(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 105324956 B
(45)授权公告日 2019.02.01

(21)申请号 201480034284.4

(22)申请日 2014.06.19

(65)同一申请的已公布的文献号
申请公布号 CN 105324956 A

(43)申请公布日 2016.02.10

(30)优先权数据
13/929,589 2013.06.27 US

(85)PCT国际申请进入国家阶段日
2015.12.16

(86)PCT国际申请的申请数据
PCT/US2014/043169 2014.06.19

(87)PCT国际申请的公布数据
WO2015/047487 EN 2015.04.02

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 R·阿万奇

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 宋献涛

(51)Int.Cl.
H04L 9/06(2006.01)

(56)对比文件
US 7797751 B1,2010.09.14,
US 2010031057 A1,2010.02.04,
US 2011191588 A1,2011.08.04,
CN 103166752 A,2013.06.19,
US 2001024501 A1,2001.09.27,
CN 103051442 A,2013.04.17,

审查员 谭美玲

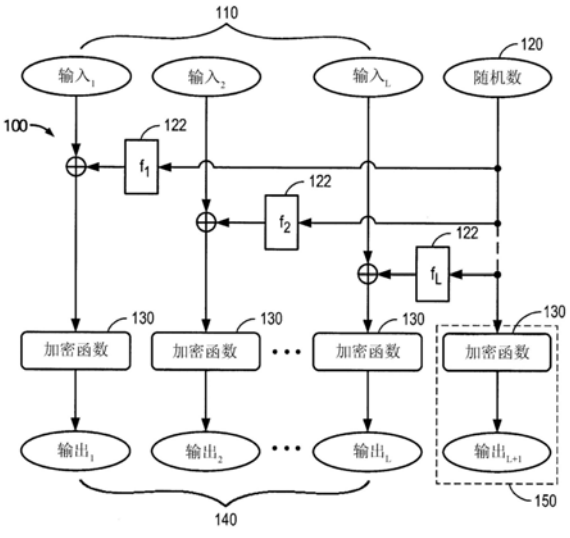
权利要求书2页 说明书9页 附图8页

(54)发明名称

加密明文数据的方法及设备

(57)摘要

发明揭示一种用于加密明文数据的设备及方法。所述方法包含:接收至少一个明文数据输入;通过函数将随机数应用到所述至少一个明文数据输入以形成临时明文数据输出和/或到应用于所述至少一个明文数据输入的加密函数的一部分的中间值以形成中间临时数据输出;以及将所述加密函数应用到所述临时明文数据输出和/或所述中间临时数据输出中的至少一者以形成加密的输出数据。接着将所述加密的输出数据传输到存储器。



CN 105324956 B

1.一种用以加密明文数据的方法,其包括:

接收至少一个明文数据输入;

在应用随机数之前通过模拟加密函数的第一序列的轮函数来加密所述至少一个明文数据输入从而应用所述加密函数,并且其后通过函数应用所述随机数以形成临时数据输出,以及通过模拟所述加密函数的第二序列的轮函数加密所述临时数据输出以形成经加密的输出数据;以及

将所述加密的输出数据传输到存储器。

2.根据权利要求1所述的方法,其中以加密的方式存储所述随机数。

3.根据权利要求1所述的方法,其中以未加密的方式存储所述随机数。

4.根据权利要求1所述的方法,其中所述函数包含异或函数。

5.根据权利要求1所述的方法,其中所述函数是数学函数,所述数学函数从所述随机数中导出值。

6.根据权利要求5所述的方法,其中所述函数包含二进制或算术加常数,位的环旋或任意置换表示到所述函数的输入。

7.根据权利要求1所述的方法,其进一步包括解密来自存储器的所述加密的输出数据。

8.一种包含代码的非暂时性计算机可读媒体,所述代码在由处理器执行时使得所述处理器:

接收至少一个明文数据输入;

在应用随机数之前通过模拟加密函数的第一序列的轮函数来加密所述至少一个明文数据输入从而应用所述加密函数,并且其后通过函数应用所述随机数以形成临时数据输出,以及通过模拟所述加密函数的第二序列的轮函数加密所述临时数据输出以形成加密的输出数据;以及

将所述加密的输出数据传输到存储器。

9.根据权利要求8所述的计算机可读媒体,其中以加密的方式存储所述随机数。

10.根据权利要求8所述的计算机可读媒体,其中以未加密的方式存储所述随机数。

11.根据权利要求8所述的计算机可读媒体,其中所述函数包含异或函数。

12.根据权利要求8所述的计算机可读媒体,其中所述函数是数学函数,所述数学函数从所述随机数中导出值。

13.根据权利要求12所述的计算机可读媒体,其中所述函数包含二进制或算术加常数,位的环旋或任意置换表示到所述函数的输入。

14.根据权利要求8所述的计算机可读媒体,其进一步包括用以解密来自存储器的所述加密的输出数据的代码。

15.一种用以加密明文数据的装置,其包括:

处理器,其用以:

接收至少一个明文数据输入;

在应用随机数之前通过模拟加密函数的第一序列的轮函数来加密所述至少一个明文数据输入从而应用所述加密函数,并且其后通过函数应用所述随机数以形成临时数据输出,以及通过模拟所述加密函数的第二序列的轮函数加密所述临时数据输出以形成经加密的输出数据;以及

将所述加密的输出数据传输到存储器。

16.根据权利要求15所述的装置，其中以加密的方式存储所述随机数。

17.根据权利要求15所述的装置，其中以未加密的方式存储所述随机数。

18.根据权利要求15所述的装置，其中所述函数包含异或函数。

19.根据权利要求15所述的装置，其中所述函数是数学函数，所述数学函数从所述随机数中导出值。

20.根据权利要求19所述的装置，其中所述函数包含二进制或算术加常数，位的环旋或任意置换表示到所述函数的输入。

21.根据权利要求15所述的装置，其中所述处理器进一步解密来自存储器的所述加密的输出数据。

22.一种用以加密明文数据的装置，其包括：

用于接收至少一个明文数据输入的装置；

用于在应用随机数之前通过模拟加密函数的第一序列的轮函数来加密所述至少一个明文数据输入从而应用所述加密函数，并且其后通过函数应用所述随机数以形成临时数据输出，以及通过模拟所述加密函数的第二序列的轮函数加密所述临时数据输出以形成经加密的输出数据的装置；以及

用于将所述加密的输出数据传输到存储器的装置。

23.根据权利要求22所述的装置，其中以加密的方式存储所述随机数。

24.根据权利要求22所述的装置，其中以未加密的方式存储所述随机数。

25.根据权利要求22所述的装置，其中所述函数包含异或函数。

26.根据权利要求22所述的装置，其中所述函数是数学函数，所述数学函数从所述随机数中导出值。

27.根据权利要求26所述的装置，其中所述函数包含二进制或算术加常数，位的环旋或任意置换表示到所述函数的输入。

28.根据权利要求22所述的装置，其进一步包括用于解密来自存储器的所述加密的输出数据的装置。

加密明文数据的方法及设备

技术领域

[0001] 本发明涉及一种用以加密明文数据及解密对应密文数据的方法及设备。

背景技术

[0002] 存储器分析仪的使用表现出对分布内容的完整性及机密性的较大威胁。即使十分注意致力于保护包含于代码中的数据，存储器的内容仍可能通过总线嗅探被捕获。例如，已经在安全环境中解密原始内容以用于渲染之后，这可以用来泄漏原始内容，即使原始内容是以加密形式分布。这可以通过“读取”对应于至存储器的写入的电信号来实现。其它更复杂的攻击可以甚至重放这些信号以诱使处理器读取并处理攻击者选择的数据。

[0003] 内容提供商通常对原始内容的处理具有具体要求。至少，内容决不能用普通文字存储于存储器中。在大多数情况下，至少要求将一些形式的存储器加扰或加密应用到所有存储器记录以防止物理攻击。作为实例，通常根据未加密数据、地址、主密钥将数据写入到特定地址。这保证相同数据当写入到不同地址时具有不同的编码。使用随机数来使明文数据的加密随机化(当以安全方式存储并检索这些随机数时)可以用来防止重放攻击。

[0004] 此外，针对安全通信的吞吐量要求投入当前流及块密码以测试吞吐量并投入新颖构造以提高吞吐量而同时需要控制功率及面积要求。

[0005] 令人遗憾的是，当前技术通常是低效的，并且可能需要更强的防护级别、在相同安全级且无功率显著增加的情况下更高的吞吐量以及就硬件实施方案来说的面积要求。

发明内容

[0006] 本发明的方面可以涉及一种用于加密明文数据的设备及方法。所述方法包含：接收至少一个明文数据输入；通过函数将随机数应用到至少一个明文数据输入以形成明文数据输出和/或到应用于至少一个明文数据输入的加密函数的一部分的中间值以形成中间临时数据输出；以及将加密函数应用到临时明文数据输出和/或中间临时数据输出中的至少一者以形成加密的输出数据。接着将加密的输出数据传输到存储器。

