



[12] 发明专利说明书

专利号 ZL 02807593.5

[45] 授权公告日 2005 年 9 月 21 日

[11] 授权公告号 CN 1220383C

[22] 申请日 2002.3.22 [21] 申请号 02807593.5

[30] 优先权

[32] 2001. 3. 30 [33] FR [31] 01/04342

[86] 国际申请 PCT/FR2002/001010 2002.3.22

[87] 国际公布 WO2002/080544 法 2002.10.10

[85] 进入国家阶段日期 2003.9.29

[71] 专利权人 卡纳尔技术公司

地址 法国巴黎

[72] 发明人 J·-L·多沃伊斯 M·麦拉德

审查员 梁军丽

[74] 专利代理机构 中国专利代理(香港)有限公司

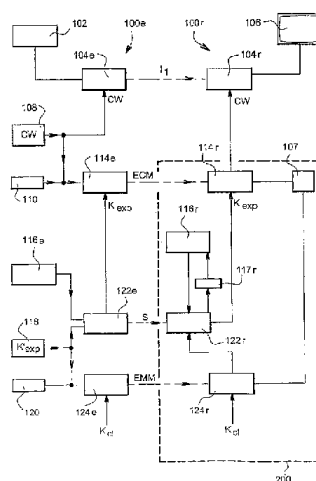
代理人 吴立明 王 勇

权利要求书 2 页 说明书 9 页 附图 2 页

[54] 发明名称 传输用加密密钥加密的信息的系统与方法

[57] 摘要

本发明涉及到发射站(100e)与多个接收站(100r)之间的数据传输方法,该方法是把用第一密钥加密的数据以及传递第二密钥的至少一个控制信息从发射站传输至接收站。本发明的特征在于,用于解密的第一密钥在每个接收站中从第二密钥以及从依据在发射站与接收站之间定期传输的选择命令而在接收站中所得数据组中选定的至少一个数据得到复原。本发明适用于收费电视。图2: 104e, 114e, 116e, 122e, 124e 为加密单元, 104r, 114r, 116r, 122r, 124r 为解密单元, A 为编码密钥, B: 权利控制信息, C: 权利管理信息, D: 操作密钥, E: 客户密钥, S: 命令信息。



1. 一种用于在一个发射站(100e)与多个接收站(100r)之间的传输信息的方法, 其中用第一密钥(K_{exp})加密的信息(ECM)以及至少一个含第二密钥(K'_{exp})的信息从所述发射站传输到所述接收站, 并且其中加密的信息在所述接收站中借助所述第一密钥或者一个与所述第一密钥匹配的密钥进行解密, 其特征在于, 根据在所述发射站与所述接收站之间定期传输的选择命令、从所述第二密钥(K'_{exp})并且从在所述接收站得到的一组可用数据中选择的至少一个数据来在所述接收站中建立所述第一密钥(K_{exp})或所述与第一密钥匹配的密钥。

2. 根据权利要求1的方法, 其中所述加密的信息(ECM)包括存取控制信息, 其含有用于对包括声音和/或图象数据的数据流进行加密的一个第三密钥(CW)。

3. 根据权利要求1的方法, 其中含有所所述第二密钥的所述信息(EMM)是由一个所谓第四“客户密钥”(K_{cl})加密的存取管理信息(EMM)。

4. 根据权利要求1的方法, 其中所述加密的信息包括声音和/或图象数据。

5. 根据权利要求1的方法, 其中不加密地传输所述选择命令(S)。

6. 根据权利要求1的方法, 其中对所述选择命令(S)加密。

7. 一种用于在一个发射站(100e)与多个接收站(100r)之间传输信息的系统, 其在所述发射站中包括至少一个利用第一密钥的信息加密装置(114e), 以及在各接收站中包括根据同样密钥或者与所述第一密钥匹配的密钥的进行解密的解密装置(114r), 其特征在于, 每个接收站都包括根据在所述发射站传输的选择信号、从由所述发射站传输的一个第二密钥(K'_{exp})并且从一组存储的数据中选择的至少一个数据来建立所述第一密钥的装置。

