[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07F 7/10

[12] 发明专利说明书

[21] ZL 专利号 99804911.5

[45] 授权公告日 2004 年 12 月 15 日

[11] 授权公告号 CN 1180383C

[22] 申请日 1999.4.9 [21] 申请号 99804911.5
[30] 优先权
[32] 1998. 4. 9 [33] FR [31] 98/04453
[86] 国际申请 PCT/FR1999/000837 1999.4.9
[87] 国际公布 WO1999/053451 法 1999.10.21
[85] 进入国家阶段日期 2000.10.9
[71] 专利权人 法商·英诺瓦特隆电子公司
地址 法国巴黎
[72] 发明人 史蒂芬·狄戴尔
法兰柯伊斯·格雷优
审查员 王娇丽
[74] 专利代理机构 上海专利商标事务所
代理人 吴蓉军

权利要求书 2 页 说明书 11 页

[54] 发明名称 以不可分割方式修改特别是非接触卡的微电路卡的非易失性存储器的多个位置的方法

[57] 摘要

卡片在执行交易之时暂时耦合至终端机，包括终端机外加多个修改指令至卡片，各指令包含至少一记录作业在卡片存储器，指令规定的个别信息项目，通过该方式写入的各项信息彼此有交互关是。该方法包含由卡片执行下列步骤。 a)当接收来自终端机的个别指令时，经由临时将有交互关是的各项信息记录在卡片存储器上，而临时修改卡片存储器但未丧失该项的对应先前数值；及然后 b)经由全部确认或全部抛弃而结束修改，因此在随后作业中，步骤 a)执行的指令已经列入考虑，否则全部不受影响。

ISSN1008-4274

1．一种用于修改微电路卡片中非易失性存储器之内容的方法，在所述方法中，卡片在执行交易时暂时耦合至一终端机，所述交易包括终端机对卡片外加多个指令，每个指令包含将该指令指定的相应数据项记录在卡片存储器中的至少一个操作，通过这种方式记录的各个数据项是相互关联的，其特征在于，所述方法包括以下步骤：

a）当接收到来自终端机的各相应的指令时，所述卡片将每个所述相互关联的信息项临时记录在卡片存储器中；然后

b）结束所述记录操作，致使在随后的操作中，在步骤 a）中执行的指令将全部都列入考虑，或者全部失效，

其中，所述指令是修改指令；

在步骤 a)中，将所述各项的新数值记录在存储器中的步骤修改了存储器的内容，但未丢失所述各项的先前数值；并且

在步骤 b)中，结束所述记录操作，致使如果在步骤 a)中执行的所有指令全部失效，那么所述非易失性存储器中的数据将保持其在步骤 a)之前的状态。

2．如权利要求 1 所述的方法，其特征在于：

在步骤 b)作出确认的情况下，将一个确认适当执行的标记记录在卡片存储器中；以及

当卡片随后接收到指令，要求读取和/或修改在步骤 a）写入的至少一个数据项或与其对应数值时，卡片开始检验所述标记的状态，若尚未记录所述标记，则卡片忽略或取消先前在步骤 a）所作的临时记录，并且基于对应所述数据项的先前值执行所述指令。

3．如权利要求 2 所述的方法，其特征在于，当卡片检验所述标记的状态时，若已经记录了所述标记，则卡片对步骤 a）中临时记录的内容执行复制操作。

4．如权利要求 1 所述的方法，其特征在于，所述卡片适合在两种模式下操作，即：

对话进行中模式，在该模式下，通过执行步骤 a）及 b）进行记录；以及

结束对话模式，在该模式下，步骤 a ）及 b）所作的记录皆未获得确认。

5．如权利要求 1 所述的方法，其特征在于，包含一认证功能， 所述认证功能与结束步骤 b）的功能相结合，在认证失败时迫使步骤 b）被抛弃。

6. 如权利要求 5 所述的方法，其特征在于，所述认证由卡片来执行，其认证了终端机的真实性及/或终端机与卡片间互换的数据的真实性，所述卡片检验由终端机产生并传输至卡片的加密认可，并且唯有在所述加密认可被辨识为正确时才确认步骤 b）中的修改。

7. 如权利要求 4 或 6 所述的方法，其特征在于，当卡片接收到来自终端机的指令，所述指令要求修改存储器的内容且包括证明一加密认可时，若指令是在结束对话后接收到的，则执行所述证明操作；若指令是在对话进行中接收到的，则不执行所述证明操作。