附图说明

[0007] 图1A是说明其中使用加密函数及随机数加密一系列明文数据输入块的过程的流程图。

[0008] 图1B是说明图1A的反向解密过程的流程图。

[0009] 图2是说明基于被称为轮的类似计算块的迭代的块密码的常用结构的流程图。

[0010] 图3是说明使用第一及第二组轮函数以展开形式加密数据输入的过程并用随机数增补加密过程的中间步骤的流程图。

[0011] 图4A是说明使用相同密钥及随机数或从随机数导出的值加密一系列明文数据输入块从而以不同方式修改个别块的加密处理的过程的流程图。

[0012] 图4B是说明图4A的反向解密过程的流程图。

[0013] 图5是说明通过将从常用随机数导出的不同值应用到加密过程的中间步骤来加密数据输入从而获得若干不同输出的过程的流程图。

[0014] 图6是实施数据加密技术以便使得能够节省及恢复加密的存储器至大容量存储装置而无须对其解密及再加密的实例计算机硬件系统的图。

具体实施方式

[0015] 词语“示例性”或“实例”在本文中用于表示“充当实例、例子或说明”。本文中描述为“示例性”或描述为“实例”的任何方面或实施例未必应被解释为比其它方面或实施例优选或有利。

[0016] 本发明的实施例涉及用以提供增强型机构以用于保护存储于存储器中的数据的技术。具体来说，描述了延伸块密码的功能性以便增强存储器加密的方法及过程。另外，这些技术还可以改进性能、吞吐量及功率消耗，如将在下文中描述。这些技术也可用以出于跨(有线或无线)网络传输的安全数据存储的目的改进性能、吞吐量及功率消耗。

[0017] 在一个实施例中，采用其中使用加密函数(例如，块密码)加密一系列L个明文数据输入块的加密方案。在通过块密码加密之前，通过函数将随机数应用到明文数据输入。具体来说，揭示一种用以加密明文数据的方法或过程，其包含：接收多个明文数据输入；通过函数将随机数应用到多个明文数据输入以形成临时明文数据输出；将加密函数(例如，块密码)应用到临时明文数据输出以形成加密的输出数据；以及将加密的输出数据传输到存储器。

[0018] 在一个实施例中，如将在下文中更确切地描述的，所述方法可以包含：接收多个明文数据输入；通过函数将随机数应用到多个明文数据输入以形成明文数据输出和/或到应用于多个明文数据输入的加密函数的一部分的中间值以形成中间临时数据输出；以及将加密函数应用到临时明文数据输出和/或中间临时数据输出中的至少一者以形成加密的输出数据。接着将加密的输出数据传输到存储器。

[0019] 使L个明文数据输入块的加密随机化

[0020] 如图1A中可见，在一个实施例中，执行方法或过程100，其中接收多个明文数据输入(输入$_1$到输入$_L$)110。通过函数122将随机数120应用到明文数据输入(输入$_1$到输入$_L$)110。随机数120可以用来使L个明文数据块(输入$_1$到输入$_L$)110的加密随机化。如图1A中可见，接收L个明文数据块(输入$_1$到输入$_L$)110并可以通过函数(f_1、f_2、…、f_L)122应用随机数120以形成临时明文数据输出。在一个实施例中，如下文将更详细地描述，应用随机数120的函数可以包含异或函数。在另一实施例中，代替异或函数，可以使用模加函数。接着可以将加密函数130(例如，块密码)应用到临时明文数据输出使得输出加密的输出数据(输出$_1$到输出$_L$)140到存储器。

[0021] 应了解，随机数120可以经受一些转换以便避免(在同时处理L个块110之中)相等数目的明文块具有相同的加密。同样，因为在用于L个并行加密的加密函数130中使用的加密密钥可以是相同的，因此不需要重做密钥次序表L次。

[0022] 此外，如下文将更详细地描述，取决于使用情况，随机数120可以未加密的方式或以加密的方式存储于存储器的较小的内部防护区中或存储于主存储器中。

[0023] 另外，为简单起见，不呈现在加密函数130中使用的具体加密密钥。然而，应了解，

加密函数采用另外的输入，所述输入是在加密过程中由加密函数使用的密钥。此外，还应了解，在加密函数是使用相同加密密钥的迭代块密码的情况下，各个竖直传递途径可以共享相同的密钥次序表，其中可以将一些固定位置换(例如，旋转)应用到轮，之后在加密函数130中使用。在硬件实施方案中，这些置换应没有性能影响，因为它们仅相当于硅中的不同的布线。

[0024] 函数(f_1、f_2、…、f_L)122可以是数学函数，其从随机数120导出值以便以攻击者不可预测的方式扰乱临时明文数据输出的计算。这些可以是具有常数的掩码、不同的环旋、或可以与所选择的加密函数130相关的其它函数。如果随机数120具有比密码块长度更大的大小，那么函数可以仅仅是随机数的分段的提取。

[0025] 此外，利用相同加密函数130的L个或L+1个实施方案(或可以采用不同加密函数)，方法100可以是可并行化的。如图1A中可见，在虚线150中，密文的展开示出为第L+1个实施方案，其输出一个另外的块。另外，因为用于加密函数130的相同加密密钥可以用于每一块，所以仅需要执行一次子密钥导出，从而节省硬件资源。

[0026] 在一些实施例中，可以通过用普通文字将随机数120存储在可存取存储器区域中来提供足够的安全性，因为其发挥的作用类似于初始化向量的作用。此方法的有利之处在于随机数120可以比块大小更短，并且因此其可以在函数运算122中仅应用到输入块110的选定位字段。此方案可以适用于存储器加密。作为实例，如果块密码具有128位的块大小并且高速缓存线是128字节长，那么通过设置L＝8，可以在整个高速缓存线从高速缓冲存储器的末级溢出时一次加密整个高速缓存线。

[0027] 因此，如先前所描述，过程100延伸块密码的功能性以便增强存储器加密。具体来说，加密方案100采用各自使用加密函数130加密的一系列L个明文数据输入块(输入$_1$到输入$_L$)110，其中在用加密函数130加密之前，通过函数122将随机数120应用到明文数据输入110。加密函数130可以应用到临时明文数据输出使得加密的输出数据(输出$_1$到输出$_L$)140输出到存储器。

[0028] 以反向步骤进行解密。例如，参考图1B，可以将加密函数130的反函数应用到来自存储器的加密的输出数据(示出为输入140)，即对应解密基元，其可以用来计算$Input_i$及随机数的合成(例如$Input_i \oplus$随机数，i＝1、2、…、L及随机数)，可从其恢复原始输入(示出为输出110)。

[0029] 使块密码随机化

[0030] 如下文将描述的，在应用随机数120之前，可以首先通过构成块密码的第一序列的轮函数(其是所选择的加密函数)加密明文数据输入110，并且其后应用随机数以形成临时数据输出。接着可以通过模拟块密码的第二序列的轮函数(其是所选择的加密函数)加密临时数据输出以形成输出到存储器的加密的输出数据。

[0031] 为了模拟加密函数130(例如，块密码)，可以使用各种构造。例如，可以使用例如Luby-Rackoff构造等构造，例如，Feistel网络(例如，数据加密标准(DES))及代换-置换(SP)网络(例如，高级加密标准(AES))。在这两种情况下，将一个参数化的非线性函数反复地应用到输入。此函数的每次应用可以被称为“轮”或“轮函数”。一个轮的输出是下一轮的输入。明文是第一轮的输入并且密文是最后一轮的输出。轮函数采用称为轮密钥的其它参数，并且轮密钥是从加密/解密密钥(例如，密码密钥)中导出的。

[0032] 参考图2，说明基于轮函数产生块密码的过程200的实例。如图2中所示，将明文数据输入202输入到轮函数的多个N轮204，从而模拟块密码。因此，通过轮函数的多个N轮204模拟块密码，其中k1、k2、…、kN分别是轮1、2、…、N的轮密钥。输出206是通过应用到明文数据输入202的轮函数(模拟块密码)加密的加密明文数据输入202。应了解，解密将是反向的完全相同的过程。

[0033] 下文将描述实例实施方案。例如，此方案的高性能实施方案可以要求相同块密码的两个并行实施方案，可能共享轮密钥。为了减少硬件实施方案成本，可以在密码当中应用随机数。借助于此，密码的在应用随机数之前的部分必须仅实施一次，而密码的在应用随机数之后的部分实施两次。