8. 根据权利要求7的系统, 其中所述第一密钥是操作密钥(K_{exp}), 并且所述加密的信息包括存取控制信息(ECM), 其含有用于对包括声音和/或图象数据的数据流进行加密的第三密钥(CW)。

9. 根据权利要求 7 的系统, 其中所述第一密钥是用于声音和/或图象数据的加密/解密 (CW) 密钥, 并且其中所述加密的信息包括声音和/或图象数据。

10. 根据权利要求 7 的系统, 其中每个接收站包括可重写存储器(116r), 用于存储能够为建立所述第一加密密钥而被选择的一组数据。

11. 根据权利要求 7 至 10 的其中之一的系统, 其中所述发射站是广播台, 并且其中所述接收站是收费电视接收机/解码器。

12. 一种根据权利要求 7 的信息传输系统的接收站, 其包括对由一个发射站 (100e) 传输的选择命令 (S) 敏感的用于从一组存储数据中选出一个数据的选择装置 (122r)。

13. 根据权利要求 12 的接收站, 其中所述选择装置包括指向存储器地址的指针表 (117r)。

14. 根据权利要求 12 的接收站, 其中能够被选择的所述存储数据组包括用于识别所述接收站的数据。

15. 一种接收站 (100r), 包括:

用于从一个发射站接收加密的信息 (ECM) 和至少一个含有第二密钥 (K'exp) 的信息 (EMM) 的装置, 其中所述加密的信息由一个第一密钥 (Kexp) 加密,

用于利用所述第一密钥或者一个与所述第一密钥匹配的密钥对所述加密的信息进行解密的装置,

所述接收站的特征在于, 还包括:

一组数据,

用于从所述发射站接收选择命令的装置,

用于根据所述选择命令从所述数据组中选择至少一个数据的装置,

用于从所述第二密钥 (K'exp) 并且从所述选择的数据中选出的至少一个数据来建立所述第一密钥的装置。

传输用加密密钥加密的信息的系统与方法

5 技术领域

本发明涉及到加密形式信息的传输系统与方法，它还涉及到一种密钥的传输，这种密钥同样被加密并用于解密信息。

本发明可在不同的通信领域得到应用，但它尤其针对通常称之为“收费电视”的电视服务或节目的分配网络。

10

背景技术

在经销商发射站与多个接收站之间进行信息，特别是收费电视节目或服务的加密传输。接收站基本上相当于用户的装有解码器的电视接收机。

15

通过无线电，光或电信道传输的信息借助密钥进行加密以便使对该信息使用留给一定数量的指定使用该信息的订户或用户。用户可以使用能够从加密信息恢复成所谓复原信息的解码设备或解码器。此复原信息可以被储存或在电视机内使用以显示图像并且再现声音。

20

使用密钥在接收站中进行信息解密，该密钥应当与发射站中用于加密的密钥相对应。因此这一密钥也必须传输给用户以便在接收站中得到此密钥。

提供了各种不同的可能性用于把加密/解密的密钥分配给电视节目经销商的用户或订户而。不过，简单的解决办法包括以与加密信息相同的方式在发射站与接收站之间对密钥进行传输。

25

为此，应对密钥本身予以加密以防止被尚未支付适当费用的用户所盗用。

因而发射站与接收站之间所传输的信息不仅包括如声音和/或图像数据的信息，而且还包括一些附带有加密/解密密钥的控制和管理用户存取该信息的信息。

可获得的控制和管理信息为一个用户或多个用户提供了对广播信息的

存取控制。这些信息还能够把不同的信息预留给不同的用户或订户。

附图 1 示意性地说明了一已知信息传输系统的主要部件。

发射站的部件在该图的左侧部分，而用户接收站的部件则在图的右侧部分。

5 某些部分用虚线连接起来，表示例如，通过无线信道远距离传输信息。

图象和/或声音通量源 102 接至发射站的第一加密单元 104e。该加密单元使用标记为 CW 的编码密钥对图象/声音通量进行加密。在接收站的解密单元 104r 中使用同样的编码密钥 CW。电视机 106 与解密单元 104r 相连接。

