[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G08B 13/14 (2006.01)
G06F 1/00 (2006.01)
H04L 9/30 (2006.01)

[12] 发明专利说明书

专利号 ZL 03818723.X

[45] 授权公告日 2007 年 11 月 21 日

[11] 授权公告号 CN 100350437C

[22] 申请日 2003.8.21 [21] 申请号 03818723.X
[30] 优先权
[32] 2002. 8.21 [33] FR [31] 0210430
[86] 国际申请 PCT/EP2003/050386 2003.8.21
[87] 国际公布 WO2004/019296 法 2004.3.4
[85] 进入国家阶段日期 2005.2.4
[73] 专利权人 汤姆森许可贸易公司
地址 法国布洛里
[72] 发明人 西尔万·谢弗罗 埃里克·迪尔
特迪·菲龙
[56] 参考文献
US6032257 A 2000.2.29
US5325499 A 1994.6.28
CN1204088 A 1999.1.6
US6249868 B1 2001.6.19
US5146472 A 1992.9.8
审查员 王 荣
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 戎志敏

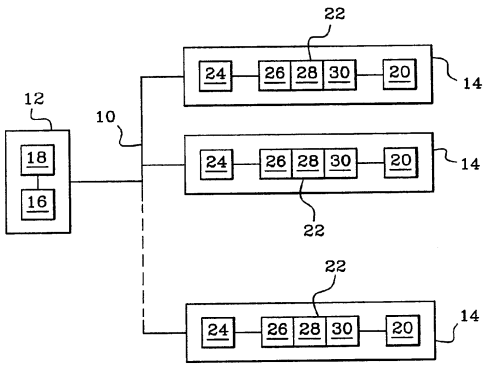
权利要求书 3 页 说明书 9 页 附图 2 页

[54] 发明名称

安全电子防盗设备、包括这种设备的防盗系统和匹配电设备的方法

[57] 摘要

本发明尤其涉及一种用于连接到包含至少一个监控设备(12)的预定网络(10)的电设备(14)。所述电设备包括：配置装置(26)，用于在存在所述监控设备(12)的情况下，授权其操作，其中此配置装置基于监控设备公共标识符(V)在电设备的存储装置(20)中的记录；识别装置(28)，用于在电设备与包括这种监控设备的任何网络相连时，识别至少一个监控设备；以及禁用装置(30)，用于如果所识别的监控设备不对应于针对其而配置的监控设备(12)，或者如果所述网络不包含监控设备，禁用所述电设备(14)。本发明还涉及一种防盗系统和一种对设备进行配对的方法。



1．一种连接到包含至少一个监控设备（12）的预定网络（10）的电设备（14），所述电设备包括：

- 存储装置（20）；

- 配置装置（26），用于在存在所述监控设备（12）的情况下，授权电设备（14）操作；

- 识别装置（28），当电设备连接到包括这种监控设备的任何网络时，识别至少一个监控设备；以及

- 禁用装置（30），如果所识别的监控设备不对应所配置的电设备的监控设备（12），或者如果所述网络不包含监控设备，禁用所述电设备（14），

其特征在于所述配置装置（26）将所配置的电设备的监控设备（12）的公共标识符V记录在所述存储装置（20）中。

2．根据权利要求1所述的电设备（14），其特征在于所述识别装置（28）包括用于询问任何监控设备以确定监控设备公共标识符V的装置。

3．根据权利要求1所述的电设备（14），其特征在于所述识别装置（28）包括用于验证所配置的电设备的监控设备（12）的验证装置。

4．根据权利要求3所述的电设备（14），其特征在于所述验证装置实现零知识询问/响应协议。

5．根据权利要求1所述的电设备（14），其特征在于从组件的单元之一选择电设备的状态，包括：原始状态（32）；已配置状态（34），用于在存在至少一个监控设备（14）的情况下进行操作；以及阻止状态（36），在激活所述配置装置（26）之后，获得所述已配置状态（34），以及在激活所述禁用装置（30）之后，获得所述阻止状态（36）。

