[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07F 17/32
G07F 7/08

[12] 发明专利说明书

专利号 ZL 98800766.5

[45] 授权公告日 2005 年 10 月 12 日

[11] 授权公告号 CN 1222916C

[22] 申请日 1998.3.20 [21] 申请号 98800766.5
[30] 优先权
[32] 1997. 4.11 [33] FR [31] 97/04733
[86] 国际申请 PCT/FR1998/000582 1998.3.20
[87] 国际公布 WO1998/047113 法 1998.10.22
[85] 进入国家阶段日期 1999.2.4
[71] 专利权人 格姆普拉斯公司
地址 法国热姆诺
[72] 发明人 H·奥鲁斯 J·-J·福格里诺
审查员 杨勤之

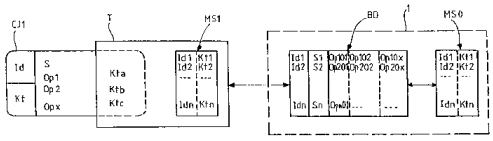
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王 勇 陈景峻

权利要求书 3 页 说明书 10 页 附图 2 页

[54] 发明名称 控制智能卡游戏系统内价值单元转移的安全方法和系统

[57] 摘要

本发明涉及游戏机如扑克牌 Jackpot 或 black jack 以及其它俱乐部游戏机。 机器设计成用游戏卡(CJ1)如片卡运作并且通过网络连接到中央管理计算机单元(1)。 本发明的技术特征包括：中央管理计算机应包含一数据库(BD)，其中贮存了与游戏卡上的数据相一致的数据如关于游戏人的数据，卡识别数据(Id)和关于贮存在卡(CJT)内帐余额的数据(S，OP1，OP2)。 本发明方法包括检查与中央管理计算机数据库有关的卡的数据，以确保用片卡或不接触卡运作的这样一种游戏机的完整性的步骤；其特征在于通过从秘密识别密钥和/或鉴别数据计算的鉴别认证完成数据的交换，和所述交换的数据通过检查每个鉴别认证来得到确认。



ISSN1008-4274

1. 一种控制多种游戏卡（CJ，CJ1，CJ2，CJn）和多种游戏机（200，200'，200''，200'''，300，300'，300''）之间的价值单元转移的安全方法，每台机器连接到游戏卡（CJ2）转录器（210），机器在安全网内通过耦合装置（123）与中央管理计算机（1）联网，在游戏运作期间本方法包括下列步骤:

－读出游戏卡存储器内的数据，卡（CJ1）的识别号码（Id）和/或记入借方和/或记入贷方的价值单元有效的数据（S，OP1，OP2，OPX），该方法的特征为它包含以下步骤:

－通过安全网络的耦合装置（123），在机器（200）和中央管理计算机（1）的数据库之间进行数据交换；以及

－确保游戏卡（CJ1）存储器内的数据与数据库（BD）内的数据相符，以便检查由这种卡、机器、网络和中央管理计算机构成的系统的完整性;

所述方法的特征在于通过从秘密识别密钥和/或鉴别数据（kt，kt'）计算的鉴别认证（C'）完成数据的交换，和所述交换的数据通过检查每个鉴别认证来得到确认。

2. 根据权利要求 1 所述的方法，其特征为：游戏运作前步骤为:

－在卡充电预备运作期间把价值单元的起始余额（S，S1）有效的数据写入中央管理计算机（1）的数据库（BD）内和游戏卡（CJ1）的存储器内。

3. 根据权利要求 1 或 2 所述的方法，其特征为：在游戏运作期间一步骤为:

－把游戏卡（CJ1）的价值单元余额（S）有效数据写入中央管理计算机（1）的数据库（BD）内。

4. 根据权利要求 1 或 2 所述的方法，其特征为：在游戏运作期间一步骤为:

