[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07D 7/00

[12] 发明专利说明书

[21] ZL 专利号 96190362.7

[45] 授权公告日 2003 年 9 月 10 日

[11] 授权公告号 CN 1121019C

[22] 申请日 1996.3.19 [21] 申请号 96190362.7
[30] 优先权
[32] 1995.3.23 [33] DE [31] 19510626.1
[86] 国际申请 PCT/EP96/01178 1996.3.19
[87] 国际公布 WO96/29683 德 1996.9.26
[85] 进入国家阶段日期 1996.12.18
[71] 专利权人 吉赛克与德弗连特股份有限公司
地址 联邦德国慕尼黑
[72] 发明人 博多·艾伯特 威廉·邦特谢克
审查员 孙桂敏

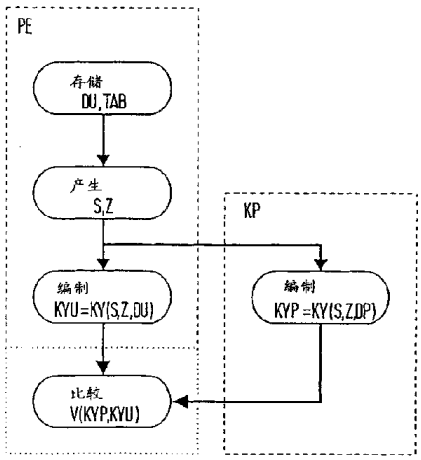
[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄 敏

权利要求书 2 页 说明书 8 页 附图 9 页

[54] 发明名称 用于测试片状材料处理装置中所存储数据完整性的方法

[57] 摘要

本发明涉及一种通过测试装置测试片状材料处理装置中所存储数据的完整性的方法。为了测试被存储数据的完整性，首先在处于完整状态的处理装置的某一工作状态下，将来自处理装置的一个组件的对应于被测试数据的完整数据存储在测试装置中。为了检验组件中被测试数据的完整性，在测试装置中为每一次测试产生一个密钥。采用这一密钥和一种密码算法来编制两个密码。其中一个密码由处理装置的一个组件根据需要被测试数据来编制，该组件中存储了需要测试的数据；另一密码由测试装置根据完整数据来编制。此后，对上述两个密码进行相互比较。如果密码相符，则被测试的数据与完整数据相符，从而判断出没有出现不希望的改变。



ISSN1008-4274

1、一种通过测试装置测试片状材料处理装置中所存储的数据的完整性的方法，所述片状材料是纸币或有价证券，该处理装置具有多个用于处理片状材料的组件，其特征在于进行如下的步骤：

在测试装置(PE)中存储完整的数据(DU)，该完整数据(DU)对应于来自处于完整状态下的处理装置的一个组件(KP)的要被测试数据(DP)；

由其数据需要被测试的组件(KP)编制第一密码(KYP)，该第一密码(KYP)是通过密码算法(KY)和密钥(S)，根据来自该组件(KP)的要被测试数据(DP)计算出来的；

由测试装置(PE)编制第二密码(KYU)，该第二密码(KYU)是通过密码算法(KY)和密钥(S)，根据完整数据(DU)计算出来的；

对所述第一密码(KYP)和第二密码(KYU)进行比较(V)；

由所述测试装置(PE)来产生所述密钥(S)；以及

在对数据完整性的每一次测试中所述密钥(S)各不相同。

2、如权利要求 1 所述的方法，其特征在于将数表(TAB)存储在测试装置(PE)中，用于测试来自处理装置的多个组件(10、20、30)的被存储数据，将下述数据存储在所述数表(TAB)中：

需要予以测试的是所述多个组件(10、20、30)中的哪些组件；

在哪些存储区域(SP)中存储了来自特定组件的要被测试数据(DP)；

在测试装置(PE)的哪些存储区域(SU)中存储了相应的完整数据(DU)。

3、如权利要求 2 所述的方法，其特征在于可以采用直接物理存储地址和/或逻辑名称来访问所述存储区域(SP)和所述测试装置(PE)的存储区域(SU)。

4、如权利要求 1 所述的方法，其特征在于在执行密码算法(KY)之前通过加入随机数(Z)来使所述完整数据(DU)和所述要被测试数据(DP)动态化。

5、如权利要求 1 所述的方法，其特征在于所述密码算法首先采用一种压缩方法来压缩所述完整数据(DU)和所述要被测试数据(DP)，然后通过采用密钥(S)的编码方法(VV)对经过压缩的数据(KD)进行编码。

6、如权利要求 1 所述的方法，其特征在于为了编制第二密码(KYU)：

将完整的数据(DU)和密钥(S)或随机数(Z)通过数据线(104、105)由测试

装置(PE)传送到计算装置(RE);

由计算装置(RE)计算出第二密码(KYU);

计算装置(RE)通过数据线(104、105)将第二密码(KYU)传送到测试装置(PE)。

7、如权利要求 6 所述的方法，其特征在于所述计算装置是处理装置的一个组件(50)。

8、如权利要求 6 所述的方法，其特征在于所述计算装置(RE)是一个外部的装置。

9、如权利要求 1 所述的方法，其特征在于所述测试装置(PE)是处理装置的另一个组件(10)。

10、如权利要求 1 所述的方法，其特征在于所述测试装置(PE)是一个外部装置(40)。

11、如权利要求 10 所述的方法，其特征在于通过可携带的载体(101)在处理装置和外部装置(40)之间传输测试所需的数据。

12、如权利要求 10 所述的方法，其特征在于通过数据线(102、103)在处理装置和外部装置(40)之间传输测试所需的数据。

13、如权利要求 1 所述的方法，其特征在于所述比较(V)由测试装置(PE)来进行。

14、如权利要求 1 所述的方法，其特征在于以可读方式输出所述第一密码(KYP)和所述第二密码(KYU)，由处理装置的操作者(BD)来进行所述比较(V)。

15、如权利要求 1 所述的方法，其特征在于所述处理装置可以工作在不同的工作状态(BZ)，并且其特征还在于哪一个组件(KP)需要予以测试至少部分地取决于某一个工作状态(BZ)。

16、如权利要求 2 所述的方法，其特征在于所述处理装置可以工作在不同的工作状态(BZ)，其中对于每个工作状态(BZ)将数据存储在数表中，所述数据至少部分地取决于相应的工作状态(BZ)。

