[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
G06F 12/14
H04L 9/28

[12]发明专利申请公开说明书

[21]申请号 98122820.8

[43]公开日 1999年11月24日

[11]公开号 CN 1236132A

[22]申请日 98.10.12 [21]申请号 98122820.8
[30]优先权
[32]97.10.10 [33]US [31]08/949,111
[71]申请人 通用仪器公司
地址 美国宾夕法尼亚
[72]发明人 布兰特·坎德洛尔
埃里克·斯普龙克

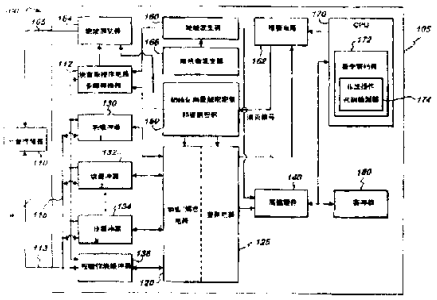
[74]专利代理机构 永新专利商标代理有限公司
代理人 蹇 炜

权利要求书6页 说明书38页 附图页数6页

[54]发明名称 应用块链接和块重新排序的带有外部存储器的安全处理器

[57]摘要

通过在外部存储设备和安全电路的块缓冲器间传送加密程序信息和鉴别信息 对加扰的数据传输解扰。以块链传送程序信息以减少鉴别信息的额外量。一 次传送程序信息的一块,甚至一次传送一个链,并将其临时存储在块缓冲器和 高速缓存中,然后提供给 CPU 处理。这些块可根据加扰地址信号存储在外部存 储设备中,还可以对字节、块、链随机地重新排序,并非顺序地传送给块缓冲 器。还可将程序信息从安全电路向外部存储器传送。



ISSN1008-4274

权 利 要 求 书

1、一种处理程序信息的装置，包括：

一安全电路，包括一中央处理单元（CPU）和用于存储至少一个程序信息块的至少一个块缓冲器；

一外部存储设备，用于存储所述安全电路外部的程序信息；

一第一通信路径，用于将一组所述程序信息块以第一块链从所述外部存储设备向所述至少一个块缓冲器传送；以及

一第二通信路径，用于将程序信息从至少一个块缓冲器向 CPU 传送，以在其中进行处理。

2、如权利要求 1 所述的装置，其中：

所述安全电路包括一鉴别电路，用于鉴别所述程序信息。

3、如权利要求 2 所述的装置，其中：

所述块链是一个简单块链，以使得在所述第一块链中的所述一组块由所述鉴别电路基本上并行地进行处理。

4、如权利要求 2 或 3 所述的装置，其中：

将所述程序信息的所述第一块链和一个后续的第二块链在外部存储设备和所述至少一个块缓冲器之间进行传送；以及

所述鉴别电路用于鉴别所述第一块链的程序信息的至少一个部分，同时将所述第二块链的至少一个部分在所述第一通信路径上传送。

5、如权利要求 2 至 4 中的一个所述的装置，其中：

所述第一通信路径用于将程序信息块以第二链从所述存储设备向所述至少一个缓冲器传送；以及

所述鉴别电路用于从所述第一块链的至少一个部分和所述第二块链的至少一个部分基本上并行地鉴别程序信息。

6、如权利要求 2 至 5 中的一个所述的装置，还包括：

一个安排在所述第二通信路径中的高速缓存器，用于在将已鉴别的程序信息提供给所述 CPU 之前临时存储已鉴别的程序信息。

7、如前面任一个权利要求所述的装置，还包括：

用于检测程序信息中的非法操作代码的装置。

8、如前面任一个权利要求所述的装置，其中：

对所述程序信息的至少一部分进行随机排列以提供所述块链。

9、如前面任一个权利要求所述的装置，还包括：

地址发生装置，用于向外部存储设备提供寻址信息，用于将所述程序信息块以所需序列从外部存储设备向所述至少一个块缓冲器传送。

10、如前面任一个权利要求所述的装置，其中：所述程序信息包括多个将由所述 CPU 连续处理的串。

11、如前面任一个权利要求所述的装置，其中：所述程序信息块被存储在外部存储设备的加扰的存储位置中。

12、如前面任一个权利要求所述的装置，其中：将带有基本上随机变化长度的所述程序信息链从外部存储设备向所述至少一个块缓冲器传送。

13、如权利要求 12 所述的装置，还包括：

地址发生装置，用于向外部存储设备提供地址信息，用于将所述程序信息块以所需顺序从外部存储设备向所述至少一个块缓冲器传送；

其中：

基本上随机变化的长度是根据所述地址信息来确定的。

14、如前面任一个权利要求所述的装置，还包括：

用于提供对所述第一块链的基本上随机的块的重新排序、以及对所述第一块链的一个块的基本上随机的重新排序以便将一个已重新排序的链从外部存储设备向所述至少一个块缓冲器传送的装置。

15、如前面任一个权利要求所述的装置，其中：使用基本上随机变化的序列将所述程序信息单元从外部存储设备向所述至少一个块缓冲器传送。

16、如权利要求 15 所述的装置，其中：所述程序信息单元包括块链。

17、如前面任一个权利要求所述的装置，其中：将多个程序信息以变化长度单位从外部存储设备向所述安全电路传送；以及

每个单元的长度根据各个单元的相关程序信息的处理等待时间来确定。

18、如前面任一个权利要求所述的装置，其中：所述程序信息包括不会由

CPU 处理的假数据。

19、如前面任一个权利要求所述的装置，其中：对存储在外部存储设备中的所述程序信息进行加密；

所述安全电路包括一个解密电路，响应于所述至少一个块缓冲器，用于对加密的程序信息进行解密；以及

所述第二通信路径用于将解密的程序信息从解密电路向 CPU 传送，以便在其中进行处理。

20、如权利要求 19 所述的装置，其中：

将所述程序信息的所述第一块链和一个后续的第二块链在外部存储设备和所述至少一个块缓冲器之间传送；以及

所述解密电路用于对所述第一块链的程序信息的至少一个部分解密，同时，在所述第一通信路径上传送所述第二块链的至少一个部分。

21、如权利要求 19 或 20 所述的装置，其中：

所述第一通信路径用于将程序信息块以第二链从所述存储设备向所述至少一个缓冲器传送；以及

所述解密电路用于从所述第一块链的至少一个部分和所述第二块链的至少一个部分基本上并行地对程序信息进行解密。

22、如权利要求 19 至 21 中的一个所述的装置，其中：

一个安排在所述第二通信路径中的高速缓存器，用于在将已解密的程序信息提供给所述 CPU 之前临时存储已解密的程序信息。

23、如权利要求 19 至 22 中的一个所述的装置，其中：

所述第一块链是一个密码块链。

24、如前面任一个权利要求所述的装置，还包括：

一个通信路径，用于将一组程序信息块以第二块链从所述安全电路向所述外部存储设备传送。

25、如权利要求 24 所述的装置，还包括：

一加密电路，用于为第二块链对程序信息进行加密。

26、如权利要求 25 所述的装置，其中：所述加密电路有条件地响应于地址

信息，以便为第二块链允许程序信息的无加密模式。

27、如权利要求 24 至 26 中的一个所述的装置，还包括：

一鉴别电路，用于为第二块链鉴别程序信息。

28、如权利要求 27 所述的装置，其中：所述鉴别电路有条件地响应于地址信息，以便为第二块链允许程序信息的无加密模式。

29、如权利要求 24 至 28 中的一个所述的装置，还包括：

一重新排序电路，用于为第二块链对程序信息进行随机地重新排序。

30、如权利要求 24 至 29 中的一个所述的装置，还包括：

一长度确定电路，用于为第二块链随机地变化程序信息的单位长度。

31、如权利要求 24 至 30 中的一个所述的装置，还包括：

一假数据插入电路，用于为第二块链将假数据加到程序信息中。

32、如前面任一个权利要求所述的装置，其中：将多个程序信息链以基本上随机变化的序列从外部存储设备向所述安全电路传送。

33、一种用于传送程序信息的装置，包括：

一安全电路，用于提供所述程序信息；

一外部存储设备，用于存储所述安全电路外部的程序信息；以及

一第一通信路径，用于将一组所述程序信息块以第一块链从所述安全电路向外部存储设备传送。

34、如权利要求 33 所述的装置，其中：

所述程序信息包括鉴别数据；以及

所述安全电路包括一鉴别电路，用于提供所述鉴别数据。

35、如权利要求 34 所述的装置，其中：

所述块链是一个简单块链，以使得在所述第一块链中的所述一组块由所述鉴别电路基本上并行地进行处理，以提供所述鉴别数据。

36、如权利要求 34 或 35 所述的装置，其中：

所述鉴别电路对至少部分程序信息进行随机排列，以提供所述鉴别数据。

37、如权利要求 33 至 36 中的一个所述的装置，还包括：

地址发生装置，用于向外部存储设备提供地址信息，用于将所述程序信息

块以所需顺序从所述安全电路向外部存储设备传送。

38、如权利要求 33 至 37 中的一个所述的装置，其中：

所述程序信息块存储在外部存储设备的加扰的存储位置中。

39、如权利要求 33 至 38 中的一个所述的装置，其中：

将带有基本上随机变化长度的所述程序信息单元从所述安全电路向外部存储设备传送。

40、如权利要求 33 至 39 中的一个所述的装置，其中：

将多个程序信息链以基本上随机变化的顺序从所述安全电路向外部存储设备传送。

41、如权利要求 33 至 40 中的一个所述的装置，还包括：

用于提供（a）对所述第一块链的基本上随机的块的重新排序、以及（b）对所述第一块链的一个块的基本上随机的重新排序中的至少之一以便将一个已重新排序的链从所述安全电路向外部存储设备传送的装置。

42、如权利要求 33 至 41 中的一个所述的装置，其中：

使用基本上随机变化的顺序将所述程序信息单元从所述安全电路向外部存储设备传送。

43、如权利要求 33 至 42 中的一个所述的装置，其中：

使用基本上随机变化的长度将所述程序信息单元从所述安全电路向外部存储设备传送。

44、如权利要求 33 至 43 中的一个所述的装置，其中：所述程序信息包括 CPU 不处理的假数据。

45、如权利要求 33 至 44 中的一个所述的装置，其中：以块链提供所述程序信息。

46、如权利要求 33 至 45 中的一个所述的装置，其中：

所述安全电路包括一个加密电路，用于对所述程序信息加密；以及所述第一通信路径用于将加密的程序信息从加密电路传送给外部存储设备。

47、如权利要求 46 所述的装置，其中：所述块链是一密码块链。

48、如权利要求 33 至 47 中的一个所述的装置，还包括：

一个通信路径，用于将一组程序信息块以第二块链从所述外部存储设备向所述安全电路传送。

49、如权利要求48所述的装置，其中：存储在所述外部存储设备中的程序信息被加密，所述安全电路还包括：

一解密电路，用于对第二块链中的加密程序信息进行解密。

50、一种用于处理加密的程序信息的装置，包括：

一安全电路，包括至少一个加密和解密电路、一中央处理单元（CPU）和用于存储至少一个程序信息块的至少一个块缓冲器；

一外部存储设备，用于存储所述安全电路外部的程序信息；

一第一通信路径，用于将一组所述程序信息块以第一密码块链在所述外部存储设备和所述至少一个块缓冲器之间传送；

所述至少一个所述加密和解密电路响应于所述至少一个块缓冲器，对所述程序信息分别进行加密和解密；以及

一第二通信路径，用于将程序信息在所述至少一个解密和加密电路与所述CPU之间传送。

说　　明　　书

应用块链接和块重新排序的
带有外部存储器的安全处理器

本发明涉及用于在一安全电路和一外部存储设备之间有效并安全地传输程序信息块的装置。为了获得更牢靠的加密、执行迷惑并减少额外的鉴别数据，将程序信息以块链形式进行传输。

在一个实施例中，程序信息以密码块链形式被加密并可选地进行鉴别。

在另一个实施例中，程序信息以块链形式被鉴别并可选地被加密。块链极大地减少了额外的鉴别数据。可以应用地址加密来增加安全性。

还可以应用对每个链中以及在全部链接中的诸如块或字节的字段的重新排序来提供进一步的安全性。

在另一个实施例中，向安全电路提供多个程序信息块以产生一个密钥。该密钥可用于对数据传输进行解密。

本发明尤其适用于防止对专有软件算法的复制和逆向工程（reverse engineering），以及保证加密应用例如付费电视节目等的解扰的安全性。

现提供如下定义：

安全电路：

安全电路是一个加密集成电路（IC），其中，甚至包括所有者的任何人都不能访问包含在该 IC 中的内部总线、寄存器和其他电路。IC 可以保存敏感密钥、标识和其他数据，但安全电路不必一定局限于为 IC。例如，它可以是在网络计算机中的执行一个来自通过网络访问的共享存储设备的程序的个人计算机（PC）。网络计算机可以通过访问一个服务器来实时地运行应用程序。将应用程序的各个部分逐步地传送给网络计算机。网络可允许多个计算机同时访问相同的应用程序。所有者应用一个 PC 可以访问接收到的已解密和/或已鉴别和/或重新排序的程序信息。此外，安全电路可以处理未加密但鉴别过的数据。

存储设备

存储设备是各种类型的一分立存储器件，例如一个 IC。但是，在如上所述的 PC 例子中，存储设备可以是一个大容量存储设备，例如位于本地或远端的硬盘驱动器。如果是位于远端的，则数据可以通过一个类似 Ethernet 的网络或者例如根据 IEEE 1394 标准在该存储设备和安全电路之间传输。对大容量存储设备的本地访问例如可以通过 PC 的 ISA、VESA 或 PCI 数据总线进行，或者甚至可以通过一个 SCSI、串行或并行接口进行。大容量存储设备可以由其他的网络计算机或安全电路来访问。该存储设备也可以是 Jazz（TM）驱动器、磁带、CD-ROM、DVD、个人计算机存储卡接口适配器（PCMCIA）、智能卡或任何其他类型的大容量存储设备。

例如，在网络计算机的情况下，有可能通过网络来访问只读的程序信息。为了外部存储安全的目的，可以应用允许读/写能力的本地存储设备，例如存储器。因此，存储设备可以是这些设备类型的任意组合。并且，在网络存储设备的情况下，程序信息可以被逐步地复制到一个更快的本地存储器，该本地存储器可以是同步动态存储器。

程序信息

程序信息一般是指在一程序执行中由安全电路使用的任何信息。这可以包括指令，例如在机器码中的操作代码（op-codes），或者包括伪码或解释码，例如 Java（TM）。程序信息还可以包括查找表、存储的密钥和各种临时数据，例如中间计算值和安全电路的状态。

程序信息甚至还可以包括一些或所有的用于加密/解密或验证/鉴别在块链中的剩下的程序信息的初始化向量和密钥。这可以允许在不同的密钥下加密相同的向量和密钥信息，以使得不同的安全电路可以单个地或作为选定组访问相同的程序信息，并具有导出的或被传送的不同的密钥。

该信息可以包括与如何将块中的字节、链中的块以及链存储在存储设备中的性质有关的密钥信息和数据。这可以包括一个链或链序列中的各种字段的顺序置换信息，这在后面将详细说明。