－从中央管理计算机（1）接收价值单元余额（S）的有效的数据以

避免使用卡（CJ2）或游戏机（200）的任何舞弊。

5. 根据上述权利要求 1 或 2 所述的方法，其特征为：检查步骤为：

－确保在游戏卡（CJ1）中读出的价值单元余额（S）的有效数据与在数据库（BD）内读出的数据（S）一致以检查游戏卡（CJ1）的完整性。

6. 根据上述权利要求 1 或 2 所述的方法，其特征为：检查步骤为：

－用中央管理计算机（1）的数据库（BD）内读出的识别密钥（kt1）检查游戏卡（CJ1）的识别号（Id），以便控制游戏卡（CJ1）的完整性。

7. 根据上述权利要求 1 或 2 所述的方法，其特征为：网络还包含一些安全装置（MSO），所述方法包括一补充步骤是：

－根据安全装置的存储器内的秘密数据（kt，kt'），网络的安全装置（MSO）计算鉴别认证（C'）。

8. 根据权利要求 7 所述的方法，其特征为：所述的补充步骤是：

－根据卡的存储器内的秘密数据（kt，kt1），读出由游戏卡（CJ1）计算的鉴别认证（C）。

9. 根据权利要求 7 所述的方法，其特征为：在机器（200）和中央管理计算机（1）的数据库（BD）之间交换的数据（Id，S）包括鉴别认证（C，C'）。

10. 根据上述权利要求 1 或 2 所述的方法，其特征为：根据游戏卡（CJ1）安全装置（MS1）与数据转录器（T，10，110，210）相结合以控制这种卡的完整性。

11. 根据上述权利要求 1 或 2 所述的方法，其特征为：安全装置（MS1）与游戏机相结合。

12. 根据上述权利要求 1 或 2 所述的方法，其特征为：安全装置与网络耦合装置相结合。

13. 根据上述权利要求 1 或 2 所述的方法，其特征为：安全装置（MSO）与中央管理计算机（1）相结合，以便检查网络的完整性。

14. 一种控制在多种游戏卡（CJ）和多种游戏机（200，300）之间价值单元转移的安全系统，每台机器装备有能从游戏卡（CJ）使来自游戏卡（CJ）的价值单元记入借方的转换器（210，310），机器通过耦合装置在

安全网内与中央计算机（1）连接，游戏卡（CJ1）把已执行的游戏运作有效的数据（S，OP1，OP2，OPX），卡的识别数据（Id）和在上述游戏运作期间记入借方和/或记入贷方的价值单元余额（S）有效的数据贮存在其存储器内，其中，中央管理计算机（1）包括一数据库（BD），它把执行的游戏运作有效的数据（S1，OP101，OP102，OP10X），卡的识别数据（Id1，Id2，Idn）以及在上述游戏运作期间记入借方和/或记入贷方的价值单元余额（S1，S2，Sn）有效的数据并行贮存在其存储器内；控制装置（MSO）确保：对一被识别的卡，来自数据库（BD）的数据和卡（CJ1）的数据一致，以检查系统的完整性；