8. 如权利要求 5 所述的方法，其特征在于，所述认证是由终端机执行的，其认证了卡片的真实性及/或终端机与卡片间互换的数据的真实性，当且仅当步骤 b）确认了所述修改，那么卡片有条件地产生一加密认可，并将所述加密认可传输至终端机 。

9. 如权利要求 4 或 8 所述的方法，其特征在于，当卡片接收到来自终端机的指令，所述指令要求修改存储器的内容且包括产生一加密认可时，若指令是在结束对话后接收到的，则执行所述产生操作；若指令是在对话进行中接收到的，则不执行所述产生操作。

10. 如权利要求 1 所述的方法，其特征在于，当卡片在步骤 b）接收到来自终端机的指令，所述指令要求修改存储器和内容且包括产生多个加密认可时，当且仅当步骤 b)确认了所述修改，才在步骤 b)中存储这些加密认可，然后共同传输至终端机 。

11. 如权利要求 4 所述的方法，其特征在于，至少部分可在步骤 b）执行的指令包括一选择抑制属性，并且若卡片在步骤 b）于对话进行中执行此种指令，则所述指令执行的修改是与步骤 b）的结果无关。

12. 如权利要求 1 所述的方法，其特征在于，进一步规定在步骤 b）之后且在修改已经确认后，执行下列步骤顺序：

d）终端机执行卡片确认后的动作；及

e）在终端机适当执行了所述动作的情况下，将实证信息记录在卡片上，以便供随后读取访问。

13. 如权利要求 12 所述的方法，其特征在于，所述步骤 e）的记录指令为隐式指令，卡片在步骤 b）之后接收到的任何指令都被解译为命令将实证数据记录在卡片上。

以不可分割方式修改特别是非接触卡的微电路卡的非易失性存储器的多个位置的方法

技术领域

本发明关于微电路卡，特别是关于对本身的非易失性存储器执行多种修改的微处理卡。

背景技术

执行交易时，存储器通常修改一次或多次，当然在利用新记录信息前必须确定全部修改都正确，当有错误或记录讹误时，新记录的信息必须被忽略或消除。

US-A-4 877 945 叙述在多个数据项写入过程中如何检测异常以防交易基于错误情况持续下去。

在异常情况下，也希望可恢复原状，换言之，随后交易是对卡片执行不正确交易前已经记录的信息值进行。

前述 US-A-4 877 945 无法提供该优点，原因为某些案例中，当执行不正确交易时老旧信息值已经丧失，故无法将信息回复至稍早状态，至少单纯基于卡片所合信息无法复原。

WO-A-89/02140 叙述一种作业方式，但仅应用于单项信息已被修改或多项以彼此独立方式修改的情况。

但许多案例中，在单一笔交易期间需要修改多个数据项，而此等多个数据项处理时须视为“彼此有交互关联”，从而确保多个数据项全部都作妥善修改。

使用”无接触”型卡片在此种情况下，卡片环绕终端机可正确作业的空间边界无法察觉时，多个关联数据项的交易不完美或不完全的风险特高。此种情况下，卡片在终端机间意外通信中断的风险无法忽略，可能由于卡片在处理结束前已经移离超过终端机的范围，或因暂时性的干扰例如有一块金属通过旁边。

一范例（当然为非限制性）为此种卡片用于遥控验票交易，例如在大众运输网的入口，此时卡片扮演两种角色：旅行车票；以及电子钱包角色。

曾经提出若干解决办法来缓和前述困难且作多个写入或其他修改至彼此相关的“无法划分的”数据项。

前文举例说明的特殊用途中已知系统始于由电子钱包扣帐，然后记录使用者取得旅行权利。若使用者在两次操作间抽出卡片，则要求使用者再度出示该卡片且重新开始写入旅行权利。但若使用者走开而未再度出示卡片，则使用者可能出差错。显然无法以相反顶序进行，后来使用者尝试在钱包扣帐前抽取卡片是不可能。

该解决之道暗示终端机特别配置成在交易中断的情况下激发例外处理来重新开始交易(要求将卡片重新插入终端机)。除了终端机的软件特别复杂外，如所述该种解决之道并非全然满意，若未重新开始交易使用者仍出差错。