[0034] 作为实例，参考说明过程300的图3，可以通过N轮的M轮(1≤M<N)加密明文数据输入302，例如，使用M轮密钥用参数表示M轮304(k1、k2、…、kM)。接着，应用随机数(v)306-例如，针对第M轮的输出X对其进行异或运算-并且对经过异或运算的输出及随机数进一步独立地加密(分离块308)-并且以第(M+1)轮恢复过程。如图3中可见，N-M轮310的下一轮的轮密钥k'及k″可以是相同组的轮密钥或可以是彼此的略微变型，例如，不同旋转或经不同的机密常数掩蔽。另外，可以串接(块314)输出从而产生输出316。

[0035] 略微不同的实施方案的另一实例可以由X的位及由随机数的置换构成。例如，如果X设置成＝$X_{hi}|X_{lo}$(分解为两个相等长度的位串的串接)，并且v(随机数)设置成v＝$v_{hi}|v_{lo}$，那么A将是A＝$X_{hi}|v_{lo}$且B将是B＝$X_{lo}|v_{hi}$。因此，如果最后N-M轮具有足够扩散，那么X及随机数两者对输出的两半部分C及D存在足够影响。应了解，这仅是实例，其它位置换是可能的。然而，如果块大小足够大，则所述方案可以不导致对于相同明文的相同密文的频繁(部分)重复。因此，可以可取的是随机数影响下一输入的整体，例如方程式如$A = (X_{hi} \oplus v_{hi}) \| v_{lo}$及$B = (X_{lo} \oplus v_{lo}) \| v_{hi}$。应了解，此处重要的是所述过程是可简单地反向的，使得一旦解密过程已经执行N-M轮就可以恢复随机数。此外，串接函数314可以是最后并行轮的两个输出的串接，但是此处可以使用两个输入的任何其它位置换。所述过程的有利之处在于无须复制第一M轮的硬件实施方案而仅须复制最后N-M轮。在此情况下同样以反向步骤进行解密。对于最后N-M轮，输出的两“侧”C及D是并行解密的，直到恢复随机数v，颠倒分离运算，并且接着在M轮中完成输入的解密。

[0036] 参考图4A，说明过程400的实例，一般化先前技术，以同步加密L个明文数据输入块(输入$_1$到输入$_L$)410，其中将随机数420在进行适当转换之后连同使用各个轮一起添加到每一块。具体来说，图4A的过程400说明可以在应用随机数420之前通过第一序列的轮函数(M轮404)加密明文数据输入410，并且其后应用随机数420以形成临时数据输出。如图4A中可见，接收L个明文数据块(输入$_1$到输入$_L$)410并且将函数(f_1、f_2、…、f_L)422应用到随机数420从而以不同方式形成临时数据输出。在一个实施例中，应用随机数420的函数可以包含异或函数。替代地，可以使用其它简单可逆的函数，例如模加函数或模减函数来应用随机数(从随机数导出的值)。接着可以通过第二序列的轮函数(N-M轮406)加密临时数据输出以形成输出到存储器的加密的输出数据440。应了解，通过采用M轮404及N-M轮406，由此模拟及应用全部加密函数。此外，方法400可以是可并行化的，采用轮函数404及406的L个(在随机数不加密的情况下)或L+1(在随机数加密的情况下)实施方案以形成输出到存储器的加密的

输出数据。

[0037] 应了解，函数(f_1、f_2、…、f_L)422执行如参考图1A所描述的实质上相同作用。然而，直到块密码下面的第(M+1)轮406才实施函数的事实允许来自随机数的更复杂导出。就AES实施方案来说，可以采用AES密钥调度过程的一些变化以产生函数。在一个实施例中，可以与块密码的第一M轮404并行地计算函数。可为有利的是不将所有相同的轮密钥馈给各个轮，但是仍应用一些固定置换和/或掩码到各个轮，这对每一竖直传递途径是唯一的。另外，可为有利的是，取决于使用情况要求，仅用普通文字将随机数420存储在可存取的或受保护的存储器区域中，因为其发挥的作用可以类似于初始化向量的作用并且仍然可以是足够安全的。

[0038] 以反向步骤进行解密。例如，参考图4B，输入440是图4A的加密的输出关且输出410应相当于原始输入(即，原始明文输入)。

[0039] 资源节省

[0040] 应了解，所有的先前方案已经基于直接通过加密函数加密明文的想法。然而，用于块密码的若干运算模式使用加密基元以产生密钥流，所述密钥流针对明文经过异或运算以推导密文，例如计数器(CTR)模式。下文将描述这种类型的加密的实例。当尝试节省用于密钥流产生的资源时，需要确保不会有过多节省的发生是以安全性为代价，即，各个密钥流块必须呈现出彼此不相关。举例来说，可以尝试重复使用来自“密钥流”的块以加密若干输入块，在存储器加密的情形下，这可以简单地解决存储器加密电路的区域问题。然而，如果两个明文块P1及P2都是经过异或运算的，具有相同的填补π，那么密文块将是$C1=P1 \oplus \pi$及$C2=P2 \oplus \pi$，其满足$P1 \oplus P2=C1 \oplus C2$。这会显示关于明文的有价值的信息，并且因此不适合用以存储关键信息。然而，可为有利的是使用常用硬件以仅计算两个或更多个密钥流块的第一轮，并且接着单独地执行最后的轮。此类方法的安全性取决于所使用的密码的减少的轮型式的密码分析及在一些轮之后的中间值的可预测性。

[0041] 参考图5显示其实例。在此实例实施例过程500中，输入502及随机数(v)520是用以产生L个密钥流块的值。输入502不是明文。类似地，输出$_1$、输出$_2$、…、输出$_L$ 540不是密文，但是L个密文块如在CTR运算模式中针对这些值经过异或运算(或在仅使用块密码的加密基元的其它加密模式的一些变型中以更复杂的方式来使用)。在其它方面，图5类似于图4A，包含在应用随机数520之前的第一轮(M轮504)的轮密钥，并且其后应用随机数520以形成临时数据输出。可以通过函数(f_1、f_2、…、f_L)522应用随机数520以形成临时输出。应用随机数520的函数可以包含异或函数。接着可以通过第二轮(N-M轮506)的轮密钥加密临时输出以形成加密的输出540。

[0042] 如果选择AES(例如，AES-128)作为块密码，那么鉴于可以使用的当前密码分析结果，M＝3或4。基本原理是：降到6或7轮的AES-128仍然相当难以攻击，除非攻击者可以控制输入，这在这种情况下是不可能的。例如，假设使用情况是存储器加密，其中整个高速缓存线经过加密，这些是128字节，因此我们需要8块(L＝8)。这意味着，对于M＝3，代替80，在硬件中总共需要实施3+8×7＝59轮的AES，产生约26％的区域及功率节省。对于M＝4，实施的AES的轮数为4+8×6＝52，产生约35％的节省。如果最后N-M轮的密钥次序表对于所有传递途径是共同的，则节省可以更多一些(可能在并行传递途径中具有轮密钥的仅一些固定位置换，但是可能不超过这些)，因为这应超过经由从随机数导出将针对第(M+1)轮的输入经

过异或运算的不同值的逻辑的偏移。

[0043] 随机数的计算

[0044] 在一个实施例中，每次一个新的块(或一组L个块)需要写入到存储器时，可以刷新随机数。如果块密码具有足够扩散(或其在最后N-M轮中具有足够扩散)，那么其可以足以仅将随机数移位(例如)s位，并且接着将s个新的刷新随机位附加到所述随机数。例如，这可以计算随机数(v)为$v \leftarrow (v << s) \oplus r$，其中r是s位串。此外，刷新位可以从最高有效位置移入，或v可以在经独立地移位及刷新的各个子寄存器中分隔。然而，如果使用此策略，那么随机数不应用普通文字存储于存储器中，而是应经过加密，因为用普通文字存储随机数会可能使未来随机数可部分地预测，由此可能助长密码分析。应进一步指出，随机数可以是：(a)与数据将存储于其中的物理存储器地址无关的值；或(b)附属于所述地址。对于后一种情况，其可以是以下的串接：(i)物理存储器地址及(ii)随机值、(加密的)计数、或通过以上所描述的方法或通过不同方法计算出的值。

[0045] 实例硬件

[0046] 图6中说明可以实施先前描述的方法及过程的实例计算机硬件600。计算机系统600示出包括可以经由总线电耦合(或适当时可以另外的方式通信)的硬件元件。硬件元件可以包含至少一个主处理器602(例如，中央处理单元(CPU))以及其它处理器604。应了解，这些处理器可以是通用处理器和/或一或多个专用处理器(例如数字信号处理芯片、图形加速处理器和/或类似者)。处理器可以耦合到相应存储器管理单元(MMU)610，所述MMU可以继而通过高速缓冲存储器612(例如，高速缓冲存储器可以或可以不存在和/或可以是独立的或并入到其它元件中)(以虚线围绕)耦合到加密机处理单元620和/或到存储器630和/或存储装置640。如下文将描述，加密机620可以采用先前描述的方法及过程以延伸密码块的功能性以便增强对于存储于存储器中的数据的存储器加密。