散列：

散列并不是严格地意味着一个单向函数。虽然一个严格的单向函数是一种

可能性，该函数在一个保密密钥下也可以是可逆的，或者是一个捕获门（trap-door）单向函数，或者是一个非常简单的函数，例如 XOR 操作。

数据传输和加密处理

数据传输用于各种类型的文本、消息、视频和音频信号。这些包括通过通信信道的来自广播和交互电视和无线电、节目预告、新闻服务以及交互消息通讯的文本、消息、视频和音频，但并不仅限于这些。加扰的数据传输可以以各种方式发送，例如通过广播、卫星、电缆、电话或其他通信线路，或者通过一个可移动的大容量存储介质，例如数字视频磁盘、磁带、激光磁盘（CD）、软盘或其他安全电路，并且由一个解扰接收机接收，例如解码器，诸如在消费者家中的机顶盒、播放机或个人计算机。

数据传输可以仅仅是对一个口令（challenge）的响应。该口令使得安全电路用某种类型的加密处理来变换口令信息，以产生一个验证安全电路确实保存了某些保密或专用密钥的输出。

在安全电路中的内部寄存器可以增加或减少。可以与保密或专用密钥一起计算这些值，以计算出要输出的值。这种口令和响应技术一般可以用于在给予一个服务之前鉴别有效安全电路的存在。

加密处理：

这是由一个安全电路执行的处理，其结果一般是产生一个密钥。该密钥然后可以用在很多方面：对数据传输进行加扰和解扰，由客户或主机进行身份验证，等等。该密钥不必总是保存在安全电路中。例如，可以将其从安全电路发送出去以用于验证。

现在提出在现有技术方案中存在的各种问题。

问题：各种专有算法可以被窃取

以很大的代价辛苦开发出来的软件可以轻易地从外部存储设备上复制出来。由于开放的网络例如因特网允许被侵权的代码迅速而广泛地分布，这个问题更加严重。

随着通用处理器芯片的速度的提高，有一种将许多以前在硬件上完成的处理任务在软件上执行的趋势。软件通过使用分立的存储元件和/或包括大容量存

储设备的存储设备来传输。通过仅仅执行不同的软件，可以便于为不同的应用程序快速重构处理系统。但这种趋势被这样一个事实所阻碍，即由于软件可以容易地复制、分解、逆向工程、并且接着被散布，从而剥夺了开发者和/或发明者对于该知识产权的利益。

并且，随着网络的速度和可靠性的提高，例如 Ethernet 从 10 兆比特每秒提高到 100 兆比特每秒，等等，可以实现在网络上实施系统，其中软件可以实时地执行。这种所谓的网络计算机将总能访问一个装在一个基于网络的服务器上的应用程序的最新修订版。在这个服务器的档案中的任何应用程序都能够很快地被访问。但这种服务器容许某些人下载和存储整个应用程序，从而剥夺了服务提供者现在的收入。软件一旦被下载，就会很容易地与其他人共享。

因此，需要使软件分析和逆向工程、以及由通用处理器进行软件复制和再应用变得更加困难。

问题：加密密钥发生器

加密应用程序一般涉及基于保密或专用密钥信息的密钥的产生/导出。

典型的加密密钥发生器在数据传输上执行加密处理。由于需要阻止未授权的人（例如侵权者）获得对数据传输的访问，因此对数据传输进行加扰变得越来越重要。无论数据是如何被发送或传送的，加密处理的出现就是为了确保数据的提供者、例如加扰发送者从他们发送的知识产权中获得报酬。在通信网络的情况下，可以对消息加扰以确保该消息的保密，并且鉴别发送者和接收者。它可以为不可否认（non-repudiation）创造条件，以防止接收者后来宣称他们未要求该数据。不可否认对于提供者是非常重要的，因为他们对于获得报酬有较高的期望。其他任何人都不象诚意购买者一样具有鉴别消息所必须的加密密钥。在一个或多个保密加扰密钥下进行传输之前，数据传输被加密处理，例如被加扰。经加密处理的数据传输由一个加密解处理器（解扰接收机）接收，例如消费者家中的机顶盒、媒体播放机或个人计算机。

诸如由一个解扰接收机完成的加密处理一般在一个安全电路中完成。该安全电路在制造或应用程序的安装和初始化时装有所需的密钥，并且执行一种授权访问数据传输的处理。如果访问被允许，则导出解密密钥。当与有关硬件或

软件解密模块一起使用该解密密钥时，数据传输被解扰，例如，变得可观看或其他适合于用户的方式。

解扰硬件或软件可以包括在安全电路、例如一个专用 IC（ASIC）中。

同样，对诸如信用卡号等信息进行加扰以便通过因特网传送给贸易商的加扰发送者，例如某些人家中的 PC，使用在制造或应用程序安装和初始化时加载上的所需密钥来导出对要发送的敏感数据进行加扰的密钥。

在 PC 实例中，加扰可以在一个软件模块中完成，但加扰实际上并不能取代所说的安全电路。在任何一种情况下（加扰或解扰）导出的密钥可以从安全电路输出到硬件或软件加扰/解扰模块，或者在安全电路内部带有解密模块时将密钥保存在安全电路的内部。密钥最好保存在安全电路内部并且在安全电路内部执行加扰/解扰。

如果将密钥从安全电路输出，该密钥会非常迅速的变化，甚至一秒钟内几次，从而使得只能在非常短的时间内应用其内容。硬件加扰/解扰硬件或软件模块可以位于离导出用于对数据传输进行加扰/解扰的密钥的安全电路较远的地方。

对于一个通过网络执行指令的 PC，安全电路可以是 PC 本身，解扰单元可以仅仅是一个软件模块，该软件模块与合适的密钥和加密函数识别符一起接收例如在内部或外部存储器中的一条消息的长度和指针。

由安全电路中的加密处理执行的函数应用公知的散列算法和公用密钥加密法来进行消息散列、符号化以及签名鉴别。

在上述的 ASIC 和 PC 两种情况下，一般都采用一个微处理器来实施访问控制、执行散列、签名验证、符号化和鉴别功能。该处理验证安全电路确实被授权对数据传输进行解密。如果已授权，则微处理器为数据传输导出解扰密钥。安全电路一般具有一个内部存储设备，例如用于存储由微处理器使用的解扰程序信息的存储器，用于存储解扰密钥数据和解码器状态的存储器，以及用于存储中间计算值和临时数据的暂存器。解扰接收机、例如解码器的状态可以指示解码器是否被调谐到一特定频道和频道识别符。解扰接收机的状态还可以存储其是否被授权接收该频道，以及调谐到的节目是预定的、按观看次数收费的还

是请求式观看的。

因此希望使侵权者对于带有外部存储器的加密密钥发生器执行的攻击变得更加困难。

问题：使用内部 ROM 和 RAM 容量方案的不灵活性

对于一个 ASIC，由 IC 用来存储程序信息的内部存储器可以产生于只读存储器（ROM）、可擦除可编程只读存储器（EPROM）、电可擦除可编程只读存储器（EEPROM）、闪速存储器或带有后备电池的随机存取存储器。一般地，用于制造具有最小几何形状和最快电路的 ASIC 的制造工艺最初是为基于 ROM 和 RAM 的技术开发和表征的。EEPROM 和闪速能力在后来才出现。因此，通过使用基于 ROM 和 RAM 的技术来设计 ASIC，可以获得优于其他技术的性能。而且，对于 VLSI 铸造，由于带有 ROM 和 RAM 的设备的设计更简单，所以制造这种设备比制造带有 EEPROM 和闪速的设备更容易。因此，以基于 ROM 和 RAM 的设计，设计者可以实现较低的制造成本。

制造一个完全出自带有备用电池的 RAM 的内部存储器一般来说是不实用的，因为一个具有允许对数据读写能力的 RAM 单元比一个只允许读数据的 ROM 单元要包含更多的门，并且一般有一个大得多的结构。因此， RAM 存储器存储的编程信息要远远少于同样尺寸的 ROM 存储器。

然而，由于必须替换整个 ASIC 才能改变编程信息，所以将编程信息存储在内部 ROM 中也有缺陷。例如，对于修理软件问题（例如故障）或者为不同用户提供新的或定制特征，这也许是必须的或所期望的。为了达到这一点，必须制造一个带有程序信息的变化的新的芯片。

而且，无论在安全电路例如 ASIC 中安装的任何类型的存储容量为多少，对于任一给定应用程序来说都会太大或太小。如果存储容量比需要的大，安全电路的价格就会比所需的高。如果存储容量比需要的小，则或者对于该任务不适合，或者必须省略某些特征以使得软件合适。存储容量的大小很少是刚好合适的。

因此，需要提供一种方案，用于修改存储设备的容量，例如存储器数量，并且用于容易且便宜地更新诸如一个加密芯片的安全电路的程序信息。该系统

将程序信息存储在安全电路外部的一个存储设备中，并且在存储设备和安全电路之间提供安全有效的传送。即使通过网络，程序信息的传送也应该足够快，以适应代码执行的需要。此外，应该限制使安全电路工作所需的内部存储器的数量。系统可以使用有限数量的可以支持安全电路、监视器错误条件、解释伪码、或者处理实时处理事件的快速存取内部程序信息。然而，如果该内部程序信息是以一种固定形式存储的，例如ROM或只读CD-ROM，则不能象外部存储的程序信息一样容易地改变。

问题：保障外部存储-额外鉴别

在过去，已经在字节和块上使用了各种加密技术。但侵权者采用了各种各样的“攻击”（attack）来破坏系统的安全性。一种攻击是企图使安全电路读取加密的存储器并将其写到一个空白区，在这里可以捕获程序信息然后对其进行分析。这种类型的攻击实际上采用了解密电路本身对程序信息解密，排除了进行更广泛分析的需要。

另一种攻击试图破坏应用程序本身的安全性，通过改变应用程序的执行，以使得在这种情况下在解扰接收机中的安全电路对高级服务进行解扰，而不必支付适当的预定费。为了完成这些和其它攻击，侵权者试图修改外部存储设备例如存储器的内容。为了完成这一点采用的一种技术是“试探法”，其中，在外部存储设备中的程序信息被以一种试探和错误逼近的方法来处理。侵权者不知道哪个或哪些保密密钥被用来对程序信息加密，但设法处理在外部存储设备中的程序信息，直到获得了一个有用的结果。

为了防止这些或其它攻击成功，可以采用鉴别、更强的加密、链字段的重新排序或上述的任何组合。

鉴别可以被用于检验程序信息的起点。在采用鉴别的系统中安全电路将不会处理未伴随着正确的鉴别信息的程序信息。在现有技术中的强（strong）鉴别比较昂贵。但是，鉴别信息量必须足够大以提供一个恰当的安全级。在常规的采用字节加密或块加密的存储器加密方案中，对于芯片从外部存储设备中取出的每个字节或块都需要鉴别信息。对于单个字节的程序信息需要几个字节的鉴别信息来防止试探。换句话说，该字节需要被扩展以包括附加的鉴别信息。

如果一个 8 位字节的程序信息被扩展到只包括 8 位附加鉴别信息，则由于对于每字节 8 位的情况只有 2^8=256 种可能的试探组合，鉴别信息会很容易地由试探法确定。为了提供可与数据加密标准（DES）相当的安全级，可以采用 56 位（7 个字节）来提供鉴别信息的 $2^{56}=7.2\times10^{16}$ 种可能的组合。于是，鉴别信息将代表全部存储量的（7/（1+7））或 87%。该额外数据量是非常低效的。

采用块加密，将几个字节的数据在一个块中聚集并进行鉴别。例如，可以采用大小为 8 个数据字节的块。则对于 8 字节的鉴别信息，额外数据量仍高达全部存储量的（7/（7+8））或 47%。由于需要相当大的存储设备仅用来处理鉴别信息，这种过多的额外数据会严重地影响整个系统的成本。这对于必须以尽可能低的成本制造的消费者电子设备、例如手持游戏、蜂窝电话、以及电视解码器来说是无法接受的。特别地，存储设备的成本通常是一个重要的限制因素。因此，对于现有的数据鉴别方案，额外的鉴别信息量大得难以接受。

因此，需要有一种能使安全传送程序信息所需的鉴别信息（例如，校验位）量最小的系统。

问题：不合适的程序信息加密

对一单个加密字节的程序信息的试探攻击是很容易执行的。仍假设一个 8 位字节，对于该程序信息这只需要试探 2^8=256 种可能性就可获得一个确切的结果。但是，对于某些侵权攻击，仅仅改变程序信息使其与原来不同的能力是一个目标。在这个例子中，仅仅是试探一单个字节值而不影响其他字节的能力将会导致一个成功的侵权攻击。

对一单个加密程序信息块的试探攻击有一些困难，但仍然是易处理的。例如，大的通用精减指令集计算（RISC）处理器具有长度为 64 位的指令。假设每块 8 字节，每字节 8 位，对于侵权者来说，改变一个程序信息块并且只影响一个指令是相对容易的。

即使对于宽度只有一半大小、例如 32 位的指令，也只有两个指令被影响。所谓的复杂指令集计算（CISC）处理器同样也有受到攻击的危险。被称为“8 位处理器”的 CISC 处理器并不是真的是 8 位，因为这种处理器一般需要取出一个、两个或三个程序信息的操作数，这使得任何指令都在 8 位到 32 位之间，其

平均大约为20位，但这取决于对程序所使用的指令的选择。因此，对于所谓的“8位”指令，试探一个8字节块的加密值可能只影响三个指令。

因此，希望有一种更牢靠的加密算法来安全地传送程序信息。

问题：即使加密，执行也是可观察到的

即使程序信息块可以被加密或鉴别，有些人通过观察在一通信装置、例如总线或网络上的数据传输，也可以得出程序信息的函数和设计。侵权者能够得到有关程序信息的信息越多，他就会有更多的方法来改变程序执行。通过访问来自一个内部存储电路例如高速缓存的或者只进行了解密、或者进行了解密和鉴别、或者只进行了鉴别的数据，而不是必须还从外部取出程序信息，该内部存储电路可以迷惑（obfuscate）一些函数和设计。

但是，因为将程序信息载入第一位置的高速缓存的原始通信序列可以被观察到，所以又出现了一个问题。没有高速缓存的系统更容易分析，因为在外部接口上可以看到循环代码、例如循环（loop）。可以很容易地看见相同的被加密、被加密及鉴别、或者仅仅被鉴别的程序信息一次又一次地被传送。高速缓存通过使传送在高速缓存内部进行而不会在通信装置上被看到，隐蔽了该操作。然而，一个聪明的侵权者会注意到没有外部传送发生，因而作出结论，即出现了某种内部操作。原则上讲，不希望让侵权者知道有关正在执行的算法的任何信息。这包括全部结构，例如字节到块、块到链或链到程序信息序列的联系，处理顺序，例如总是在引导操作执行特定的程序信息，以及程序信息的组织，例如数据表组织。

因此，希望有用于迷惑加密的、鉴别的或任何程序信息链的执行的技术。希望以这样一种方式来传送程序信息，即打乱安全电路的真实的执行顺序。该顺序可以在一个块、链或程序信息序列内被打乱。