用于测试片状材料处理装置中所存储数据完整性的方法

本发明涉及一种对片状材料处理装置中所存储数据的完整性(intactness)进行测试的方法，所述片状材料可以是例如纸币或有价证券。

这样的处理装置通常包括若干组件，其中每一组件在对片状材料进行处理的过程中实现一定的功能。该处理装置的一个组件是控制装置，其重要性高于其余的组件。该控制装置控制处理装置的各个运作。其余的组件被设计成模块，用于实现对片状材料的实际处理。单个模块的处理操作可以是例如将叠放在一起的片状材料分离开来、测试片状材料的状态或真伪、传送片状材料、堆积或销毁片状材料。

处理装置的组件可以装有存储器，用于存储操纵处理装置所需的数据。这些数据可以是例如控制命令、程序、结果数据或基准数据。将处理装置的单个组件彼此连接起来，使得能够在它们之间进行数据传输。

上述处理装置可以在不同的操作状态下工作。所述工作状态可以例如由操作者通过输入一定的参数来确定。这样的参数可以是需要测试的张数、纸币的金额、某种测试标准的类型或等级或者类似的信息。

德国专利 DE－PS 27060453 号披露了一种这样的处理装置。为了存储数据，所述控制装置和单个的模块都设有各自的存储器，用于存储操纵处理装置所需的数据。通过一个主存储器来进行控制装置和模块之间的数据交换，所述控制装置和模块都可以访问该主存储器。此外，各个模块也都直接相互连接起来，以便进行数据交换。

德国专利申请公开 DE－OS 3347607 号披露了一种处理装置，其中采用了多个相似的模块，用于对片状材料进行光学测试。其中控制装置和单个的模块都具有用于存储数据的存储器。通过数据总线将单个的模块彼此连接起来并与控制装置相连接。此外，在该数据总线上还连接了一个级别更高的存储器，所有的组件都可以访问该存储器。

在上述类型的装置中，存储在处理装置中的数据有可能会出现不希望的变化。这些变化既可以是处理装置中的干扰所引起的，例如数据传输错

误或者数据的丢失，也可以是出于欺骗目的而对数据进行有意处置所引起的。

已知装置都没有设置用来查明存储在处理装置中的数据中的不希望变化的措施。

本发明的目的是为解决上述问题，提供一种对片状材料处理装置中所存储数据的完整性进行测试的方法，能够对所述数据的变化进行核实。

上述问题是通过本发明的技术方案来解决的。按照本发明的一种通过测试装置测试片状材料处理装置中所存储的数据的完整性的方法，所述片状材料可以是纸币或有价证券，该处理装置具有多个用于处理片状材料的组件，其特征在于进行如下的步骤：在测试装置中存储完整的数据，该完整数据对应于来自处于完整状态下的处理装置的一个组件的要被测试数据；由其数据需要被测试的组件编制第一密码，该第一密码是通过密码算法和密钥，根据来自该组件的要被测试数据计算出来的；由测试装置编制第二密码，该第二密码是通过密码算法和密钥，根据完整数据计算出来的；对所述第一和第二密码进行比较；由所述测试装置来产生所述密钥；以及在对数据完整性的每一次测试中所述密钥各不相同。

本发明的基本构思是首先在处于完整状态的处理装置的某一操作状态下，将对应于处理装置的一个组件的被测试数据的完整数据存储在一个测试装置中。为了检验该组件中的被测试数据的完整性，在测试装置中为每一次测试产生一个密钥，该密钥不同于先前测试中使用过的密钥。采用上述密钥和一种密码算法来编制两个密码。其中一个密码由处理装置的所述组件根据被测试的数据来编制，在该组件中存储了需要测试的数据；另一个密码由测试装置根据上述完整数据来编制。此后，将上述两个密码进行相互比较。如果密码相符，则被测试的数据与完整数据相符，从而判断没有出现不希望的改变。

这种方法的一个优点是其中一个密码由测试装置计算，另一个密码由被测试的组件计算产生。这也分割了形成密码所需的计算容量。

另一优点是在每一次测试中产生的密钥都不同于先前测试中使用过的密钥。因此，不必对密钥采取保密措施，不存在密钥被窃取的危险。

可以通过在每一次测试中加入一个随机数，使得用于编制密码的任选数据动态化。当对同样的数据进行多次测试时，是经过该动态化处理之后

的数据所编制的密码就会各不相同。这就防止了通过重放先前测试中的密码来对进行欺骗性测试操作。

为了编制所述密码，最好选择一种这样的密码算法，它同时还能够实现数据的压缩。由此产生的密码与原始数据量相比具有相对较小的数据量。这些密码的较小数据量使得它们能够更为方便和快速地进行交换和比较。

根据本发明，来自处理装置的多个组件的被存储数据也可以在一次操作中予以测试。为此，在测试装置中存储了一个数表，根据其组件需要被测试的处理装置的工作状态，在该数表中指明在哪些存储区域中存储了来自特定组件的被测试数据，在测试装置的哪些存储区域中存储了相应的完整数据。采用这一数表，测试装置就能够编制为检验单个组件所需的密码，并将这些密码与特定组件所产生的密码进行比较。

本发明的进一步的特点能够由以下的描述中看出。下面将结合附图对本发明的实施例进行详细说明，其中：

图 1 是本发明第一种实施例的流程图；

图 2 示出了密码算法的两种实施例的流程图；

图 3 是处理装置的方框图；

图 4 示出了本发明第一种实施例的第一种实现方式；

图 5 是包括处理装置和辅助装置的系统的方框图；

图 6 示出了本发明第一种实施例的第二种实现方式；

图 7 是本发明第二种实施例的流程图；

图 8 是经过扩充的处理装置的方框图；

图 9 示出了本发明第二种实施例的实现方式。

图 1 是本发明第一种实施例的流程图。为了通过检测装置 PE 来测试片状材料处理装置的组件 KP 中存储的数据的完整性，首先将完整的数据 DU 存储在测试装置 PE 中。在处于完整状态下的处理装置的某一工作状态 BZ 中，上述完整数据 DU 对应于处理装置的组件 KP 中需要测试的数据 DP。

在对处理装置的组件 KP 存储的数据的每一次测试中，测试装置 PE 都会产生一个密钥 S，该密钥在每次数据完整性测试中是不同的。该密钥 S 用于通过一种密码算法 KY 来产生一种密码。测试装置 PE 也能产生任选的一个随机数 Z，用于使数据 DP 或 DU 动态化。

随后，将编制密码所需的数据 S 或 Z 由测试装置 PE 传输到需要测试的

组件 KP。在测试装置 PE 和被测试组件 KP 中均采用该密码算法 KY 和密钥 S 或随机数 Z 来计算出密码。在处理装置的组件 KP 中，根据需要测试的数据 DP 来编制密码 KYP。在测试装置 PE 中，根据所述完整数据 DU 来编制密码 KYU，该完整数据 DU 对应于完整状态下的被测试数据 DP。

