(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 105406957 B
(45)授权公告日 2019.01.29

(21)申请号 201510497587.6

(22)申请日 2015.08.13

(65)同一申请的已公布的文献号
申请公布号 CN 105406957 A

(43)申请公布日 2016.03.16

(30)优先权数据
14184296.3 2014.09.10 EP

(73)专利权人 恩智浦有限公司
地址 荷兰艾恩德霍芬

(72)发明人 马塞尔·梅德韦德
马丁·费尔德霍弗
韦茨斯拉夫·尼科夫

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王波波

(51)Int.Cl.
H04L 9/00(2006.01)

(56)对比文件
CN 101779412 A,2010.07.14,
US 2010/0316217 A1,2010.12.16,

审查员 李华

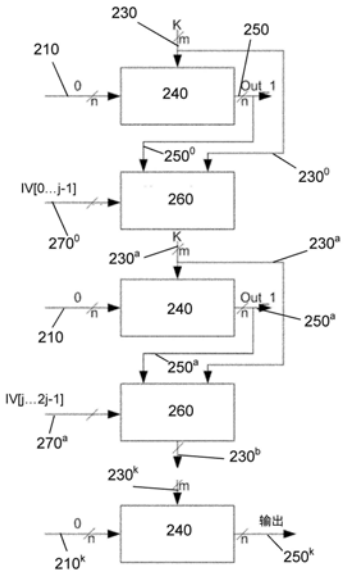
权利要求书2页 说明书8页 附图5页

(54)发明名称

保护密码设备对抗实现攻击

(57)摘要

描述了保护密码设备对抗实现攻击的方法。公开的方法包括以下步骤:从密码设备的存储器获得密钥(230);向加密模块(240)提供密钥和恒定输入(210);使用加密模块(240)导出加密数据比特的输出(250);向密钥更新模块(260)提供输出(250)、密钥(230)和输入向量(270);以及使用所述密钥更新模块(260)基于输入向量(270)的至少一部分(270^a)修改密钥以导出已更新密钥(230^a)。这防止使用已更新密钥或者通过使用边信道攻击来导出密钥的值,因为输入对于所有的密钥而言是恒定的。此外,通过改变输入向量,已更新密钥也发生了改变。



CN 105406957 B

1.一种用于保护密码设备对抗实现攻击的方法,其中所述方法使用具有单个功率痕迹的多个密钥来对抗实现攻击,所述方法包括:

a)从所述密码设备的存储器中获得密钥;

b)向加密模块提供所述密钥和恒定输入;

c)使用所述加密模块导出加密数据比特的输出;

d)向密钥更新模块提供所述输出、所述密钥和输入向量;

e)基于所述输入向量的至少一部分,使用所述密钥更新模块来修改所述密钥以导出已更新密钥;其中所述密钥更新模块针对多个密钥只产生单个功率痕迹。

2.根据权利要求1所述的方法,还包括以下步骤:

f)向所述加密模块提供所述已更新密钥和所述恒定输入;以及

g)使用所述加密模块导出已更新输出。

3.根据权利要求2所述的方法,还包括以下步骤:

h)向所述密钥更新模块提供所述已更新输出、所述已更新密钥和所述输入向量;以及

i)基于所述输入向量的至少第二部分,使用所述密钥更新模块修改所述已更新密钥。

4.根据权利要求3所述的方法,其中,所述输入向量包括两个或两个以上部分,以及针对所述输入向量的每个部分重复方法步骤f)到i),使得所述方法形成伪随机函数,以及所述方法还包括以下步骤:

借助所述伪随机函数导出伪随机输出。

5.根据权利要求4所述的方法,还包括以下步骤:

提供一个或多个附加输入向量;

使用所述伪随机函数导出针对每个附加输入向量的伪随机输出;以及

级联所述伪随机输出,以形成更大的伪随机输出。

6.根据前述权利要求中任一项所述的方法,其中,所述输入向量的所述部分是所述输入向量的至少一个比特的值。

7.根据权利要求1-5中任一项所述的方法,其中,所述密钥更新模块使用压缩、展开或排列操作中的一个或多个来修改所述密钥或先前更新的密钥。

8.根据权利要求7所述的方法,其中,根据向所述密钥更新模块提供的所述输入向量的至少一部分的值来选择用于修改所述密钥或所述已更新密钥的操作。

9.根据权利要求2-5中任一项所述的方法,其中,所述已更新密钥是所述密钥或先前更新的密钥的至少一部分与所述已更新输出的至少一部分的级联。

10.根据权利要求1-5中任一项所述的方法,其中,所述密钥更新模块将所述输出或所述已更新输出的与所述密钥或所述已更新密钥的部分相级联的部分循环多个比特。

11.根据权利要求10所述的方法,其中,所述比特的数量取决于所述输入向量的至少一部分的值。

12.一种在客户端设备与主机设备之间提供安全的数据通信的方法,所述方法包括:

向客户端设备提供客户端微处理器和客户端存储器,其中所述客户端设备包括存储在所述客户端存储器中的密钥;

向主机设备提供主机微处理器和主机存储器;

在所述主机设备与所述客户端设备之间建立安全连接;

从所述主机设备向所述客户端设备提供至少一个输入向量；

使用权利要求2到11中任一项的方法，基于所述输入向量导出至少一个已更新密钥和至少一个已更新输出；以及

通过使用所述已更新输出作为密钥流，使用所述已更新输出来加密所述客户端设备与所述主机设备之间的通信。

13.根据权利要求1-5中任一项所述的方法，其中，所述加密模块是根据加密算法的分组密码器，所述加密算法是PRESENT算法或高级加密标准算法。

14.一种用于密码设备的集成电路，所述集成电路包括微处理器和存储器，其中所述设备包括存储在所述存储器中的密钥、加密模块和密钥更新模块，从而所述集成电路被配置为执行前述权利要求中任一项的方法。

15.一种消息认证码生成方法，所述方法包括：

向密码设备提供根据权利要求14所述的集成电路；

向所述设备提供输入向量；

向所述设备提供恒定输入；

基于所述输入向量，使用权利要求2或其任一从属权利要求所述的方法，导出已更新密钥和已更新输出；以及

使用所述已更新输出作为消息认证码。

保护密码设备对抗实现攻击

技术领域

[0001] 本公开描述了用于保护密码设备的方法和集成电路，并且具体地，描述了用于保护密码设备对抗实现攻击的方法。

背景技术

[0002] 智能设备，尤其是具有低功率要求的智能设备(通常被称作无源智能设备)被广泛用于认证和访问控制。这样的设备的示例包括作为射频识别(RFID)标签的子集的非接触智能卡。这样的无源智能设备通常使用专用集成电路(ASIC)。