所述系统的特征在于通过从秘密识别密钥和/或鉴别数据（kt，kt'）计算的鉴别认证（C'）完成数据的交换，和所述交换的数据通过检查每个鉴别认证来得到确认。

15. 根据权利要求 14 所述的安全系统，其特征为：根据贮存在卡（CJ1）的存储器内的秘密数据（kt，kt'），游戏卡（CJ1）计算鉴别认证（C）。

16. 根据权利要求 14 或 15 所述的安全系统，其特征为，安全模块（MS1）提供在转录器（T，10，210，310）之内。

17. 根据权利要求 14 或 15 所述的安全系统，其特征为：安全模块提供在游戏机（200）内。

18. 根据权利要求 14 或 15 所述的安全系统，其特征为：安全模块提供在网络的耦合装置之内。

19. 根据权利要求 14 或 15 所述的安全系统，其特征为：安全模块提供在中央管理计算机（1）内。

20. 根据上述权利要求 14 或 15 所述的安全系统，其特征为：游戏卡是智能卡。

21. 根据上述权利要求 14 或 15 所述的安全系统，其特征为：游戏卡是不接触卡。

控制智能卡游戏系统内价值单元转移的安全方法和系统

技术领域

本发明涉及游戏机范畴，例如 Jack－Pot（扑克游戏）装置以及在俱乐部（Casino）内可找到的那些类型供单个人用的其它游戏设备。

尤其是它涉及到允许用游戏卡记录数据的游戏机。这些游戏卡是智能卡或不接触卡类型。这些游戏卡能贡献于下列电话卡的使用。它们有利地包括允许把总数额直接转移到游戏机的使用卡上。

本申请提供在多种游戏卡和多种游戏机之间价值单元转移的控制方法和系统，而每一机器连接到有能力对游戏卡存储器内的价值单元记入贷方和/或借方的游戏卡数据转录器。

背景技术

控制在游戏卡和游戏机之间价值单元转移的一般目的是避免用这些卡的所有舞弊。

人们已经熟悉为装备智能卡读出装置的游戏机用的经营系统，它适合于管理安排在相对封闭的位置并且像俱乐部一样受控制的多个游戏机。这些系统适合于这样的环境，因为它受到许多控制和管理，在使用智能卡形成的游戏机上接受舞弊。

专利文件 EP－A－0 360 613 描述了例如在智能卡和多个带有在智能卡内处理机器数据传输和贮存装置的机器之间的一种数据转移系统。这样一种系统用贮存在会计或财务目的执行的游戏运作清单的收集卡来收集游戏运作。

这样一种系统的缺点是它不能控制所有实施的游戏的运作，除非用收集卡收集所有机器的必要数据，这会引起令人厌烦的操作。

另一方面，面对不断增长的公众要求，打算在比俱乐部更少受到保护的场所如私人游戏厅、或酒吧，甚至在游戏人的住所（私人住宅）内安装

一些游戏机。

显然这种游戏机的分散会对游戏操作固有的交易产生重大的交易安全问题。

发明内容

本发明的目的应当允许在未保护的场所发展一种用游戏卡可工作的游戏机。

本发明的另一目的应加强用游戏卡工作的游戏机系统的完整性。

本发明提供游戏机在网内应与中央管理计算机联网。根据本发明规定中央管理计算机应包含一数据库，在数据库内贮存了与贮存在游戏卡上的信息（如有关游戏人的信息）相应的信息以及鉴别卡的数据和指明有关贮存在卡内的价值余额有关数据。针对在中央管理计算机数据库内的数据检查卡的数据允许确保用跳蚤卡或不接触卡工作的这种游戏机系统的完整性。

因此本发明控制在多种游戏卡和多种游戏机之间价值单元转移的安全技术，每一机器依靠游戏卡连接到数据转录器上，因此在一安全网内机器与中央管理计算机联网，而本技术在游戏运作过程中包含一些阶段，如:

－读出存储在游戏卡存储器中的数据，特别是在上述游戏卡的运作期间卡的识别号码或记入贷方和/或记入借方的价值单元的有效数据，

－通过安全网的耦合装置在机器和中央管理计算机的数据库之间交换数据，特别是卡的识别号码和/或价值单元余额的有代表性数据；以及

－存储游戏卡的数据与数据库的数据一致，以便校验由这样的卡、这样的机器、网和中央管理计算机构成的系统的完整性;

－通过从秘密识别密钥和/或鉴别数据计算的鉴别认证完成数据的交换，和所述交换的数据通过检查每个鉴别认证来得到确认。

本发明有益地提供允许鉴别网上交换数据的消息，即允许用表标表示这些消息。

本发明还提供在多种游戏卡和多种游戏机之间控制价值单元转移的安全系统，而每一机器提供有能力把游戏卡价值单元记入借方的转录器，这

些机器在安全网内通过耦合装置与中央管理计算机联网，而游戏卡贮在其已执行游戏运作的数据有效的存储器内，特别在上述游戏运作期间记入借方和/或记入贷方价值余额有效数据和卡的识别数据，其中，中央管理计算机包含把执行游戏运作的有效数据平行贮存入存储器内的数据库，特别是卡的鉴别数据和在上述游戏运作期间记入借方和/或记入贷方的数据余额的有效的数据，以及对于已识别的卡而言，控制装置确保数据库的数据和卡的数据一致以及尤其是余额的有效数据的一致，以便检查系统的完整性，其特征在于通过从秘密识别密钥和/或鉴别数据计算的鉴别认证完成数据的交换，和所述交换的数据通过检查每个鉴别认证来得到确认。