随后，在比较 V 中对密码 KYU 和 KYP 进行比较。为此，将密码 KYP 由需要测试的组件 KP 传输到测试装置 PE。上述比较 V 例如可以直接由测试装置来进行。另一种进行比较 V 的方式是以可读方式输出密码 KYU 和密码 KYP，然后由处理装置的操作者 BD 来进行密码的比较 V。

如果需要测试的是处理装置中的几个组件，或者处理装置的不同工作状态 BZ 中的一个组件，或者是上述两种可能性的结合，则可选择地在测试装置中存储一个数表 TAB。在上述数表 TAB 中，根据其组件需要予以测试的处理装置的可能工作状态 BZ，指明在哪些存储区域 SP 中存储了特定组件的需要测试的数据 DP，在测试装置 PE 的哪些存储区域 SU 中存储了所述完整数据 DU。此外，根据处理装置的各种可能的工作状态，将所有的完整数据 DU 都存在测试装置的上述数表 TAB 中。

可以采用例如直接物理存储器地址或者逻辑名称来确定存储区域 SP 或 SU。直接物理存储器地址通常用于半导体存储器，例如 RAM、ROM、EPROM、EEPROM 或者类似存储器。通过例如指定存储器中的起始地址和结尾地址，或者通过指定存储器中的起始地址和存储区域的长度来确定存储区域。对于大容量存储器来说，例如硬盘、磁盘、CDROM 驱动器或类似存储装置，通常采用逻辑名称(文件名)来确定一定的存储区域。

图 2a 示出了密码算法 KY 的一种实施例。在执行实际密码算法 KY 之前，可以通过加入随机数 Z，使需要予以编码的数据 DU 或 DP 动态化。可以进行这种动态化处理，以便采用本来是相同的密码算法 KY 获得不同的密码 KYU 或 KYP。这一步骤可以防止通过对处理装置的欺骗性操作由已往的测试来盗窃密码，进而在处理装置中重新使用来模仿正确的测试。

采用压缩方法 KV，对采用随机数 Z 予以动态化之后的数据 DU 或 DP 进行压缩。随后，通过采用密钥 S 的编码方法 VV 对经过压缩所获得的数据 KD 进行编码。采用编码方法 VV 获得的结果就是所需要的密码 KYU 或 KYP。

可以采用所有的公知方法来进行上述压缩和编码。已知的压缩方法例

如可以是散列函数。所采用的编码方法 VV 例如可以是数据加密标准(DES)或者诸如 RSA 算法之类的公共密钥(Public key)方法。

图 2b 示出了密码算法 KY 的另一种实施例。根据这种实施例，首先在需要编码的数据 DU 或 DP 中加入密钥 S，然后采用压缩方法 KV 直接将它们压缩成为密码 KYU 或 KYP。一般说来，也可以采用其他类型的密码算法 KY。

图 3 是片状材料处理装置的结构方框图。它包括 3 个组件 10、20、30，通过数据线 100 将这些组件彼此连接起来。控制组件 10 是一个其重要地位高于其他组件的组件，用于控制其他单个组件的运行。该控制组件 10 除了其他部分之外，主要包括处理器 11，它可以访问半导体存储器 12 和大容量存储器 13。

半导体存储器 12 可以由易失性 RAM 或非易失性 ROM、EPROM、EEPROM 或类似存储器构成。在执行程序的过程中处理器 11 通常是采用易失性 RAM。非易失性存储器中存储用于操纵该处理装置所需的数据。通常采用直接物理存储器地址来确定半导体存储器 12 的存储区域。

大容量存储器 13 用于存储大量的数据，可以采用例如硬盘、磁盘、CD－ROM 驱动器或类似存储装置来实现。大容量存储器 13 中存储操纵处理装置所需的数据。大容量存储器 13 的存储区域通常采用逻辑名称来确定。

如图所示的处理装置另外的组件是两个模块(module)20 和 30。尽管它们具有相同的方框结构，但是在处理装置对片状材料进行处理的过程中却能够实现不同的功能。在图中将模块的数目表示为两个仅仅是为了清楚起见。

与控制装置 10 相似，每一个模块 20、30 都分别具有处理器 21、31，半导体存储器 22、32 和大容量存储器 23、33。存储在存储器 22、23、32、33 中的数据用于操纵相应的模块。

存储在存储器 12、13、22、23、32、33 中的数据一般是不同的，通常取决于处理装置的工作状态 BZ 和组件的功能。

在图 4 所示的本发明第一种实施例的第一种实现方式流程图中，测试装置 PE 的功能由控制装置 10 来完成。与在完整状态之下存储在存储器 12、13、22、23、32、33 中的被测试数据 DP 相对应的完整数据 DU 如图 3 所示被存储在控制装置 10 的大容量存储器 13 的相应存储区域 D12、D13、D22、

D23、D32、D33 中。此外，在大容量存储器 13 中还存储了相应的数表 TAB，用于对处理装置的多个组件进行测试。为测试所需的密码 KYU 由控制装置 10 编制。相应的密码 KYP 由被测试的组件编制。被测试的组件 KP 可以是模块 20 或 30 或者是控制装置 10 本身。随后，由控制装置 10 来进行所编制的密码 KYU 或 KYP 的比较 V，或者由控制装置 10 以可读方式输出所述密码，以便由处理装置的操作者可以进行该比较 V。

图 5 示出了配有一个辅助装置 40 的处理装置的结构方框图。该辅助装置 40 可以是一个个人计算机，可以将该计算机置于不同于处理装置的位置。所述辅助装置 40 也包括一个处理器 41、半导体存储器 42 和大容量存储器 43。由于辅助装置 40 被用于执行如下的测试装置 PE 的功能，因此将测试所需的完整数据 DU 或数表 TAB 存储在辅助装置 40 的大容量存储器 43 中。

为了进行测试，所述辅助装置 40 与处理装置之间所需的数据交换可以通过不同的方式来进行。其中一种可行的方式是由辅助装置 40 将该数据写在一个可携带的数据载体 101 上，然后将该载体 101 送入到控制装置 10 中。上述可携带的数据载体可以是例如芯片卡或软盘。

另一种可行的方式是提供数据线 102，用于在控制装置 10 与辅助装置 40 之间进行数据交换。根据具体空间状况，上述数据线可以是直接连接两个组件或者是直接连接一个网络组成。