[0003] 考虑到无源智能设备在安全关键应用中的应用，使用密码术来认证正在使用的无源智能设备。相反地，由于对无源智能设备可以保存或允许访问的信息的渴求，它们也是恶意的试图使用的兴趣所在。

[0004] 大量的时间和努力花费在了对安全集成电路(IC，例如智能卡)中的边信道对策的实现和分析。边信道攻击是以根据密码系统的物理信息获得的信息为基础的任何攻击。这样的攻击不同于软件强力攻击或者加密算法中的开发或弱点。边信道攻击通常检查系统的内部操作(例如系统汲取的功率、电磁(EM)辐射或其它‘边信道’)来确定模式和实现步骤。一种这样的已知边信道攻击是差分功耗分析(DPA)。这可以包括恶意用户研究设备使用期间功率使用的痕迹，并且利用统计分析来确定加密算法的特征。

[0005] 随着当前可用的标准化算法和协议的使用(像是在银行业务或电子政务中使用的算法和协议)，针对差分功耗分析(DPA)(以及差分故障攻击)的攻击情形是存在的，导致设备实现受这样的边信道攻击威胁的协议(例如，由于始终以相同的(主)密钥来加密变化的输入，系统的功率签名中的变化仅取决于或一般取决于加密算法的变化)。

[0006] 对这种攻击的一种解决方案是使用密钥更新(re-keying)方法。在这样的方法中，会话密钥从主密钥导出，随后将该会话密钥用于实际操作。该会话密钥有规律地变化，以减少针对具体的(主)密钥可以从设备获取的功率痕迹的量。

[0007] 该密钥更新的特殊实例已经应用在CIPURSE协议中。在该方法中，通过使用随机输入以及更容易进行保护以对抗实现攻击的函数(称作NLM(非线性映射))，使用主密钥导出中间会话密钥。然后，该中间会话密钥与主密钥一起使用，以得到所使用的会话密钥(参见参考US2010316217A1)。上述对这样的DPA攻击的解决方案依靠双方之间的随机数协定。这样的方法防止验证先前交易。具体地，在没有随机数的情况下不可能重复会话。

[0008] 相对新的研究领域是泄露弹性密码术。在泄露弹性(LR)中寻求避免典型的DPA情形，在典型的DPA情形中，可以以针对每个执行的改变的输入，逐组块地(即以组块为单位，例如逐字节地)攻击分组密码的密钥。在LR方法中，多次执行分组密码，其中仅逐组块地(例如，每次1个比特)来使用完整的输入向量并且将其复制到分组密码的整个输入状态。在每个迭代中，下一个输入组块被用作输入(再次地，复制到整个状态)。这限制了数据复杂性，即可以用于攻击的痕迹的数量，并且在不同密钥组块的边信道信息之间创建依从性。然而，由于针对每个密钥有N＞1个痕迹，对手仍然可以应用DPA攻击。

[0009] 总的来说，在没有实现重大对策且不需要详细的边信道调查的低成本IC上执行对称密码安全服务时仍然存在问题。以下公开旨在处理这些问题。

发明内容

[0010] 根据本发明的第一方案，提供了用于保护密码设备对抗边信道攻击的方法，该方法包括：

[0011] 从密码设备的存储器获得密钥；

[0012] 向加密模块提供密钥和恒定的数据比特输入；

[0013] 使用加密模块导出加密数据比特的输出；

[0014] 向密钥更新模块提供输出、密钥和输入向量；以及

[0015] 使用所述密钥更新模块基于输入向量的至少一部分来修改密钥以导出更新的密钥。

[0016] 以这种方式使用密钥减少或去除了下层加密模块中对攻击对策的需求，并且还防止了详细的边信道调查。因为使用了密钥更新技术，不能使用已更新密钥来通过边信道攻击来导出原始的主密钥。密钥更新模块所应用的变换需要知道原始主密钥，因为它们使用根据输入向量和密钥导出的加密模块输出。此外，因为向加密模块的(明文)输入是恒定的，仅可获得单个功率痕迹。这提供了对抗边信道攻击(例如DPA，其试图将统计分析应用到密码过程和算法的功率管理痕迹)的安全性。

[0017] 在本公开的实施例中，方法还包括以下步骤：向加密模块提供已更新密钥和恒定输入；以及使用加密模块导出已更新输出。

[0018] 这样的实施例通过提供已根据已更新密钥和所提供的输入向量导出的已更新输出来提高已更新密钥的安全性。因为已更新输出使用已更新密钥而不是原始的主密钥来进行加密，保护了原始的主密钥的安全性。

[0019] 此外，该方法还可以包括以下步骤：向密钥更新模块提供已更新输出、已更新密钥和输入向量；以及使用所述密钥更新模块基于输入向量的至少第二部分来修改已更新密钥。通过进一步修改已更新密钥，该步骤从主密钥中发展出进一步更新的密钥。

[0020] 输入向量可以包括两个或两个以上部分。因此，这样的方法步骤可以针对输入向量的每个部分进行重复。具体地，以下步骤可以迭代多次，其次数等于输入向量的部分的数量：向加密模块提供已更新密钥和恒定输入；以及使用加密模块导出已更新输出，并且向密钥更新模块提供已更新输出、已更新密钥和输入向量；以及使用密钥更新模块来更新已更新密钥。

[0021] 换言之，可逐组块地(即以组块为单位，例如以字节或比特为单位)提供输入向量。例如，针对长度为128比特的输入向量，该输入向量可被看做包括64个部分或组块，每个部分长2比特。然后可以借助伪随机函数来导出伪随机输出。因此，密钥更新模块可被看做是担当伪随机函数步骤，基于输入向量的至少部分的值来处理输入向量和密钥以导出伪随机输出(例如已更新密钥)。在该考虑中，输入向量和密钥是伪随机函数的输入。

[0022] 在实施例中，可以提供一个或多个附加输入向量。然后可以针对每个附加输入向量，使用伪随机函数来导出伪随机输出。然后可以将每个伪随机输出级联以形成更大的伪随机输出。