[0047] 应了解，计算机600可以包含其它装置(未示出)，例如：输入装置(例如，键盘、鼠标、小键盘、麦克风、相机等)；以及输出装置(例如，显示装置、监视器、扬声器、打印机等)。计算机600可以进一步包含一或多个存储器元件630、存储装置640(和/或与其通信)，所述存储器元件及存储装置可以包括本地和/或网络可接入的存储装置，和/或可以包含(但不限于)磁盘驱动器、驱动器阵列、光学存储装置、例如随机存取存储器(“RAM”)和/或只读存储器(“ROM”)等固态存储装置，其可为可编程的、可快闪更新的和/或其类似者。计算机600还可以包含通信子系统，所述通信子系统可以包含调制解调器、网卡(无线或有线的)、红外通信装置、无线通信装置和/或芯片组(例如蓝牙装置、802.11装置、Wi-Fi装置、WiMax装置、蜂窝式通信装置等)和/或类似者。通信子系统可准许与网络、其它计算机系统和/或本文中所描述的任何其它装置交换数据。应了解，计算机600可以是移动装置、非移动装置、无线装置、有线装置等，且可以具有无线和/或有线连接，并且可以是任何类型的电子或计算装置。

[0048] 在一个实施例中，如果数据将存储在加密的位置处(决策块650)，那么加密机620(例如，用以加密数据的装置)可以实施先前描述的过程(另外参考图1A)，包含：接收多个明文数据输入(输入$_1$到输入$_L$)110；通过函数(f_1、f_2、…、f_L)122应用随机数122以形成随机的临时明文数据输出；以及将加密函数130应用到临时明文数据输出，使得将加密的输出数据(输出$_1$到输出$_L$)140输出到存储器630。此数据可以进一步存储于存储装置640中。在其它实施例中，如先前所描述，为了应用加密函数，加密机620可以在应用随机数之前采用模拟加

密函数的第一序列的轮函数来加密明文数据输入。之后，应用此随机数以形成临时数据输出。接着可以通过模拟加密函数的第二序列的轮函数加密临时数据输出以形成输出到存储器630的加密的输出数据。如先前所具体描述的，图2到5说明了这些实施方案的实例。

[0049] 然而，如果在决策块650处确定数据将不存储在加密的位置处，那么通常可以将数据存储到存储器630和/或可以采用普通存储器映射输入/输出及控制655来实施对存储装置640的直接存储器存取(DMA)控制。

[0050] 通常，当存储器加密可用时，需要在将它们写入到虚拟存储器系统中的存储装置之前对其内容进行解密。然而，为了适应此目的，根据本发明的实施例，DMA数据传送信道可以用来读取存储器630(例如，RAM、DDR RAM等)的实际加密内容并且可以用来将所述内容写入到存储装置640(例如，硬盘驱动器或快闪存储器)的区段，以及从区段读取内容并将所述内容直接放入存储器630中。因此，这些存储器加密方法可以与物理地址无关，并且可以在无另外的加密/解密附加项的情况下换出及返回换入页面。

[0051] 先前描述的系统的有利之处在于不需要在每次移动存储器内容以调换文件及换回到存储器时解密及再加密存储器内容，从而产生明显的功率节省及时间节省。此外，本文中所描述的技术不仅提供针对物理或电性存储器攻击(即，针对存储器的直接读取)的良好直接防护，而且提供针对使用总线流量作为侧信道的攻击的抵抗，因为相同或相关数据重复写入到相同位置是实际上随机的。此外，本文中所描述的技术需要相对较少的额外硬件实施方案。再者，本文中所描述的技术足够通用，使得它们可以应用到基本上任何常用块密码。另外，每一轮的输入及输出大小不必全部相等并且在这些情况下必须仅最低限度地调适掩蔽运算。此外，用于节省加密的存储器的直接DMA信道也可以带来功率消耗及时间的明显节省。

[0052] 此外，如先前所描述，取决于实施方案，随机数可以明确的未加密的方式或加密的方式存储于主存储器630中。替代地，如先前所描述，随机数可以是存储于专用存储器的较小的防护区中。

[0053] 另外，应了解，在一个实例中，如果在装置启动时随机选择了固定密钥，那么可以在那时预先计算出对应密钥次序表。作为特定实例，可以存在主密钥，或必要时可以放入密钥中的对存储器地址的依赖。作为另一实例，随机数可以是：固定值(在此情况下为所有导出的常数，例如：可以预先计算出的函数的输出(f_1、f_2、…、f_L))、每页面值、或可以取决于物理存储器地址。这些实例方案可以用于简化目的。

[0054] 应了解，如先前所描述的用以提供增强型机构以用于通过延伸块密码的功能性保护存储于存储器中的数据的技术可以实施为软件、固件、硬件、其组合等。在一个实施例中，先前描述的函数可以由计算机600的一或多个处理器(例如，加密机620或其它处理器)实施以获得先前所需的函数(例如，图1到5的方法运算)。此外，如先前参考图1到5所描述，简单地以反向步骤进行解密。

[0055] 应了解，先前描述的本发明的方面可以结合如先前所描述的由装置的处理器对指令的执行来实施。特定来说，装置的电路(包含但不限于处理器)可以在程序、例程或用以执行根据本发明的实施例的方法或过程的指令的执行的控制下操作。例如，此类程序可以固件或软件(例如，存储于存储器和/或其它位置中)实施且可由处理器和/或装置的其它电路实施。另外，应了解，术语处理器、微处理器、电路、控制器等是指能够执行逻辑、命令、指令、

软件、固件、功能性等的任何类型的逻辑或电路。

[0056] 应了解，当装置为移动或无线装置时其可经由通过无线网络的一或多个无线通信链路通信，所述无线通信链路基于或以其它方式支持任何合适的无线通信技术。例如，在一些方面中，无线装置及其它装置可以与包含无线网络的网络相关联。在一些方面中，网络可包括人体局域网络或个人局域网络(例如，超宽带网络)。在一些方面中，网络可以包括局域网络或广域网络。无线装置可以支持或以其它方式使用多种无线通信技术、协议或标准中的一或多者，例如，3G、LTE、先进的LTE、4G、CDMA、TDMA、OFDM、OFDMA、WiMAX及WiFi。类似地，无线装置可以支持或以其它方式使用多种对应调制或多路复用方案中的一或多者。无线装置因此可以包含适当组件(例如，空中接口)以使用上文或其它无线通信技术建立一或多个无线通信链路及经由一或多个无线通信链路来通信。例如，装置可以包括具有相关联的发射器及接收器组件(例如，发射器及接收器)的无线收发器，其可以包含促进无线媒体上的通信的各种组件(例如，信号产生器及信号处理器)。众所周知，移动无线装置因此可以无线方式与其它移动装置、手机、其它有线及无线计算机、因特网网站等通信。

[0057] 本文中的教示可并入到多种设备(例如，装置)中(例如，在多种设备内实施或通过多种设备执行)。例如，本文中教示的一或多个方面可并入到计算机、有线计算机、无线计算机、电话(例如，蜂窝式电话)、个人数据助理(“PDA”)、平板计算机、移动计算机、移动装置、非移动装置、有线装置、无线装置、膝上型计算机、娱乐装置(例如，音乐或视频装置)、头戴装置(例如，头戴式耳机、耳机等)、医疗装置(例如，生物计量传感器、心率监测仪、计步器、EKG装置等)、用户I/O装置、固定计算机、台式计算机、服务器、销售点(POS)装置、娱乐装置、机顶盒、ATM、或任何其它合适的电子/计算装置中。这些装置可以具有不同的功率及数据要求。

[0058] 在一些方面中，无线装置可以包括用于通信系统的接入装置(例如，Wi-Fi接入点)。此类接入装置可以提供(例如)经由有线或无线通信链路到另一网络(例如，广域网，例如因特网或蜂窝式网络)的连接性。因此，接入装置可以使得另一装置(例如，Wi-Fi站)能够接入另一网络或某一其它功能性。

[0059] 所属领域的技术人员将理解，可使用多种不同技艺及技术中任一者来表示资讯与信号。例如，可由电压、电流、电磁波、磁场或磁粒子、光场或光粒子或其任何组合表示在整个以上描述中可能提及的资料、指令、命令、资讯、信号、位元、符号及码片。