6．根据权利要求5所述的电设备（14），其特征在于只在电设备处于已配置状态（34）时进行操作。

7．一种防盗系统，包括：

至少一个网络（10）；

与所述网络相连且包含公共标识符V的至少一个监控设备（12），以及

至少一个电设备（14），用于与所述网络相连，且包括：

- 存储装置（20）；

- 配置装置（26），用于在存在所述监控设备（12）的情况下，授权电设备操作，其中所述配置装置用于记录所配置的电设备的监控设备的公共标识符；

- 识别装置（28），用于在电设备与包括这种监控设备的任何网络相连时，识别至少一个监控设备；以及

- 禁用装置（30），如果所识别的监控设备不对应所配置的电设备的监控设备，或者如果所述网络不包含监控设备，禁用所述电设备。

8．根据权利要求7所述的防盗系统，其特征在于所述监控设备（12）包括用于存储由监控设备产生所述公共标识符V的秘密标识符S的安全装置（16）。

9．根据权利要求7所述的防盗系统，其特征在于从以下网络之一选择所述网络（10）：电子网络、数字传输网络和电信网络。

10．一种用于对第一监控设备（12）和第二设备（14）进行配对的方法，其中所述第二设备（14）连接到与所述第一监控设备（12）相连的网络（10），所述方法包括只有在存在所述第一监控设备（12）的情况下才配置所述第二设备（14）以授权第二设备（14）操作的步骤（38），其特征在于第二设备（14）配置步骤（38）包括将第一监控设备（12）的公共标识符V记录在所述第二设备（14）的存储装置（20）中。

11．根据权利要求10所述的配对方法，其特征在于所述第二设备（14）从组件单元之一选择状态：原始状态（32）；已配置状态（34），用于在存在至少一个第一监控设备（12）的情况下进行操作；以及阻止状态（36），以及所述配置步骤（38）包括对所述第二设备（14）的状态的改变，从所述原始状态（32）到所述已配置状态（34）。

12．根据权利要求11所述的配对方法，其特征在于包括在第二设备（14）与没有配置第二设备的第一监控设备相连时禁用所述第二设备（14）的步骤（40），其中此禁用步骤包括将所述第二设备（14）的状态从所述已配置状态（34）改变到所述阻止状态（36）。

13．根据权利要求11所述的配对方法，其特征在于包括当所述第二设备（14）与此网络相连时识别与网络相连的第一监控设备的步骤。

14．根据权利要求13所述的配对方法，其特征在于所述识别步骤由连接第二设备（14）到所述网络、第二设备和常规或随机识别程序的启动构成的事件组的触发事件之一触发。

15．根据权利要求13所述的配对方法，其特征在于所述识别步骤包括所述第一监控设备的验证。

16．根据权利要求15所述的配对方法，其特征在于所述验证通过使用零知识询问/响应协议来实现。

17．根据权利要求16所述的配对方法，其特征在于所述第一监控设备（12）包括用于安全存储由其产生公共标识符V的秘密标识符S的装置（16），所述识别包括询问所述第一监控设备以确定第一监控设备（12）公共标识符V的步骤，以及所述验证包括所述第一监控设备（12）通过使用所述零知识询问/响应协议，向第二设备（14）证明其知道所述秘密标识符S。

18．根据权利要求13所述的配对方法，其特征在于如果所述识别步骤得出所述网络包含对所述第二设备（14）进行配置的第一监控设备（12）的结论，而所述第二设备（14）处于所述阻止状态（36），则将所述第二设备（14）的状态从所述阻止状态（36）改变到所述已配置状态（34）。

安全电子防盗设备、包括这种设备的防盗系统和匹配电设备的方法

技术领域

本发明涉及一种用于连接到包含至少一个监控设备的网络的电设备。本发明还涉及一种包含监控设备与之相连的网络的防盗系统。最后，本发明涉及一种对第一和第二设备进行配对的方法，所述第一设备被称为监控设备。

背景技术

现有技术已经公开了这种用于到包含监控设备的网络的连接的电设备。对所述监控设备进行配置，从而在盗窃的情况下，防止电设备的操作。

例如，在文献WO 98/04967中，其特征为一种保护系统的一种电设备只有其与授权其操作的监控设备相连时才能进行操作。监控设备在关联数据库中管理由惟一标识码标识的电设备列表，并包含针对记录在列表中的设备的操作授权装置。通常，监控设备是固定的、隐藏的、甚或处于远程位置，从而使得窃贼只能窃取与此监控设备相连的电设备。因此，窃贼不能拥有使被盗的设备能够进行工作的监控设备，并且不能使用或重新出售这些设备。

这种系统的缺点在于监控设备对电设备得以操作的授权进行控制。此外，监控设备控制列表上的所有其他设备的操作的授权。在多个电设备与监控设备相连的情况下，这种控制系统可能会变得繁复和困难。