为鉴别数据消息能有益地在网内，在转录器处，在机器处、在主计算机处或甚至在网的耦合装置处提供安全模块。

使用以下，只作示例说明但非限制其范围的说明和附图，将更清楚地理解本发明。

附图说明

－图 1 表示控制在能实施本发明的多个游戏卡和多个游戏机之间价值单元转移的安全系统。

－图 2 表示本发明的数据交换和检查图。

－图 3 表示由本发明的安全装置执行的鉴别认证计算。

具体实施方式

在图 1 表示如本发明提出并包含多台游戏机 200，200'，200''和 200''' 的游戏机安全系统。

这样的游戏机 200 与俱乐部内可以找到的相似、并包括以下称为游戏卡数据转录器 CJ 的电子自动售货机。

卡数据转录器 210 例如通过 RS485 型串联耦合线连接到机器 200 的电子电路上。机器和读出装置包含与这种耦合线匹配的输入/输出接口。

按照传统的方式机器装备显示屏 211，它允许游戏人在任何时刻知道游戏的内容。

所表示的机器 200 可充分确信是一台专用电子自动售货机，但属于一台双自动售货机。

以智能卡形式表示的游戏卡 CJ 包含一个电可擦除的存储器，例如 EEPROM 存储器。

也可能涉及包含一微处理器、程序存储器和 RAM 型工作存储器的智能卡。

这些智能卡也可以是可再充电型的单装入卡。为此这些卡包含计算盘方式的电可编程存储器。

此外游戏卡能通过不接触卡构成，而该卡包含一个存储器和微处理器集成电路以及无任何电接触的电子数据传输电路。例如能应用如专利请求 FR－96 16061 里描述的转发器。

游戏机 200 的实施例以及其对游戏卡数据转录器的连接在这里不详细说。例如有关游戏机实施例的一些例子在专利请求 FR－96 10031 里详述，其说明现在汇集到本发明的文件。

为了控制用卡进行游戏运作和事务处理，考虑使机器 200，200'，200''，200'''与图 1 在标志 1 之下表示的中央管理计算机联网。网络的机器通过耦合装置 123 连接中央管理计算机。正如图 1 所示，机器 200，200'，200''，200'''也可以彼此通过网络在它们之间连接。

在局部网情况下，耦合装置由俱乐部中那样通过局部耦合线构成。局部耦合线例如是 RS485 型串联耦合线，并联耦合总线，光纤，无线电耦合线或任何其他配套传输线。

在游戏厅分散的网络的情况下，耦合装置能由基于网络的传输通路或由电话线构成。

为了建立电话耦合线，网络包含 MODEM 型 120，120'，120''和 120''' 的调制解调器，作为接口分别安置在耦合装置 123 和游戏机 200，200'，200''，200'''之间。

中央管理计算机例如也通过MODEN101连接到耦合装置123的中央计算机构成，以成为网的一部分。

图 1 以连接游戏机 200，200'，200''和 200'''的环形线的形式表示耦合

装置123。机器连接在其间并且连接到中央管理计算机1上。而耦合能取各种等效形式。

在电话线耦合的情况下机器单独连接到（中央）集中的管理装置上，而机器不需要彼此相连。管理装置的MODEM101能有益地包含多种电话线耦合的交换。

使用电话线耦合的优点是能扩大网络到游戏人住所。游戏机最好由PC型个人计算机300，300'构成。每个机器可以连接到最好使MODEN130或130'整体化的游戏卡310或310'，例如由申请人标志的“Gemtel”型。