10 在发射站中设置第一密钥发生器 108 来产生编码密钥 CW。例如，该发生器为随机发生器。

设置发射站的第二加密单元 114e 对编码密钥 CW 进行加密。第二加密单元传递加密的信息条目，这些信息为标记成 ECM（授权控制信息）的存取控制信息。ECM 信息包含有加密的编码密钥 CW 和关于广播图象或声音节目的说明性信息。在接收站中接收 ECM 信息并由第二解密单元 114r 在其中解码。第二解密单元提供第一解密单元所需的编码密钥 CW 以便对图象/声音通量进行解密。解密后从 ECM 信息中得到密钥 CW。

15

发射站中 ECM 信息的加密如何在接收站中的解密一样借助称为操作密钥并标记成 Kexp 的另一密钥进行。例如，操作密钥由第二密钥发生器 118 提供。

20

由于操作密钥还应提供给大量的用户，其分配的解决办法包括以与像其他信息相同的方式在发射站与接收站之间对其进行发射。

由于该密钥应当预留给某些用户或订户，该密钥还由第三加密单元 124e 对其加密。

25 第三加密单元传递标记为 EMM（授权管理信息）的存取管理信息。这些信息除包含有加密的操作密钥以外，还包括用户权利的管理数据。这些数据可以，例如，为各用户或用户群体确定已预定的节目或广播内容的类别。EMM 信息被传输到接收站并由第三解密单元 124r 在站中对其解密，第三解密单元 124r 再把操作密钥 Kexp 提供给第二解密单元 114r。

发射站的第三加密单元 124e 和接收站的第三解密单元 124r 使用标记成 Kc1 的称之为客户密钥的一种密钥。

应当指出,如果编码密钥 CW 和 ECM 信息为大量用户,甚至是所有用户所共用,那么 EMM 信息和客户密钥 Kc1 则是针对某一特定用户或有限数量的用户。

在 EMM 和 ECM 信息通过与像图像和声音信息同样的广播信道进行广播时,这些信息可能得到的传输带宽之阻塞问题就产生了。大量用户所共有的 ECM 信息可以经常发射,因而其可以携带快速变化的解码密钥。通过快速地改变这些密钥,能够限制其复制盗用的危险。

另一方面,EMM 信息及其携带的操作密钥是针对大受限制的用户群体,或用于单独的用户。因此,在用于传输信息指定的传输带宽内它们对各用户的经常发射及其快速更新是不可能的。

举例来说,编码密钥通常以几秒钟的周期改变,而 ECM 信息则每秒钟都进行传输。操作密钥通常每月改变一次,而 EMM 信息则每小时传输一次。最终,客户密钥 Kc1 通常不变。

在接收站中,一部分装置可以集成进芯片卡一类的电子卡中。这种卡,例如,包括第二和第三解密单元以及管理各种不同密钥的装置。客户密钥可以永久性地写入此芯片卡。操作和解码密钥可暂时储存在其中直至其更新。

为此目的,接收站的芯片卡包括有微处理器以及用于数据储存的存储器。存储器特别是提供对解密密钥的储存。

信息传输系统没有防止包括把一个或几个密钥复制进空白芯片卡的盗用问题。

在不同阶段,即通过使用各不同密钥之一就可以事先达到对接收站芯片卡的剽窃。视情况而出现各种不同的限制。

接收 EMM 信息的客户密钥的复制与假冒者将被识别出来的可能有关。事实上,客户密钥和 EMM 信息是针对各用户或有限的用户群体的。因此,广播商就能够防止在发射站中为这些用户发射新的 EMM 信息。

