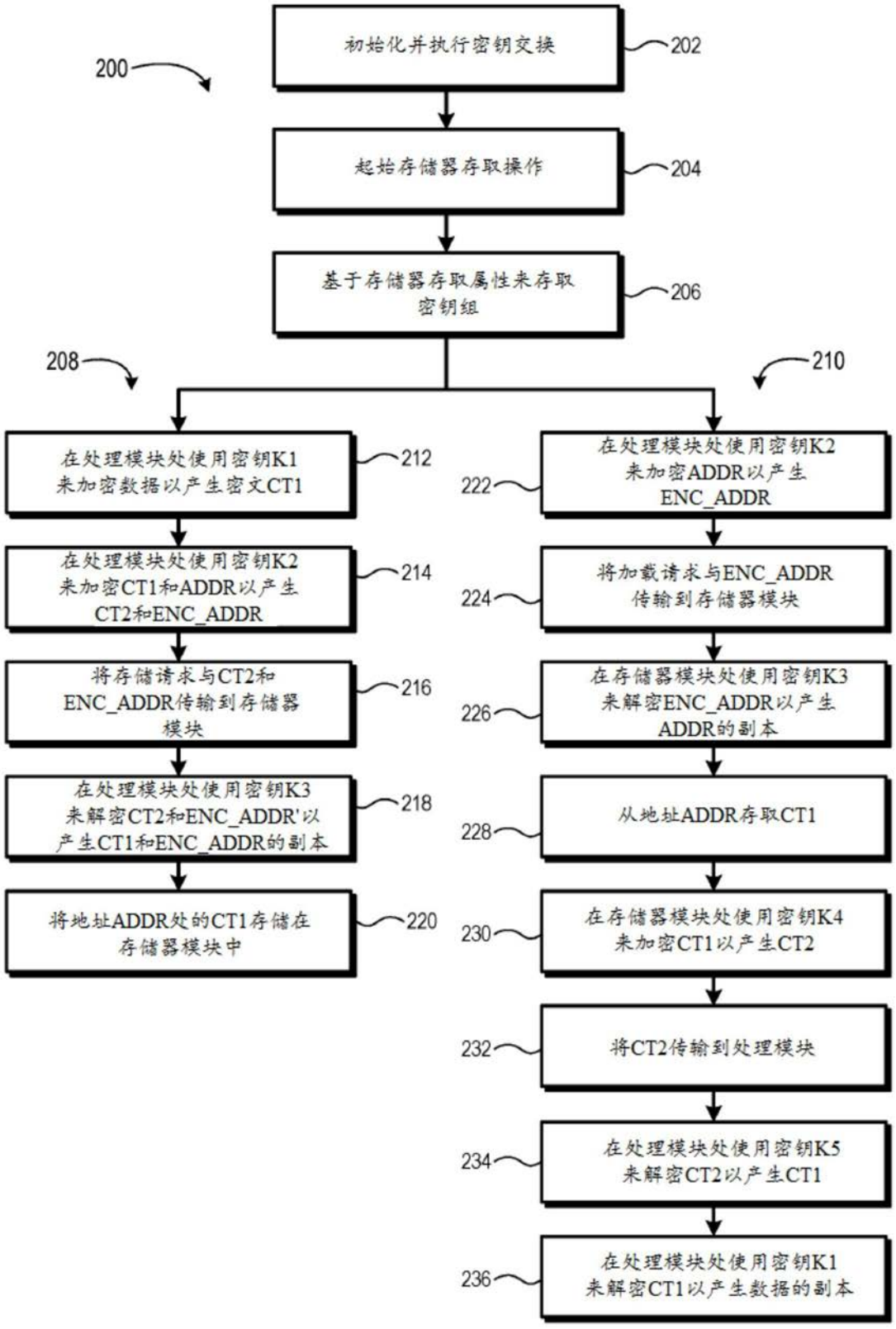

200
初始化并执行密钥交换
202
起始存储器存取操作
204
基于存储器存取属性来存取密钥组
206
208
210
在处理模块处使用密钥K1来加密数据以产生密文CT1
212
在处理模块处使用密钥K2来加密CT1和ADDR以产生CT2和ENC_ADDR
214
将存储请求与CT2和ENC_ADDR传输到存储器模块
216
在处理模块处使用密钥K3来解密CT2和ENC_ADDR'以产生CT1和ENC_ADDR的副本
218
将地址ADDR处的CT1存储在存储器模块中
220
222
在处理模块处使用密钥K2来加密ADDR以产生ENC_ADDR
224
将加载请求与ENC_ADDR传输到存储器模块
226