再一种可行方式是将辅助装置 40 直接与处理装置的内部数据线 100 相连接。在这样的情况下，可以将辅助装置 40 看作是处理装置的一个组件。

图 6 示出了本发明第一种实施例的第二种实现方式的流程图，亦即采用辅助装置 40 的处理装置的流程图。如上所述，完整数据 DU 或数表 TAB 被存储在辅助装置 40 中。在辅助装置 40 中产生另外的密钥或随机数 Z。为了测试存储在处理装置中的数据的完整性，通过上述连接 101、102、103 中的一个将密钥 S 和随机数 Z 传输到控制装置 10。

为了测试数据的完整性，此时必须将控制装置 10 置于检查所需的工作状态 BZ。这一点可以通过由操作者直接将信息输入到控制装置 10 之中来实现，也可以通过由辅助装置将相应的信息传送到控制装置 10 来实现。根据这样的信息，控制装置 10 就能够将处理装置置于所需的工作状态 BZ。

根据所需的工作状态 BZ，通过辅助装置 40 可以将测试所需的信息，亦即被测试的是哪个组件以及来自特定组件 10、20、30 的被测试数据 DP

被存储在哪个存储区域SP中，从数表TAB中读出，并传送到控制装置10中。

另一种可行的方式是将数表TAB复制件存储在控制装置10中。此后，控制装置10就能够根据选择的工作状态BZ，从复制的数表TAB中直接读出所需的信息。

辅助装置40随后编制所需的密码KYU，同时在处理装置的特定组件10、20、30中编制为进行比较所需的密码KYP。

为了密码KYU和密码KYP的比较V，现在可以将密码KYU由辅助装置40传输到控制装置10中，以便在控制装置10中进行比较。此外，也可以从控制装置10中以可读方式输出密码KYU和密码KYP。此后，由处理装置的操作者来进行密码的比较。

如果选用可携带的数据载体101来作为辅助装置40和控制装置10之间的传送介质，为了更为经济起见，可以在一个工作步骤中将密钥S或随机数Z以及编制的KYU写在可携带的数据载体101上，然后立即送到控制装置10中。

图7是本发明另一种实施例的流程图。如果需要对处理装置中多个组件的被存储数据进行测试，在测试装置PE中就必须编制多个密码KYU。在这一实施例中，为了减轻测试装置PE，将密码的计算转移到附加的计算装置RE。为此，将计算密码所需的完整数据DU和密钥S或随机数Z转移到该计算装置RE之中。此后，由计算装置RE根据完整数据DU来编制密码KYU，并将该密码KYU送回到测试装置RE。其余的方法步骤与上述第一种实施例的步骤相似。

图8示出了一种经过扩充的处理装置，它具有附加的计算装置50。该计算装置50也具有处理器51、半导体存储器52和大容量存储器53。计算装置50例如可以采用个人计算机来实现。计算装置50通过与数据线102相似的数据线104，或者通过与数据线103相似的数据线105与处理装置相连接。

尽管从理论上讲可以采用可携带的数据载体来连接计算装置50和控制装置10，但是在本实施例中不推荐采用这种方式，因为这样需要将数据量很大的完整数据DU由控制装置10全部转移到计算装置50中。

图9是在配有计算装置50的处理装置中实现本发明第二种实施例的流

程图。该流程图与图 4 所示的实现第一种实施例的流程图之间的区别点仅仅在于密码 KYU 的计算是在计算装置 50 中进行，然后再将该密码转移到控制装置 10 中。同样，对密码 KYP 和 KYU 的比较 V 即可以直接在控制装置 10 中进行，也可以在以可读方式输出该密码之后由处理装置的操作者来进行。