发明内容

本发明的目的在于：通过提供一种能够防盗而无需其与之相关联的监控对电设备列表的管理的电设备，来克服此缺点。

为此，本发明的主题是一种用于连接到包含至少一个监控设备的网络的电设备。所述电设备包含：存储装置；配置装置，用于在存在所述监控设备的情况下，授权电设备操作；识别装置，用于在电设备与包括这种监控设备的任何网络相连时，识别至少一个监控设备；以及禁用装置，如果所识别的监控设备不对应所配置的的电设备的监控设备，或者如果所述网络不包含监控设备，禁用所述电设备。所述电设备的配置装置适用于将针对其配置电设备的监控设备的公共标识符记录在所述电设备的存储装置中。

此外，根据本发明的电设备的特征还在于以下一个或多个特征：

- 所述识别装置包含用于询问任何监控设备以确定监控设备公共标识符的装置；

- 所述识别装置包含用于验证配置了监控设备的验证装置；

- 所述验证装置实现零知识询问/响应协议；

- 所述电设备处于从组件单元之一选择的的状态：原始状态；已配置状态，用于在存在至少一个监控设备的情况下进行操作；以及阻止状态，在激活所述配置装置之后，获得所述已配置状态，以及在激活所述禁用装置之后，获得所述阻止状态；以及

- 所述电设备只在处于已配置状态下时进行操作。

本发明还涉及一种防盗系统，包括至少一个网络和与所述网络相连且包含公共标识符的至少一个监控设备，其特征在于其包含至少一个如上所述的电设备。

此外，根据本发明的防盗系统的特征还在于以下一个或多个特征：

- 所述监控设备包含针对由监控设备产生所述公共标识符的秘密标识符的安全存储装置；以及

- 从以下网络中选择所述网络：电子网络、数字传输网络和电信网络。

最后，本发明的目的是一种用于对第一和第二设备进行配对的方法，其中所述第二设备连接到与所述第一“监控设备”相连的网络。所述方法包括只有在存在所述监控设备的情况下才配置所述第二设备

以授权第二设备操作的步骤。此第二设备配置步骤包括将监控设备公共标识符记录在所述第二设备的存储装置中。

此外，根据本发明的配对方法的特征还在于以下的一个或多个特征：

- 所述第二设备处于从组件单元之一选择的状态：原始状态；已配置状态，用于在存在至少一个监控设备的情况下进行操作；以及阻止状态，以及所述配置步骤包括对所述第二设备的状态的改变，从所述原始状态到所述已配置状态；

- 所述方法包括在此设备与没有配置电设备的监控设备相连时禁用所述第二设备的步骤，其中此禁用步骤包括将所述第二设备的状态从所述已配置状态改变到所述阻止状态；

- 所述方法包括当所述第二设备与此网络相连时识别与网络相连的监控设备的步骤；

- 所述识别步骤由来自由以下事件构成的事件组的触发事件之一触发：所述第二设备与所述网络的连接、所述第二设备和常规或随机识别程序的启动；

- 所述识别步骤包括所述监控设备的验证；

- 所述验证通过使用零知识询问/响应协议来实现；

- 在所述监控设备包括用于安全存储由其产生公共标识符的秘密标识符的装置时，所述识别包括询问所述监控设备以确定监控设备公共标识符的步骤，以及所述验证包括多个步骤，所述监控设备在多个验证步骤中通过使用所述零知识询问/响应协议，向所述电设备证明其知道所述秘密标识符；以及

- 如果所述识别步骤得出针对其对所述第二设备进行了配置的所述监控设备出现在所述监控网络中的结论，同时所述第二设备处于所述阻止状态，则其后为对所述第二设备的状态的改变，从所述阻止状态到所述已配置状态。

附图说明

根据以下仅作为示例且参照附图而给出的描述，本发明将得到

更好的理解，其中：

- 图1示意性地示出了根据本发明的防盗系统；

- 图2示出了针对根据本发明的电设备的状态改变方法的功能图；以及

- 图3示出了根据本发明的用于将电设备与监控设备配对的方法的功能图。

具体实施方式

图1示出了如电力网络、数字传输网络甚或电信网络等本地网络10。监控设备12和电设备14与此本地网络10相连。

监控设备12可以是隐藏的或固定于支撑件上，从而使其难以被盗取。其包括如安全处理器等计算装置16和网络接口18。监控设备12将非常大的保密数S和数V存储在存储器中(在图中未示出)，此后将其称为监控设备12的公共标识符。S和V验证以下公式：