[0023] 输入向量的部分可以包括至少比特串的值。此外或备选地，输入向量的部分可以是输入向量的至少1个比特的值。因此，密钥更新模块可以基于输入向量的比特值来导出已更新密钥。密钥更新模块可以进行动作，以应用所限定的密钥更新协议来根据输入向量的比特的值来修改密钥或已更新密钥。例如，针对比特0的0比特值可以指示密钥更新函数将密钥的所选择的比特向右循环1个比特位置。相反地，针对比特0的比特值1可以指示密钥更新函数将密钥的同一比特或其它比特向右循环2个比特位置。根据可用于更新函数的算法，可以有其它排列。

[0024] 如上所述，基于输入向量的比特的值，密钥更新模块可以使用压缩、展开或排列操作中的一个或多个来变换或修改密钥或先前更新的密钥。

[0025] 利用迭代增加了原始获得的密钥(称作主密钥)与已更新密钥之间依从性的复杂性，因此使得更难以导出密钥树中较高的密钥。这进而借助差分故障分析阻碍了密钥恢复，特别是针对原始获得的主密钥而言。此外，因为每个密钥只使用相同的输入(即，向每个加密模块提供的输入是恒定的)，每个密钥迭代的功率痕迹是相同的，并且因此每个密钥的功率测量对于上述差分功耗分析攻击是有弹性的。

[0026] 在一些示例中，密钥更新模块可以将输出的值或者已更新输出循环多个比特。例如，比特的数量可以取决于输入向量的至少一部分的值。

[0027] 备选地或附加地，已更新密钥可以是密钥或先前已更新密钥的至少一部分与已更新输出的至少一部分的级联。如上所述，向密钥更新模块提供加密模块的输出以及密钥和输入向量。因此，为了生成长度足够的已更新密钥，先前的密钥可被压缩或分成单独的部分(例如左部分和右部分，这基于比特的数量)，并且与输出或已更新输出相组合以生成已更新密钥。在处理输入的一部分并且因此对已更新密钥进行更新之前，如果输出长度/密钥长度比允许，还可以使用输出对密钥的完全替换。可以设想到的是，还可以使用用于生成已更新密钥的备选技术，例如使用盐(salt)来填充输出或已更新输出以及先前密钥中的一个或多个的一些或全部，以生成已更新密钥。

[0028] 所描述的方案提供了不依赖于各方之间的密钥协定的泄露弹性类型方案。这允许再现和/或验证先前的交易或消息认证码。此外，不同于通过继续沿着输入向量的值发展或通过提供新的输入向量来针对每一个实例生成已更新密钥，当前的方法只使用一次临时的或已更新的密钥(本质上不存在会话密钥)。

[0029] 在第二方案中，提供了在客户端设备与主机设备之间提供数据安全通信的方法，所述方法包括：

[0030] 向客户端设备提供客户端微处理器和客户端存储器，其中，客户端设备包括存储在客户端存储器中的密钥；

[0031] 向主机设备提供主机微处理器和主机存储器；

[0032] 在主机设备与客户端设备之间建立安全连接；

[0033] 从主机设备向客户端设备提供至少一个输入向量；

[0034] 基于输入向量，使用第一方案的方法的至少一部分来导出至少一个已更新密钥和至少一个已更新输出；以及

[0035] 通过使用所述已更新输出作为密钥流，使用所述已更新输出来加密客户端设备与主机设备之间的通信。

[0036] 该方案可以有利于临近耦合设备和邻近集成电路芯片之间的通信协议。智能卡连同RFID设备是这种芯片的一个示例。这样的设备需要主机设备与客户端设备之间的认证。此外,这样的设备允许客户端设备基于主机设备提供的输入向量来向主机设备提供拥有密钥的证据。

[0037] 在上述方案中,加密模块可以是根据任何加密算法的分组密码器。这样的加密算法包括PRESENT算法或者高级加密标准算法。使用还可在设备上提供备选功能的现有分组密码允许所描述的密码密钥生成的门等效(ge)元件封装(footprint)保持最小。这使得设备可低成本。

[0038] 在另一个相关方案中,提供了对数据进行加密的方法,所述方法包括:

[0039] 向密码设备提供微处理器和存储器,其中该设备包括存储在存储器中的密钥以及加密模块;

[0040] 向设备提供输入向量;

[0041] 基于输入向量和伪随机输出,使用第一方案的至少一部分方法来导出已更新密钥;

[0042] 提供将要加密的数据;以及

[0043] 使用已更新密钥对数据进行加密。

[0044] 在另一个实施例中,加密模块可以用于认证协议,使得协议对于DPA攻击不脆弱。这提高了这样的认证协议的安全性。

[0045] 另一个方案可以涉及用于密码设备的集成电路,该密码设备包括微处理器和存储器,其中该设备包括存储在存储器中的密钥、加密模块和密钥更新模块,从而集成电路被配置为执行任何前述方案的方法。

[0046] 该方案提供了保护密码设备对抗实现攻击(例如边信道攻击)的安全性。

[0047] 在另一方案中,提供了消息认证码生成方法,所述方法包括:

[0048] 向密码设备提供根据上述集成电路方案的集成电路;

[0049] 向该设备提供输入向量和恒定输入;

[0050] 基于输入向量,使用第一方案的至少一部分方法来导出已更新密钥和已更新输出;以及

[0051] 使用已更新输出作为消息认证码。

[0052] 此外,输入向量可以与计数器级联,以产生若干输入并且由此产生更长的输出。

[0053] 在实施例中,加密模块可以是解密模块或者是加密解密模块。

[0054] 使用标准加密模块(例如对称分组密码器)以及如上所述的方法提供了加密密钥,该加密密钥使得在分组密码实现本身中,在没有任何特殊对策(除了以并行方式(parallelism)阻止简单功率分析以外)的情况下,不能发生如差分功耗分析和故障攻击等的实现攻击。通过重复地执行分组密码并同时使数据输入保持恒定(例如全部是0、全部是1),从原始密码密钥开始,基于输入向量来修改密钥。这允许在没有昂贵的对策并且不需要详细的边信道分析的情况下具有“通过设计得到的安全”方法。本公开可以在例如认证协议中替换标准分组密码。

[0055] 可以提供计算机程序,当在计算机上运行该程序时,导致计算机配置包括本文公开的电路、控制器、传感器、滤波器或设备的任何装置,或者执行本文公开的任何方法。该计