在存储器模块处使用密钥K3来解密ENC_ADDR以产生ADDR的副本
228
从地址ADDR存取CT1
230
在存储器模块处使用密钥K4来加密CT1以产生CT2
232
将CT2传输到处理模块
234
在处理模块处使用密钥K5来解密CT2以产生CT1
236
在处理模块处使用密钥K1来解密CT1以产生数据的副本

图2

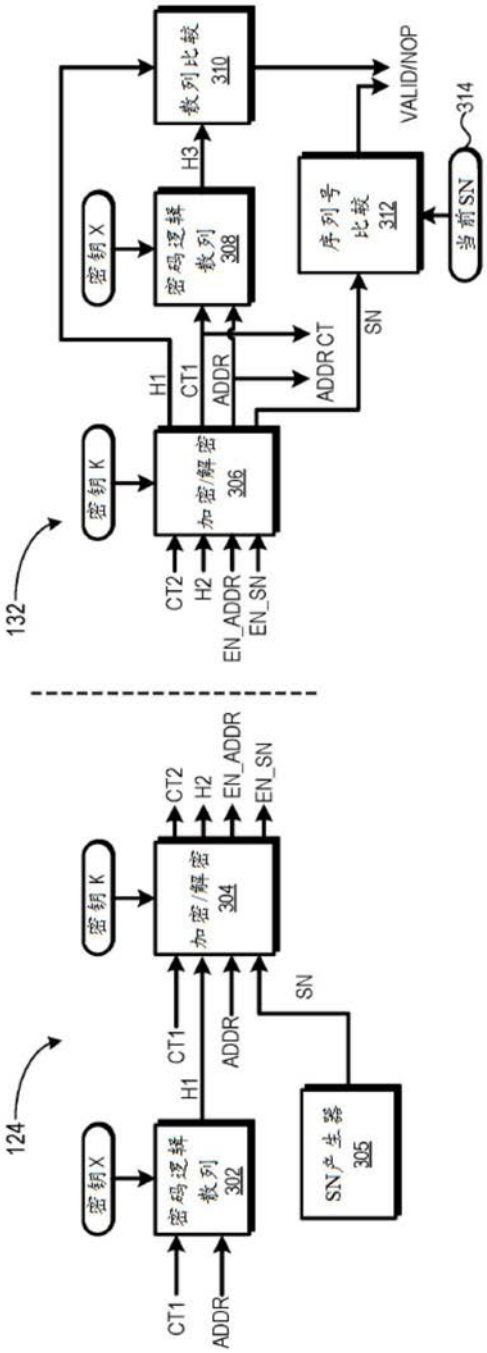

密码逻辑裁列 302
密钥 X
密钥 K
加密/解密 304
SN产生器 305
密码逻辑裁列 308
加密/解密 306
裁列比较 310
序列号比较 312
当前SN
VALID/NOP
314
124
132
CT1
ADDR
H1
CT2
H2
EN_ADDR
EN_SN
SN
H3
ADDR CT