另一方面,当编码密钥 CW 被复制时,识别出不诚实用户的危险是不可

能的。但是，由于这些密钥缺乏持久性，使得这种假冒工作毫无成果。

因而，主要的复制风险涉及到含有操作密钥的 ECM 信息。由于这一密钥在相当长的时间，大约一个月，保持不变，故其通过超级媒体系统（因特网）的传播就会使大量用户能够盗用。

5

发明内容

本发明的目的是为大大减少盗用危险而提供一种信息传输系统与方
法。

本发明的目的还在于提高旨在欺诈性模仿接收站工作的芯片卡成本。

10

本发明的目的另外还在于通过避免因重复发送信息或加密密钥而造成
的对带宽的限制来保持对传输图象和声音信息的最大传输带宽。

15

为了达到这些目的，本发明更为具体地涉及到一种用于在一个发射站
与多个接收站之间的传输信息的方法，其中用第一密钥加密的信息以及至
少一个含第二密钥的信息从所述发射站传输到所述接收站，并且其中加密
的信息在所述接收站中借助所述第一密钥或者一个与所述第一密钥匹配的
密钥进行解密，其特征在于，根据在所述发射站与所述接收站之间定期传
输的选择命令、从所述第二密钥并且从在所述接收站得到的一组可用数据
中选择的至少一个数据来在所述接收站中建立所述第一密钥或所述与第一
密钥匹配的密钥。

20

在本发明的意义上，信息被理解为能够在发射站与接收站之间进行交
流的所有数据或信号。因此，信息既可以是图象或声音数据，也可以是代
码或密钥，或甚至是控制信息。控制信息是，例如，用来说明提供给用户
的广播节目或服务的信息以及用来管理用户单独或集体使用这些服务的信
息。

25

使用本发明，在发射站与接收站之间传输的至少一个密钥不是可以直
接用来进行解密的密钥。如上所示，适用于解密的密钥，即第一密钥是依
据第二密钥以及能够从一组附加数据中选出的一个或几个数据而在接收站
中重新建立的。

在接收站中具有能够选择的数据，例如在芯片卡中就可得到这些数

据, 如果接收站配备有这种卡的话。

建立第一密钥所考虑的数据选择要周期性的更新并且其涉及到比一个简单密钥要远大得多的一组数据这一事实决定了欺诈性复制芯片卡需要有与接收站中存储容量同样大小的存储器容量。它还要承担对这组数据的连续更新。

这些重大的限制势必会增加一些复制芯片以及欺诈性复制接收站存储信息的成本。

根据本发明的具体实施方案, 此方案有助于保护系统免遭因更新时间相当长而与敏感操作密钥相关的任何欺诈, 本发明所针对的传输信息, 如上面所限定的那样, 主要是存取控制信息 ECM。需提示一下, 这些信息为特别用于声音和图象数据加密与解密的代码密钥 CW 的载体。于是第一密钥就是操作密钥。用于选择形成第一密钥进一步所需数据而使用的选择命令可以在发射站与接收站之间进行传输, 而不论其加密与否。事实上, 除了接收站全部或部分存储器的存储信息外, 它本身不包括可以使用的任何信息。

在本发明的其他可能实施方案中, 当然不排除上面讨论过的方案, 本发明所针对的加密信息主要包括图象和/或声音数据。在这种情况下, 第一密钥为代码密钥 CW。

本发明还涉及到一种用于在一个发射站与多个接收站之间传输信息的系统, 其在所述发射站中包括至少一个利用第一密钥的信息加密装置, 以及在各接收站中包括根据同样密钥或者与所述第一密钥匹配的密钥的进行的解密装置, 其特征在于, 每个接收站都包括根据在所述发射站传输的选择信号、从由所述发射站传输的一个第二密钥并且从一组存储的数据中选择的至少一个数据来建立所述第一密钥的装置。

传输系统按照讨论过的方法进行工作。为此, 每个接收站都包括一些依据发射站所传输的第二密钥以及根据发射站传输的选择信号从一组储存数据中选出的至少一个数据来建立第一加密密钥的装置。