也就是说，希望打乱组成一个块的字节的顺序、组成一个链的块的顺序、以及组成一个程序信息序列的链的顺序。顺序置换可以是固定的，但在字节和字节之间、块和块之间、链和链之间、或者程序信息序列的基础上是不同的。希望将顺序打乱推广到更深一步，即比一个块要大，例如在两个块或整个链上进行。同样希望将其用在所有其他字段上。

问题：顺序置换算法可能被发现

任何在硬件上实现的顺序置换算法都可以被侵权者用探测 VLSI 或其他分析来发现。置换函数可以用密钥加密，并且依赖于地址和单位。但是，这并不能防止一确定侵权者发现密钥和依赖关系是什么。

因此，还希望有一种使对顺序置换的分析和逆向工程更加困难的方法。

问题：基础顺序并不改变—地址单元总是相同的

即使采用顺序置换，侵权者也可以观察到在存储设备之间的每一次通信，知道哪些字节属于哪些块以及哪些块属于哪些链。也就是说，在存储设备中的一特定地址单元是与一特定字节、块或链序列相联系的。地址单元将总是包含相同的信息。由于顺序打乱，侵权者可能不知道确切的位置信息是什么，但他知道它与其他字节、块或链的关系是固定的。侵权者不需要知道存储在一特定单元的程序信息的值是什么。侵权者可以试探在该存储单元的值。虽然由于顺序置换技术存储单元在不同时间被访问，侵权者可以通过搜索所有值来有计划地完成这一工作。

因此，希望有一种用于动态地改变存储着表示一特定字节、块或链序列的数据的存储设备中的地址单元的方案，以防止某些人有计划地试探代码。

问题：每次传送都是相关的

侵权者可以观察在存储设备之间的每次程序信息传送，并得知其是加密的、鉴别的、顺序置换的还是上述的全部。

对于其他迷惑，希望与传送的程序信息一起传送“假信息”或不是必须需要的数据。

问题：所需的双向写和读

存储设备可以是只读的，但也有许多原因表明存储设备也应该是可写的。不同的加密和未加密但为独有的应用程序对于数据存储有着不同的要求。

现代的加密应用程序常常采用公用密钥加密，这通常比保密密钥加密法需要更大的密钥。加扰发送机或解扰接收机可以执行某种类型的加密应用程序，该应用程序可以在一个开放的网络例如因特网上交互，可能需要存储许多例如来自一个根特权（Root Authority）或验证特权（Certification Authority）

的各种公用密钥。而且，对于付费电视解码器，有多个用于访问控制系统和/或解码器制造商的公用密钥。随着时间的变化，会有更多的公用密钥作为在网络上交互的结果需要被存储。这些密钥中的一些密钥可能会很长，例如，如果公用密钥为2048、4096位或更大。因此，需要大容量存储设备、例如大量的读/写存储器来存储密钥和其他相关信息，以影响一个可行的加密应用程序。

这对于许多专有的应用程序来说也是一样的。趋势就是处理越来越多的数据。由于现有的存储器只能用于读程序信息，因此希望对于用于写程序信息和以后检索程序信息的存储器的类型和数量有很大的灵活性。

因此，希望在一个外部存储设备和一个安全电路之间有一种安全双向通信，其具有适应对于附加程序信息存储的不断增长的需求的灵活性，而不需改变安全电路的设计。并且整个设备的安全性不会减小。

问题：与非保密外界的通信和备用安全模式

安全电路可能必须与没有解密装置的显示设备、外围电路或计算机连接。在涉及与一个人交互时这是很重要的。例如，如果一个用户输入了一个错误的个人识别号（PIN）代码，则安全电路必须将这个问题通知给该用户，以便可以重新输入 PIN。这可能需要与主机设备进行通信，将错误条件或错误消息适当地显示在一屏幕上。在专用于外部通信的引脚、通信端口或总线上存在着一种缺陷。

一些程序信息的执行可以具有减少的执行等待时间要求，需要除了由链进行的一个备用通信模式。而且，安全电路可能需要与具有不同安全方案的其它设备进行互操作。

还希望提供一种条件无加密模式，从而不执行程序信息的加密/解密、鉴别产生/验证、或顺序置换。该条件无加密模式不仅允许一个可能的芯片调试工具，还允许安全电路与世界自由地进行联系，即发送和接收明文数据，例如与显示设备、其它计算机等进行联系，从而允许通信装置不仅仅被用作为程序信息的运输工具。这将减少用于外部通信的分离引脚、通信端口和总线的数目。

还希望换掉程序信息的链加密/解密、鉴别产生/验证、或顺序置换，而采用不是基于链的不同类型的加密/解密、鉴别/验证、或顺序置换。例如，不是

采用链，而是可以采用字节或块处理。

问题：链长度的检测

侵权者也许能够分析程序信息的执行，以确定何种程序信息属于一特定链。该认识可以允许侵权者以一种更富选择性的形式来试探程序信息。原则上，这是一种防止一个潜在的侵权者得到任何有关程序信息是如何执行的信息的好主意。

因此，希望以随机序列从一个链到下一个链传送带有可变链长度的程序信息块，而不对所执行的程序信息进行任何特别的考虑。

问题：不同的等待时间要求

实时中断子程序具有与背景或维护程序不同的执行等待时间要求。现在设计者有一种自然的趋势，就是为所有程序信息设计更短的链，只为了处理实时中断子程序的更快的执行要求。但减少所有程序信息的链长度会不必要地增加存储设备的存储容量，以容纳增大的鉴别信息量。

因此，希望以块链传送程序信息块和相关的鉴别信息，其中，可以采用不同的链长度来传送具有不同等待时间要求的不同类型的程序信息。放置在较低地址单元中的程序可以具有较低的等待时间，而在存储设备的较高地址单元中的那些可以具有较高的等待时间要求。

问题：一般的通信/存储等待时间要求

虽然某些程序具有特定的执行等待时间考虑，等待时间对于某些应用程序来说仍然是太长了。因此，必须研究出一些装置以便于更有效的程序信息传送和存储。

为了帮助减少程序信息等待时间以提高执行速度，希望将某些特征设计进通信装置和安全电路的结构中。

问题：鉴别/验证等待时间要求

虽然某些程序具有特定的执行等待时间考虑，用于鉴别/验证的等待时间对于某些应用程序来说仍然是太长了。因此，必须研究出一些装置以便于更有效的鉴别/验证。

因此，希望将某些特征设计进鉴别/验证函数中，以帮助减少程序信息执行

等待时间。

问题：加密/解密等待时间要求

虽然某些程序具有特定的执行等待时间考虑，用于加密/解密的等待时间对于某些应用程序来说仍然是太长了。因此，必须研究出一些装置以便于更有效的加密/解密。

因此，希望将某些特征设计进加密/解密函数中，以帮助减少程序信息执行等待时间。

本发明提供了一种具有上述和其它优点的系统。

依据本发明，提供了一种装置，用于在一存储设备和一安全处理电路之间以密码块链安全地传送加密的程序信息块。

提供了一种装置，用于在一存储设备和一安全处理电路之间以块链安全地传送鉴别的程序信息块。

提供了一种装置，用于在一存储设备和一安全处理电路之间以链接安全地传送程序信息的重新排序字段。

本发明还提供了一种装置，用于加密地产生一密钥，从而可以使用该密钥来获得对数据传输等的访问。

在本发明的一个方面中，一种用于在一存储设备和一安全电路之间安全地传送程序信息块的装置包括用于提供至少一个程序信息块的装置，其中该程序信息块包括一包含具有第一字节序列的多个字节的特定块。

由于数据可以被顺序地处理，每次处理一个数据块，一个大小能存储一个数据块的块缓冲器就是一个最小的实施装置所需的全部。

还提供了用于在存储设备中存储程序信息块的装置，例如一个地址发生器。

密码块链接是一种牢靠的加密算法，因为在一个块中的变化将接连导致其他块的变化，因而对于侵权者来说实现对程序信息的简单改变变得很困难。

密码块链接可以用在用于保密的散列和加密中。可以在加密的鉴别块上对最新的明文块进行异或操作（XOR），以提供整个密码块链接对鉴别块的解密的依赖性。

例如，可以以两个或更多八字节块来传送程序信息和鉴别信息。由于鉴别信息相对于已鉴别数据的相对较低的额外量，所以块链接是比较有效的。鉴别信息与最新的明文数据（例如，程序信息）块进行 XOR，并且可选地被解密，以产生一验证值。将该值与一个由硬件已知的值进行比较，以验证该鉴别数据是正确的。该值可以对于不同的链是不同的，也可以对于所有的链都是固定的。为了提供在密钥之间的附加独立性，用于对鉴别信息进行解密的密钥与用于对已鉴别的信息进行解密的密钥可以是不同的。而且，可以在每一次解密操作以地址修改密钥，以提供在一个链内的每个块对地址的依赖性。

密码块链接可以与另一种散列算法一起使用，来获得更牢靠的安全性。由于每个块必须以一种顺序方式处理，所以完成这些不会花费另外的等待时间。当第一块被解密时，不仅将其与第二块的密文进行 XOR，还将其送至鉴别电路。最后一块为多个鉴别位，不需要将其送到鉴别电路，而只是对其解密，并与在硬件中保存的一个值进行比较。

提供第一通信路径例如一总线，以便在外部存储设备和一个或多个块缓冲器之间以一个链来传送程序信息和鉴别信息块。由于数据可以串行处理，每次一个块，所以一个大小能存储一个数据块的块缓冲器就是一最小实施设备所需要的全部。鉴别信息由鉴别电路读入并验证。

如果需要，在一个与鉴别电路相连的解密电路中对程序信息进行解密。来自一相关的存储设备的加密密钥数据可以被用于此目的。

如果侵权者为了试探而改变了链中的前面块中的任何数据，则计算出的与鉴别信息进行比较的散列数据将是不正确的，所得的验证值将不匹配。安全电路，例如一个 ASIC 或 PC，就会得知出现了窜改，从而可以采取对抗措施。

有多种方式可以实现鉴别操作。散列法可以以密钥加密，例如使用一个保密密钥，而鉴别信息是以明文出现，或者散列法不以密钥加密，而鉴别信息被加密，或者为了更牢靠的安全性，对散列法以密钥加密，同时鉴别信息被加密。可以使用不同的密钥来用于散列和解密。散列密钥可以是一个保密密钥，而鉴别信息可以在一个公用密钥下加密。用于对鉴别信息进行加密的相同的密钥也可以用于对被鉴别的程序信息加密。其优点是可以以与程序信息相似的方式来

处理鉴别信息。然而，使用单独的密钥可以增加安全的级别。

在另一个实施例中，使用块加密用于保密。这些块在解密时被鉴别。使用的鉴别技术可以是一种散列，这可能需要一个严格顺序的散列，例如，块#1 被散列，然后以块#1 的散列输出对块#2 进行散列，以此类推。可以使用已知的算法例如 MD5 和 SHA 用于这种类型的严格的散列。

虽然可以应用这种散列法，由于操作的串行特性，散列法会引入一等待时间。可以提供一种简化的散列函数，执行所有明文块的 XOR。该散列值可以用鉴别信息来验证。事实上，鉴别信息可以作为一个块与程序信息一起被 XOR。这种技术改进了程序信息执行等待时间，这对于实时操作系统是很重要的。这里，在为整个链计算散列的同时，每个数据块不仅可以如同在由 FIPS 调用的电子码书中那样被独立地加密，还可以被独立地 XOR。这种被称为“简单块链接”的技术重点在于减少执行等待时间。

对非法操作代码或非法解释代码命令的检测可以被用作鉴别的一种形式。在接收到一个非法操作代码或命令之后，系统可以确定如何响应，例如复位、增量计数器或一些其它行动。

由侵权者生成一非法操作代码依赖于一给定处理器的指令集。有些指令集是完全开发的，只有很少的未定义的或非法的操作代码，而另一些指令集是精减的，具有较多未定义的或非法的操作代码。例如，如果一个指令集具有 20% 的未定义或非法操作代码，则意味着侵权者有 80%的随机生成一合法操作代码的机会。这并不是说侵权者产生了一特定操作代码而不只是一个合法操作代码。但一随机合法操作代码而不是一想要的代码就可以形成一次成功的侵权攻击。例如，如果目标是原始操作代码的简单无效，则将是这种情况。由于具有 80%对侵权者有利的可能性，这种仅仅检测非法操作代码的方法还存在着很多问题需要考虑。

因为随着在一特定链中的每个后续块被影响，侵权者生成一非法操作代码的可能性增加，所以非法操作代码检测作为鉴别的一种形式与密码块链接一起使用则更有效。例如，如果在一个链中有十六个指令块，则如果侵权者改变了链中的第一个块，侵权者成功的可能性如下：$(.8)^{16}=0.028$。情况发生了变化，

现在侵权者失败的机会大约为97%。由于这个原因，密码块链接是一种更牢靠的加密方法—这隐含着通过检测非法操作代码来进行鉴别。但密码块链接更好的原因还在于，它使得侵权者试探程序信息的加密以便隔离对一单个块所作的任何改变、从而增加生成带有不想要的副作用的非故意的操作代码的机会变得更加困难。

一个问题是外部存储设备存储的不只是操作代码。只有操作代码可以由CPU的指令解码电路来验证。更牢靠的安全性需要明确的鉴别。

可以通过鉴别信息与明文数据块的散列的XOR来执行鉴别，以产生一验证值，接着将该验证值与一预先存储的值进行比较，或者也可以仅仅将鉴别信息与散列的程序信息进行比较。

鉴别函数可选地将以明文传送的多个程序信息块散列，以便与解密的鉴别信息进行 XOR。为了防止侵权者使用一种已知的散列算法生成他们自己的已鉴别的程序信息，必须使用一个加密密钥。这可以用两种方式来完成—对散列法用密钥加密或对鉴别用密钥加密，或者两者兼而有之。

作为解决等待时间问题的另一种技术，简单块链接对每个程序信息块使用一种单独的块加密。于是，每个块被独立地加密和解密，所以处理可以并行地进行。此外，整个块链或块组被鉴别。一种散列方法是将程序信息块一起与鉴别信息进行XOR。这都可以立刻完成。

为了获得更牢靠的安全性，可以采用更复杂的散列法，但这些方法会引入一顺序依赖性，从而一个块可能需要在另一个块之前进行散列。如上所述的使用加密和鉴别处理的简单块链接，与密码块链接一样，减少了额外鉴别位，但当采用并行解码电路时，可以避免密码块链接的等待时间问题。如果只使用一单个块缓冲器，则密码块链接和简单块链接的等待时间大约相同，唯一的区别是，一个块解密的输出是与下一个块解密的输出进行 XOR（对于简单块链接），而不是与下一个块解密的输入进行XOR（对于密码块链接）。

应用明文块的XOR进行解密和鉴别的简单块链接方法存在的问题是任何一个块可以被重新排序出序列，而鉴别仍会检验出来。所以虽然解密和鉴别操作可以并行地完成，但引入了一个潜在的问题。应该将带有地址依赖性的加密与

应用简单 XOR 散列函数的简单块链接一起使用。

这就是说，在链中的每个块使用的密钥与作为特定块地址的一个函数的密钥不同。如果使用 DES 加密，则为了试探而改变一个块的任何程序信息都将导致解密输出的大约一半的位改变，导致鉴别验证检验不出来。没有密钥的情况，侵权者找到正确的鉴别信息来校正将是很困难的。