另一种解决之道在于数据交叉，终端机保留有关卡片的电子钱包状态信息，反之亦然。但该解决之道仍令人满意，原因为除了复杂以外也增加卡片与终端机间交换数据的容量，因而减慢交易的执行。当有多笔（三笔或三笔以上）写入无法划分时也难以应用。

发明内容

本发明的一个目的是提议一种致能以无法划分方式对卡片存储器作多次修改的方法。

本发明的另一目的是提出可完全由卡片执行的方法。如此可执行该方法而未修改终端机且无需对终端机提供另外处理，该方法使用原有指令的语法，因此可选用的指令上极有弹性。

为了达到上述目的，本发明提供了一种用于修改微电路卡片中非易失性存储器之内容的方法，在所述方法中，卡片在执行交易时暂时耦合至一终端机，所述交易包括终端机对卡片外加多个指令，每个指令包含将该指令指定的相应数据项记录在卡片存储器中的至少一个操作，通过这种方式记录的各个数据项是相互关联的，并且

a）当接收到来自终端机的各相应的指令时，所述卡片将每个所述相互关联的信息项临时记录在卡片存储器中；然后

b）结束所述记录操作，致使在随后的操作中，在步骤 a）中执行的指令将全部都列入考虑，或者全部失效。

所述方法的特征在于，所述指令是修改指令；在步骤 a)中，将所述各项的新数值记录在存储器中的步骤修改了存储器的内容，但未丢失所述各项的先前数值；并且在步骤 b)中，结束所述记录操作，致使如果在步骤 a)中执行的所有指令全部失效，那么所述非易失性存储器中的数据将保持其在步骤 a)之前的状态。

在本发明的方法中，在步骤 b)作出确认的情况下，将一个确认适当执行的标记记录在卡片存储器中；以及当卡片随后接收到指令，要求读取和/或修改在步骤 a）写入的至少一个数据项或与其对应数值时，卡片开始检验所述标记的状态，若尚未记录所述标记，则卡片忽略或取消先前在步骤 a）所作的临时记录，并且基于对应所述数据项的先前值执行所述指令。当卡片检验所述标记的状态时，若已经记录了所述标记，则卡片对步骤 a）中临时记录的内容执行复制操作。

在本发明的方法中，所述卡片适合在两种模式下操作，即：对话进行中模式，在该模式下，通过执行步骤 a）及 b）进行记录；以及结束对话模式，在该模式下，步骤 a ）及 b）所作的记录皆未获得确认。

在本发明的方法中，可以包含一认证功能， 所述认证功能与结束步骤 b）的功能相结合，在认证失败时迫使步骤 b）被抛弃。所述认证由卡片来执行，其认证了终端机的真实性及/或终端机与卡片间互换的数据的真实性，所述卡片检验由终端机产生并传输至卡片的加密认可，并且唯有在所述加密认可被辨识为正确时才确认步骤 b）中的修改。

在本发明的方法中，当卡片接收到来自终端机的指令，所述指令要求修改存储器的内容且包括证明一加密认可时，若指令是在结束对话后接收到的，则执行所述证明操作；若指令是在对话进行中接收到的，则不执行所述证明操作。

在本发明的方法中，所述认证是由终端机执行的，其认证了卡片的真实性及/或终端机与卡片间互换的数据的真实性，当且仅当步骤 b）确认了所述修改，那么卡片有条件地产生一加密认可，并将所述加密认可传输至终端机。

在本发明的方法中，当卡片接收到来自终端机的指令，所述指令要求修改存储器的内容且包括产生一加密认可时，若指令是在结束对话后接收到的，则执行所述产生操作；若指令是在对话进行中接收到的，则不执行所述产生操作。

在本发明的方法中，当卡片在步骤 b）接收到来自终端机的指令，所述指令要求修改存储器和内容且包括产生多个加密认可时，当且仅当步骤 b)确认了所述修改，才在步骤 b)中存储这些加密认可，然后共同传输至终端机。

在本发明的方法中，至少部分可在步骤 b）执行的指令包括一选择抑制属性，并且若卡片在步骤 b）于对话进行中执行此种指令，则所述指令执行的修改是与步骤 b）的结果无关。