总之，也可以采用说明书中没有提到的另外的实施方式来实施本发明。可以采用单个的方式为单个的组件提供上述实施例中提到的存储器，如果希望的话，甚至可以部分地省略它们。

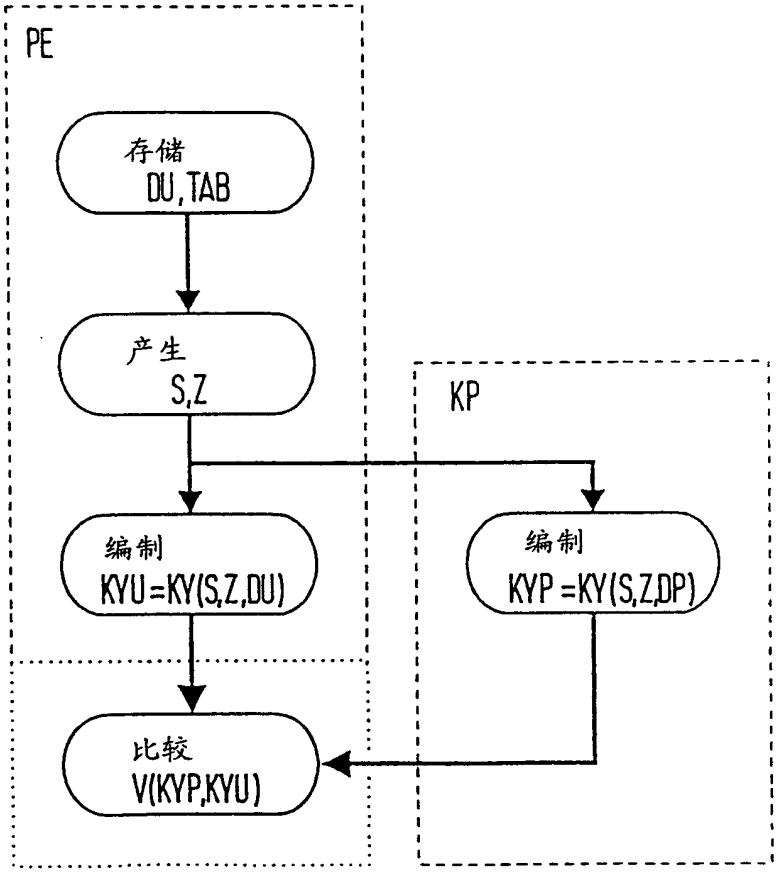


图 1

图 2 a

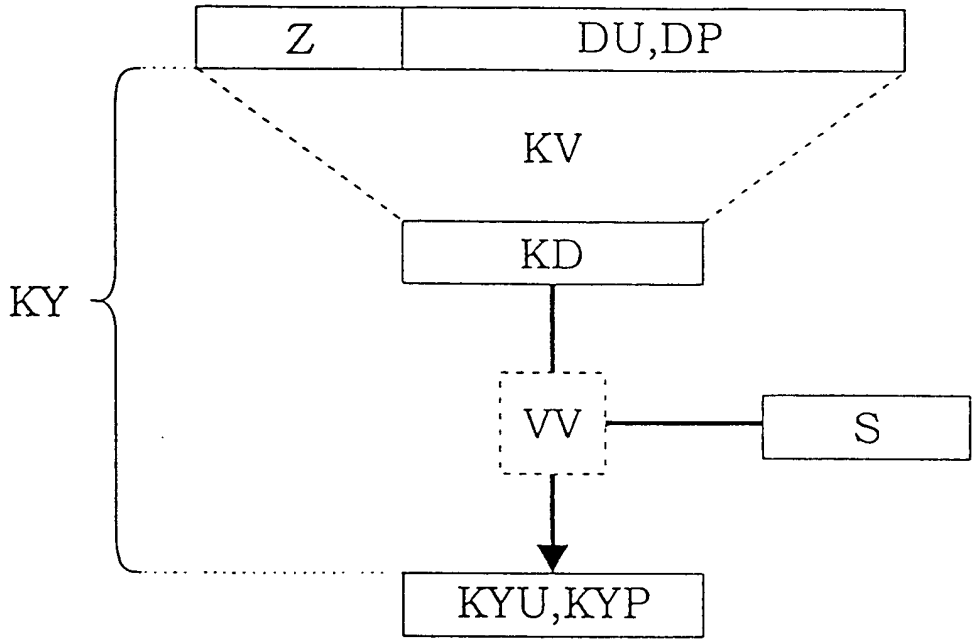


图 2 b

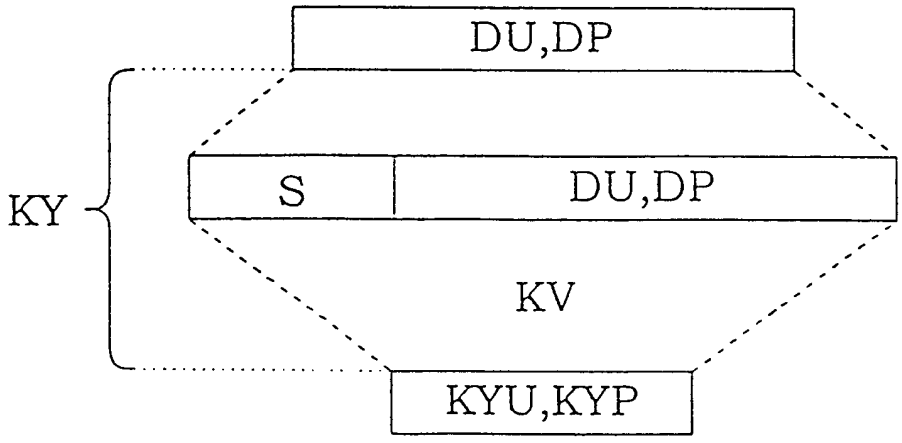
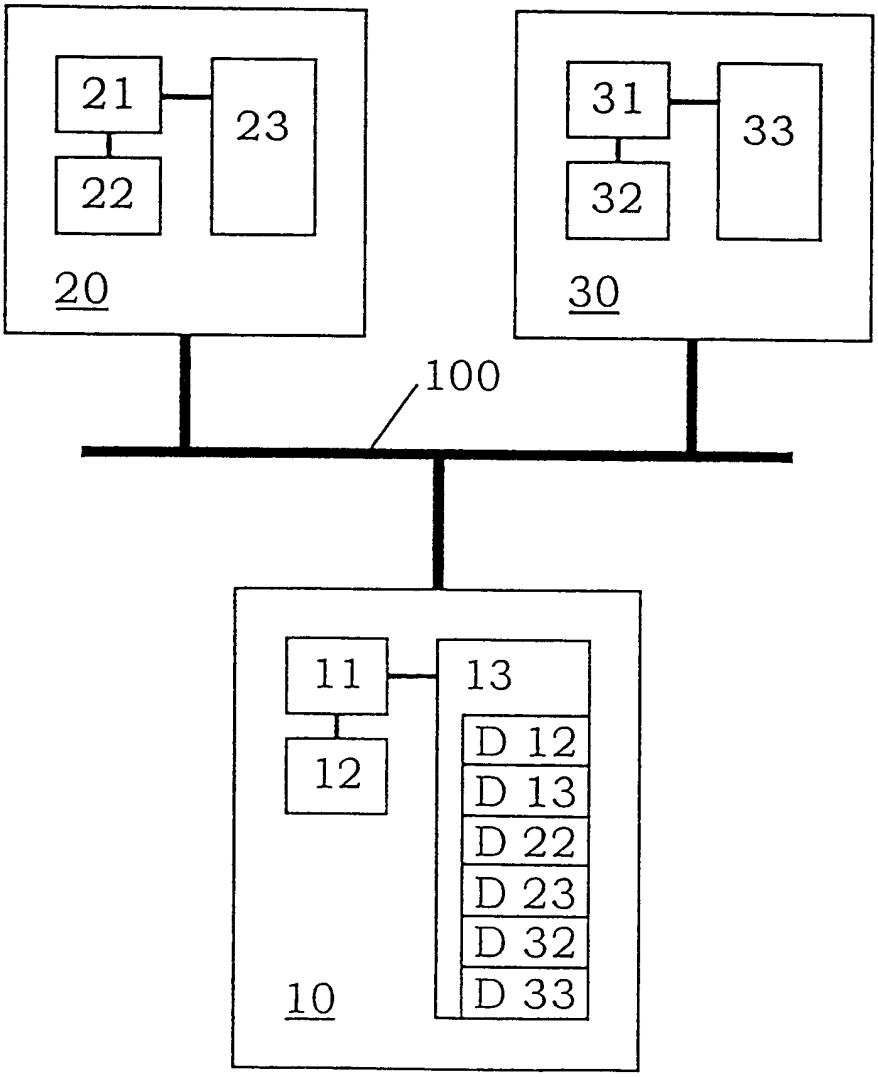