图3

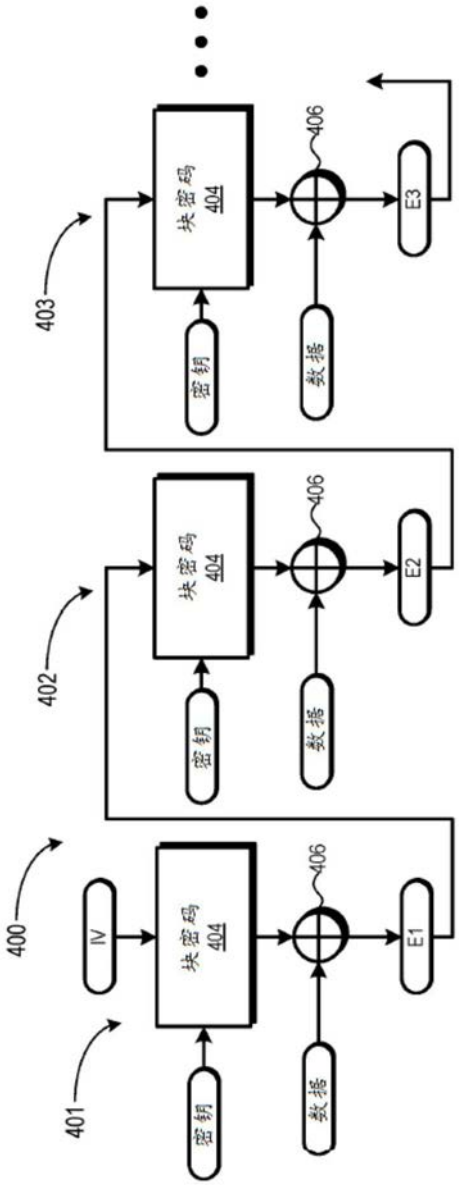


图4

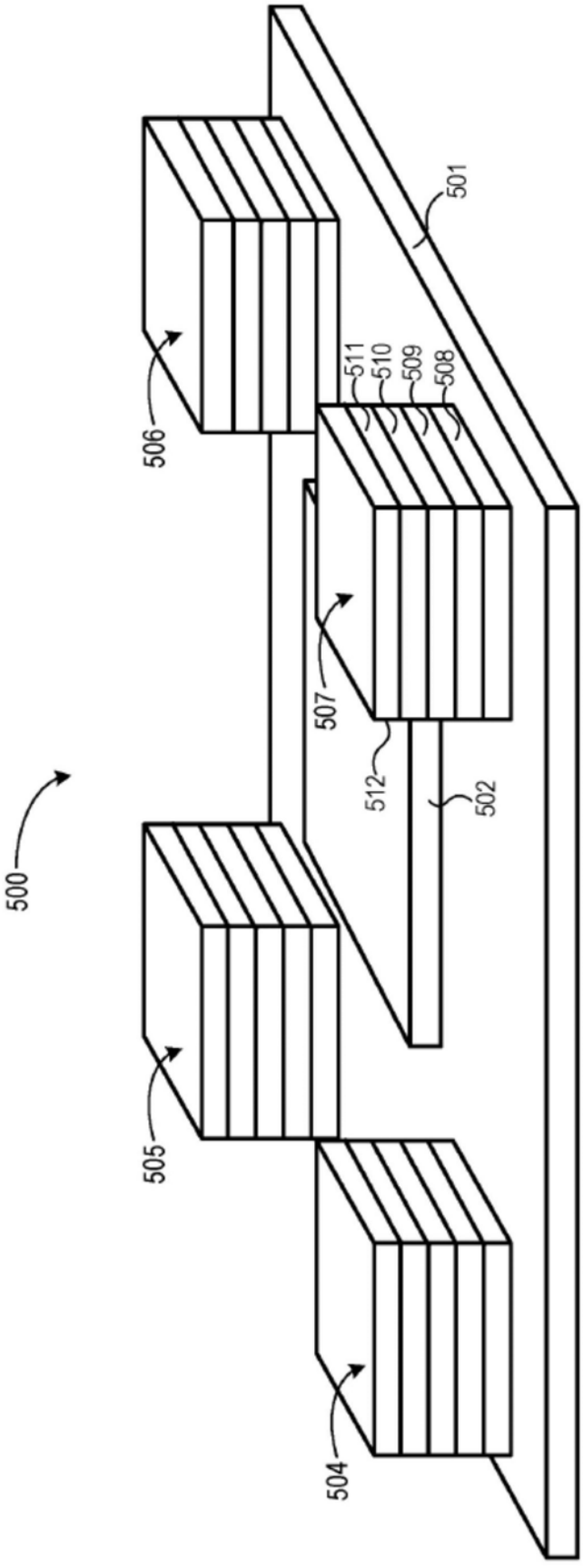


图5