[0060] 所属领域的技术人员将进一步了解，结合本文所揭示的实施例描述的多个说明性逻辑块、模块、电路和算法步骤可以实施为电子硬件、计算机软件或两者的组合。为了清楚地说明硬体与软体的此可互换性，各种说明性组件、区块、模块、电路及步骤已在上文大体按其功能性加以描述。此类功能性是实施为硬件还是软件取决于具体应用及施加于整个系统的设计约束。所属领域的技术人员可以针对每一特定应用以不同方式实施所描述的功能性，但不应将此类实施决策解释为导致脱离本发明的范围。

[0061] 可通过通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或其经设计以执行本文中所描述功能的任何组合来实施或执行结合本文中所揭示的实施例而描述的各种说明性逻辑块、模块和电路。通用处理器可为微处理器，但在替代方案中，处理器可为任何常规处理器、控制器、微控制器或状态机。处理器还可实施为计算装置的组合，例如，DSP与

微处理器的组合、多个微处理器、结合DSP核心的一或多个微处理器，或任何其它此类配置。

[0062] 结合本文中所揭示的实施例而描述的方法或算法的步骤可直接体现于硬件、由处理器执行的软件模块中或两者的组合中。软件模块可驻留在RAM存储器、快闪存储器、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移除磁盘、CD-ROM，或此项技术中已知的任何其它形式的存储媒体中。示例性存储媒体耦合到处理器，使得处理器可以从存储媒体读取信息及将信息写入到存储媒体。在替代方案中，存储媒体可集成到处理器。处理器及存储媒体可以驻留在ASIC中。ASIC可驻留在用户终端中。在替代方案中，处理器及存储媒体可以作为离散组件驻留在用户终端中。

[0063] 在一或多个示例性实施例，所描述的功能可在硬件、软件、固体或其任何组合中实施。如果在软件中实施为计算机程序产品，那么可将功能作为一或多个指令或代码存储于计算机可读媒体上或经由计算机可读媒体予以传输。计算机可读媒体包含计算机存储媒体及通信媒体两者，通信媒体包含促进将计算机程序从一处传送到另一处的任何媒体。存储媒体可为可由计算机存取的任何可用媒体。借助于实例而非限制，此类计算机可读媒体可以包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储装置、磁盘存储装置或其它磁性存储装置，或可用于携载或存储呈指令或数据结构的形式的所要程序代码且可由计算机存取的任何其它媒体。同样，任何连接恰当地称为计算机可读媒体。例如，如果使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)或如红外线、无线电以及微波的无线技术从网站、服务器或其它远程源传输软件，那么同轴电缆、光纤电缆、双绞线、DSL或如红外线、无线电以及微波的无线技术包含于媒体的定义中。如本文中所使用，磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软性磁盘和蓝光光盘，其中磁盘通常以磁性方式再现数据，而光盘利用激光以光学方式再现数据。上述各项的组合也应该包含在计算机可读媒体的范围内。

[0064] 提供所揭示实施例的先前描述以使得任何所属领域的技术人员能够制作或使用本发明。所属领域的技术人员将容易地了解对这些实施例的各种修改，并且可在不脱离本发明的精神或范围的情况下将本文所定义的一般原理应用到其它实施例中。因此，本发明并不希望限于本文所展示的实施例，而应符合与本文所揭示的原理和新颖特征相一致的最广泛范围。

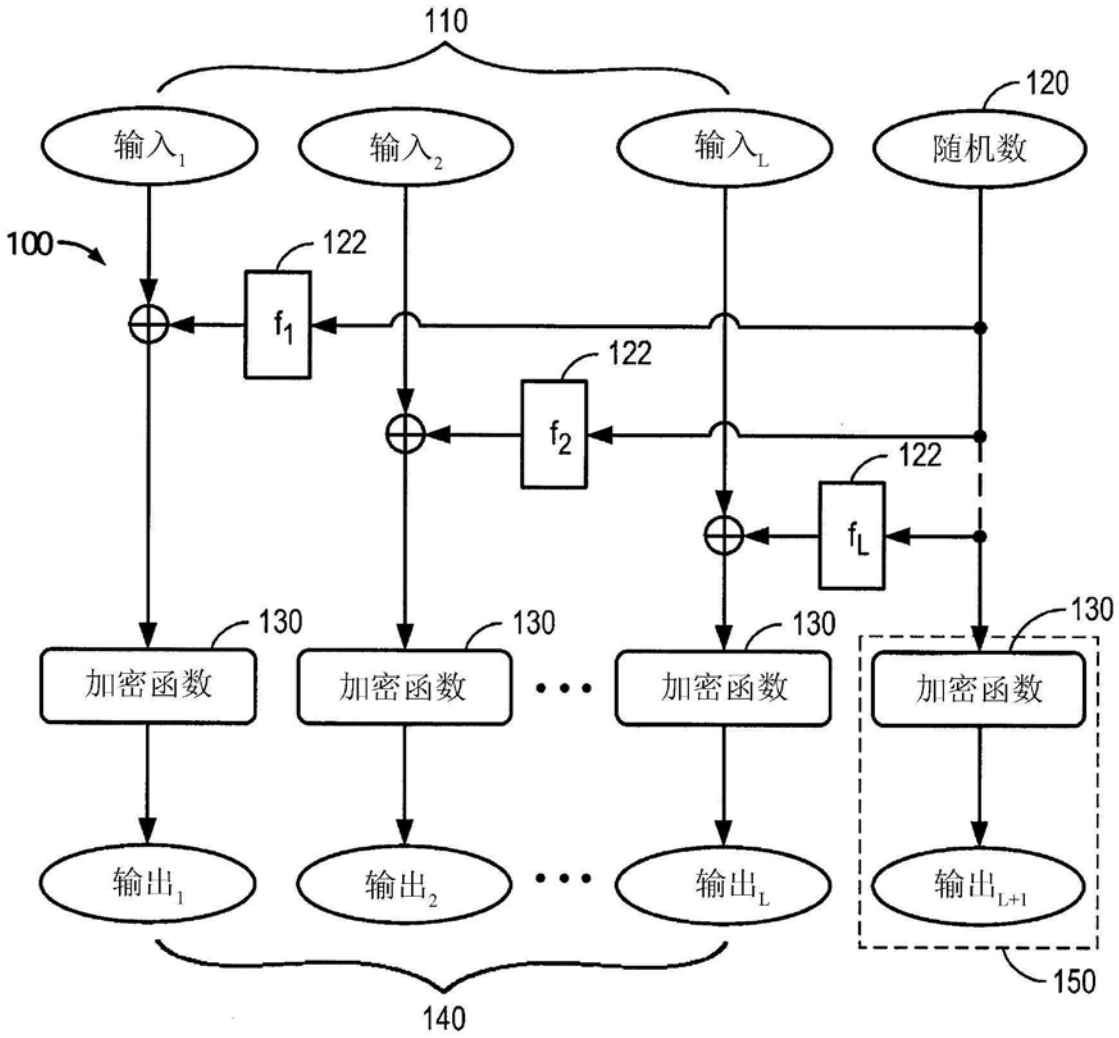

110
120
输入1
输入2
输入L
随机数
100
122
f1
122
f2
122
fL
130
130
130
130
加密函数
加密函数
加密函数
加密函数
输出1
输出2
输出L
输出L+1
140
150