图 3



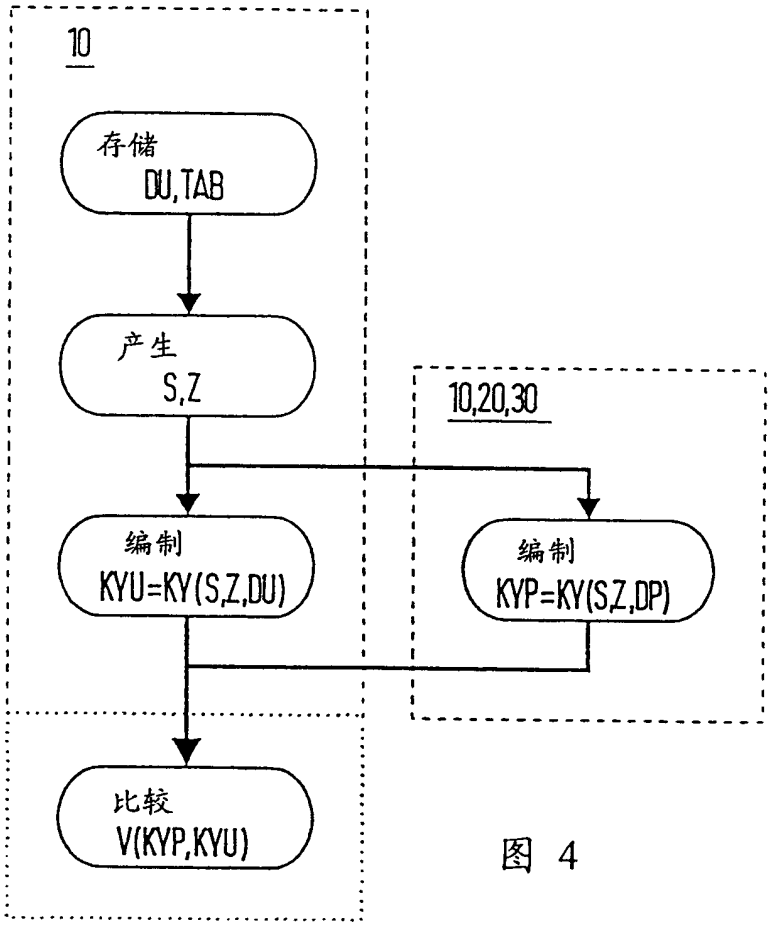
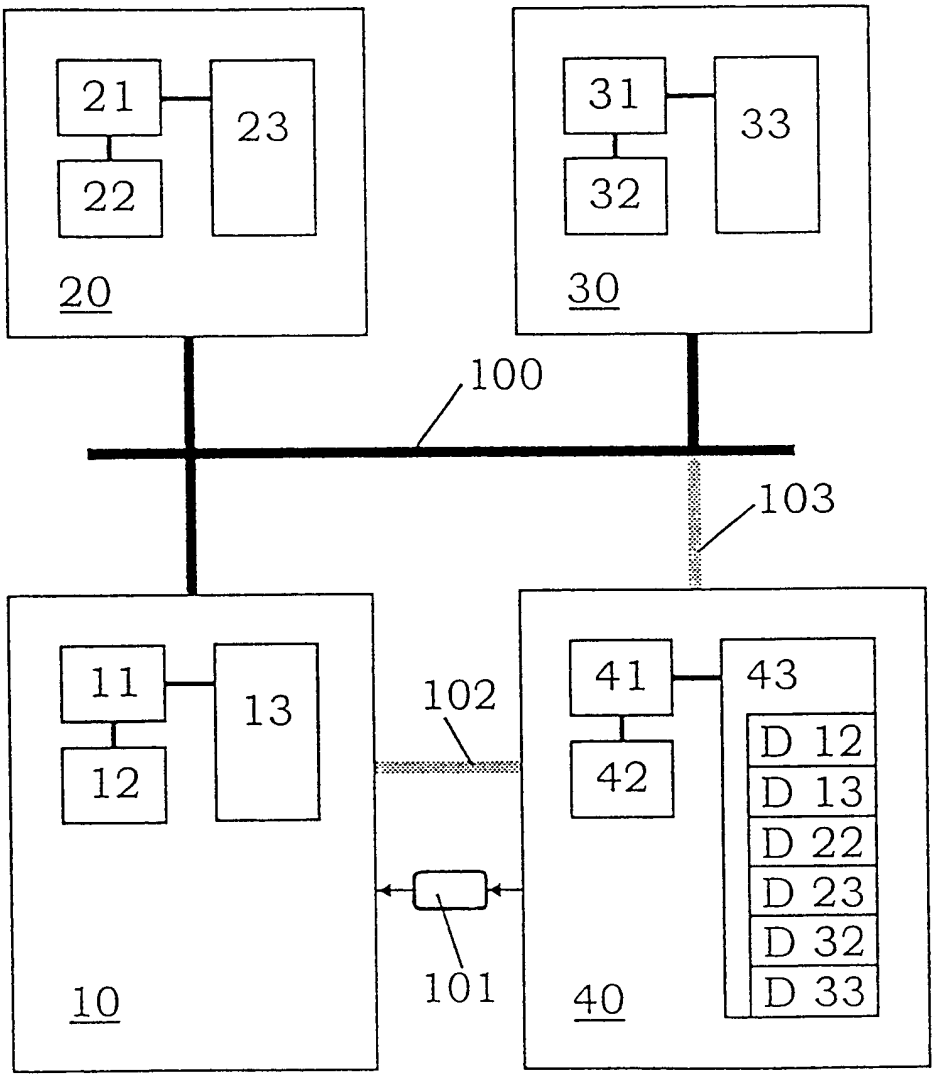

10
存储
DU,TAB
产生
S,Z
编制
KYU=KY(S,Z,DU)
比较
V(KYP,KYU)
10,20,30
编制
KYP=KY(S,Z,DP)