$$S=\sqrt{V}\bmod n$$

其中n是具有秘密因数分解的整数，例如是两个非常大的保密素数的乘积。

容易验证，如果$S=\sqrt{V}\bmod n$，则$S^2=V\bmod n$。

监控设备12还存储由控制授权方利用公共密钥K计算出的公共标识符V的签名SigV。

V和n是公共值，即为监控设备12所知，但其也可以与电设备14进行通信。尽管在构造时，数值n被存储在电设备14中，但数值V在其配置期间被传送给电设备14。

例如，电设备14是家用设备、视听设备、计算机或需要保护以防盗且适合于与网络10相连的任何其他设备。每个电设备14包括如非易失性存储器等存储装置20、如处理器等计算装置22和类似于监控设备12的网络接口18的网络接口24。

计算装置22包括用于配置每个电设备14的装置26、用于识别监控设备的装置28和用于禁用每个电设备14的装置30。有利地，这些装置26、28和30是按照传统方式编程在每个电设备14的处理器22中的软

件装置。

每个电设备14在其存储器20中存储由计算出签名SigV的控制授权方所发布的数值n和公共密钥K。此密钥使其能够根据V的值来验证签名SigV。

在所示实施例中，本发明的目的在于：限制每个设备14对本地网络10的使用，即只有其与监控设备12相连时，每个电设备14才能进行操作。在这种情况下，每个电设备14的存储器20除了n和K之外，只存储监控设备12的公共标识符V。

在另一实施例中，可以将每个电设备14的使用限制于几个本地网络，每个本地网络均具有监控设备。因此，每个电设备14可以与几个监控设备相关联。在这种情况下，每个电设备的存储器20存储其与之相关联的每个监控设备的公共标识符V。

如图2所示，电设备14可以处于三种基本状态：原始状态32、已配置状态34和阻止状态36。

原始状态32对应于其中电设备14的存储器20未存储监控设备公共标识符的状态。

已配置状态34对应于其中电设备14将监控设备12的公共标识符V存储在其存储器20中的状态。于是，只有在存在监控设备12的情况下，即当设备14与监控设备12也与之相连的网络相连时，电设备14才能进行操作。

在另一实施例中，已配置状态对应于其中每个电设备14的存储器20存储几个预定监控设备的公共标识符V的状态。于是，只有在电设备14与其包含有该监控设备的公共标识符V的监控设备之一时，电设备14才能进行操作。

阻止状态36对应于其中由于其与未针对其而配置的监控设备相连，即其不具有公共标识符V，或者其未与任何监控设备相连，尽管已配置，但电设备仍然不能操作的状态。

在本文档的其余部分中，通过存储在其存储器20中的变量e来定义电设备14的状态，如果电设备14处于原始状态32，则向其分配数值0，如果其处于已配置状态34，向其分配数值1，以及如果其处于阻止

状态36，向其分配数值2。

可以通过其中将监控设备12的公共标识符V记录在电设备14的存储器20中从而使电设备14识别监控设备12并能够在其存在的情况下进行操作的配置步骤38，从原始状态32转移到已配置状态34。

在所述实施例中，配置步骤38是自动的，例如，在电设备14与网络10相连期间，或者当第一次启动电设备14时。

作为变体，配置步骤38可以由用户手动触发，例如，通过输入秘密代码、使用物理或电子密钥、或者通过如数字或语音指纹识别等生物装置的用户验证。

已配置状态34通过当电设备14与除针对其而配置的监控设备12以为的其他监控设备（即，其公共标识符V并未被存储在电设备14的存储器20中的监控设备）相连时、或者当其未与任何监控设备相连时而触发的自动禁用步骤40转为阻止状态。

阻止状态36通过自动解除阻止步骤42转为已配置状态34。当被阻止的电设备14再次与电设备14包含针对其的公共标识符V的监控设备12相连时，触发此步骤。于是，在完成了稍后参照图3所述的零知识询问/响应型测试之后，电设备14处于已配置状态34。