根据本发明, 以及如上所述, 至少其中一个密钥, 例如操作密钥从不在发射站与接收站之间进行传输。所传输的密钥, 在此情况下为第二密钥,

就不能够原封不动地用来进行解密。

当第一密钥为操作密钥时，所考虑的加密信息包括含有第三密钥(CW)的存取控制信息(ECM)，第三密钥用于对包括声音和/或图象数据的数据流进行加密。

- 5 根据另外一种可能性，也不排除前面的那种可能性，第一密钥也可以是对声音和/或图象数据进行加密/解密的密钥。在此情况下，有关的加密信息包括声音/图象数据。

为了储存能够根据选择命令选定的一组数据，可以设计出接收站。这些数据可全部或部分地写入固定的存储器。

- 10 根据本发明的信息传输系统的接收站，其包括对由一个发射站传输的选择命令敏感的用于从一组存储数据中选出一个数据的选择装置。

不过，在传输系统的优选实施方案中，能够选择的部分或全部数据可以储存在可重写存储器中。这一特点能使这些数据被更新，因此这对接收站的假冒者是个附加的障碍。

- 15 接收站可进一步包括选择装置，选择装置可以包括指向存储器地址的指针表。

- 选择装置可以以直接的方式，例如，根据从发射站传输的待选择数据的地址进行选择或通过针对每个接收站的指针表来进行选择。然后指针可指明各不同接收站中的不同地址。在这种情况下，建立密钥所需的数据可以不储存在不同接收站中的相同地址内，而是可以将其有变化地分配在为储存这些数据所指定的整个存储器内。这一特点还增加了复制接收站存储信息的难度。
- 20

- 此外，能够在储存数据中分配用户标识数据，该储存数据能够被选择或不被选择。由于用这些数据，在欺诈性复制的情况下，能够识别出不诚实的用户并阻止相应接收站的工作。例如通过停止向一些站传输存取处理信息 EMM，可以阻止这些站的工作。
- 25

根据本发明的一种接收站，包括：用于从一个发射站接收加密的信息和至少一个含有第二密钥的信息的装置，其中所述加密的信息由一个第一密钥加密，用于利用所述第一密钥或者一个与所述第一密钥匹配的密钥对

所述加密的信息进行解密的装置，所述接收站的特征在于，还包括：一组数据，用于从所述发射站接收选择命令的装置，用于根据所述选择命令从所述数据组中选择至少一个数据的装置，用于从所述第二密钥并且从所述选择的数据中选出的至少一个数据来建立所述第一密钥的装置。

- 5 参照附图，通过下述说明，本发明的其他特点和优点将会变得显而易见。完全示范地且非限定地给出这一说明。

附图说明

- 10 - 已经画出的图 1 为对一已知类型加密信息的传输系统的示意简化说明。
- 图 2 为根据本发明的加密信息传输系统的示意简化说明。

具体实施方式

- 15 在下述说明中，参照图 2，与在图 1 中已叙述过的部件相同，相似或相等的部件均使用同样的参考数字标记。

 特别是，在图 2 中可发现自经销商发射站 100e 的图象和/或声音通量源 102。发射站将加密的信息流 I_1 ，例如以图象或声音数据的形式，传输给多个接收站 100r。为了明晰起见，该图只绘出说明了一个接收站，随后的本文将参照此图。但是在收费电视应用中，接收站的数目却非常之大，

20 例如相当于订户数。

 应当说明的是，除了声音和/或图象数据之外的信息可以在通量 I_1 中传输。例如，这可以是互动应用，暂时的数据，节目，等等。

 例如为了在电视机 106 上复原，所传输的信息可以用发射站的加密单元 104e 加密和用接收站 100r 的解密单元 104r 解密。

- 25 使用类似于图 1 标记 CW 的代码密钥进行加密与解密。利用发生器 108 产生代码密钥 CW。它与由单元 110 提供的通量 I_1 的信息的描述符相结合，然后像对 ECM 信息形式以加密方式进行传输。例如，描述符表示出所传输电视节目的内容。