图 4

图 5


21
23
22
20
31
33
32
30
100
103
11
13
12
102
41
43
D 12
D 13
D 22
D 23
D 32
D 33
42
101
10
40

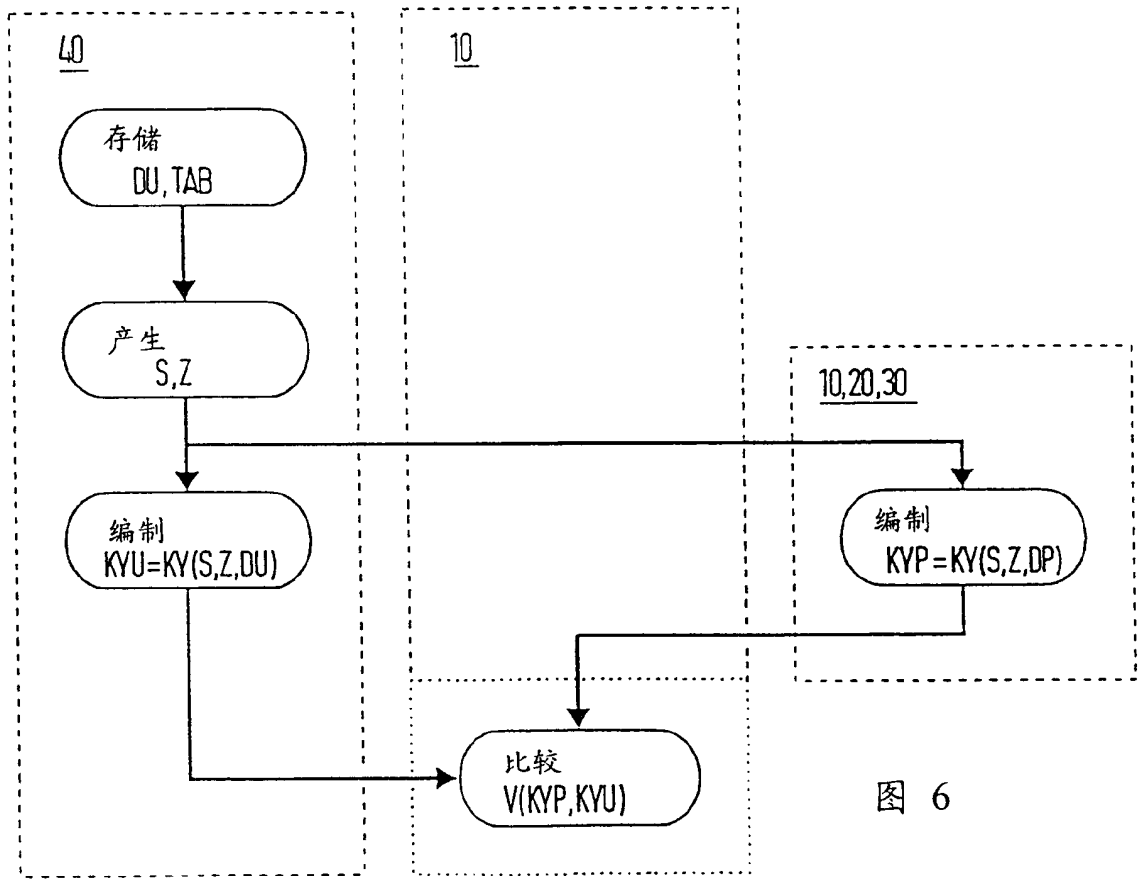

40
10
存储
DU,TAB
产生
S,Z
编制
KYU=KY(S,Z,DU)
10,20,30
编制
KYP=KY(S,Z,DP)
比较
V(KYP,KYU)

图 6

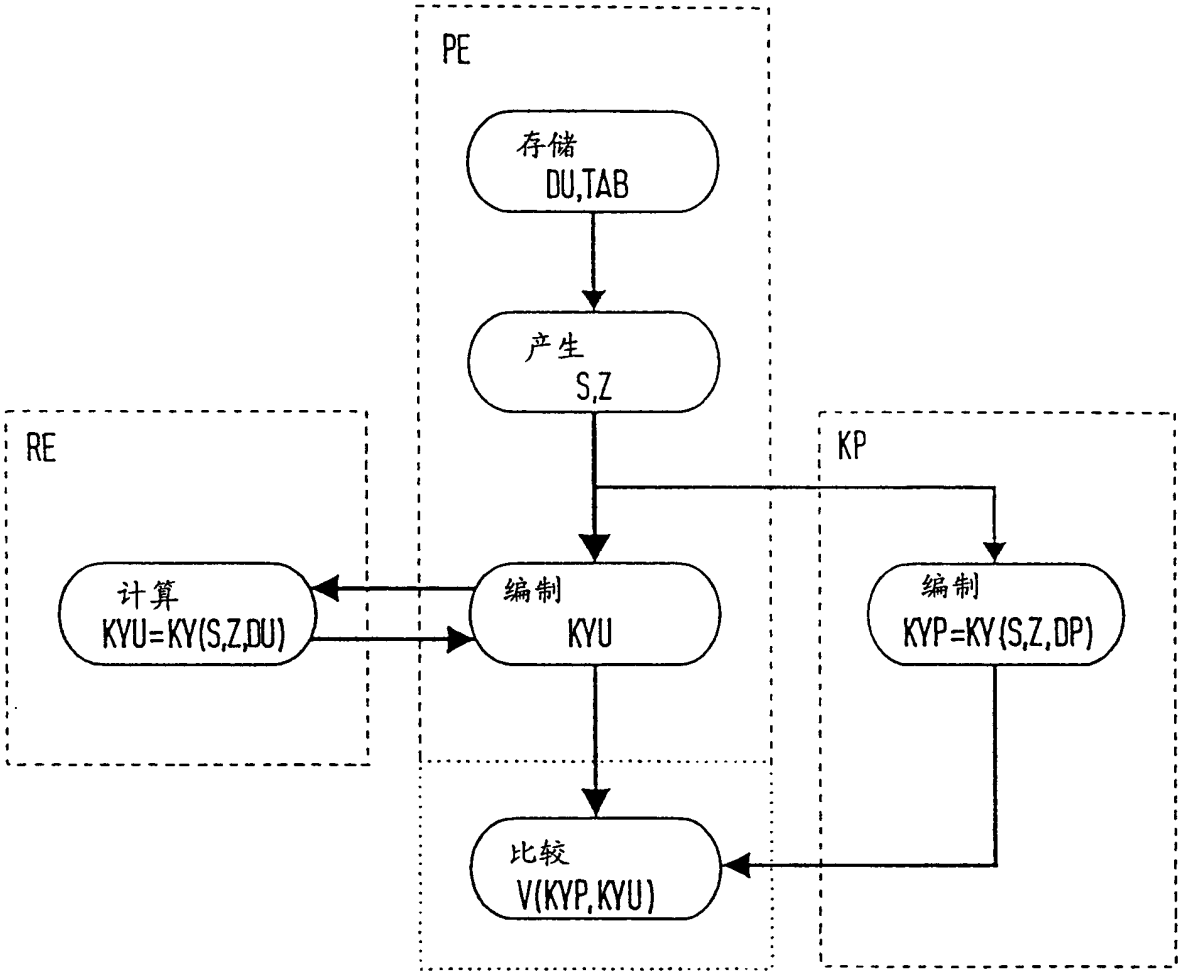
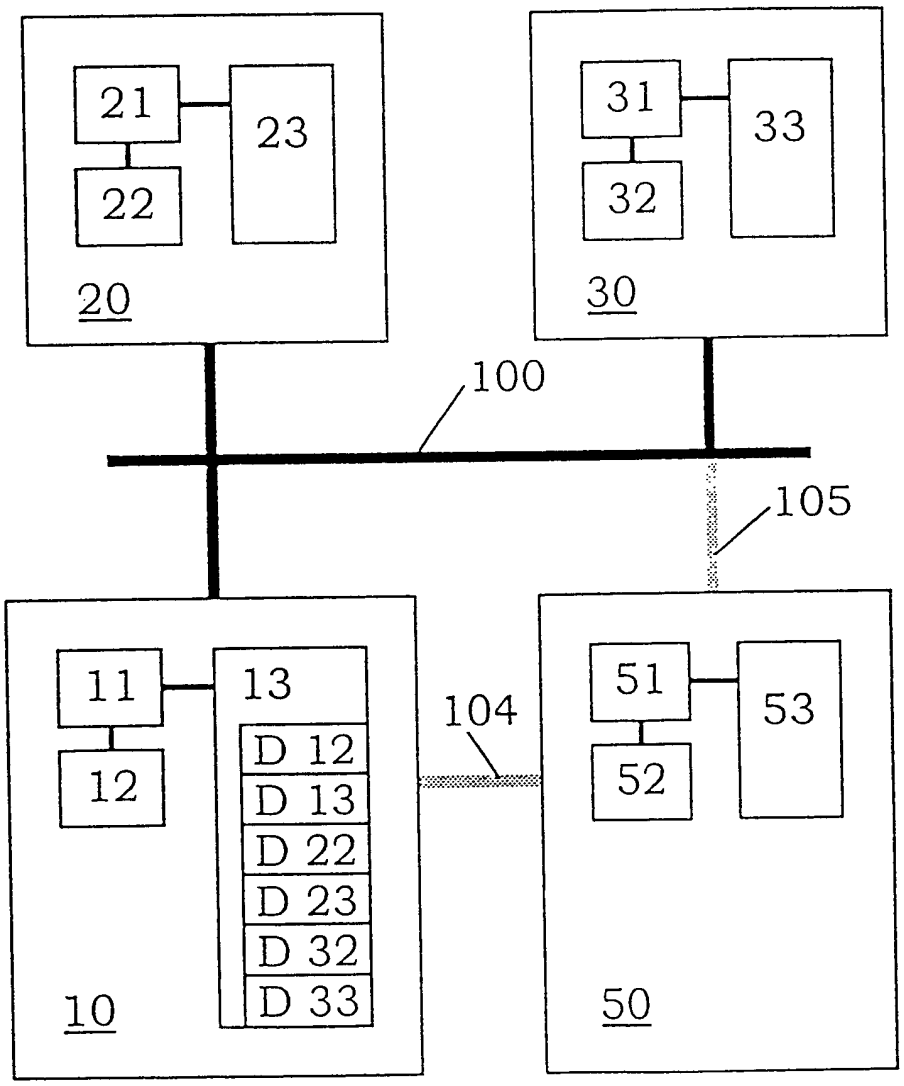