在本发明的方法中，进一步规定在步骤 b）之后且在修改已经确认后，执行下列步骤顺序：d）终端机执行卡片确认后的动作；及 e）在终端机适当执行了所述

动作的情况下，将实证信息记录在卡片上，以便供随后读取访问。

在本发明的方法中，所述步骤e）的记录指令为隐式指令，卡片在步骤b）之后接收到的任何指令都被解译为命令将实证数据记录在卡片上。

具体实施方式

本发明方法属于一种卡片在执行交易之时暂时耦合至终端机，交易包括终端机对卡片外加多个修改指令，各修改指令包含至少一个操作，用于在卡片存储器上记录由指令指定的个别数据项，通过这种方式记录的个别数据项彼此有相互关联。以本发明的特征方式，该方法包括由卡片执行下列步骤：a）当接收来自终端机的个别指令时，经由临时将有交互关系的各项信息记录在卡片存储器而临时修改卡片存储器但未丧失该项的对应先前数值；及然后 b)经由全部确认或全部抛弃而结束修改，因此在随后作业中，步骤a）执行的指令已经列入考虑，否则全部不受影响。

如此本发明原理包含将待进行的多个修改以无法分割方式集合于单一步骤a)，然后在修改已经执行后于卡片中整体确认此等修改。若确认成功，则其次由该卡片执行的操作(无论在相同交易期间或在随后交易期间)，存取的内容必然反映出已经作的修改。

相反地，在步骤 a）期间卡片进行操作有任何中断则将取消全部执行的修改，非易失性存储器中的数据保持在步骤a）之前的状态。

特殊实务中，在步骤b）的确认情况下，在卡片存储器上记录一标记证实已经适当执行；当卡片随后接收一指令要求步骤a）写入的至少一数据项或其对应值被读取及／或修改时，卡片开始检视标记状态，若尚未记录标记，则卡片忽略或取消先前在步骤 a）所作的临时记录，并基于对应该数据项之先前数值执行该等指令。若卡片检视标记状态时发现已经记录，则卡片执行拷贝在步骤a）执行的临时写入作业。

最佳卡片适合以双模式作业，即对话进行中模式，其中经由执行步骤a）及b）作记录；及结束对话模式，其中步骤a）及b）都未确认作记录。

开启一段对话例如可以卡片复置为零表示或可于一指令具有两种动作之后，一者执行预定作业而同时被解译为开启一段对话。

例如当籍一证明无法完成通常核准记录时，卡片自动开启一段于此对话进行中处理记录。

以相同方式，结束对话例如可于一指令可执行两种动作之后：执行预定作业

且同时被解译为关闭一段对话的指令。

例如电子钱包扣帐作业结束对话，因而避免须与所得的认可通信，如此使对话认可与电子钱包交易认可变成无法分割。

更佳该方法包含认证功能组合结束步骤 b)功能，在认证失败的情况下强迫步骤 b)被抛弃。

第一实务中，认证的执行方式是通过卡片进行其证实终端机的真实性及/或终端机与卡片间交换数据的真实性，卡片检查由终端机产生加密认可并传输至卡片，唯有在认可被确认为正确时才证实在步骤 b)的修改。

在对话模式过程中可作临时修改，故当卡片接收到来自终端机的指令要求修改存储器内容且包括证实密码认可时，证明该指令是否接收到结束对话，若指令是在对话进行中接收，则无需如此执行。

换言之，由卡片在步骤 b)执行的指令以及通常（亦即结束对话）的指令证实加密认可，当在对话进行中执行时，则不再包括此种确认，以“对话认可终端机的真实性”来执行相当的功能。

第二实务中，认证真实性是由终端机进行，其认证卡片的真实性及/或终端机与卡片间交换的数据的真实性，若且唯若在步骤 b）确认修改，卡片才以有条件方式产生并传输加密的认可至终端机。

在对话模式中，可作临时修改，故卡片接收来自终端机的指令用于修改存储器内容且包括产生加密认可，若指令是在结束对话后接收，则进行该作业，若指令是在对话进行中接收，则无需进行该项作业。

换言之，由卡片在步骤 b）执行的指令以及正常（亦即停止结束对话）产生加密认可的指令时，当是在对话进行中执行则不再产生此种认可，而以“执行认可证实终端机真实性”来执行相当的功能。

可作临时修改，故当卡片在步骤 b）接收到来自终端机的指令要求修改存储器内容且包括产生多个加密认可时，该等认可存储在步骤 b)，且最后共同传输至终端机，若且唯若修改已经在步骤 b）获得证实。