 在本发明的意义上，ECM 信息也构成了加密的信息。对 ECM 信息更为

详细的说明可参看本文的引言部分。

ECM 信息的加密与解密分别在发射站和接收站的单元 114e 和 114r 中完成。借助照图 1 类似标记成 Kexp 的所谓操作密钥来进行加密和解密。

5 然而，与图 1 中说明的系统不同，操作密钥不在发射站与接收站之间传输。

操作密钥 Kexp 依照密钥发生器 118 提供、标记为 K'exp 的第二操作密钥以及取自存储器 116e 所存数据组中的一个或几个数据来建立。存储器 116e 中得到的数据与储存在各接收站存储器 116r 中的一组数据相同。应当说明，存储器 116e 和 116r 可以是单一的存储器或由不同类型的不同存储器（ROM，RAM，EEPROM 等）组成。

10 设置计算单元 122e 来选择存储器 116e 中的数据并将这些数据与第二操作密钥 K'exp 组合起来以便为加密单元 114e 形成操作密钥 Kexp。可以对此组合归结为数据的简单并列或者是更为复杂的组合。单元 122e 还形成了选择命令信息 S，此 S，例如，含有选定存储器中数据的地址。此信息 S 以加密或不加密的方式传输给所有的接收站。

另外，加密单元 124e 接收第二操作密钥 K'exp 以及管理由单元 120 所提供的用户权利的管理数据。这些权利管理的数据对于具体的用户或用户群体来说描述了已预定节目的类型。管理权利的数据和第二操作密钥 K'exp 都包含在 EMM 型信息中。

20 如图 2 所示，选择命令信息 S 由接收站的计算机 122r 接收。该计算机 122r 还在解密元件对信息 EMM 解密之后接收第二操作密钥 K'exp。计算机 122r 根据选择命令 S 从存储器 116r 读入数据并且以像发射站计算机 122e 同样的方式将这些数据与第二操作密钥 K'exp 组合起来，以便为解密单元 114r 形成操作密钥 Kexp。

25 由发射站传输到接收站的选择命令信息可以包含指出存储器 116r 地址的一个或一组地址。例如，在此地址应当读出形成操作密钥的一个数据。在这种情况下，在所有接收站中至少有一部分存储器空间的内容及配置应当是相同的。

但是，根据一种优化方案，接收站可以包括指针表 117r，而选择命令

则可指出表内其中一个指针。然后使此字符指向不同接收站中的不同地址，而最终则得到了形成操作密钥的相同数据。使用这一提高方案，能够在不同的接收站中处置明显不同的存储器中的内容或者至少是配置不同的内容。这就增大了对其进行欺诈复制的难度。

- 5 根据已经提到的另一优化方案，存储器的存储信息可包括识别用户的数据，这样的数据可以利用来识别可能的假冒者。

最后，在发射站与接收站之间传输的 EMM 可以包括将要储存在存储器 116r 中的数据或用来取代存储器 116r 中业已存在数据的数据。这些同样的数据也存储在发射站中，例如存储在存储器 116e 中，以便可以用作建立操作密钥的数据。

10

图 2 中的标记 107 指明了能够接收 ECM 和/或 EMM 信息的测试电路。对于每个使用者来说，这一电路用来控制接收广播节目的订户资格。当不再为将被识别出为未经授权用户的某用户传输 EMM 信息时，这一公知的电路可以阻止信息流 I_1 的解密。

- 15 在接收站中，至少一部分部件可以集成进芯片卡。图 2 中，一些部件用虚线圈了起来。例如，这些部件就是芯片卡 200 的一部分。特别看到，芯片卡 200 可包括用于 EMM 信息解密的客户密钥 $Kc1$ 。后者可以储存或通报。

芯片卡的欺骗复制要求从存储器或存储器 116r 复制下所有的数据。存储器的容量和分布，例如，如下所述：RAM: 32kO, EEPROM: 32kO, RAM: 1kO。此外，EEPROM 存储器的存储信息应当连续地更新并由假冒者分配给所有不诚实的用户，这就代表了巨大的数据流。这些限制使芯片卡的复制在经济上变得没有价值或至少是大大地降低了其收益。