在减少程序信息执行等待时间的尝试中，可以使用有密钥的散列或鉴别信息的加密在密文数据上执行鉴别。解密和鉴别可以同时进行，而不是在加密之后进行鉴别。对于简单块链接，这存在着一个问题，就是依赖于地址的解密将不会已在程序信息上执行，有可能使其容易出现解码器无序的情况。

在外部存储设备和安全电路通信期间，可以使用在一个链内的字节的随机顺序置换。这里提供了用于与安全电路进行程序信息通信的装置，例如数据总线或网络。

提供与安全电路相连的装置，以便对该链的重新排序字段进行重新排序，来恢复在第一字段序列中的字段。一个程序信息链可以被重新排序成两个或多个字段，可以提供重新排序。

也就是说，可以在外部存储设备和块缓冲器之间以一种不反映安全电路的块的真实执行顺序的随机的非顺序序列来传送块。而且，重新排序可以在一个或多个块内的字节中进行，也可以在整个链中进行。任何字段都可以重新排序。

这种非顺序传送在阻止侵权者确定在安全电路中执行的程序信息结构、顺序和编排中是非常有效的。通过用一个程序信息序列或多个程序信息序列中的一个链或多个链或整个链的相对位置对任何字段进行重新排序，可以阻止侵权者检测关于在处理电路中的程序信息的执行顺序的信息。应用重新排序，可以阻止侵权者容易地得到程序信息的正确的明文或密文，使得完成某些加密攻击变得更加困难。程序信息最好被加密，以增加分析的困难。

该装置的另一个实施例从存储设备向安全电路传送程序信息块，同时对一个程序信息序列的字段进行大体上随机的重新排序。采用一个新顺序将字段从安全电路传送回存储设备，从而改变了与存储设备中一特定存储单元相联系的字段。在安全电路的内部提供了用于存储在存储设备中的程序信息的新的“真

实”序列。

然后将一程序信息序列的字段的新的基本序列顺序存储在安全设备中，这样在将来向相同块的传送将允许基于安全电路中的新序列进行正确的重新排序。这里提供了用于与安全处理电路进行程序信息通信的装置，例如数据总线或网络。

虽然当字节在存储设备和安全电路之间进行传送时可以使用上面的序列重新排序技术进行重新排序，但程序信息的每个字节仍然是与一特定存储单元相联系的。例如，一个程序信息序列的第一链的第一块的第一字节总是存储在一特定存储单元，即使由于重新排序侵权者可能无法确定事实上它就是第一块的第一字节。则侵权者还是可以以一种系统的和有组织的方式来试探该特定存储单元（例如，地址）中的值。

改变存储设备中的数据的基本存储单元可以防止侵权者试探存储在存储设备的一特定单元中的程序信息。通过在每次使用之后动态地改变存储设备中的程序信息单元，则侵权者对于在存储设备的一特定单元中的程序信息的试探在每次并不是都精确地涉及相同的程序信息。因此这种攻击变得难以控制。

在本发明的另一个方面中，数据子字段、字节、块、链和程序信息序列可以是固定的，不是随机的。对于访问的每个字节、块、链或程序信息序列，顺序可以不同。这是在输入的程序信息上的合适的字段上不同地执行的置换。由于没有随机化，这种置换功能可以容易地在硬件中实现。

在一特定实施例中，安全电路使用程序信息来产生一加密密钥。

使用密码块链接对程序信息进行加密，并可选地进行鉴别和/或重新排序。在另一个实施例中，对程序信息进行鉴别，并可选地使用块链接进行加密和/或重新排序。在另一个实施例中，对程序信息进行鉴别，并可选地使用块链接进行加密和/或重新排序。

在软件中可以使用密钥来对一数据传输进行解密或解扰。通过鉴别指令，阻止侵权者向安全电路提供假程序信息来解扰数据传输。

在本发明的另一个方面中，一安全电路使用程序信息来产生一加密密钥。该密钥可以被用于在硬件中对一数据传输进行解扰。该解扰可以在内部或外部

完成，这取决于安全电路的分布。

可以产生密钥并将其传送给一软件模块，以便对数据传输进行加扰。软件模块可以在安全电路内部，或者在安全电路外部。

在上述的两个例子中，安全电路可以包括一个集成电路（IC），具有一鉴别电路、一中央处理器单元（CPU）以及一个或多个适于存储一个或多个程序信息块的块缓冲器。

外部存储设备可以是闪速存储器、可擦除可编程只读存储器（EPROM）、电可擦除可编程只读存储器（EEPROM）、带有后备电池的随机存取存储器（RAM）、RAM、或者上述的组合。它也可以是硬盘驱动器、CDROM 或者任何类型的大容量存储设备。外部存储设备也存储当被接收到安全电路中时用于鉴别程序信息的鉴别信息（例如，校验位）。在一些实施例中，希望将存储设备的内容复制到一个较快的存储设备中，例如同步动态存储器，以使得安全电路可以从较快的存储设备例如动态存储器中取出程序信息，而不是从具有相关的等待时间的较慢的存储设备中取出程序信息。例如，一网络计算机可以通过网络从服务器复制程序信息。在网络计算机的情况下，较快的存储设备可以是本地的，而较慢的存储器可以是远端的，通过网络进行访问。

为了减少实时执行代码的执行的整个等待时间，第一通信路径可以具有一足够的带宽，以使得两个或多个串、一个或多个块、或者一个或多个链可以基本上同时与块缓冲器进行通信。

因为存在着一个瓶颈问题，程序信息总线一般不比指令带宽宽。CPU 只以一特定速率执行。程序信息必须存储在某些地方。然而，当存在着与其它处理—加密或鉴别—有关的等待时间时，这可以帮助减少整个等待时间。

例如，安全电路本质上可以同时读取不止一个程序信息块，其中使用不止一个块缓冲器来存储另外的块，例如每块一个缓冲器。在安全电路中，鉴别电路从一个或多个块缓冲器接收程序信息和鉴别信息，用于鉴别程序信息。在 IC 中的第二通信路径中，将来自鉴别电路的已鉴别的程序信息提供给 CPU 执行，从而对加扰的数据传输解密。程序信息可以包括多个指令串，例如成行的计算机代码，或者包括相关的数据序列，这些数据序列是要由 CPU 连续地处理的。

可以将一个高速缓存安排在第二通信路径中，以便在将已鉴别的程序信息提供给 CPU 之前临时存储这些信息。高速缓存可以存储至少一个程序信息串，以使得可以将至少两个程序信息串基本上同时提供给 CPU（例如，存储的串和最新的已鉴别和已解码的串）。以这种方式，程序信息与 CPU 有效地进行通信。高速缓存的优点是 CPU 可以从高速缓存中取出已经鉴别的程序信息，而不是使用外部存储设备通信装置，例如总线或网络，在这些装置中牵涉到各种等待时间。

当一第一链和后续的第二链从外部存储设备向一个或多个块存储器传送时，鉴别电路对第一和第二密码块链进行鉴别，以提供相应的已鉴别的程序信息。另外，CPU 可以处理来自第一链的已鉴别的程序信息的至少一个部分，同时鉴别电路鉴别第二链的程序信息的至少一个部分。同样，在需要时对程序信息进行的解码也可以以一种重叠的方式来执行。

该装置的另一个实施例在存储设备和安全电路之间传送程序信息字段，同时传送不是由安全电路处理的立即（例如，当前的或下一个）程序信息序列所使用的字段。这种迷惑技术使用假的数据字节，这些数据字节可以仅仅是干扰字节，例如在任何程序信息执行期间都不会由安全电路使用，或者可以是其他程序信息序列的一部分，仅仅在当前不在安全电路和存储设备之间进行处理。这里提供了与安全电路相联系的装置，用来消除特定块的假字节，以恢复第一字节序列中的字节以及剩下的块中的后续的字节序列。在由安全电路接收之后，在消除之前，在解密和/或鉴别期间可选地使用假字节。另外，提供了可以以相同的方式去除的块和链。

这里所说的密码块链接或简单块链接可以用在用于保密的散列和加密中。例如，程序信息和鉴别信息可以用两个或更多个八字节块来传送。由于其相对于已鉴别的数据来说相对低的鉴别信息的额外量，块链接是有效的。鉴别信息与最后一个明文数据（例如程序信息）块进行 XOR，并可选地被解密，产生一验证值。将该值与由硬件所知的一个值进行比较，以验证鉴别数据是正确的。该值对于不同的链可以是不同的，也可以对于所有链是固定的。

在加密和散列中使用密码块链接是减少与安全功能相联系的硬件量的一种

方式。由于需要的所有块可以以串行方式来处理，所以只需要一个缓冲器。XOR 功能比简单块链接中完成的功能更牢靠，因为在一个块中作出改变是很困难的，可以通过改变另一个块来补偿。由于 XOR 是在解码步骤之前完成的，控制一个块来取消所作出的任何改变则更加困难。但这需要串行处理。

附图简要说明

图 1 是依据本发明的一加密密钥发生器/解扰接收机装置的示意图。

图 2 是依据本发明的密码块链接加密方案的图解表示。

图 3 是依据本发明的密码块链接解密方案的图解表示。

图 4 是依据本发明的简单块链接加密方案的图解表示。

图 5 是依据本发明的简单块链接解密方案的图解表示。

图 6 是依据本发明的另一个加密密钥发生器/解扰接收机装置的示意图。

这里提出了一种用于安全处理器的装置。最佳实施例重点在于安全性。

加密的、鉴别的、以及顺序置换的程序信息块和假数据在一外部存储器和一加密 ASIC 之间以密码块链进行安全地传送。对程序信息的处理允许 ASIC 导出一个用于对收费电视的视频和音频数字包进行解密的密钥。

图 1 是依据本发明的一加密密钥发生器/解扰接收机装置的示意图。在总体上如 100 所示的解扰接收机包括一安全电路，例如，一个诸如 ASIC 的集成电路（IC）105，还包括一存储设备，例如处于 ASIC 105 外部的存储器 110。由于存储器 110 不是封在 ASIC 组件中的，则存储器 110 处于 ASIC 105 外部。例如，存储器 110 和 ASIC105 可以是在解码器母板上的分离组件。

在另一种情况下，可以通过移去或替换存储器 IC 来增加或减少存储器 110，而不会影响或修改安全电路 105。另外，新程序信息例如插入码可以通过电话线、卫星连接或有线电视连接等下载到外部存储器 110。或者，程序信息可以在本地例如通过一智能卡安装在解扰接收机内，或者由插口连接或者焊在同一块板上。或者，存储器 110 本身可以处于一智能卡中，在这种情况下，可以以相对较低的成本提供一个新的智能卡来更新一解码器。这种安排允许存储在外部存储设备 110 中的程序信息（例如，软件或固件）容易地被更新或修改，以提供新特征或修理软件问题，从而提供了相当大的益处。

例如，外部存储设备 110 可以被容易地替换或修改，以便为商业和个人提供定制特征，或者根据诸如人口统计分布、地理位置、时区等因素向团体提供专用特征。

相反，如果存储器 110 为 ROM 并在 ASIC105 内部，则必须替换整个 ASIC，因而会产生相当大的成本和延迟。可以采用使用 RAM 和 ROM 技术的高级 VLSI 工艺来制造 ASIC，以便不仅为在 ASIC 和外部存储器之间的程序信息传送达到高的处理和位传输速率，而且为由高速缓存进行的内部执行以及对视频和音频数字包进行解扰达到高的处理和位传输速率。用 RAM 和 ROM 技术生成的 ASIC 与用其他技术生成的 ASIC 相比可以对更高位速率的成组数据进行解密。因此外部存储器给 ASIC 提供了更大的灵活性。

外部存储设备 110 可以是闪速存储器、可擦除可编程只读存储器（EPROM）、电可擦除可编程只读存储器（EEPROM）或带有后备电池的易失性存储器，例如随机存取存储器（RAM）。或者，也可以使用常规的只读存储器（ROM）。

EPROM 允许在存储器中的编程可以由在强紫外线下暴光来反变换。以一种被称为再烧（re-burning）的工艺可以很容易地将新代码存储在 EPROM 中。可以通过使用大电流对内部存储单元复位来改变 EEPROM。通过使用 EEPROM 或带有后备电池的 RAM，外部存储器还可以用于存储短期或长期数据。存储器空间还可以被划分，以提供不同的物理器件，这样不同的存储类型可以一起使用。在有电源的情况下，非易失性存储器可以被复制到快得多的存储器例如同步动态存储器中。这可以减少外部存储器的读/写操作的等待时间。

外部存储设备 110 可以使用密码块链接来加密，或者使用简单块链接来鉴别并可选地加密。程序信息可以由 ASIC105 用来对加扰数据传输进行解码。程序信息可以包括要由 ASIC105 中的一中央处理单元（CPU）170 执行的代码行（例如串）。每一行代表一可执行的命令或者由程序使用的数据。代码可以遵守一精减指令集计算机（RISC）结构，其中每行代码可以在一单个芯片时钟周期内执行。

使用密码块链接来处理程序信息。块加密方法是三次（triple）DES。有三个密钥可供使用。一个密钥用于高位地址线。另一个密钥用于低位地址线。这

就提供了与地址有关的解密。第三个密钥可以是与单位有关的。

散列算法可以使用双前馈散列（double feed-forward hash）（DFFH），例如，如同在1995年12月22日申请的美国专利申请08/577,922中所描述的。散列是用密钥加密的。该密钥可以是地址和单位密钥的XOR，以便为鉴别提供对地址和单位的依赖性。可以使用不同的散列算法，从而密钥可以是一起附带的，而不是进行了XOR的。

在最佳实施例中，由指令解码器172处理产生的操作代码。非法操作代码可以由指令解码器编码器172中的非法操作代码检测器174来进行标记，并采取适当的行动。例如，CPU170可以向报警电路162发送一信号，该报警电路162又向存储初始化向量、解码密钥和鉴别密钥的存储设备150发送一消灭（擦除）信号。

应用密码块链接，任何对程序信息的试探将使得对每个后续块进行不同的解密。

此外，可以对外部存储设备的地址线进行加扰，以使得程序信息的顺序块是非顺序地存储的。也就是说，例如，每个包括八位的字节可以存储在非顺序的存储器的地址单元中。于是，外部存储设备110被称为是加扰的存储器。这里同样可以使用密钥。密钥对于各个组或单位可以是不同的。

存储设备110还存储用于通过总线115将程序信息安全地传送给ASIC105的块缓冲器130、132和134的鉴别信息。鉴别信息也被称为校验位，被传送到ASIC105的校验位块缓冲器136。

鉴别信息是附加在一个消息例如程序信息链后面的数据，用以允许接收机验证该消息应该作为可靠信息被接受。鉴别信息是消息（例如，链）内容的一个函数，例如何时使用一散列值或加密校验和（checksum）。散列值是通过用一公用函数映射一任意长度的数据链而获得的固定长度值。在最佳实施例中，散列法用密钥加密，鉴别信息在一个不同的密钥下被加密。