作为变体，可以手动地触发解除阻止步骤42，例如，在输入口令期间，在使用物理或电子密钥期间，或在通过生物装置的用户验证期间。

最后，已配置状态34通过复位步骤44转为原始状态32，在复位步骤44期间，授权用户删除存储在电设备14的存储器20中的所有监控设备公共标识符。

在如图3所示的功能图中，对用于将电设备14与任意类型的监控设备46进行配对的方法进行了描述。

此配对方法包括由如电设备14的启动、其与网络的连接或周期性的时钟同步脉冲等触发事件形成的第一初始化步骤48。在任何情况下，均假设电设备与监控设备46也与之相连的网络相连。

在下一步骤50期间，电设备14在网络上发送请求监控设备46的命令，以识别其自身。

接下来，在步骤52期间，监控设备46向电设备14发送其公共标识符V和签名SigV。

在此步骤52之后，电设备14执行测试54。此测试涉及使用由监控设备46发送过来的公共标识符V和存储在电设备14中的公共密钥K来检查签名SigV。

如果测试54的结果是否定的，即如果签名SigV并不对应于所发送过来的标识符V，则将所述方法推迟到初始化步骤48。

如果测试54的结果是肯定的，则对存储在电设备14的存储器20中的变量e进行测试56。

如果变量e为0，即如果电设备14处于原始状态32，则到达步骤58，其间设备14将公共标识符V存储在其存储器20中。步骤58之后为上述配置步骤38。在此步骤期间，变量e取值为1，且电设备14随后处于已配置状态34。然后，过程推迟到初始化步骤48。

如果在步骤56，变量e为1或2，则到达测试步骤60，其间电设备14将由监控设备46发送过来的公共标识符V与存储在其存储器20中的公共标识符V_0进行比较。

如果测试60的结果是否定的，则电设备14执行对变量e的测试61。如果e为2且已经禁止了设备，则到达初始化步骤48。否则，利用为1的e，到达上述禁用步骤40。在此步骤期间，变量e取值为2，即电设备14随后处于阻止状态36。然后，过程推迟到初始化步骤48。

如果测试60的结果是肯定的，则到达步骤62，其间监控46首先通过产生随机数r，触发零知识询问/响应协议。此过程跟随步骤62到86。

跟随此步骤62，到达步骤64，其间监控设备46选择作为从两个数r^2和$r.S$中随机选取的数的安全数G，其中S是监控设备46的保密数。其将安全数G发送给电设备14，而无需告知其选择。

在下一步骤66期间，电设备14将数值A或B随机分配给询问C。然后，其将询问C发送给监控设备46。

在步骤66之后，监控设备46对询问C执行测试68。

如果测试68表示询问C是A，则到达步骤70，其间监控设备46将

数值r^2分配给A，并将A发送回电设备14。

在此步骤70之后，电设备14执行测试72，以检查安全数G的数值。

已知的是，在步骤64之后，安全数G是r^2或$r \cdot S$。由于$A = r^2$，因此存在两种可能性：或者$G = A$（其中$G = r^2$），或者$r^2 \cdot S^2 = A \cdot V \bmod n$（其中$G = r \cdot S$）。事实上，在后一种情况下，如果公共标识符V对应于监控设备46，即如果$S^2 = V \bmod n$，则$r^2 \cdot S^2 = A \cdot V \bmod n$。所以，如果V事实上是监控设备46的标识符，则$G = A$或$G^2 = A \cdot V \bmod n$。

如果测试72是肯定的，即如果$G = A$或者如果$G^2 = A \cdot V \bmod n$，则到达步骤74，其间将数值1赋予e，即将电设备设置为已配置状态34。

在此步骤74之后，到达触发事件监视步骤76。在此步骤76期间，一旦检测到属于预定触发事件集合的触发事件，就到达步骤62。例如，这些触发事件与步骤48的那些触发事件相同。

如果测试72是否定的，即如果$G \neq A$或者如果$G^2 \neq A \cdot V \bmod n$，则到达步骤78，其间将数值2赋予e，即将电设备设置为阻止状态36。

在此步骤78之后，到达触发事件监视步骤76。

如果测试步骤68表示询问C是B，则到达步骤80，其间监控设备46将数值$r \cdot S$分配给B，并将B发送给电设备14。

在此步骤80之后，电设备14执行测试82，以检查安全数G的数值。

已知的是，在步骤64之后，安全数G是r^2或$r \cdot S$。由于$B = r \cdot S$，因此存在两种可能性：或者$G = B$（其中$G = r \cdot S$），或者$r^2 \cdot S^2 = G \cdot V \bmod n$（其中$G = r^2$）。事实上，在后一种情况下，如果公共标识符V对应于监控设备46，即如果$S^2 = V \bmod n$，则$r^2 \cdot S^2 = G \cdot V \bmod n$。所以，如果V事实上是监控设备46的标识符，则$G = B$或$B^2 = G \cdot V \bmod n$。