20

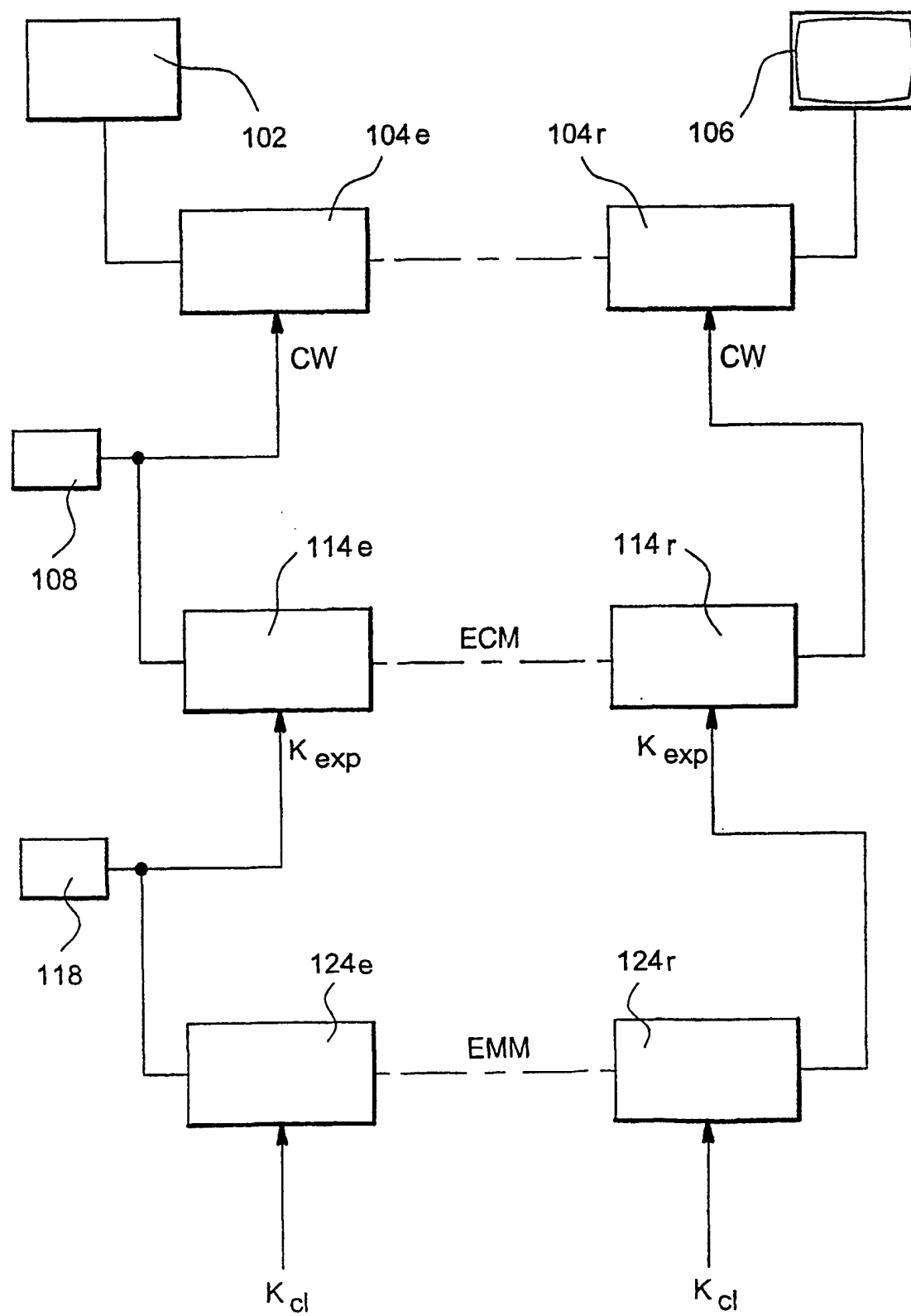


图 1