算机程序可以是软件实现，并且该计算机可以看做是任何合适的硬件，包括数字信号处理器、微控制器以及在只读存储器(ROM)、可擦可编程只读存储器(EPROM)或电可擦除可编程只读存储器(EEPROM)(作为非限制示例)中的实现。软件实现可以是汇编程序。

[0056] 计算机程序可以在计算机可读介质上提供，该计算机可读介质可以是物理计算机可读介质，例如磁盘或存储设备，或者可以表现为瞬态信号。这样的瞬态信号可以是包括因特网下载的网络下载。

附图说明

[0057] 现在将参照附图对本公开进行描述，其中类似的附图标记用来表示类似的元素：

[0058] 图1是现有技术安全服务的框图；

[0059] 图2是主机设计与客户端设备之间通信的框图；

[0060] 图3是根据本发明的密码术基本要素；

[0061] 图4是图3的密码术基本要素的流程图；并且

[0062] 图5是图3的密码术基本要素的备选流程图。

[0063] 应当注意的是，附图是概略图并且未按比例绘制。为了在附图中清楚和方便，这些附图的部分的相对尺寸和比例已经在尺寸上扩大或缩小地示出。一般使用相同的附图标记在修改实施例和不同实施例中表示对应或类似的特征。

具体实施方式

[0064] 图1示出了具有输入IV(输入向量)20、密钥(K)30、分组密码器40和输出50的现有技术安全服务10。这样的现有技术安全服务的操作是：使用密钥30对输入向量20进行加密，以提供已加密的密文或输出50。分组密码器40提供如何使用密钥来对输入进行加密的指令。

[0065] 攻击方法是检查分组密码器的内部代码，例如S-box。进行该活动的一种方法是使用边信道攻击。例如，通过分析电磁功率消耗和使用统计，可以确定S-box的结构。这样的攻击通常被称为差分功耗分析攻击。

[0066] 例如图1中示出的安全服务可以用在用于读取并且与无源设备(例如射频识别(RFID)标签)通信的服务器或主机上，例如计算机或临近耦合设备。

[0067] 图2示出了主机120和客户端无源设备140的示例。在示出的示例中，主机120可以是临近耦合设备(PCD)，并且客户端设备140可以是临近集成电路芯片(PICC)，例如适于用在根据本公开的密钥分布协议中的RFID标签或智能卡140。在该实施例中，主机120是计算机，其中包括处理器130、存储器132和卡接口134。智能卡140包括输入/输出接口142、处理器144和存储器146。主机120通过卡接口134和输入/输出接口142与智能卡140通信。处理器144可以是被配置为提供如下文更加详细描述的密码处理操作的微处理器或有限状态机。卡140的存储器146可以是电子静态或动态随机存取存储器(RAM)、磁性存储器或信息存储元件的其它合适的布局。卡接口134和输入/输出接口142可以与标准卡接口相一致，例如个人电脑存储卡接口适配器(PCMCIA)标准或非接触通信接口(如ISO 14443)。

[0068] 在如图2中示出的本公开示例性实施例中，卡140用于生成密钥流。然后，在主机120上操作的处理向卡提供加密数据输入以用来解密。然后卡140使用密钥流执行解密。这

允许卡140被实现为具有相对有限的计算功率和低输入/输出带宽的设备。在该示例中，假设卡140将作为无状态设备来操作，使得当前的输出仅取决于当前的输入，而不取决于任何先前的输入。针对给定的输入n，卡140将因此输出具有由输入n、存储在存储器146中的密钥K以及在卡140中产生或者通过主机120向卡140提供的随机或伪随机比特序列所确定的值的函数。该假设认识到很多当前可用的智能卡包括有限的存储、处理和输入/输出能力。

[0069] 本公开使用单个常数(密钥)，其与已知输入组合以生成伪随机输出。如指出的，为了防止使用边信道攻击(如差分功耗分析攻击)的攻击，一项技术是频繁地改变密钥，或者建立硬件来防止攻击。

[0070] 图3描绘了保护密码处理对抗实现攻击(例如边信道攻击)的过程。通过与图1中示出的类似的方法，加密模块(例如分组密码器240)被配置为基于恒定的输入210和密钥230来产生输出250。在所示出的示例中，输入210长n个比特，密钥230长m个比特，以及对应的输出长n个比特。在示出的示例中，输入210具有0值(即全部n个比特的值是0)。应当设想到输入和输出可以是任意长度。通常，密钥长128个比特。

[0071] 向密钥更新模块260馈送输出250连同密钥230的值。还向密钥更新模块260提供输入向量270。逐组块地(即以组块为单位，例如逐字节地)向密钥更新模块馈送输入向量。在图3中，输入向量270长k*j个比特，并且以j个比特的组块为单位向密钥更新模块260馈送。第一次迭代按比特[0…j-1]、第二[j…2j-1]比特、直至最后一个组块[(k-1)j…kj-1]来进行馈送。这将输入向量270分为多个部分270^0、270^a…270^k。密钥更新模块260包含(在第一次迭代中)提供已更新密钥230^a的密钥更新函数(参见图4)。还可向密钥更新模块260提供输入向量270的一部分270^0(即逐比特地提供输入向量，每次单个比特)。由输入向量270^0向密钥更新模块260提供的单个比特或组块的值来确定如何更新密钥230。基于输入向量270^0(或270^a…270^k)提供的单个比特或组块的值、输出250^0(或250^a…250^k)、密钥230^0(或230^a…230^k)的值和密钥更新模块260中的密钥更新函数，密钥更新模块260提供已更新密钥230^a(或230^b…230^k)。

[0072] 针对输入向量270的每个部分或比特重复上述过程。因此，如图4所示，将已更新密钥230^a连同输入210一起向分组密码器240提供(同样，在示出的实施例中，输入210具有0值)。假设密钥230^a的值已经改变，输出值250^a也与第一次迭代的输出250不同。同样，将输出250^a和已更新密钥230^a连同输入向量270^a的下一个比特一起向密钥更新模块260提供。基于输入向量270^a的下一个比特的值、已更新输出250^a和已更新密钥230^a，密钥更新模块260的密钥更新函数提供第二已更新密钥230^b。