外部存储设备110的程序信息通过总线115传送给一个或N个块缓冲器，例如包括块缓冲器130、132和134。虽然显示了多个块缓冲器，但最小只需要一个。

提供了加密/解密电路 120 来对这些块进行加密或解密。例如，当由块缓冲器或其他源接收明文数据、并且需要对明文数据进行加密时，电路 120 还可以提供编码。编码的数据接着可以通过缓冲器被发送到外部存储设备。

鉴别电路 125 使用例如上述的 DFFH 功能对程序信息的明文块进行散列。随着这些块被解密，可以以一种同时串行的方式来执行鉴别。当块 1 被解密时，可以将其散列。当块 2 被解密时，可以用第一块的散列输出对其进行散列，以此类推。数据的散列用密钥加密，以便只有知道了一保密或专用密钥才能产生正确的散列。或者，如上所述，对与鉴别过的数据（例如程序信息）进行了 XOR 的鉴别信息（例如校验位）进行解密，产生可以由硬件验证的一已知值。鉴别电路 125 和加密/解密电路 120 可以相互通信，并且可以共享相同的电路。

密码块链接可以用在从外部存储设备向安全电路 105 传送的块链上。在 1995 年 IEEE 出版的美国新泽西 Englewood Cliffs 的 W. Stallings 的网络和因特网的安全性第 59-61 页中对密码块链接进行了讨论，该文章在此作为参考。密码块链接可以用在加密和散列中，但在最佳实施例中，它只用在牢靠的加密上。采用了一种单独的散列函数。与密码块链接一起使用的块加密算法是三次 DES。

链长度可以在 16 和 32 个块之间变化。链长度根据密钥和地址参数在每个链的基础上变化。

在存储器和 ASIC 之间传送的块的序列顺序是随机的。与地址发生器相联系的随机数发生器访问存储器中各个块的正确的存储单元。

鉴别信息作为传送的 16 到 32 个块中的一个被发送。它可以以任何顺序传送。在解密后，将其与散列值进行比较。

例如，在密码块链接中可以使用 N=16 个块，每个块具有八字节数据。应用密码块链接，每个加密的数据块依赖于当前块的明文数据和所有以前块的明文数据。由于相同的明文输入将产生依赖于其他明文块的不同的加密数据，所以块链接提高了安全性。另外，处于鉴别信息中的额外数据也显著地减少了。如果将 16 个块中的一个指定为鉴别信息，则这表示只有程序信息的 1/16=.0625 或 6.25%。如果 N=32，则数值为 1/32=.03125 或 3.13%。在最佳实施例中，

链大小可以在16和32之间变化，所以平均下来该数值将为1/24=.0417或4.17%。也就是说，只有程序信息的4.17%是鉴别信息。

如果举例来说提供了两个鉴别信息块而不是一个鉴别信息块，这将发生变化。还存在着许多可能性。但动态地链接降低了只由鉴别所需的存储容量。

由于从存储设备存取的鉴别信息量减少了，链接还允许使用更小的存储部件，这就极大地减小了系统的成本，并且/或者提高了系统的通过量。下面还将结合图2和3讨论密码块链接。

密码块链接的一个潜在缺陷是当一个在原定时间之前还没有被解密和鉴别并且可能保存在高速缓存中的新代码段需要被访问时指令执行的等待时间。由于只有在先前的块已经被解密时才能开始对一个块进行解密，所以这些块必须顺序地被解密。

可以使用更复杂的散列函数，例如消息摘要（MD）5、安全散列算法（SHA）、甚至密码块链接。由于DFFH是基于DES的，所以选择了DFFH。可以使用相同的硬件来完成解密和鉴别。可以控制DES机的输入，以最大限度地利用硬件。虽然希望是单向函数，但这并不是必须遵循的，因为如果鉴别算法使用了一保密密钥，则由于任何了解保密密钥的人都可以计算出正确的鉴别信息与提供的任何鉴别信息一致，一单向函数并不比一可逆算法例如密码块链接好多少。使用公用密钥加密的鉴别比较好，因为了解安全电路的专用解密密钥并不会使侵权者得知如何对第一位置的散列进行加密。公用加密密钥必须是已知的。

对于任一种方案，总线115的大小可以为具有允许至少两列指令或成组的程序信息立即被传送的带宽。或者，总线115的大小可以为能够传送链的一整个块（例如，八个字节）、甚至两个或更多个整块。总线115的大小还可以为能够立即传送一个或多个整个链。

一序列块或者是已鉴别的并且可选地加密的指令，例如块B_1、B_2、…、B_{N-1}，或者是加密的并且可选地已鉴别的密码块。加密块与密码块链接一起使用，但对于简单块链接是可选的。鉴别信息被包括在程序信息传输的一个校验位块、例如块B_N中。

下面可以看到，在用密码块链接或简单块链接节省了额外数据的同时，还

获得了所需的安全级。解开鉴别的试探的平均数是 2^{n-1}，其中鉴别长度为 n 位。为了提供足够的安全级，鉴别应该在某些程度上反映出用于对指令加密的密钥或多个密钥的长度。否则，侵权者将攻击系统最薄弱的部分，这有可能是鉴别信息本身。也就是说，侵权者不去试探密钥以发现程序信息是在哪个密钥下被加密的，而是可以试探鉴别信息，并使 CPU 处理合成的程序信息。如果加密为 DES 使用了一个至少七个字节的密钥，则最好应该为鉴别信息使用七个或八个字节。例如，对于长度为七字节（例如，长度为 n=56 位）的鉴别信息，平均需要 2^{55} 次试探，这与解开 DES 密钥的困难程度是相似的。

当一个八字节鉴别信息块附加在一个八字节消息块后时，鉴别信息的额外量是 50%（例如，8/（8+8））。然而，当依据本发明使用块链接时，例如，一个七字节块附加在一个包括 16 到 32 个八字节块的链上，如上所述，额外量只有大约 4.17%，安全性更牢靠了。因此，块链接提供了鉴别信息额外量的显著减少，同时保持了所需的安全级。

在本发明的另一个方面，提供了对于从外部存储设备向 ASIC105 传送的链的重新排序。下面将讨论，在将块加扰存储在存储设备之外还采用了这种重新排序，但也可以单独使用重新排序。通过将链中的多个块随机地重新排序，可以阻止侵权者检测关于处理电路中的程序信息执行顺序的信息。与字节和链的重新排序一样，可以随机地完成块重新排序，这样对相同代码的重复执行在每次将以不同的顺序从外部存储器取出数据。例如，对于字节的重新排序，如果每块有八个字节，则有 8！=40,320 种不同的顺序对这些字节排序。同样，对于块的重新排序，如果每个链有十六个块，则有 16！$=2.09\times10^{13}$ 种不同的顺序对这些块排序。对于链的重新排序，如果每个程序信息序列有 4 个链，则有 4！=24 种不同的顺序对这些链排序。并且，可以一起使用这三种重新排序。则可能的置换总数将为 $40,320\times2.09\times10^{13}\times24=2.02\times10^{19}$。

应该注意的是，任何字段都可以是重新排序的基础，字节、块和链都是位的任意单位。重新排序的字段可以是四位字节。而且，字节并不一定是八位，块也并不一定是八字节，等等。

了解了这一点，重新排序操作可以允许在两个或多个块中进行字节重新排

序、在两个或多个链中进行块重新排序、以及在两个或多个程序信息序列中进行链重新排序。这样我们就得到了一个不同的结果。例如，对于字节重新排序，如果每块八字节，在两块上进行字节重新排序，则有 16！=2.09×10^{13}种不同的顺序对这些字节排序。

如果密码块链接与重新排序一起使用，其中需要对块的串行处理，则在解码之前需要多个块缓冲器来存储所有相关字段。而且，如同下面结合图 6 进一步要讨论的，如果在两个或更多链中进行重新排序，则需要够两个或多个链使用的块缓冲器。程序信息序列中的重新排序则需要更多的块缓冲器。解码可以一直被延迟到与最后的块序列相联系的字段被读出的时候，因为当内部进行了重新排序时，读出的最后一块可能是该链序列的第一块。

使用密码块链接加强了安全性。然而，如同与在图 3 中的 XOR 散列函数一起描述的，简单块链接避免了等待时间问题，并且可以与链、块、字节或任何字段重新排序一起使用。不考虑链、块、字节或字段的排序，在一个块中的所有字节都可以用于执行鉴别。另外，当需要解密时，每个块独立地进行解密。

提供给外部存储设备的地址数据可以随机地选择字段、字节、块或链向 ASIC105 传送。可以提供一个块重新排序电路多路转换器 112，与总线 115 进行通信，根据需要为加密/解密电路 120 和鉴别电路 125 对重新排序进行逆变换，以执行其功能。块重新排序电路多路转换器 112、地址发生器 160 和地址加扰器 164 可以相互通信，并且可以根据需要与 CPU170 进行通信，以协调重新排序步骤。地址发生器 160 可以响应于一随机数发生器 166。随机数发生器 166 可以为不需要遵守硬件中包含的任何算法的一个或多个链的字段提供随机或伪随机序列置换。

链、块、字节和字段序列加扰一般可以用于实际上的任何将数据块从一存储器向安全电路传送用于处理的方案。如上所述，由于在鉴别和解密可以开始之前所有字节必须被汇集，对每个块内的字节或子字段的顺序进行加扰不会影响解密等待时间。但重新排序使侵权者不清楚哪个密文相应于哪个指令和其他数据块。它还使侵权者不清楚存储设备中的程序信息的结构、顺序和组织。

在最佳实施例中，由安全电路 105 读入一整个八字节块，第一字节相对于其

他字节读出的顺序将一块一块地变化，并且在每次存储设备被访问时可以随机地变化。但当在安全电路中重新排列时，对于一个必须进行解密的块只有一种正确的顺序。对于密码块链接，其具有的优点是只需要一个块缓冲器，因为是一单个块的字节被重新排序了，但这将迷惑缩短到一更小的时间周期内。在将单个字节装入块缓冲器之前，可以对外部存储设备进行重新安排或分类。

在本发明的另一个方面，可以将一个链中的各块以一种新的模式写回进存储设备。在对存储设备的每次随机读取之后，以一种不同的随机序列写回数据。与每个链相联系的是一个存储链的当前基本顺序序列的存储设备。重新排序可以是随机的。

还可以在存储设备 110 和安全电路 105 之间传送假数据。假数据可以是由存储设备 110 存储的干扰（chaff）。这是永远不会由安全电路处理的数据，但它可以可选地用作填充数据，并且由安全电路解密并可选地鉴别。产生干扰是很容易的。在该干扰之前只执行一转移或跳转操作。如果对于干扰所处的位置没有进行过调用、转移或跳转，则该干扰将永远不会被执行。假数据可以是其它链和指令序列的真解密数据，这些链和指令序列可以在以后的时间被存取，并且可以处于不同的状况。与干扰相同，该数据可以可选地用作填充数据，并且被解密并用其它程序信息可选地鉴别。但安全电路并不对该数据进行处理。冗余数据扰乱了侵权者分析鉴别过的程序信息的企图。

传送假数据的最好方式之一是通过可变长度链。所传送块的实际数目可以保持相同，而假块数目可以改变。由于块的重新排序，侵权者很难确定哪些块可能是假块。最佳实施例中的假块实际上是永远不会被处理的数据。

可以对外部存储设备 110 进行加密，以使得程序信息块和鉴别信息被存储在存储设备的非顺序地址单元中。在存储设备的加密中最好包括高位地址位，以使得任何程序信息块都可以处于存储空间中的任何位置。可以使用替换表（S 表）来消除规律性并增加地址加密中的非线性。

特别地，对在外部存储设备链接的已鉴别块进行加密，以便可以对一直在观察存储设备在通信路径 113 上的存取的侵权者隐藏加密代码的执行。可以防止侵权者了解正被执行的专有算法。因此加密可以阻止侵权者确定存储设备的

内容和通过其它硬件装置有计划地攻击安全电路 105。存储设备的加密阻止侵权者确切地了解哪一个被加密的程序信息可能是攻击目标。通过确切地了解哪一个程序信息会使得系统的安全性易受破坏，侵权者将集中于扰乱该程序信息的处理。

如果单独使用地址加扰和数据加密和鉴别，例如，不进行数据重新排序，则在最小实施方案中只需要一个块缓冲器。

伴随着加扰可以使用一与安全电路 105 相联系的地址发生器，以便向外部存储设备提供寻址信息。可以提供一个数、例如随机数来改变程序信息传送的序列。将该序列信息用来多路传输适当的字段、字节或块缓冲器，以便在正确的时间与适当的字节或块进行通信。然后根据寻址信息以所希望的顺序将数据子字段、字节或块的单个串从外部存储设备传送到块缓冲器。将寻址信息提供给鉴别和解码电路，以允许这些电路对数据进行解扰以完成相应的功能。

可以使用各种块加密算法，例如三次 DES。而且，加扰算法可以使用相同的替换框（S 框）表作为 DES，但可以只有较少的循环（round）。对于不同的应用程序可以选择循环数，例如一个需要较低安全性的应用程序使用较少的循环，而一个需要更高安全性的应用程序则使用 DES 调出的整个十六个循环。减少循环数会减少解码操作的等待时间。

程序信息的与地址有关的解密和鉴别可以阻止侵权者在存储设备中将正确地加密和鉴别的块链到处移动从而使得解码器无序地处理程序信息。这种无序处理会使得解扰接收机对一数据传输进行不正确地访问和解扰。

如果可能的话，用于加密和解密和/或鉴别的密钥应该既有与地址有关的加扰，又有单元密钥的依赖性。单元密钥是对于每个解码器唯一的密钥，可以依赖于例如在制造时提供的解码器编号。于是，希望密钥与单个单元或单个单元组有关。否则，侵权者有可能从一个单元读出外部存储设备中的加扰密钥，然后将相同的加扰密钥放进另一个单元的外部存储设备中。这可能会成为侵权者在单元之间复制对服务的授权的一种方式，必须被阻止。

与地址有关的加扰和单元密钥的相关性还防止将对在一个解码器中用于鉴别和/或加扰一程序信息块的密钥的知识用在另一个解码器中。例如，在没有单

元相关性的情况下，如果该保密密钥通过 VLSI 试探被发现了，则可将其用于为其他解码器对程序信息进行正确地鉴别和解密。换句话说，如果一个或多个密钥对不止一个单元是有用的，则侵权者可以使用从一个单元获得的该密钥或这些密钥来为另一个单元对程序信息进行加密、加密和鉴别或鉴别。为了获得与单元有关的加扰，可以在单元形成时使用一个应用一可选的芯片上的编码电路的下载处理来加载外部闪速、EPROM、带有后备电池的 RAM 或大容量存储设备。这种编码电路可以与用于在安全电路和存储设备之间提供双向读/写能力的电路是同一个电路。或者，由构造系统在单元形成时应用单元的保密或专用密钥或多个密钥知识对这些外部存储设备进行加载。

图 2 是依据本发明的密码块链接加密方案的图解表示。将明文程序信息块变换为一个包含加密的程序信息块的链，其中程序信息包括鉴别信息。在显示的例子中，每个加密的程序信息块依赖于当前块的明文程序信息和前一块的明文程序信息。