图1A

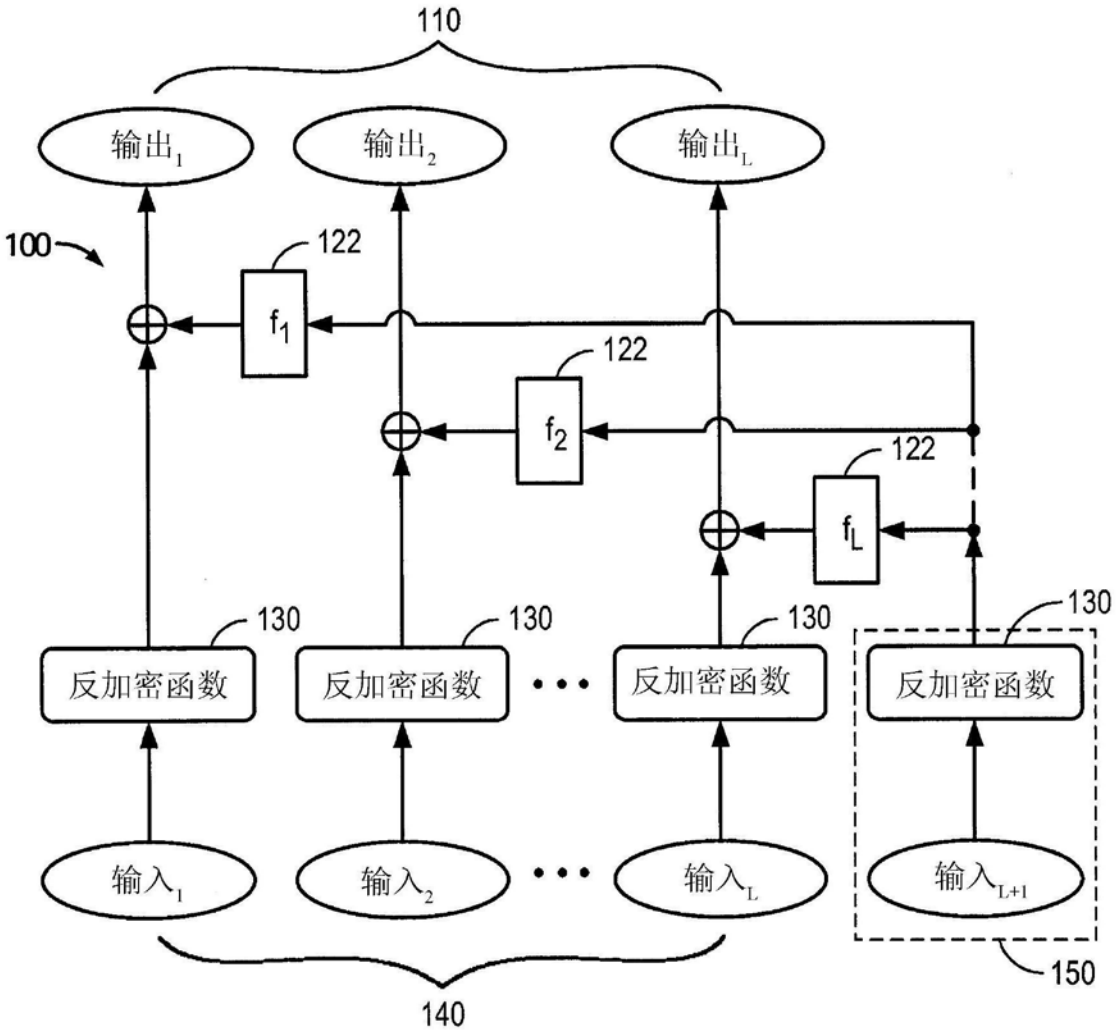

110
输出1
输出2
输出L
100
122
f1
122
f2
122
fL
130
130
130
130
反加密函数
反加密函数
反加密函数
反加密函数
输入1
输入2
输入L
输入L+1
140
150

图1B

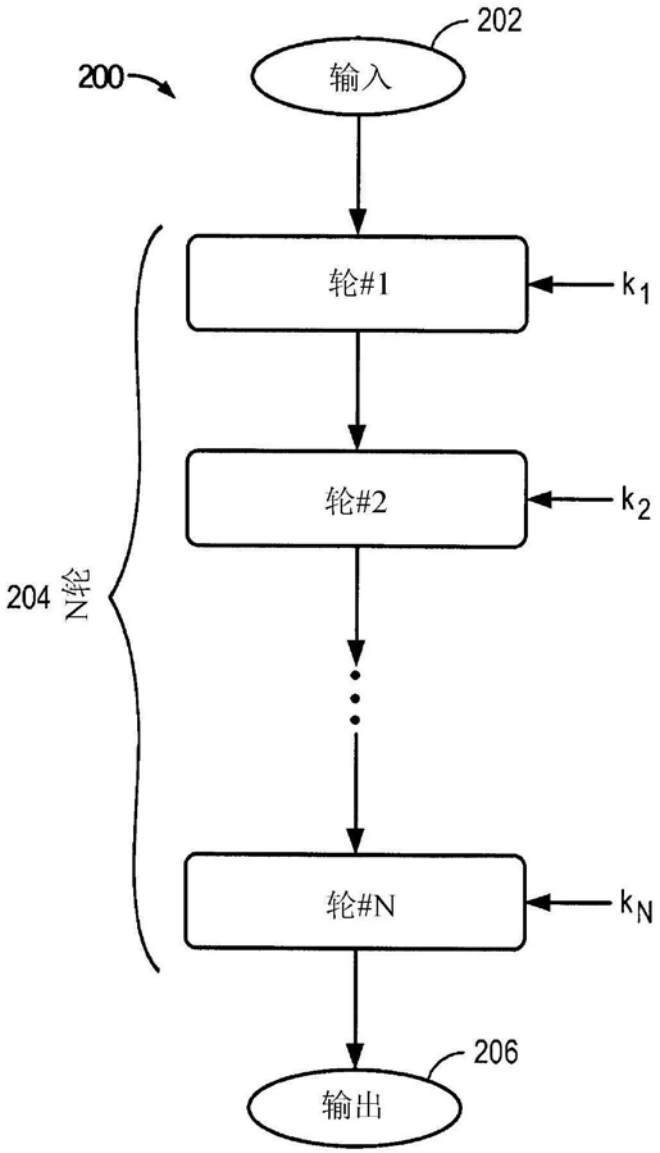


图2

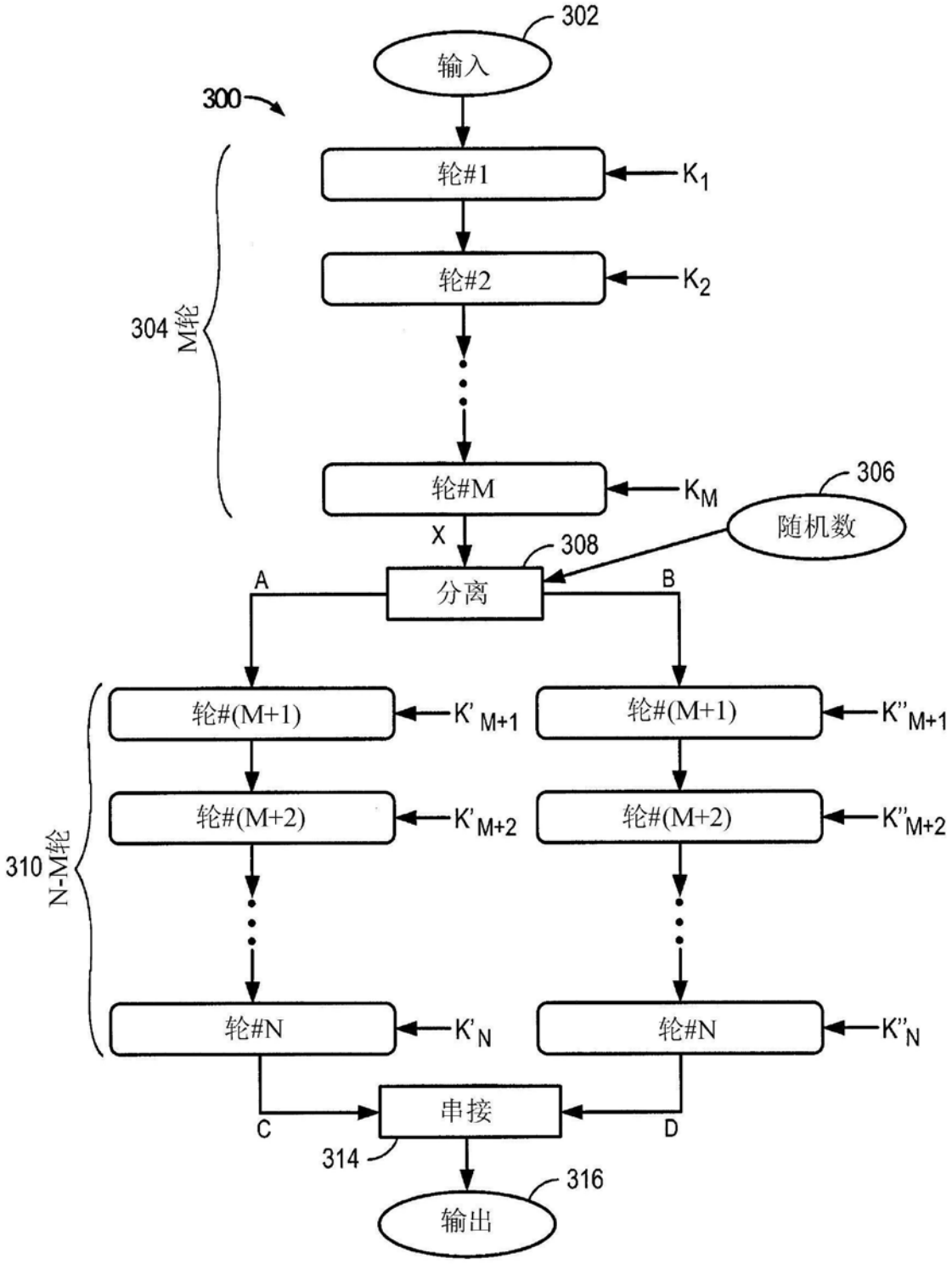

302
输入
300
轮#1
K1
轮#2
K2
304 M轮
轮#M
KM
306
随机数
X
308
分离
A
B
轮#(M+1)
K'M+1
轮#(M+1)
K''M+1
轮#(M+2)
K'M+2
轮#(M+2)
K''M+2
310 N-M轮
轮#N
K'N
轮#N
K''N
C
D
串接
314
316
输出