[0073] 针对输入向量270的所有比特迭代重复上述过程，直到提供(最后一次迭代)已更新密钥230^k。然后，该已更新密钥230^k可以与输入210^k组合，并且向分组密码器240提供，以提供输出值250^k。输出250^k可以用作密钥流。输出250^k还可以用于馈送密钥流生成函数。输出250^k可以用作针对输入的消息认证码。输出250^k还可以用于馈送消息认证码生成函数。

[0074] 图4详细描述了密码术基本要素，且具体地，图3所示的密钥更新模块260中的密钥更新函数。在图4中，密钥230包括左半边232^0和右半边234^0。密钥230的每个半边包含密钥比特的一半，所以针对128个比特的密钥，左半边包含比特127:64，并且右半边包含比特63:0。将密钥230连同输入210一起向加密模块240(例如分组密码器)提供。输出250^0是由加密模块240输出的的密文(C0)252。除了密钥、加密模块和输入以外，提供被逐比特地分析的输入

向量270^0，使得可确定输入向量270^0的每个比特272的值274。取决于输入向量270^0的每个比特272的值274，使用密文输出252与原始密钥230的级联来导出密钥230^a。在示出的示例中，输入向量的两个值都规定输出252与原始密钥230的右手侧234^0级联。丢弃原始密钥的左右侧232^0。取决于所选择的输入向量270^0的比特272的值274，可以对原始密钥的右手侧234^0执行操作。例如，如图4所示，比特272的0值274导致密钥234^0的右手侧以1比特的值进行第一循环(即输出252相对于密钥234^0的右手侧的位置C0)。相反地，比特272的1值274导致密钥的不同循环(在示出的示例中是2比特的循环)，以及密钥234^0的右手侧相对于输出252的不同位置。在两种情况下，这形成了已更新密钥230^a1或230^a2。

[0075] 可以看出，如果将128比特的原始密钥与64比特的输入一起使用，则输出的值可以长64比特。将该输出值与原始密钥的一半级联提供128比特的已更新密钥。级联的形式可以取决于输入向量270的比特272的值274。级联的形式还可以采取备选的形式，例如使用盐、常数、计数器、随机数或其它密码结构。

[0076] 可以设想到的是，除了级联以外或作为级联的备选，还可以对密钥执行其它函数。例如，密钥的右手侧234可以循环若干个比特。图4中示出的示例使用原始密钥的简单压缩来提供已更新密钥。也可使用展开和其它排列。

[0077] 还可以设想到的是，对密钥执行的函数可以取决于输入向量270的一个以上的比特。图5中示出了一个这样的示例。图5示出了图4中示出的基本要素的单个迭代的备选结构。在该变体中考虑输入向量270的两个比特的值。可以设想到的是，可以应用输入向量270的任何部分(即1或更多的比特)。

[0078] 例如，输入向量提供备选树形路径270^a1、270^a2、270^a3、270^a4来更新密钥。选择路径270^a1、270^a2、270^a3、270^a4取决于输入向量的比特ab的值。在示出的示例中，针对比特ab的值00的是路径270^a1，其导致密钥234^a右手侧与输出252^a的级联，并伴随密钥向右循环1比特。路径270^a2(比特值01)导致密钥234^a的右手侧与输出252^a之间的备选级联，2比特的循环被应用到密钥。比特值10导致路径270^a3以及密钥234^a的右手侧与输出252^a之间的级联并伴随3比特的循环，并且最后，值11导致路径270^a4与路径270^a3的备选级联并伴随4比特的循环.

[0079] 取决于所确定的输入向量比特的值，基于原始密钥的值和输出导出已更新密钥230^b。然后，可通过分析输入向量270^b的下一个组块的比特cd的比特值来进一步修改已更新密钥，导致已更新密钥230^b的左手侧232^b和右手侧234^b(图5中只示出了右手侧234^b)与已更新输出值252^b的级联(同样伴随根据比特cd的值而应用的循环)。针对第二次迭代，取决于输入向量270的比特cd的值，备选路径270^b1、270^b2、270^b3、270^b4是可能的。

[0080] 输入向量270的该部分的大小可以允许密钥更大数量的可能变换或更新，该变换或更新取决于输入向量的该部分的值。例如，使用输入向量的8比特部分为密钥更新函数提供众多路径。将更大的比特值用于输入向量的该部分还允许更短的处理。

[0081] 本公开减少对密钥随机性的需要。允许基于任何常数的加密。通过改变输入向量的值，最终的已更新密钥230^k也发生变化。此外，对于每个密钥来说只存在一个输入，并因此只存在单个功率测量。因此，统计方式的边信道攻击(如差分功耗攻击)是低效的。

[0082] 本公开描述了逐比特地处理输入。因此，针对任意长度输入的输出将会是n个比特的输出。一般而言，使用密钥来加密常数。在本示例中使用了0值，然而输入可以具有任意长

度和任意值。在使用密钥对常数进行加密之后，对输入因子进行细分，并将其用于逐步地修改密钥。这针对密钥创建了树状的结构。这还创建了伪随机函数。

[0083] 密钥更新模块260的密钥更新函数可以应用到任何加密协议。通过针对每个密钥只产生单个功率痕迹，防止了边信道攻击。此外，不存在从外部不能控制的随机性。可以对每个交易进行相同的重放。如果提供的输入向量270相同，则最终的已更新密钥230^k也将会是相同的。

[0084] 不同于其它加密密钥更新方法，不存在会话密钥。相反，针对输入向量的比特值的每个迭代，对先前的密钥进行重写。因此，不可能根据会话密钥来确定或重新创建先前的密钥，并且因此主密钥对于攻击而言并不脆弱。

[0085] 本公开的另一个应用可以在认证中。参照图2，临近集成电路芯片能够在客户端存储器146中存储主密钥230。在客户端设备140与主机设备120之间的接触期间，标准认证协议可被用于确定主机和客户端两者之间是相互可信任的。客户端设备140可以应用上述的伪随机函数，该伪随机函数使用从主机设备120接收的输入向量以生成输出。在这个阶段，该输出可以被看做是消息认证码(MAC)，并且然后可以通过I/O和卡接口134、142向主机设备传递。

[0086] 通过阅读本公开，其它变化和修改对于本领域技术人员来说将会是显而易见的。这样的变化和修改可以包括等同物和其它特征，该等同物和其它特征在密码领域中是已知的，并且可以使用来替代或附加本文已经公开的特征。