所用的网络尤其可以是由开口端的“INTERNET”式的通信网络。

还提供系统和网络包含至少在图 1 以出纳机 100 表示的充电终端设备。而充电终端设备100包含一转录器110。终端100和转录器110通过与耦合装置123相连的MODEM111连接到网络上。

照例规定奉献于游戏的智能卡是非可再充电的卡，如同电话卡一样，它们应由专门的中央机构制造和充电。

在由非再可充电的卡的一些应用里规定：集中管理装置1的数据库BD应知道卡CJ1，CJ2，…，CJn上记入贷方的价值的开始余额S1，S2…Sn（在其流通前）。

然而根据有利的方案，规定卡通过充电终端可对价值单元再充电。

实际上该终端最好可以是俱乐部出纳员的终端。另一方面按照选择的方式能够提供安排在烟草店或其它游戏人可接近的商店内大批充电终端。

因此当一游戏人希望获得信贷时，则他把其游戏卡CJ1交给有资格使用终端的操作员，操作员把卡插入该终端100的转录器100部分并且用出纳机键盘收进游戏人希望接收的贷方数额。该数额将转移到转录器110，该转录器在智能卡CJ1上记录相当于希望信贷的有效的信息。

根据本发明再充电终端设备能够通过网络的耦合装置 123，把在再充电卡读取的数据，尤其是其识别号 Id 及价值单元余额传达给中央管理机1。可以直接通过再充电终端100或者通过其数据转录器110或由中央管理计算机1检验游戏卡CJ1的识别号码。因此本发明考虑游戏运作的预备阶段，在于把卡 CJ1 的起始充电运行期间开始的余额值有效的数据登记在中

央管理计算机 1 的数据库内以及在游戏卡 CJ1 的存储器内。

根据第一方案如图 2 所示的再充电终端或者其转录器 T 使所有游戏卡 CJ1，CJ2，…，CJn 的秘密识别密钥 kt1，kt2，…，ktn 投入流通。这些秘密密钥最好贮存在包含一存储器和计算单元的安全模块 MS1 内，而贮存的数据从外面是不可以存取的。而终端 100 将检验：当按照已知方法应用鉴别算法或加密算法时，智能卡 CJ1 的密钥识别 Id1 同密钥 kt1 匹配。

根据第二方案在中央管理计算机 1 中实现这种卡的鉴别，因而识别号码 Id1，Id2，…，Idn 以及相应的鉴别密钥 kt1，kt2，…，ktn 贮存在中央管理机构的数据库 BD 内或者最好贮存在与 MS1 类似的安全模块 MS0 内。这第二方案的优点是避免所有秘密鉴别密钥的分数。

本发明提供在终端和中央管理计算机之间的数据交换与储存在该中央管理计算机 1 中的数据相关。最好这种数据交换包括鉴别认证。允许发送这种证明的安全协议在以后详细说。该协议有利地避免网络寄生机构过分依赖数据库。因此终端 T 能把游戏卡 CJ1 预先记入借方和/或记入贷方入的价值余额 S 传送给中央管理机 1。在卡的识别号码 Id1 或包括余额数据的认证被鉴别后，可能检验游戏卡 CJ1 的存储器内记录的余额 S 是否很好与贮存在数据库 BD 内的余额一致。如果检验结果是肯定的，则考虑中央管理计算机发一协调信号以便由终端 T 和转录器对卡再充电。在检验否定情况下，在中央管理机或充电终端能触发警戒过程或信号。例如对于俱乐部游戏机网络里出纳员能通过充电终端报警，以便发现这种机能障碍的起因。在更扩展的网络里考虑由终端转录器 T 把卡 CJ1 吞下以便调查机能障碍。