图中显示了一鉴别电路 203 和一加密电路 200。特别地，鉴别电路 203 包括散列函数 204、206 和 208 和一个加法器 214。函数 204、206 和 208 可以使用上面讨论的 DFFH 函数或实际上的任何散列函数。在函数 204、206 和 208 对一密钥进行连续地散列，以便向加法器 214 提供一散列值。加法器 214 还接收一个由硬件已知的零或其他值，以便向加密电路 200 提供一输出值，加密电路 200 可以包括一个由加密函数 218、222 和 224 表示的三次 DES 加密函数。

加密函数 218 接收一个为低位地址位和一密钥 D_{K6} 的 XOR 的保密密钥，而加密函数 222 接收一个为高位地址位和一密钥 D_{K5} 的 XOR 的保密密钥，加密函数 224 接收一个为一单元密钥和一密钥 D_{K6} 的 XOR 的保密密钥。一加法器 226 接收来自加密函数 224 的输出和明文块 A_{N-1}，并提供密文鉴别块 B_N。加法器 226 实质上对明文数据进行了散列。

由相应的三密钥加密函数接收包括用于对数据传输进行解扰的程序信息的明文块 A_1，…，A_{N-1}，并用于后续的密文块的 XOR。例如，由加密函数 228、232 和 234 处理 A_1，其中每个函数响应于如图所示的密钥。一加法器 236 接收加密函数 234 的输出和一初始化向量（IV），以提供密文块 B_1。

由加密函数 242、244 和 246 处理 A_2，其中每个函数响应于如图所示的密钥。一加法器 248 接收加密函数 246 的输出和明文块 A_1，以提供密文块 B_2。因此，B_2 是 A_1 和 A_2 的函数。同样，由加密函数 252、254 和 256 处理 A_{N-1}，其中每个函数响应于如图所示的密钥。一加法器 258 接收加密函数 256 的输出和明文块 A_{N-2}，以提供密文块 B_{N-1}。

IV 可以为零，或者为提供给块重新排序电路 112 或其它随机化函数的地址数据或单元密钥的函数。对于该实例假设块大小为八个字节。而且，虽然显示的三次 DES 对于每个 DES 操作使用三个不同的密钥，也可以使用更少或更多的密钥。通过在循环中使用不同的密钥而不是一单个密钥，可以将更多的密钥引入 DES 操作中。

可以将更多密钥用在加密函数中，并且可以采用附加的和/或替代的加密步骤。每个密文块加密函数最好使用相同的加密算法，虽然这并不是必须的。

可以将 N 个加密块 B_1 到 B_N 提供给另一个加密函数，例如图 1 中的块重新排序电路多路转换器 112，根据一地址数据信号执行对 N 个块的块加扰。例如，对于 N=8 块，这些块可以以下列顺序存储在外部存储设备 110 的顺序地址中：B_1，B_3，B_2，B_5，B_4，B_6，B_8，B_7。这些块被称作以一种随机或非顺序的方式存储，因为它们不是存储在存储设备的连续地址中的。

应用上述的临时重新排序方案，可以接着以另一种序列将这些块传送到块缓冲器中，例如，B_5，B_3，B_2，B_6，B_4，B_7，B_8，B_1，这与将块提供给重新排序电路 112 的顺序和存储序列都不一样。

鉴别和加密函数和相关的元件不必与外部存储设备 110 安排在一起。也就是说，加密电路 200 可以位于一有线电视系统始端或一卫星上行链路，而存储设备是在消费者家中的一解扰接收机的一部分。已鉴别和/或已加密的程序信息可以通过任何方便的信道提供给存储器 110，例如，通过电话、卫星、有线电视链路或计算机网络。已鉴别和/或已加密的程序信息也可以通过一智能卡进行本地安装，或者可以在解扰接收机的安装和初始化之前以加密的程序信息对存储设备 110 本身进行预加载。

再参考图 1 中的解扰接收机 100，由地址加扰器 164 使用的地址数据可以被

存储在 ASIC105 的一地址发生器 160 内。将地址数据通过路径 165 提供给外部存储器 110，以便可以以所希望的序列（例如，B_1，B_2，…，B_N）读出加密指令的加扰块。特别地，可以将组成一个链的块从存储器 110 中非顺序地读出来，以便通过线 113 以未加扰的顺序提供这些块。可选地，可以将这些块以加扰的或随机时间序列从外部存储设备 110 向安全电路 105 发送，并且在 ASIC105 应用块重新排序电路多路转换器 112 解扰。地址数据还可以由外部存储设备 110 用来以一种加扰（例如，非顺序的顺序）方式来发送不同的块链。

将地址数据和连续的密码块链的加密块 B_1 到 B_N 提供给 ASIC105 的加密/解密电路 120 和鉴别电路 125。加密/解密电路 120 根据需要使用地址数据对密码块链序列进行解扰。在块重新排序电路多路转换器 112 还会进行重新排序。加密/解密电路 120 还从 ASIC105 的解密密钥存储器 150 接收保密解密密钥，并执行一解密算法，该算法是用于提供加密块的算法的逆算法。下面将结合图 3 讨论该解密处理。

应用块链接方案，每个链的块 B_1 到 B_N 必须连续地被解密。也就是说，B_1 第一个被解密，然后将结果用于对 B_2 解密，以此类推。一旦 B_1 到 B_{N-1} 已经被解密，则可以对鉴别块 B_N 进行解密，并且可以由鉴别电路 125 计算鉴别信息（例如，校验和或散列），以鉴别该链。正确的鉴别信息可以被预先存储在鉴别电路 125 中，并与计算出的鉴别信息进行比较，以提供所必需的验证。最后，得到成行的明文（例如，解密的）程序信息并提供给高速缓存 140。

为了实现外部存储设备 110 和安全电路 105 之间的安全通信，从安全电路向存储设备输出的程序信息还必须被鉴别和/或加密。于是，为了改变外部存储设备 110 中的字节或数据串，整个块和块链必须被读进 ASIC，作出改变，然后才可以计算出正确的鉴别信息。在计算出鉴别信息之后，例如使用简单块链接写出新加密的块信息和改变的鉴别信息。可以以一个与取出时不同的基本序列将程序信息写回到存储设备。

未修改的块不需要被写出，除非在存储器中的单元已经改变。对于密码块链接，改变一个数据块可以改变一个链中的后续数据块。这些受影响的块同样需要被写出来。

这里有一些安全电路需要同外界以明文模式进行通信的例子，例如打印机、错误消息、显示目的等等。因此，加密/解密电路 120 和/或验证/鉴别电路 125 应该有一种禁止模式，从而程序信息可以被传送或有条件地绕过。在这样一种模式中，由于不需要加密或鉴别，则程序信息不必以一个块或链的形式被传送。这种模式还可以用于系统调试和测试。

从存储设备传送不同类型的程序信息可以使用不同的链长度。需要较少等待时间的程序时间可以具有较短的链长度。可以容忍较长等待时间的程序信息可以具有较长的链长度，从而节省相应的鉴别信息的存储量。因此，可以根据各个链的程序信息的处理等待时间来设置每个链的长度。

例如，在一个链中可以只有两个程序信息块，一个是数据块，一个是鉴别信息块。虽然即使只改变一单个字节也必须首先取出并解密整个程序信息链，数据中的改变不必立即写出外部存储设备。数据可以存储在内部，例如存储在高速缓存 140 中，直到外部存储设备需要被更新。此时，ASIC 必须将带有修改的整个链写回到外部存储设备。

再回到加密/解密电路 120，将解密的程序信息提供给一高速缓存 140 临时存储，并提供给一 CPU170 执行。可以采用附加的处理硬件或软件和步骤应用程序信息对一加扰数据传输进行解码，这些在图中未显示，但是是本领域中所公知的。

高速缓存 140 是一个具有相对高速存取并提供缓冲能力的 RAM，大小可为能存储相当大的数据量。高速缓存 140 可以存储成千上万个字节，这相应于许多块链的指令和操作数据的大小。CPU 可以执行来自第一密码块链的程序信息，同时加密/解密电路 120 对来自后续的第二密码块链的块进行解密。第二链可以直接跟着第一链，或者由一个或多个中间链将其与第一链分开。因此，由于鉴别电路、解码电路和 CPU 的交错工作，可以提高系统的通过量。一般地，虽然在 CPU 中程序信息的执行时间一般比加密/解密电路 120 中的解密时间要快，通过协调解码和执行行为，并且使加密/解密算法中使用的循环数最优化，可以达到高效率。

通过写由 CPU 执行的程序信息例如指令以便与块链传送方案一致，可以实

现更高的效率。特别地，成行指令中的程序信息量可以与链中的块大小和块数量相一致。例如，成行指令应该在一个块链中整个地传送，而不是将其分成两个链，以避免要等到第二块链被解码才能恢复一行的剩下部分。一个指令一般只有几个字节长（例如，1-4 个字节），所以一个块链一般包括几个指令。

高速缓存 140 可以可选地接收一个来自地址发生器 160 的信号，以协调程序信息向 CPU170 的存储和传送。例如，该信号可以通知高速缓存 140 另外的块链正被传送到缓冲器、鉴别电路 125 和加密/解密电路 120，以使得另外的可执行程序信息将由高速缓存 140 接收。

可以提供一个或多个与高速缓存 140 和 CPU170 相连的寄存器 180。而且，可以使用一个小的内部 ROM 来存储在 ASIC105 中需要的引导或其它程序信息。

图 3 是依据本发明的一个密码块链接解密方案的图解表示。所显示的方案是图 2 中的加密方案的对应方案。当需要获得所需序列的字段用于解密时执行重新排序。提供了一鉴别电路 303 和解密电路 300。在解密电路，对每个密文块 B_1，…，B_N进行解密。

首先，各个密文块与先前的明文块或一初始化向量进行 XOR。特别地，B_1和在加密期间使用的 IV 在一加法器 320 接收，以便向一三次 DES 函数提供一输出，该三次 DES 函数包括解密函数 322、324 和 326。从解密函数 326 输出明文块 A_1，并将其提供给一加法器 330 和一散列函数 304。在散列函数 304，A_1和一密钥被散列，以便向连续的散列函数 306 和 308 和一加法器 310 提供一输出。

加法器 330 接收 A_1和 B_2，以便向解密函数 332、334 和 336 提供输出，以提供明文块 A_2。同样，一加法器 340 接收 A_{N-2}和 B_{N-1}，以便向解密函数 342、344 和 346 提供输出，以提供明文块 A_{N-1}。一加法器 350 接收鉴别块 B_N和 A_{N-1}，以向解密函数 352、354 和 356 提供一个值。将解密函数 356 的输出与来自散列函数 308 的一散列值一起提供给一加法器 310，以产生一个为 1 或 0 的输出。如果输出为 0，则鉴别值是有效的，因为它与散列值相匹配，并且设置一允许信号以使处理继续进行。然而，如果加法器 310 的输出为 1，则鉴别值无效，并且可以在报警电路 162 初始化一报警状态，以提供一消灭（擦除）信号来部分或全部地擦除密钥存储设备 150 的内容。

当使用块重新排序时，试图试探程序信息和鉴别信息值的侵权者很可能会生成无效的操作代码。无效的操作代码是没有相应的操作的虚（hex）数据指令。存在着各种选项，用于处理未检查出的鉴别值或操作代码。一种可能性是执行安全电路的复位，这需要侵权者为另一次攻击重新构造和重新初始化ASIC。

另一种可能性是使ASIC中的处理器跳转到一个无限的“空操作”（NOP）循环。这是ASIC不执行任何实质操作的状态，需要侵权者首先检测NOP操作，然后它自己强制复位，并为另一次攻击重新构造和重新初始化ASIC。或者，可以对在预先存储值和解密值之间的不匹配进行计数，以便当检测到的不匹配数达到一阈值时擦除一个或所有存储的密钥。这些密钥可以是敏感密钥，从而外界的了解将对安全性产生主要的破坏。对它们的擦除将会使一个原本为好的单元出现永久性的故障。

另一种可能的对抗措施是擦除一个临时密钥，例如一个传送的密钥，而不是一个在单元初始化或制造时加载的密钥。这强迫侵权者与网络服务提供者联系以便重新授权，从而潜在地暴露出侵权者。在侧重于安全性的最佳实施例中，所有密钥都被擦除。

图4是依据本发明的一个简单块链接加密方案的图解表示。如上所述，这种结构可以避免图2和3中的密码块链接技术所具有的等待时间问题。对所有明文块的加密可以独立地并且大致并行地进行。鉴别信息的加密和解密依赖于明文块。但由于对一个块的修改不会影响除了鉴别信息的其它块，简单块加密技术对于侵权者的一些试探攻击具有更大的敏感性。

这里提供了鉴别电路403和加密电路400。对明文程序信息块A_1，A_2，…，A_N进行处理，以分别提供相应的密文块B_1，B_2，…，B_N。密文块中的一块，一般表示为B_i，是一个鉴别块，并且可以处于其它密文块中的任何位置（例如，$1 \leqslant i \leqslant N$）。

在加密电路400，块A_1在函数402被加密，以提供块B_1，块A_2在函数404被加密，以提供块B_2，块A_{N-1}在函数408被加密，以提供块B_{N-1}，以及块A_N在函数410被加密，以提供块B_N。另外，将每个明文块提供给鉴别电路403中的一加法器412，以便向一加密函数406提供一个值，产生一密文鉴别块B_i。B_i可以

是第一个块 B_1、最后一块 B_N、或者二者之间的任何块。加法器 412 还接收一个硬件已知的零或其它值。

每个用于非鉴别块的加密函数，例如函数 402、404、408 和 410 可以在相同的密钥 K_1 下操作，该密钥 K_1 是由一单元密钥、高位地址位、一保密密钥 D_{K1} 和低位地址位的 XOR 得到的。用于鉴别块的加密函数、例如函数 406 可以在一个不同的密钥 K_2 下操作，该密钥 K_2 是应用一保密密钥 D_{K2} 得到的。如前所述，可以将加密的块提供给块重新排序电路。

依据本发明，通过提供一个对明文块 A_1，A_2，…，A_N 和一个预先存储的值进行 XOR 的加法器 412，从明文块导出鉴别信息。接着在函数 406 对加法器 412 的输出进行加密，以提供加密的鉴别块 B_i。事实上，在加法器 412 之外，还可以使用任何散列函数，或者用来代替加法器 412。而且，不必将每个明文块都输入进加法器 412。

图 5 是依据本发明的一简单块链接解密方案的图解表示。解密器是图 4 中的加密器的对应装置。当需要获得所需序列的块用于解密时执行重新排序。

这里提供了解密电路 500 和鉴别电路 503。解密函数 502、504、508 和 510 使用如图所示的密钥 K_1，用来分别对密文块 B_1，B_2，B_{N-1} 和 B_N 进行解密，以提供明文块 A_1，A_2，A_{N-1} 和 A_N。在函数 506 使用一个不同的密钥对密文鉴别块 B_i 进行解密。将每个解密函数的输出提供给一加法器 512，以提供一散列值，该散列值随后在加法器 514 与一个预先存储的硬件值进行求和。

如果加法器 514 的输出为 0，则散列值和硬件值相同，鉴别数据被证实，从而允许后续的处理。但如果加法器 514 的输出为 1，则散列值和硬件值不同，鉴别数据未被证实，于是设置一报警状态。