[0087] 虽然附带的权利要求针对特征的特定组合，但是应该理解的是，本发明的公开范围还包括这里明确或隐含公开的或由此归纳的任何新特征或特征的任何新组合，不管其是否涉及与任何权利要求中当前所要求保护的发明相同的发明或是否如本发明一样解决了部分或全部的相同技术问题。

[0088] 分离的实施方式的上下文中描述的特征也可在单个实施方式中组合提供。反过来，为了简明而在单个实施方式的上下文中描述的各个特征也可被分别提供或以任何适当的子组合来提供。

[0089] 申请人在这里注明，可在本申请或由此导出的任何进一步申请的答辩过程中对这种特征或特征的组合构成新的权利要求。

[0090] 为了完整起见，还注明术语“包括”不排除其他元素或步骤，术语“一”不排除多个，单个处理器或其它单元可实现权利要求中所记载的若干装置的功能，而且权利要求中的参考符号不应被理解为限制权利要求的范围。

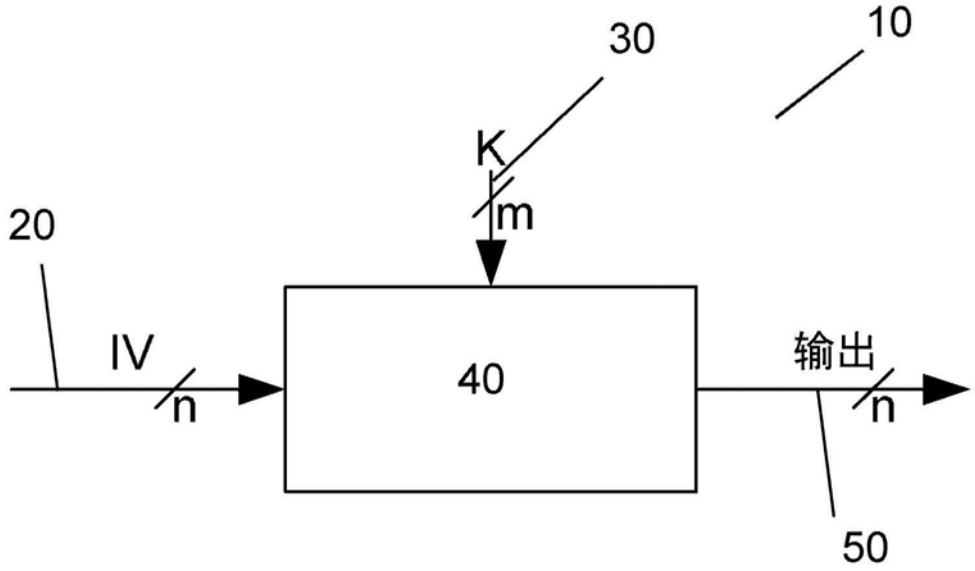


图1

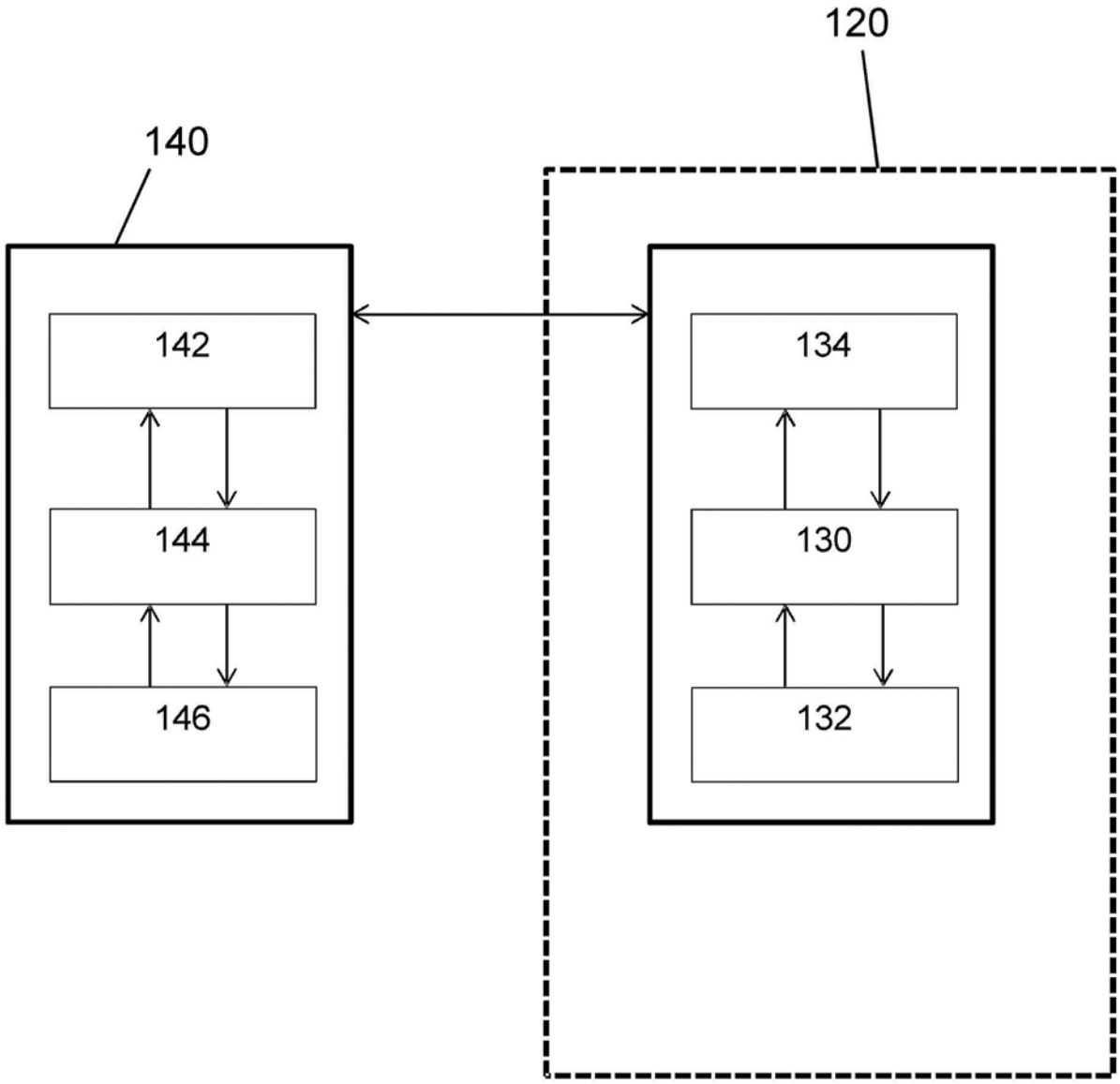


图2

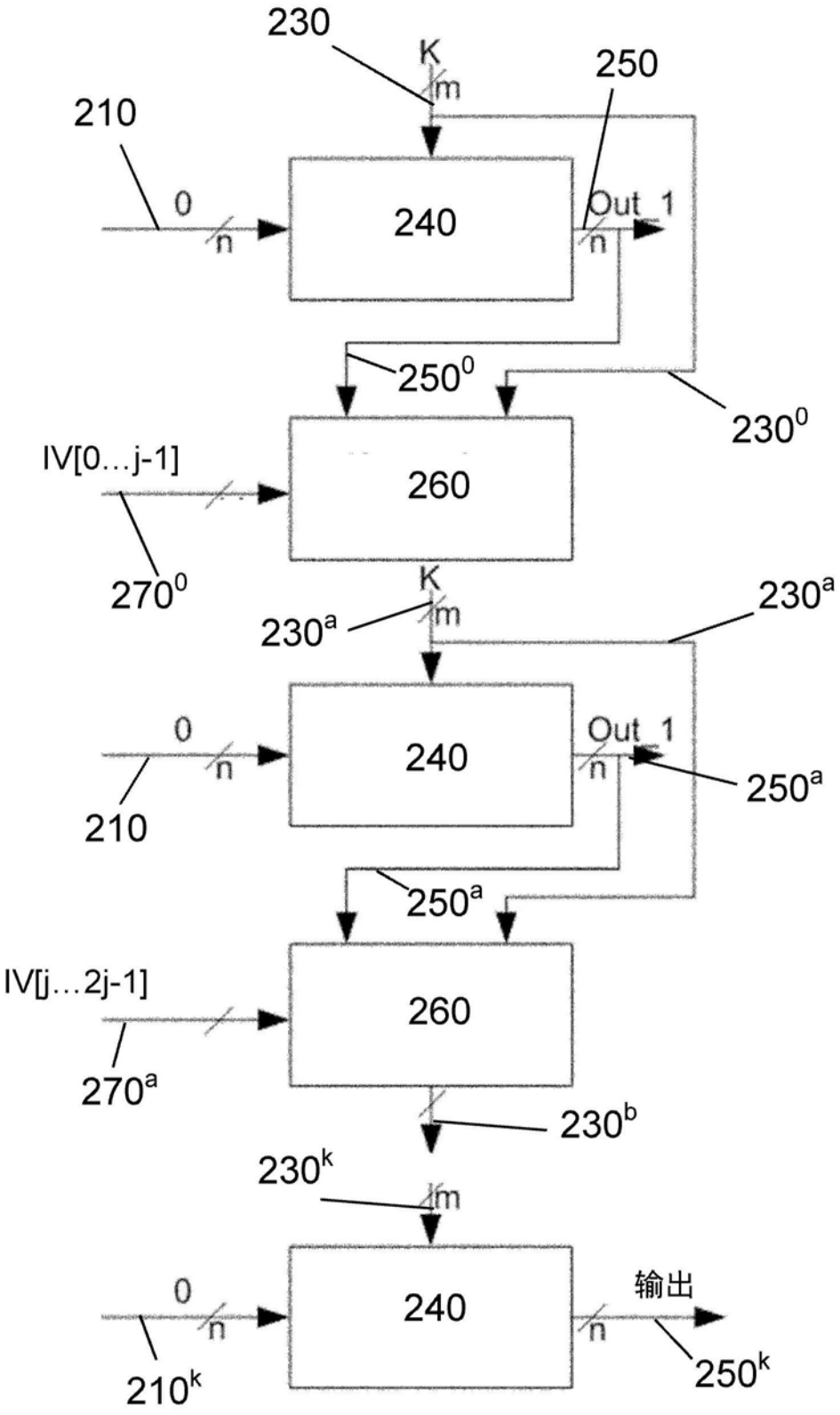

230
K
m
250
210
0
n
240
Out_1
n
250^0
230^0
IV[0…j-1]
260
270^0
K
m
230^a
230^a
0
n
240
Out_1
n
250^a
210
250^a
IV[j…2j-1]
260
270^a
230^b
230^k
m
0
n
240
输出
n
210^k
250^k