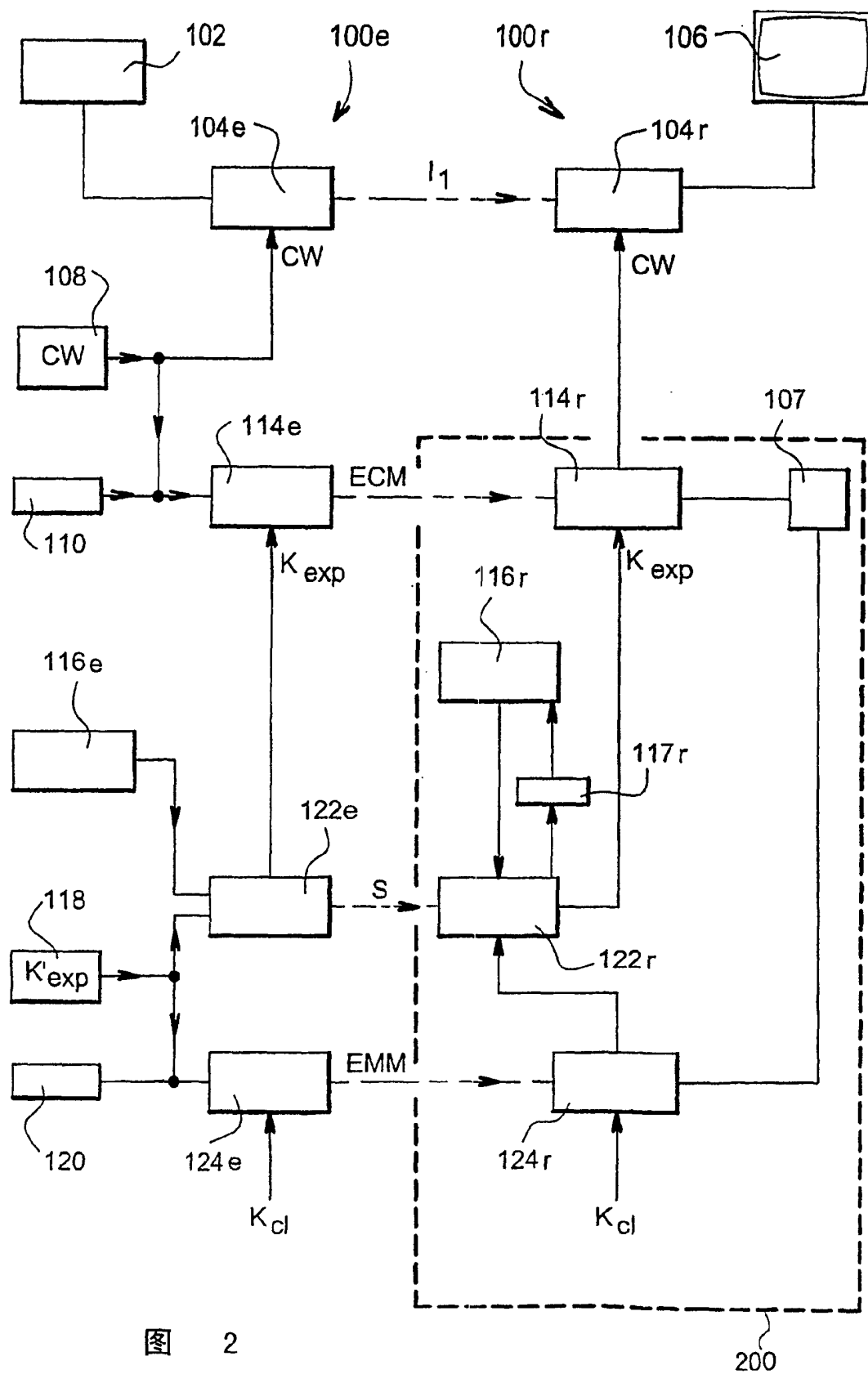


图 2

200