图 6 是依据本发明的另一个加密密钥发生器/解扰接收机装置的示意图。相似标号的部件与图 1 中的部件相对应。接收机一般地显示为 600，包括分别用于第一链的第一、第二和第 N 块的链块缓冲器 130、132 和 134，和分别用于第二链的第一、第二和第 M 块的块缓冲器 630、632 和 634。采用这个方案，两个或多个块（每个链中一个块）可以同时在线 113 上进行传送。此外，可以提供另外的块缓冲器来存储来自多于两个链的数据。每个链可以具有相同的或不同

的长度。

加密/解密电路 120 和鉴别电路 125 处理链 1，同时加密/解密电路 620 和鉴别电路 625 处理链 2。可以根据需要为每个链将来自密钥存储设备 150 的数据提供给电路 120、125、620 和 625。此外，虽然显示的是分离部件，鉴别电路 125 和加密/解密电路 120 可以与鉴别电路 625 和加密/解密电路 620 共享共同的电路。

图 6 的实施例在使用密码块链接时可以在两个或更多链中进行重新排序。如上所述，当使用密码块链接时，一个链中的每个块必须被临时存储以恢复鉴别块。因此接收机 600 可以提供两个或更多密码块链的并行处理、在两个或更多链中的链与链的重新排序或者块与块的重新排序。

因此，可以看到，本发明提供了一种通过以一简单块链从外部存储设备向一安全电路传送已鉴别并可选地加密的程序信息、对加扰数据传输进行解扰的装置。还以密码块链从外部存储设备向安全电路传送加密并可选地鉴别的程序信息。该方案允许容易地对解扰指令作出修改或其它改变而不必修改安全电路。

另外，使用块链接提高了系统通过量，并通过减少额外鉴别信息量而减少了系统成本。通过提供一个高速缓存来在一个时钟周期内向 CPU 传送两行或更多行已解密或已鉴别的程序信息，并且通过控制解密数据向高速缓存和 CPU 传送的块解码的计时，可以获得更高的效率。

本发明的另一个实施例使用简单块加密来代替密码块链接。采用这个方案，与密码块链接一样，使用一个大的鉴别字段对链中的块进行鉴别。但可以大致并行地而不是串行地对块链进行解密和鉴别。

除了对外部存储设备的存储进行地址加扰之外，还提供了使用任何字段例如字节、块和/或链对块链进行的重新排列。

另外，可以提供一种双向能力，允许程序信息从安全电路向外部存储设备传送。程序信息不必被加密，而为了安全只进行鉴别。

虽然已经结合各种特定实施例对本发明进行了说明，本领域普通技术人员将会理解，在不偏离由权利要求陈述的本发明的精神和范围的情况下，可以作

出许多修改和改变。

例如，本发明特别适用于阻止专有软件算法的复制和逆向工程，并且用于对加密的应用程序进行保密，例如诸如收费电视节目的数据传输的解扰，以防止未授权的用户接收电视广播。本发明同样还可用于其它应用程序，包括用于电子存款交易、房屋访问控制、电子游戏、由交易者使用的商品和股票数据、通过因特网或其它计算机网络传送的数据的终端和智能卡。

此外，本发明可与其它加密方案兼容，例如流密码，或者流密码和密码块链接的组合，例如共同加扰算法（CSA）。

另一个这样的方案是公用密钥加密。因为每个块和链与大小可以为 2048 位（256 个八位字节）的所谓的 RSA 公用密钥系统的组件尺寸相比相对较小，所以可以使用 RSA 对一个或多个程序信息链进行加密。如果使用了 RSA 公用密钥系统，则最好使用一个不平衡的指数对，从而解密专用指数较小，例如等于三。这将降低程序信息等待时间。在解密之后，如同如上所述的在块加密技术中一样，可以对鉴别信息进行校验，进行解密和校验，或者只进行校验。这使得设置解密的鉴别值变得很困难。并且，如上所述，可以使用保密密钥和公用密钥的组合。

说 明 书 附 图

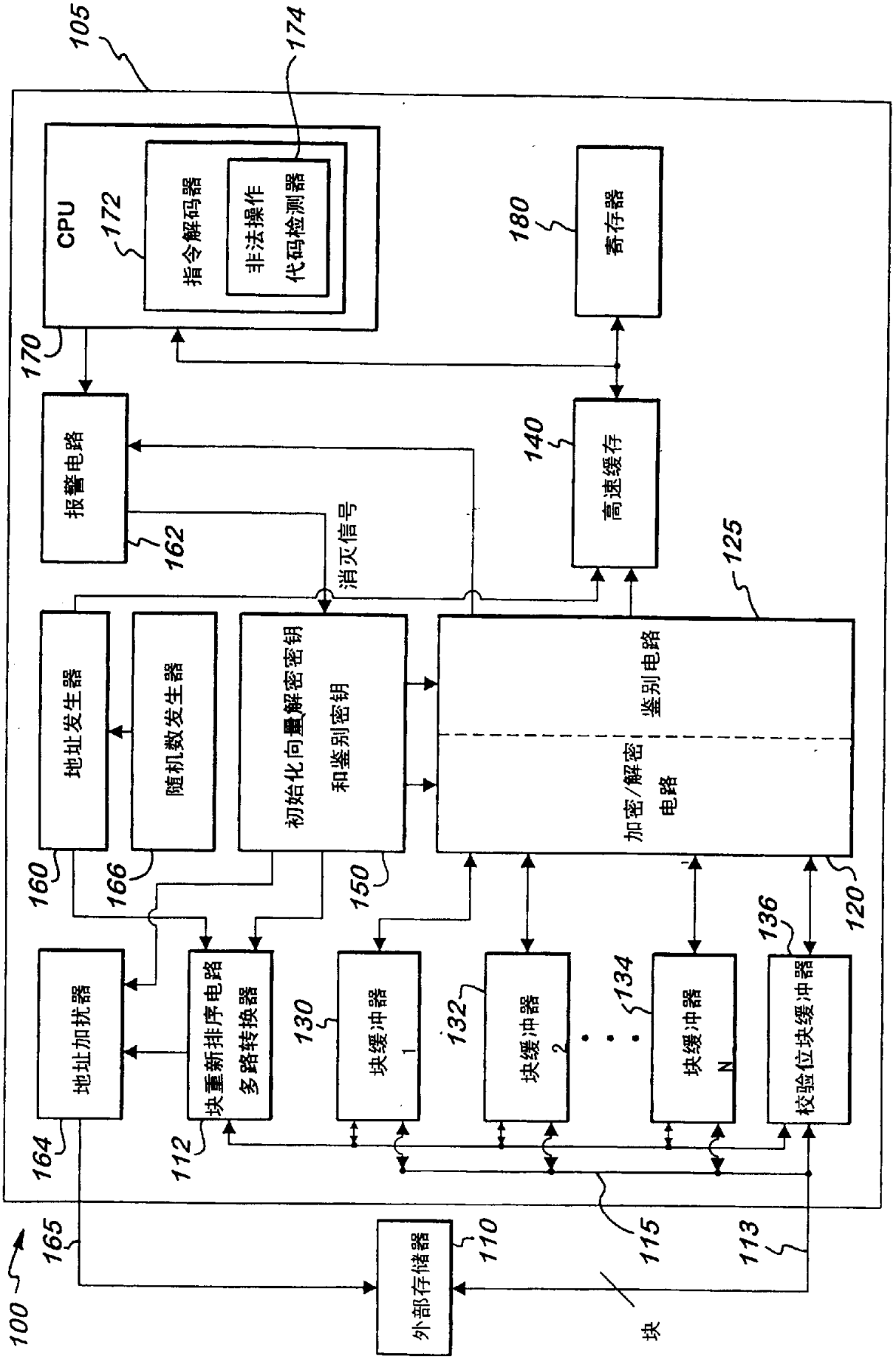

105
174
CPU
172
指令解码器
非法操作
代码检测器
180
寄存器
170
报警电路
162
消灭信号
140
高速缓存
125
地址发生器
随机数发生器
初始化向量解密密钥
和鉴别密钥
鉴别电路
加密/解密
电路
160
166
150
120
136
地址加扰器
块重新排序电路
多路转换器
130
块缓冲器
1
132
块缓冲器
2
134
块缓冲器
N
校验位块缓冲器
164
112
165
110
115
113
100
外部存储器
块

图1

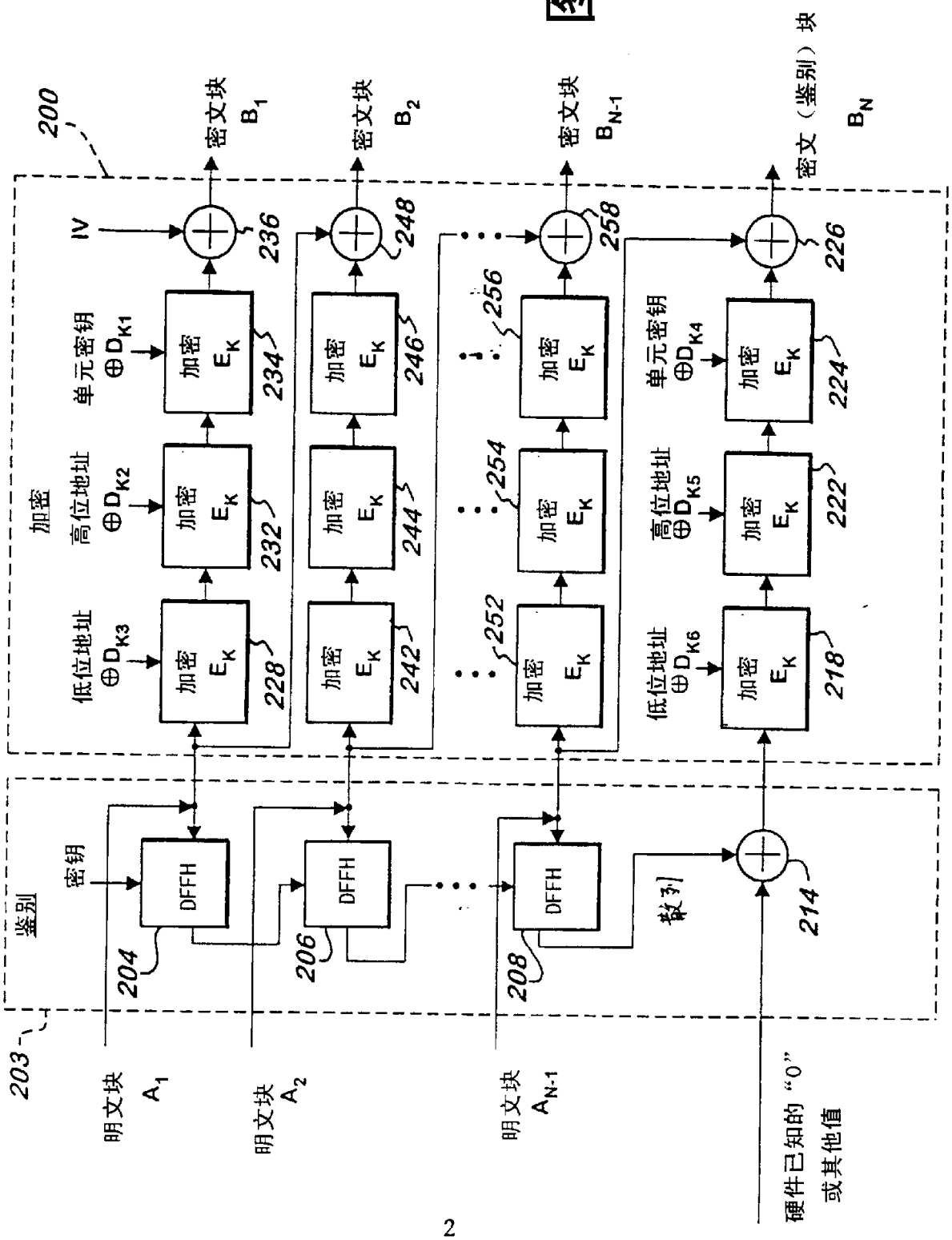

200
203
鉴别
密钥
DFFH
204
206
208
明文块 A_1
明文块 A_2
明文块 A_{N-1}
硬件已知的"0"或其他值
214
加密
低位地址 $\oplus D_{K3}$
高位地址 $\oplus D_{K2}$
单元密钥 $\oplus D_{K1}$
低位地址 $\oplus D_{K6}$
高位地址 $\oplus D_{K5}$
单元密钥 $\oplus D_{K4}$
E_K
228
232
234
242
244
246
252
254
256
218
222
224
IV
236
248
258
226
密文块 B_1
密文块 B_2
密文块 B_{N-1}
密文（鉴别）块 B_N

图2

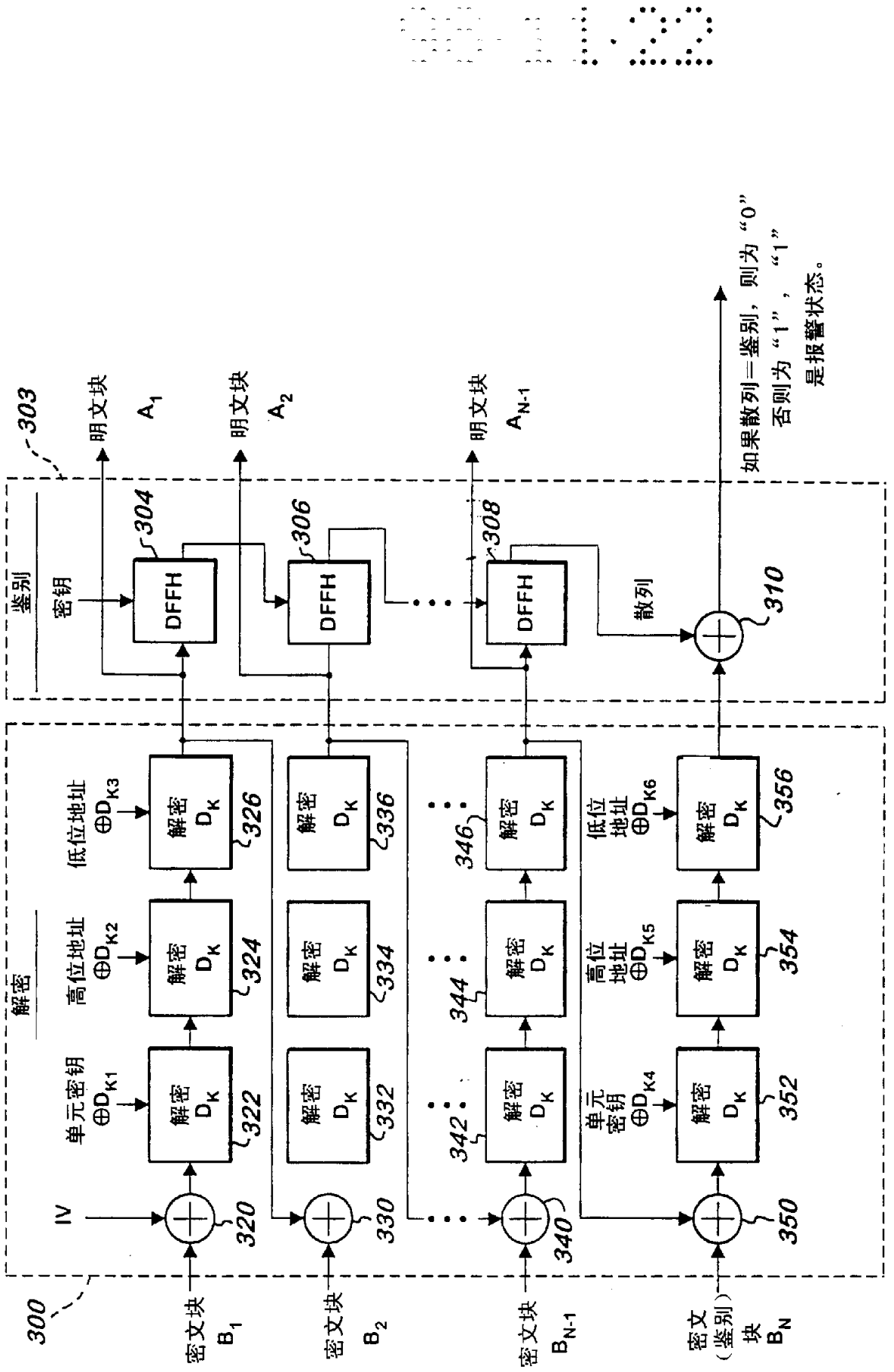

300
303
解密
鉴别
IV
单元密钥 ⊕D_{K1}
高位地址 ⊕D_{K2}
低位地址 ⊕D_{K3}
单元密钥 ⊕D_{K4}
高位地址 ⊕D_{K5}
低位地址 ⊕D_{K6}
解密 D_K
322
324
326
332
334
336
342
344
346
352
354
356
320
330
340
350
密钥
DFFH
304
306
308
散列
310
密文块 B_1
密文块 B_2
密文块 B_{N-1}
密文（鉴别）块 B_N
明文块 A_1
明文块 A_2
明文块 A_{N-1}
如果散列=鉴别，则为“0”
否则为“1”，“1”
是报警状态。