换言之，规定由卡片展期通信通常由步骤 b)的命令产生的加密认可。特别若核可的写入指令产生某种写入认可，则希望唯有在写入已经不可变更的执行之后认可才离开卡片。

特定实务中，至少部分可能在步骤 b）执行的指令包括选择性抑制属性，及若卡片于步骤 b)在对话进行中执行此种指令，则该指令执行的修改是在步骤 b)的结

果独立无关地执行。

换言之，该属性定义指令是在对话进行中执行(即若对话未完成则将被取消)，或在结束对话时执行(即，即刻有效仿佛已经完成对话，即使就时间上而言仍然处在对话进行中亦如此)。

最佳本发明在步骤b）之后且在确认修改情况下进一步提供下列步骤顺序：d)终端机遵照卡片的确认执行某种动作；及e）若该动作由终端机妥当执行，则实证信息记录在卡片方便随后通过读取存取。

此种“实证”对话通知卡片在执行对话之后终端机确实可采行决策（例如应用于大众运输网的进出口开启栅门)。

观察到此种实证是由卡片处理而无需额外写入（临时写入的拷贝则为迟早需要执行的作业)。此外，此种卡片在拷贝端执行的情况唯有当动作已经在终端机端适当执行的情况，换言之，唯有整个交易符合一致。

全部操作皆由卡片执行的情况下较佳规定步骤 e)的记录指令为隐式指令，卡片在步骤b）之后接收到的任何指令被解译为命令记录实证信息在卡片上。

其他特点及优点由后文说明本发明的二实施例显然易明。

此等实例中且确实于全文中，”指定”一词用以表示”特定多个中之一者”，且是有关于卡片所含的多个项目当中特征化一项特定信息的动作。

此种指定可能为内部者，由于指令本身规定一项特定信息，例如指令“由电子钱包中扣帐x量”指示存储器位在含有“电子钱包结馀”数据项数值。

指定也可为明确者，如下实例I所示，规定写入指令有一位址或扇区识别记号，指令是通过指标I加索引。

实例I

提供一卡片其可存储100个8-位元组债，且可执行下列命令：

*读取在1至100范围由指标i规定的8-位元组值v；

*写入在1至100范围由指标i规定的8-位元组值v；

*开启一段对话；

*结束一段对话。

卡片在一次对话进行中至多允许三次写入。习惯上使用大写字母来标示非易失性存储器（例如EEPROM）的值而小写字母用于标示易失性存储器（RAM，其内容当未供电时即消失）的值。

非易失性存储器区段分配作业存储器的主要数据存储区（确定写入)；

*V [i] 对 1 至 100 范围的 i：100 x 8 位元组。

另一非易失性存储器区段分配给对话机制且包含：

*T[k]用于 1 至 3 的 j：3x8 位元组

含有一对话过程写入的值（临时写入）；

*I[K]用于 1 至 3 范围的 j：3xl 位元组

含有对话过程写入值的指标；及

*C：于对话结束时写入的计数位元组。

C 编码于对话过程中执行的写入次数；适当冗馀机制（例如结合该值的补数）可检测于计数位元组存储值不确定的案例。

作业如下进行。

步骤 0：在卡片供电与执行第一指令间的瞬间检验 C。若为 1 至 3 范围的确定值，则对 k 等于 1 至 C 而言，于指标 I[k]的值 T[k]由表 V[i]拷贝。随后 C 复置至零及内部变量 j 设定为-1(指示尚未开启对话)。

步骤 1：读取中，进行测试了解 j 是否大于 0：若是，则要求的指标 i 对 k 由 j 至 1 以递减顶序与 I[k]比较。若有匹配则送返 T[k]。所有其他案例则送返 V[i]。

步骤 2：在开启一段对话时，j 初始化为 0(若对话已经开启则取消)。

步骤 3：在各次写入时若 j=-1(对话未开启)，通信值 V 是于 T[0]写入，通信指称 i 是于 I[0]写入，写入 C=0 随后 v 于 V [i] 写入及写入 C=0：若 O≤j<3（于对话进行中写入），则 j 递增 l，v 于 T[j]写入，及 i 于 I[j]写入；若 j=3 则操作被拒绝（已经超过一次对话进行中的写入上限）。

步骤 4：结束对话进行中，若 j>0，则 j 于 C 写入，然后对 j 为 1 至 C，拷贝于表 V[]于指称 I[j]的值 T[j]。然后 C 设定为 0 及 j 设定为-l。

显然卡片的电源可能于任一瞬间被中断，读取数值需正确，亦即对各指标 i 而言最末写入值非于对话进行中或写入已经结束的对话（在一个非零值写入 C 时，写入已经完成或对话已经结束）。