图3

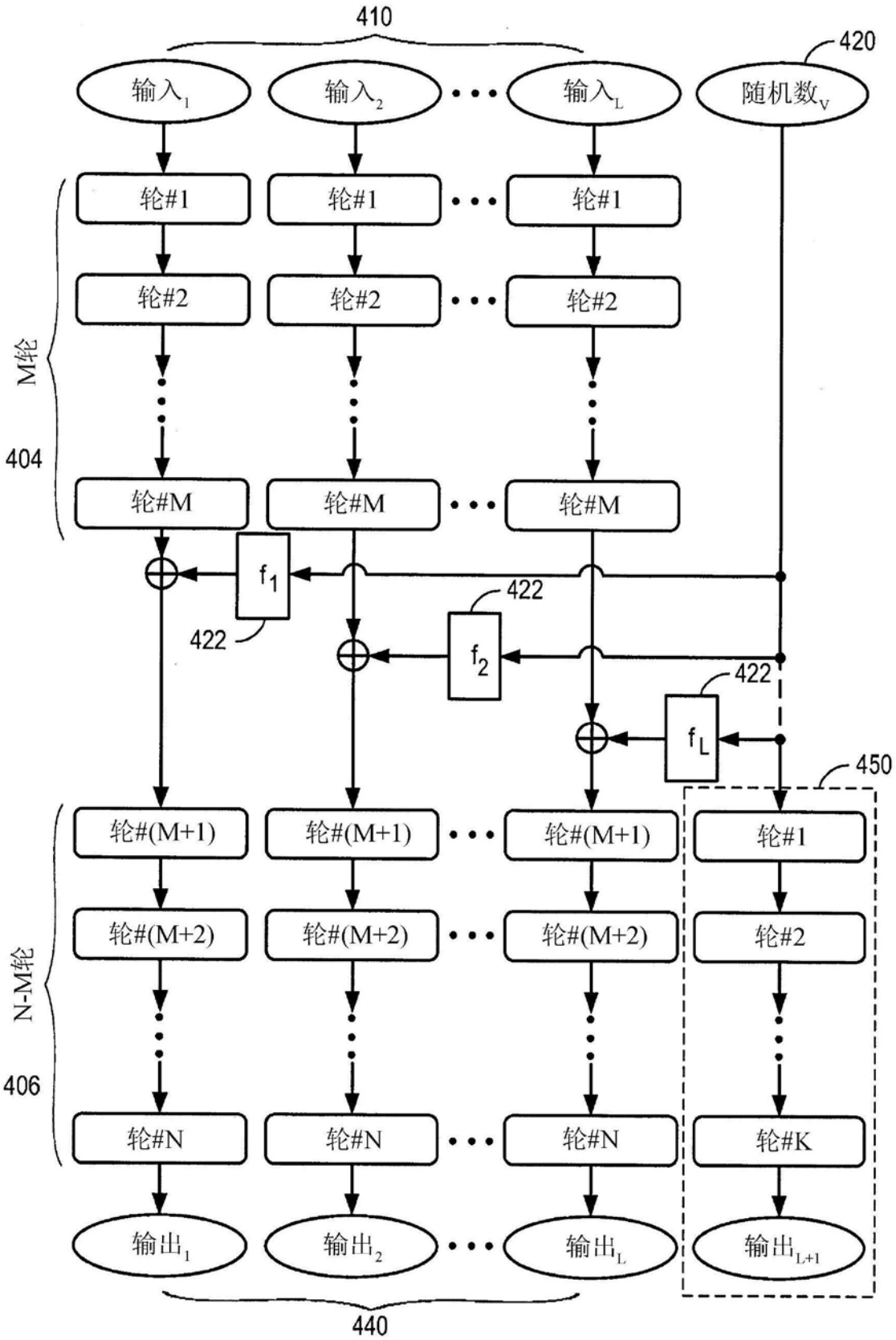

410
420
输入1
输入2
输入L
随机数V
轮#1
轮#2
轮#M
M轮
404
f1
f2
fL
422
450
轮#(M+1)
轮#(M+2)
轮#N
N-M轮
406
轮#K
输出1
输出2
输出L
输出L+1
440

图4A

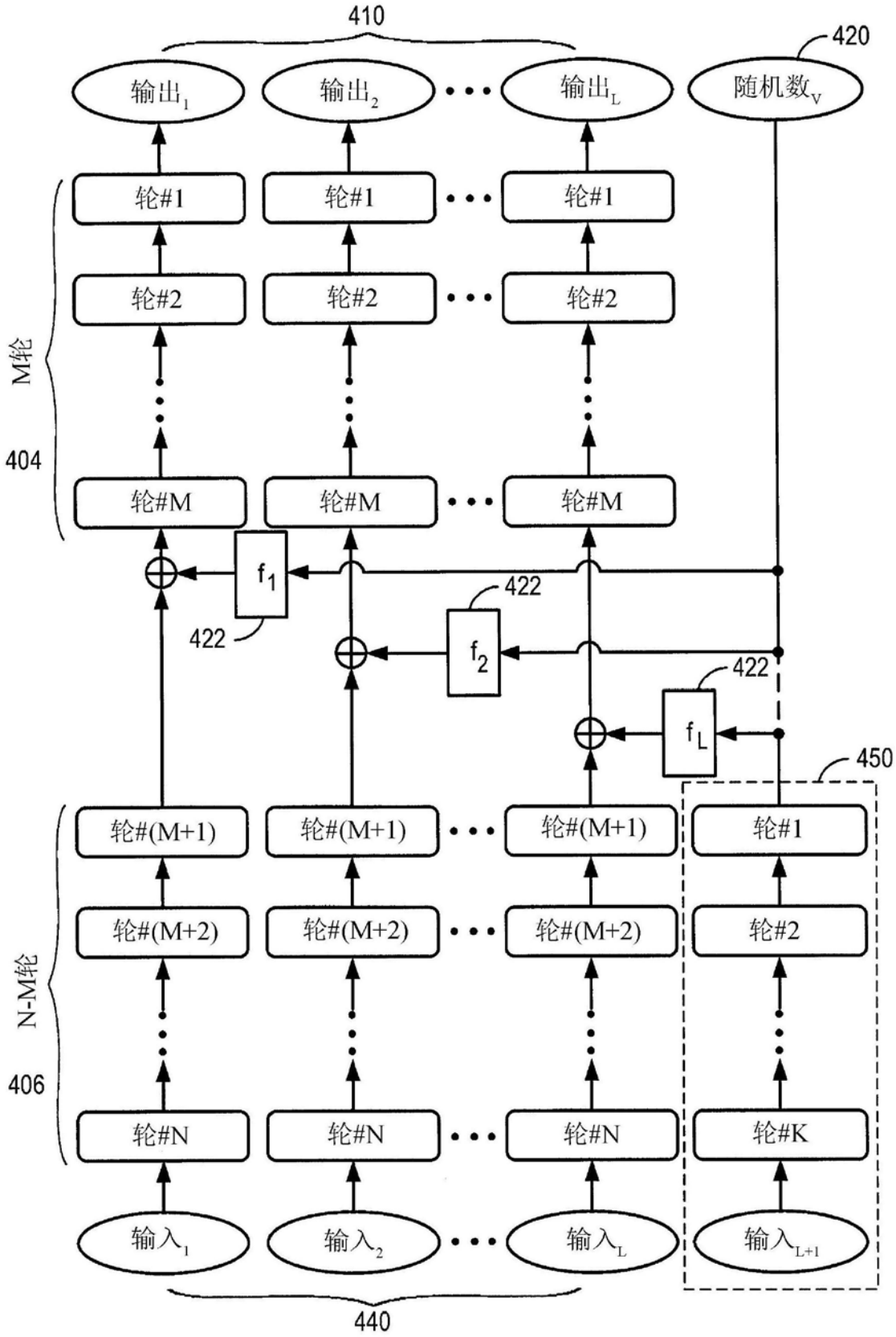

410
420
输出1
输出2
输出L
随机数V
轮#1
轮#2
轮#M
M轮
404
f1
422
f2
fL
轮#(M+1)
轮#(M+2)
轮#N
N-M轮
406
450
轮#K
输入1
输入2
输入L
输入L+1
440