PE
存储
DU,TAB
产生
S,Z
RE
KP
计算
KYU=KY(S,Z,DU)
编制
KYU
编制
KYP=KY(S,Z,DP)
比较
V(KYP,KYU)

图 7

图 8


21
23
22
20
31
33
32
30
100
105
11
13
12
D 12
D 13
D 22
D 23
D 32
D 33
10
104
51
53
52
50

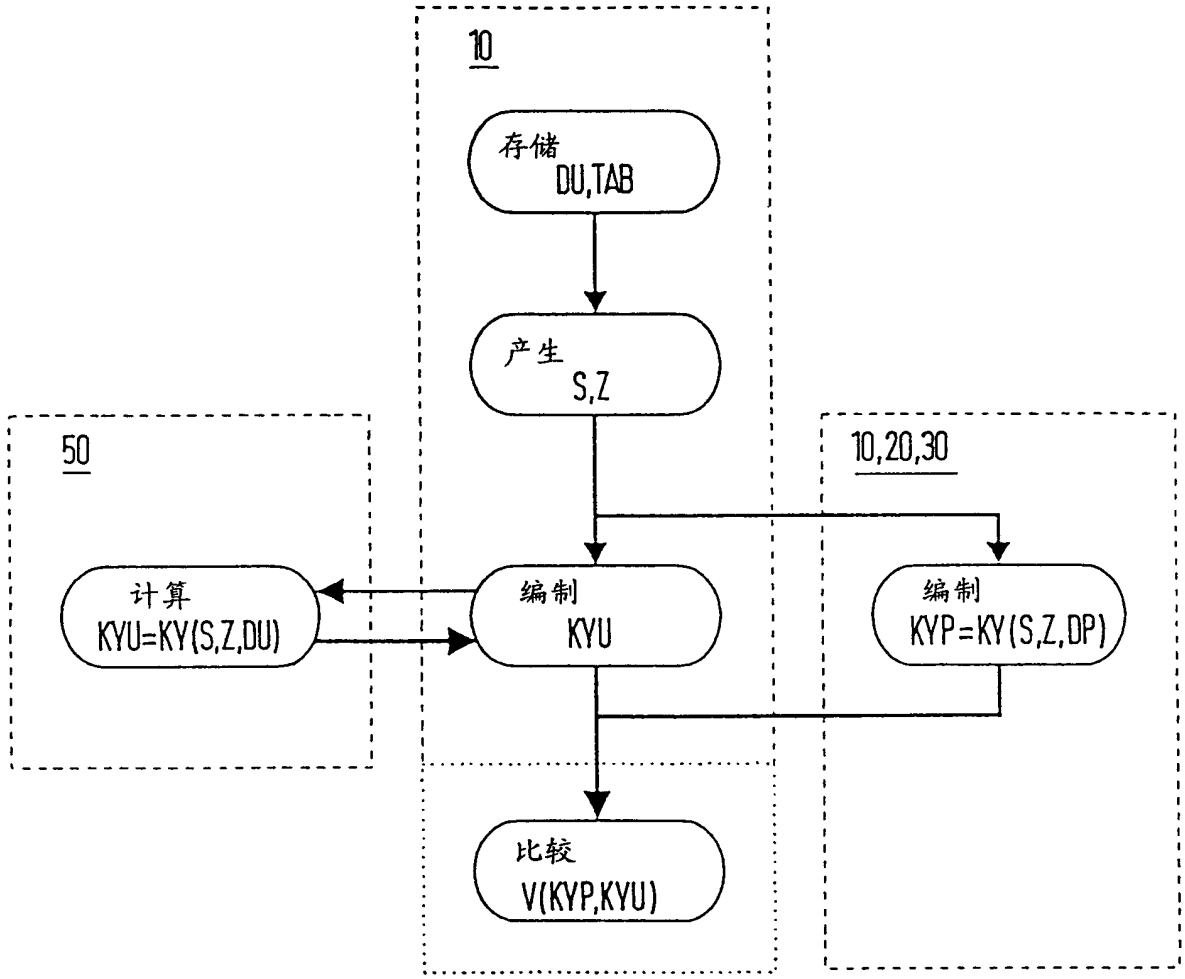

10
存储
DU,TAB
产生
S,Z
50
计算
KYU=KY(S,Z,DU)
编制
KYU
10,20,30
编制
KYP=KY(S,Z,DP)
比较
V(KYP,KYU)

图 9