增加加密以防当供给卡片的加密认可不正确时出现某种作业，及／或在某个作业结束时对卡片产生加密认可。

使用的加密认可是基于已知的密码类型。例如“对话认可证实卡片的真实性”（或终端机）的获得方式是当开启对话时在卡片端及在终端机端对卡片（或终端机）供给的数据及／或对终端机（或卡片）供给的乱数应用安全杂散演算法（SHA）；由其中所得信息确认码(MAC)由卡片（或终端机）使用卡片（或终端机）所含密钥

籍数位签章演算法（DSA）核章；终端机（或卡片）使用公钥证实签章。对称加密演算法例如数据加密标准也可用于产生信息确认码(MAC)及/或产生签章。

本发明中产生信息确认码的步骤为双向认证所共通，且载于全部对话的数据。当使用对称加密时，籍由认证卡片的认可及认证终端机的认可是由信息确认码编译密码的单一步骤获得，卡片及终端机的认可是藉单元操作例如撷取某个预定住元导出。

实例 II

本实例中，存储器的数据被组织作为扇区，各个扇区包含四栏位：

1．数据；

2．识别者（可选定某个扇区的存取钥）；

3．合适性：若二节段具有相同识别者用于决定何扇区为适合；及

4．检验：饶实前三个栏位皆未讹误（例如执行同位型检验）。

一扇区以其识别者标示，以此通知置换位置通知。扇区写入过程具有一识别者作为参数随同该识别者相关数据。读取扇区程序有个识别者作为参数，其送返末次使用该识别者（或若识别者未曾使用则为适当指示）执行写入时关联该识别者的数据。换言之，是执行关联型存取而非索引型存取。

读取一扇区过程中，卡片搜寻扇区其带有含要求值的识别者且非讹误（通过检验栏位决定）。当多个扇区可满足此两项标准时，基于适合性栏位保有一特定扇区。

当写入一扇区时，卡片将下列写于适当扇区：要求的数据；识别者；适当栏位故在读取过程中，此扇区为最适合的具有此种识别者的非讹误扇区；及一检验栏位匹配前三栏位（换言之，写入的处理方式为随后可适当进行读取）。

较佳写入过程后，接着去除已经通过写入新扇区而变成不适合的扇区，如此可利用一新扇区。

较佳也提供（额外）资源回收型系统，亦即由一系统回收可能由于讹误或由于不适合而已经无用的扇区。

较佳提供一系统其可延迟因写入造成的磨耗，确保不会经常使用同一扇区，例如由可利用的多个扇区中随机运用一扇区。

搜寻一扇区程序的概略优异变化方法包括利用搜寻步骤来消除已经发现讹误的扇区及＊或并非最适合的扇区藉此重新产生自由扇区（放特定读取过程耗费时间对随后读取与写入速率有利）。较佳于消除一个已经发现为非讹误但非适合的扇区

前，再度写入适合扇区原因为可能是写入不当所致。

存储器的工作量等于可利用的扇区数目减一个必须保持被消除的扇区。全部扇区（包括被消除扇区）是动态分布在存储器内部。

若数据待于档案结构化，例如应用 ISO / IEC 7816－4 标准结构化，则扇区识别者分成两栏位：档案识别者及档案内部的扇区识别者。

使用此种特定扇区的结构的写入/读取作业的非限制性实务列举如下：

后文说明使用此种特定扇区结构（非限制性）执行读写作业的说明：

*检验栏位以二元码含有其他三栏位的零位元数目；显然若有问题，例如中断写入或消除修改扇区内全部相同方向的位元数目，则检查检验栏位的数值可经常测知已经发生问题。

*适合栏位是以二位元编码的 0 至 3 的整数。

*读取程序循序议取全部扇区至找到第一扇区具有寻找的识别者且非讹误为止。若未找到任何扇区，则程序结束且报告“未找到扇区”。若找到第一扇区，其位置连同其数据及其适合性 P 存储。持续搜寻。若找到第二扇区具有寻找的识别者且非讹误，则测试其适合性 q 是否为 p+1 除以 3 整除的余数；若是，则改写第二扇区，消除第一扇区，及来自第二扇区的数据被送返；否则改写第一扇区，第一扇区被消除，送返来自第一扇区的数据。若未找到第二扇区且若第一扇区的适合性为 p=3，则此扇区被消除且报告“未找到扇区”；否则被送返的数据是来自找到的第一扇区。