图3

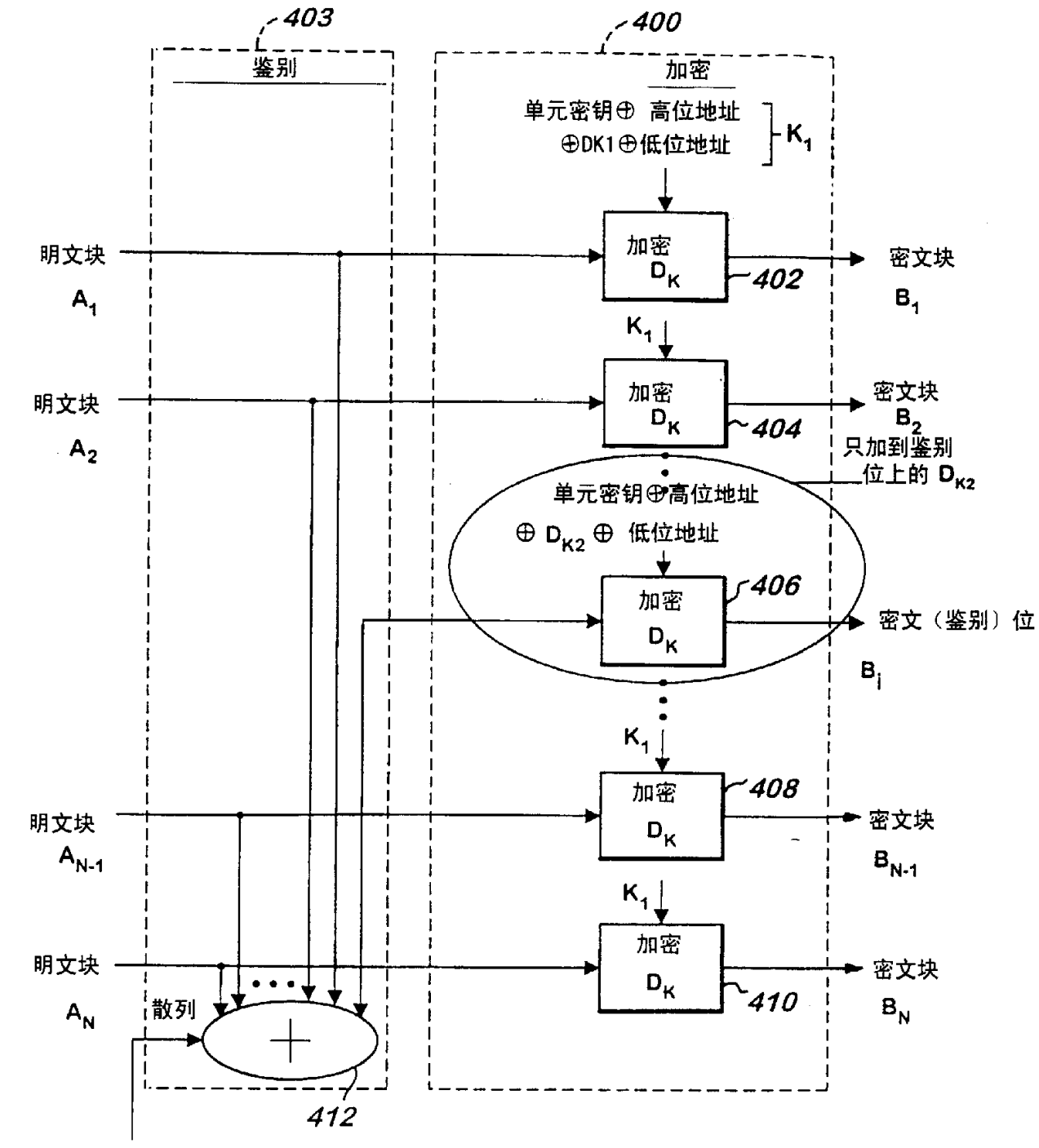

403
鉴别
400
加密
单元密钥⊕ 高位地址
⊕DK1⊕低位地址
K1
明文块
A1
加密
DK
402
密文块
B1
K1
明文块
A2
加密
DK
404
密文块
B2
只加到鉴别
位上的 DK2
单元密钥⊕高位地址
⊕ DK2 ⊕ 低位地址
406
加密
DK
密文（鉴别）位
Bi
K1
明文块
AN-1
加密
DK
408
密文块
BN-1
K1
明文块
AN
散列
加密
DK
410
密文块
BN
412
硬件已知的“0”或其他值

图4

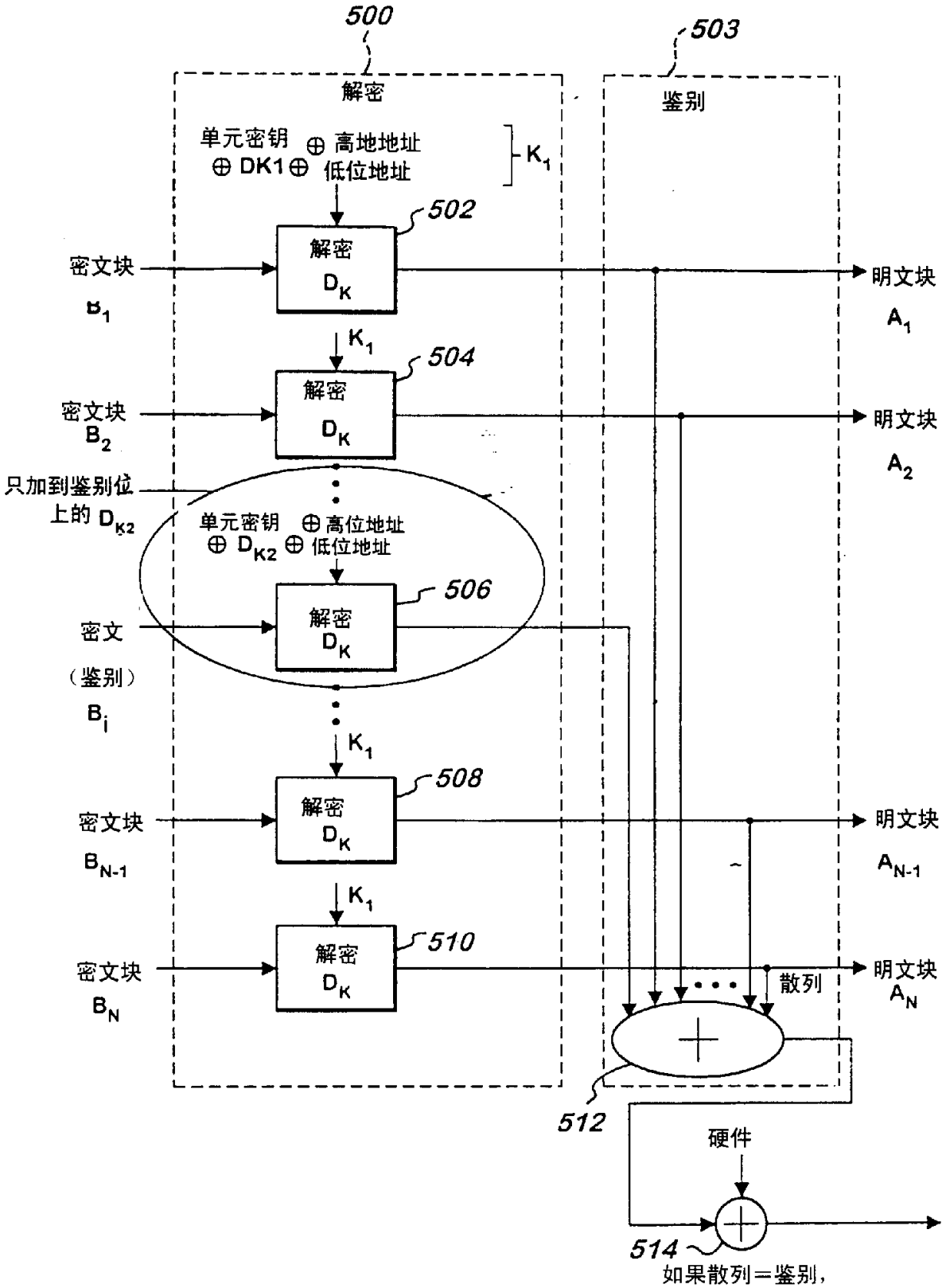

500
503
解密
鉴别
单元密钥 ⊕ 高地地址
⊕ DK1 ⊕ 低位地址
K1
502
解密
DK
密文块
B1
明文块
A1
K1
504
密文块
B2
明文块
A2
只加到鉴别位
上的 DK2
单元密钥 ⊕ 高位地址
⊕ DK2 ⊕ 低位地址
506
密文
（鉴别）
Bi
K1
508
密文块
BN-1
明文块
AN-1
K1
510
密文块
BN
明文块
AN
散列
512
硬件
514
如果散列＝鉴别，
则为“0”，否则
为“1”，“1”是
报警状态。

图5

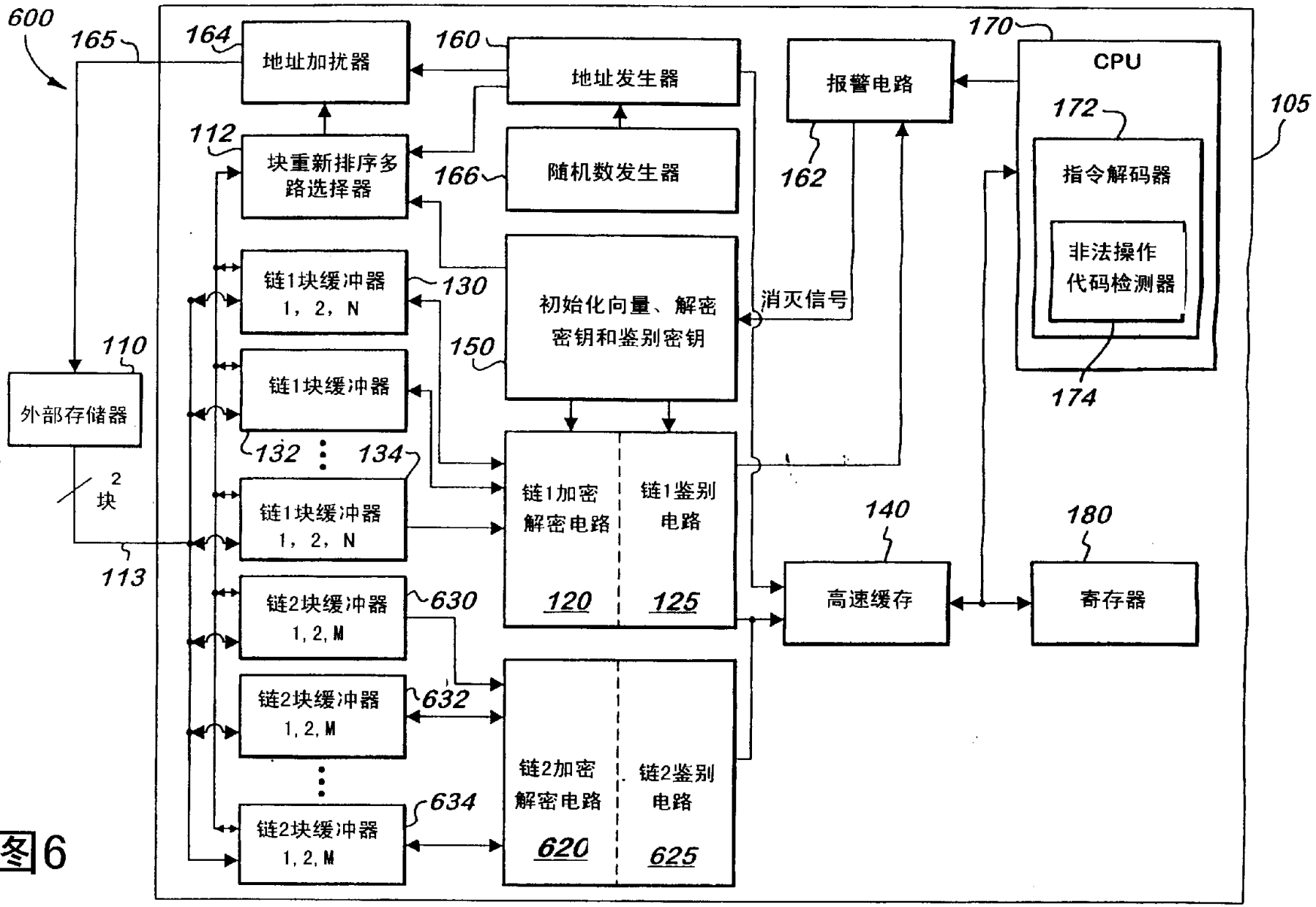

600
165
164
地址加扰器
160
地址发生器
170
CPU
报警电路
105
172
指令解码器
非法操作
代码检测器
174
112
块重新排序多
路选择器
166
随机数发生器
162
链1块缓冲器
1，2，N
130
初始化向量、解密
密钥和鉴别密钥
消灭信号
150
110
外部存储器
链1块缓冲器
132
134
2
块
链1块缓冲器
1，2，N
链1加密
解密电路
120
链1鉴别
电路
125
140
180
113
链2块缓冲器
1，2，M
630
高速缓存
寄存器
链2块缓冲器
1，2，M
632
链2加密
解密电路
620
链2鉴别
电路
625
链2块缓冲器
1，2，M
634

图6