如果测试82是肯定的，即如果$G = B$或者如果$B^2 = G \cdot V \bmod n$，则到达步骤84，其间将数值1赋予e，即将电设备设置为已配置状态34。

在此步骤84之后，到达触发事件监视步骤86。

如果测试82是否定的，即如果$G \neq B$或者如果$B^2 \neq G \cdot V \bmod n$，则到达步骤86，其间将数值2赋予e，即将电设备设置为阻止状态36。

在此步骤78之后，到达触发事件监视步骤76。

在本发明的优点中，应当注意的是，其使每个电设备只在存在

针对其而配置的监控设备的情况下才能进行操作，而无需监控对授权设备列表进行管理。

还应当注意的是，本发明允许自动防盗测试，而无需任何中心权威机构的干涉。

最后，由于将零知识询问/响应协议用于验证，在电设备14中未存储任何秘密信息。

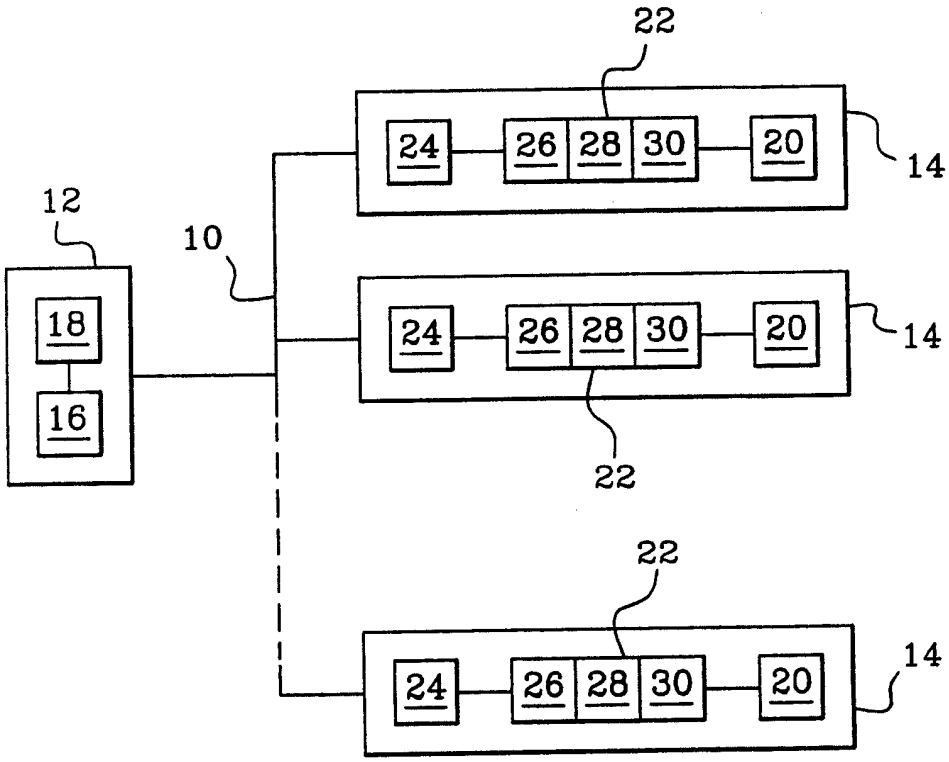


图 1

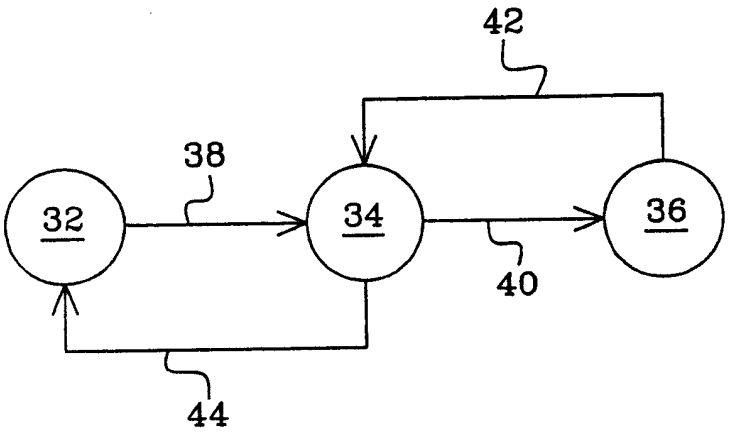


图 2

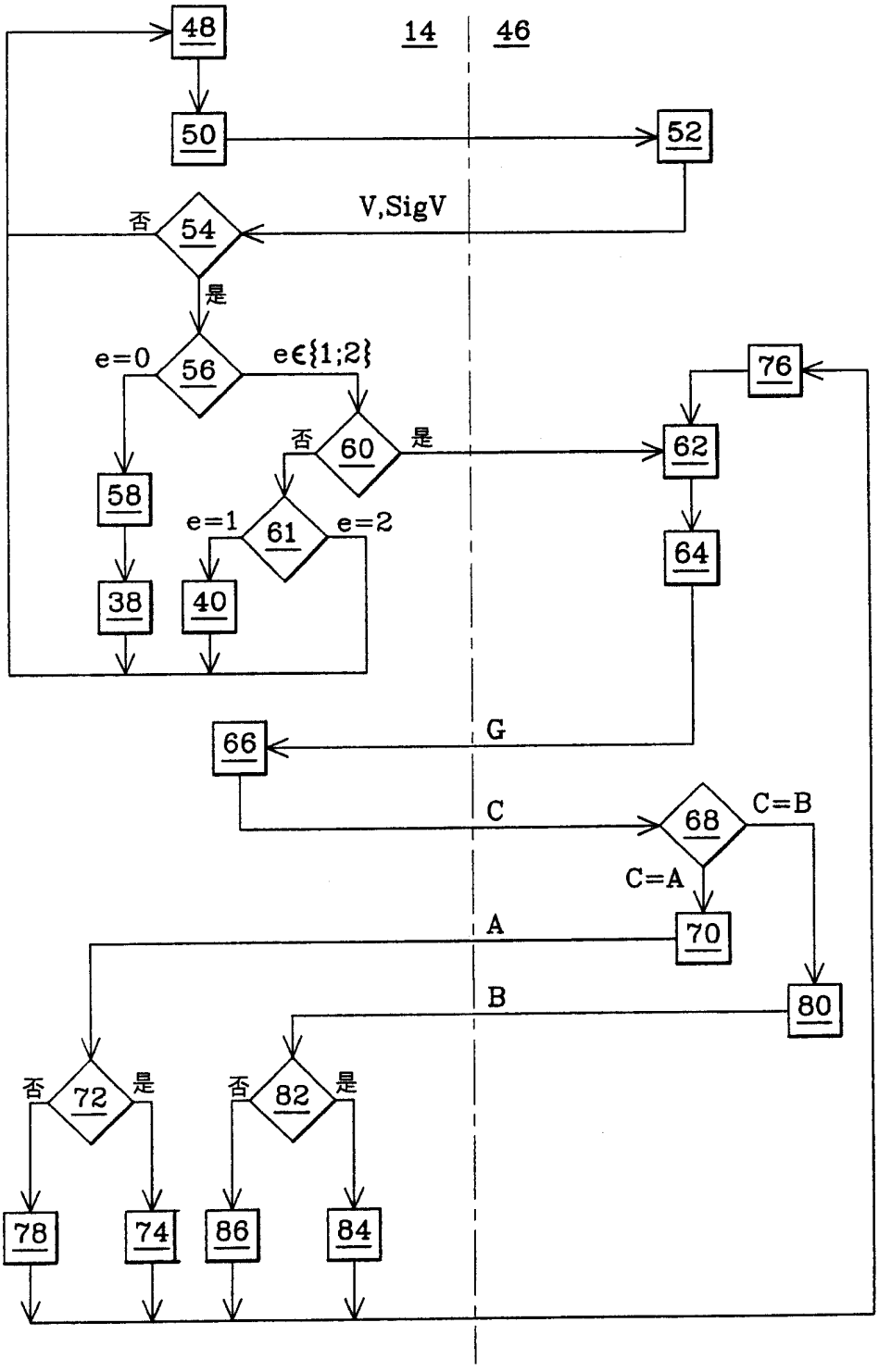

48
14
46
50
52
V,SigV
否
54
是
e=0
56
e∈{1;2}
76
否
60
是
62
58
e=1
61
e=2
64
38
40
66
G
C
68
C=B
C=A
70
A
B
80
否
72
是
否
82
是
78
74
86
84

图 3