图3

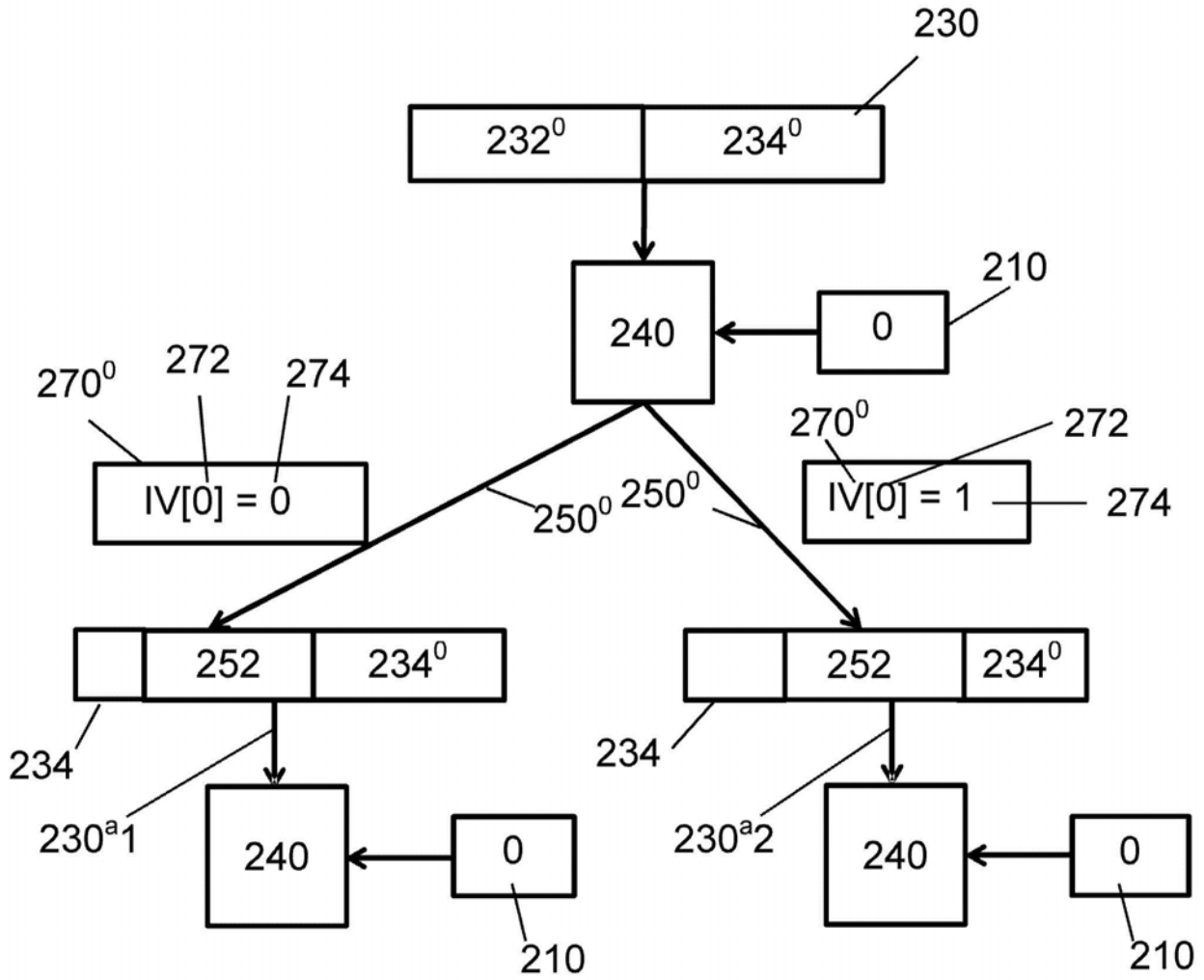

230
232^0
234^0
240
0
210
270^0
272
274
IV[0] = 0
250^0
250^0
270^0
272
IV[0] = 1
274
252
234^0
234
230^a1
240
0
210
252
234^0
234
230^a2
240
0
210

图4

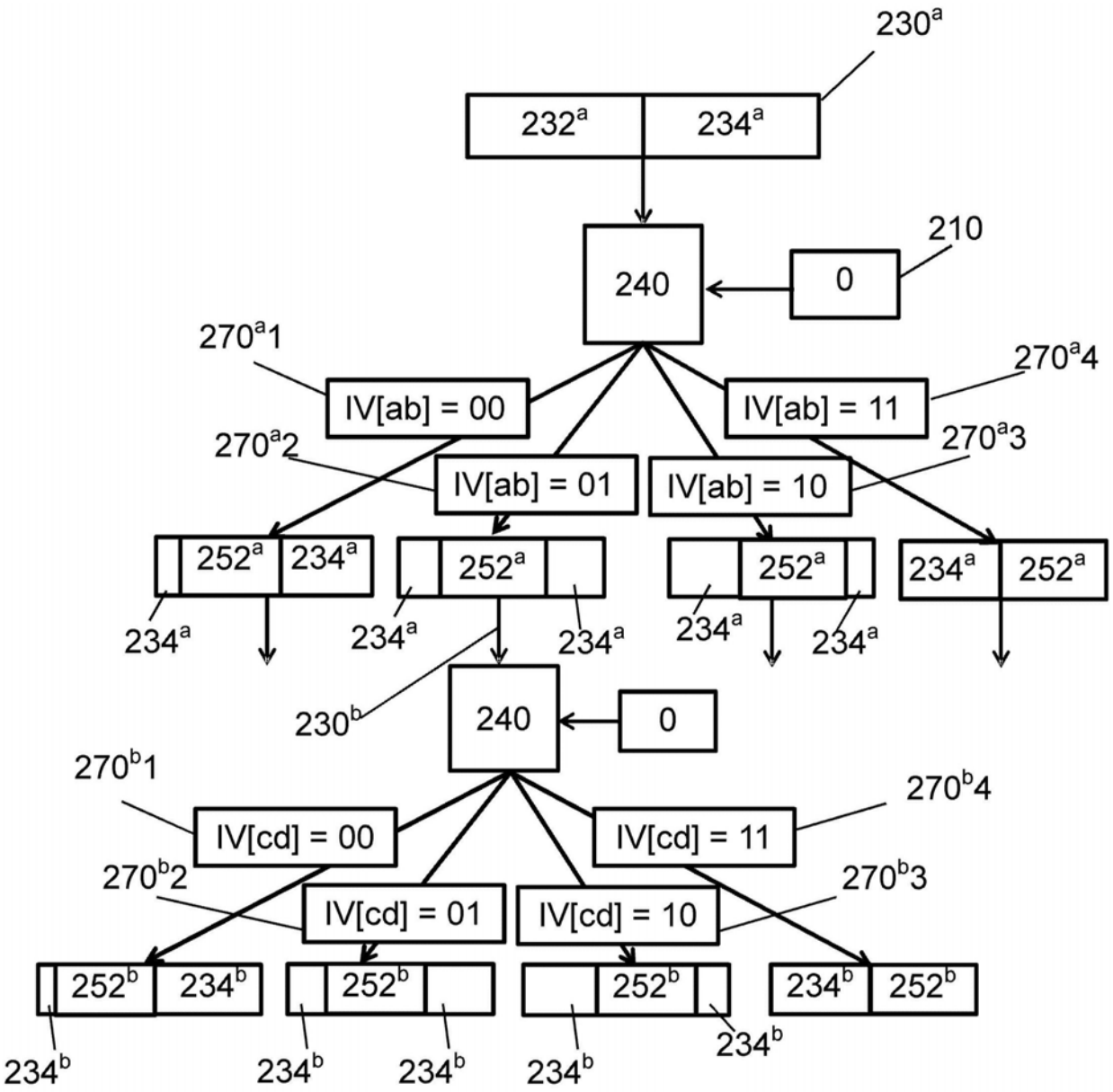

230a
232a
234a
240
0
210
270a1
270a4
IV[ab] = 00
IV[ab] = 11
270a2
270a3
IV[ab] = 01
IV[ab] = 10
252a
234a
234a
234a
234a
234a
234a
252a
230b
240
0
270b1
270b4
IV[cd] = 00
IV[cd] = 11
270b2
270b3
IV[cd] = 01
IV[cd] = 10
252b
234b
234b
234b
234b
234b
234b
252b

图5