图4B

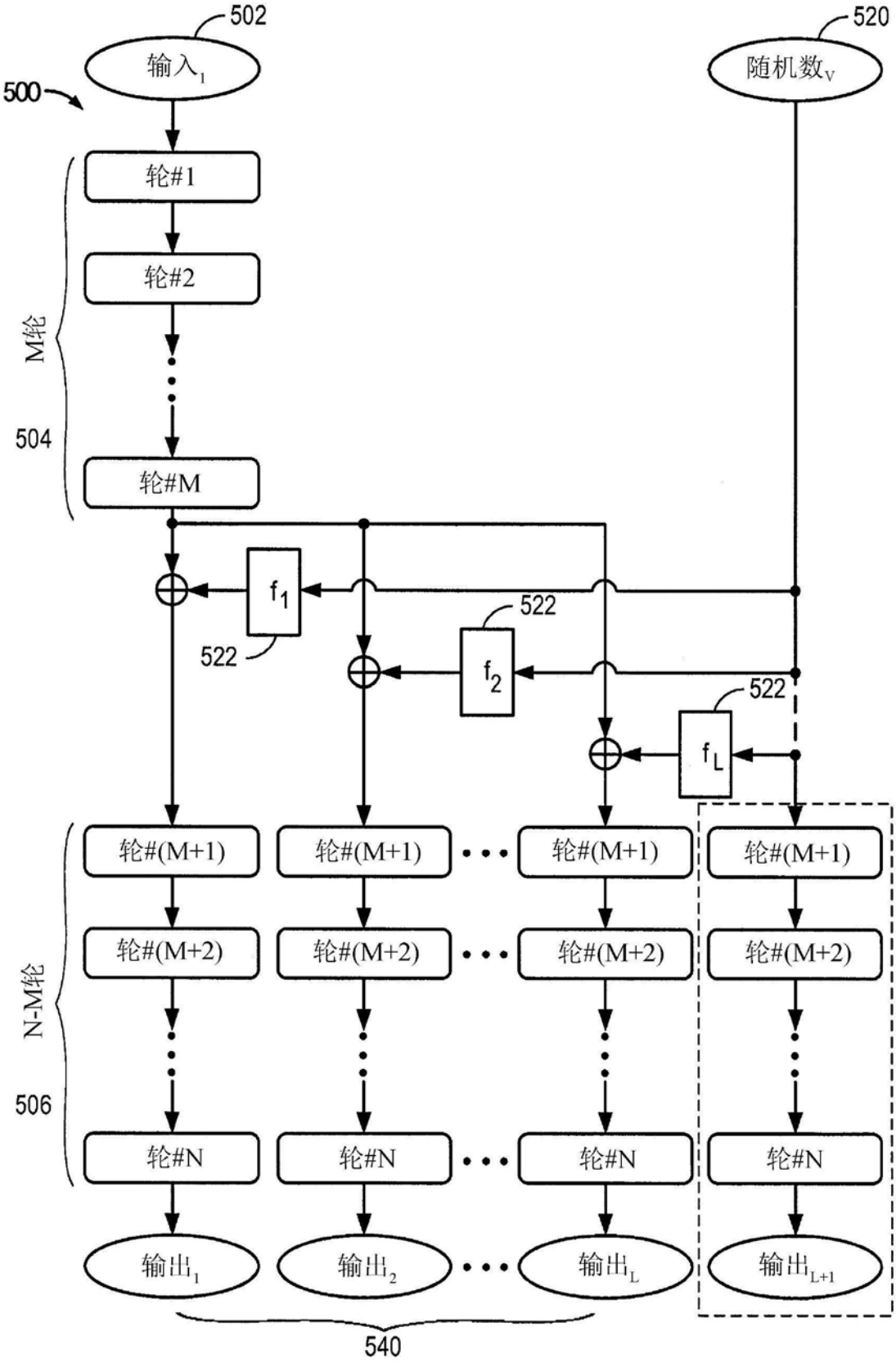

502
520
输入1
随机数V
500
轮#1
轮#2
M轮
504
轮#M
f1
522
522
f2
522
fL
轮#(M+1)
轮#(M+1)
轮#(M+1)
轮#(M+1)
轮#(M+2)
轮#(M+2)
轮#(M+2)
轮#(M+2)
N-M轮
506
轮#N
轮#N
轮#N
轮#N
输出1
输出2
输出L
输出L+1
540

图5

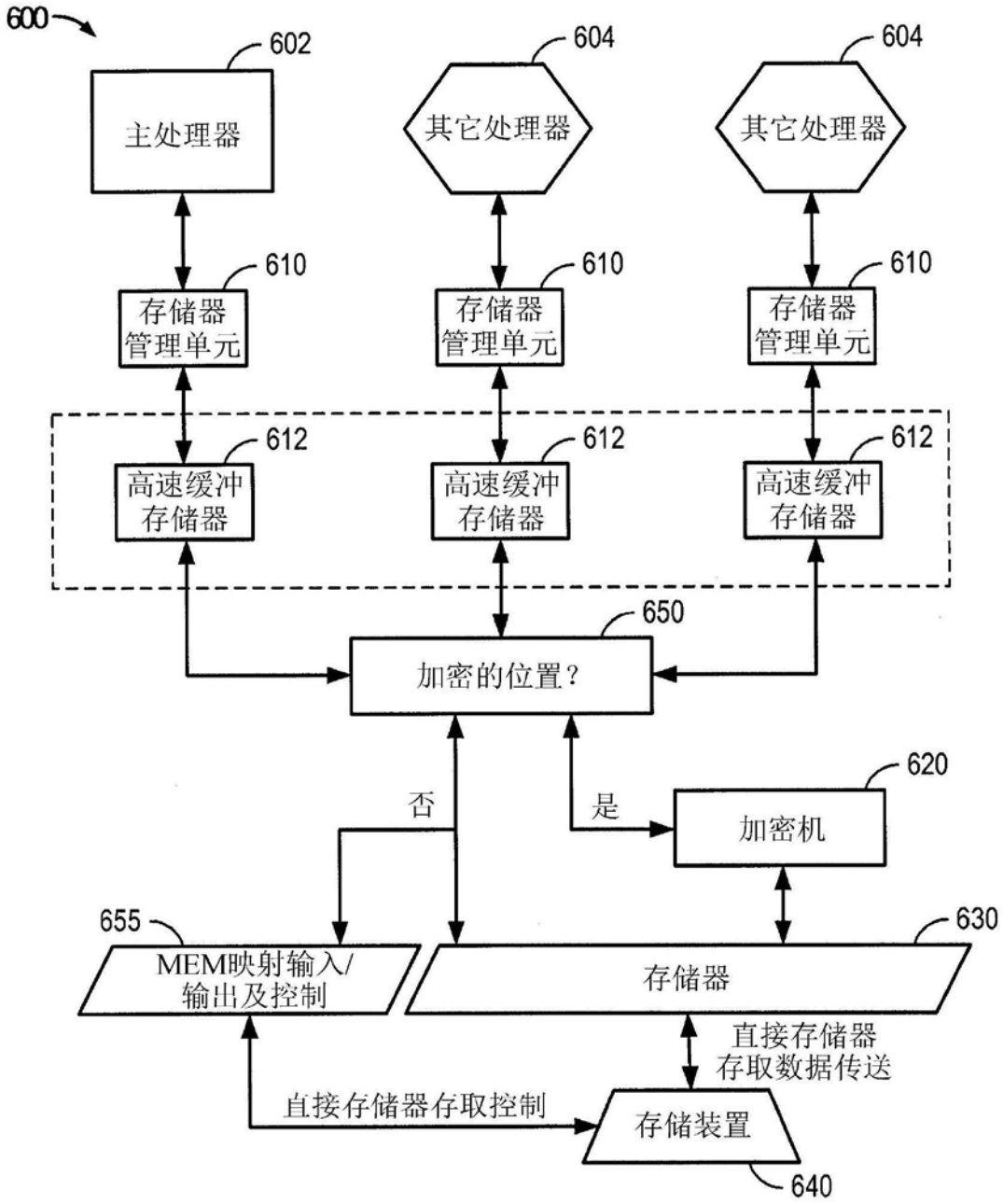

600
602
主处理器
604
其它处理器
604
其它处理器
610
存储器管理单元
610
存储器管理单元
610
存储器管理单元
612
高速缓冲存储器
612
高速缓冲存储器
612
高速缓冲存储器
650
加密的位置?
否
是
620
加密机
655
MEM映射输入/输出及控制
630
存储器
直接存储器存取数据传送
直接存储器存取控制
存储装置
640

图6