*写入程序类似前述读取程序般开始。若找到先前存储的扇区其已经由读取程序通过特定识别者送返，则此扇区位置连同其适合性 p（等于 0、1 或 2）保留；若未找到此种扇区，则选择一自由扇区（使用下述程序选择）及识别者、数据、适合性 p=3 及检验栏位写至该扇区，保留该扇区的位置及适合性。两种情况下经由选择一自由扇区（使用下述程序）继续进行。识别者、数据、适合性 P（计算为 P+1 除以 3 整除的余数），及检验栏位写入此扇区。随后若有任何先前存储的扇区则消除它。

为了寻找一自由扇区，找到自由扇区数目 n 初始化为零。循序检验扇区。对非空白且讹误的扇区则消除它使其变空白（如此促成前述资源回收）；若扇区非讹误及若适合性为 p=3 则消除它（也送到资源回收）；若该扇区非讹误及若其适合性非 p=3，则尚未扫描区段被搜寻是否有另一非讹误扇区具有相同的识别者：若找到一者则非适合属区被消除，如同读取程序般进行：若此过程结束时扇区为空白，则

找到自由扇区数目 n 递增，随机整数是以 0 至 n－1 的范围取出；若整数为 0，则存储空白扇区位置。当全部扇区皆已经扫描时，全部非空白扇区会非讹误，并无任何两个扇区具有相同的识别者，空白扇区数目 n 为已知，及其中一者已经存储作为以相等机率方式的随机选择。若未找到自由扇区，则写入过程中断。

后文说明卡片使们此种特定扇区结构处理无法分割的修改对话的方式。

为了存储无法分割的修改，卡片于非易失性存储器有 n 个可利用的已经被消除的扇区（此处 n 对应于单一对话进行中可能需要作的无法分割的修改数目）。此外，卡片处理专用于处理一对话的非易失性存储器区段（不含于扇区），被称作“对话描述者”。

此种实务并无对话的特定认证。

对话描述者是以三栏位定义：

*无法分割扇区的参考表单(LRSA)；

*形成无法分割扇区参考表单的检验值(VCC)；及

*考虑无法分割扇区参考表单的检验值(VCPC)，用于发现对话是否结束。

步骤 0：初始化：自从最近中断卡片作业例如复置开始初次存取数据前，卡片必须确定对话描述者已经被消除。某些案例依据对话描述者的状态需列入考虑。

*完全消除：卡片保持未改变；

*未完全消除，及 VCPC 为正确：卡片搜寻及消除（若有所需）全部已经被写入而变化无用的扇区（来自参考表单），然后消除对话描述者；

*未完全消除，VCPC 被消除或不正确，及 VCC 完全正确：卡片消除 LRSA 所给扇区然后消除对话描述者；或

*未完全消除，VCPC 被消除或不正确，及 VCC 被消除或不正确：卡片消除对话描述者。

步骤 1：开启对话：卡片寻找 n 个被消除的扇区，然后将参考表单记录在对话描述者(假定被消除）的 VCC。

步骤 2：对话进行中：卡片接受指令。当其中一指令产生一或多个无法分割的修改时，用于记录此等修改的扇区是记录在 LRSA 至多高达全部 n 个修改扇区。

步骤 3：结束对话：为了结束对话，卡片写入 VCPC，其确保 LRSA 及其 VCC 已经列入考虑。随后搜寻并消除全部已经被写入而变化无用的扇区（来自参考表单）。随后消除对话描述者。

此外，若为处理实证的卡片，则对话处理包括下列修改：

步骤 0：初始化：在对话描述者未完全消除及 VCPC 为正确的情况下，卡片寻找并消除（若有所需）全都已经被写入而变无用的属区（来自参考表单），但未消除对话描述。

步骤 1：开启对话：卡片于易失性存储器记录对话被开启。若对话描述者非空白，则卡片指示前一对话尚未被实证，经由分析 LRSA 甚至指示哪个数据项尚未被实证。总而言之未修改对话描述者。

步骤 2：对话进行中：在第一指令带有无法分割的修改时，若有所需卡片消除对话描述者，搜寻 n 个被消除的扇区，然后写入 LRSA 及其 VCC。

步骤 3：结束对话：卡片在易失注存储器记录无开启的对话。无论如何不消除对话描述者。