还能考虑：数据库或游戏卡 CJ 的存储器包含一些游戏人信息，例如其年令，游戏习惯以便努力发展忠诚游戏人，授权无偿游玩，等等。

现在进行介绍在由本发明技术和系统执行的游戏运作期间控制价值单元转移协议。

在游戏运作开始，依靠游戏机的卡数据转录器 210 读出游戏卡 CJ 存储器内的识别号码。正如图 2 先前的描述，该识别号码 ID 最好由转录器 T 内提供的安全模块 MS1 鉴别。号码 Id 或许能传送给中央管理计算机 1 以便用包含在安全模块内的识别密钥鉴别卡 CJ1。对于某些在相同机器上用相同卡

的游戏运作该识别步骤最好只执行一次，对于下列操作，机器或终端可能存储该识别号码。

每一个下列的运作，对分配给游戏人用的价值单元余额 S 进行检查。

根据本发明的第一实施例，预先考虑把有关执行的游戏运作的数据，即在该游戏运作期间得到价值单元的新余额简单传送到中央管理计算机 1。因此中央管理计算机 1 以记录在卡 CJ1 的安全记入贷方或记入借方清单形式贮存执行的运作清单。该运作清单 OP101，OP102，…，OP10X 例如依靠使用的卡 CJ1 的识别号码 Id1 记录在数据库 BD 内。

余额 S1 或运作 OP101，OP102，…，OP10X 在中央管理计算机 1 数据库 BD 内的复制以印行运作帐目统计表或执行财务检查。这样一种过程记事也允许在检查伪卡时估计舞弊的范围。

根据本发明的第二实施例考虑一补充情况，在于确保在卡 CJ1 的存储器内的数据和数据库 BD 内的数据相符以便检验由这样的卡 CJ1，这样的机器 200，网络 123 和中央管理计算机构成的系统的完整性。

可以考虑两类检查，检查可以针对识别号码 Id 或针对卡的余额 S。

如以前所述卡 CJ1 的识别号码 Id1 的检查可以用识别密钥 kt1 实现。根据本发明的第二实施例，识别号码 Id 经网的耦合装置 123 传送给中央管理计算机 1。主计算机 1 把流通的卡 CJ1，CJ2，…CJn 的识别密钥 kt1，kt2，…，ktn 贮存在其数据库 BD 内或最好贮存在安全模块 MSO。因此安全模块 MSO 在内部执行识别计算。

此外，检查能针对卡 CJ1 的价值单元的余额。在这种情况转录器 T 依靠卡读出价值单元的余额 S 并通过网的耦合装置 123 把它们送往中央管理计算机 1。因此，卡 CJ1 的余额 S 检查依靠识别号码 Id1 对数据库 BD 内指示的余额 S1 相比进行。如果两余额 S 和 S1 相符则由中央管理计算机 1 准许游戏运作。

根据另一方案也可以检查从游戏卡 CJ1 交换的数据的证明。标准数据加密 DES 型算法标准允许证明在卡 JC1，转录器 T，游戏机和中央管理机 1 之间交换的数值数据。伴随传输数据的证明的加密和解密是可能的和一致的，如果只使用秘密密钥。

数据加密 DES 的算法包含复杂的计算系列，在这里不详细说。

在按下述公式例子，根据给定的称为识别密钥 K 的第一数以及随机数简单考虑算法提供一称为对话密钥的加密数 K'的同时，将公布 DES 算法的实施例:

K'=DES(K，Rnd)

算法 DES 的复杂性使得根据对话密钥 K'和随机数 Rnd 出发不可能求出秘密 k 识别密钥。

图 3 给出了应用算法 DES 的一例。它能够描述网络的安全装置，尤其是通过网络的耦合装置执行的数据交换的安全。游戏卡把至少一个可利用的秘密识别密钥 Kt 安排在不可存取的存储区内。卡的微处理器产生一伪随机数 Rnd1。从这两个数 Rnd1 和 kt 出发，通过由微处理器实施的 DES 算法计算对话密钥 kt'。

该对话密钥 kt 能用来作鉴别认证，并与随机数 Rnd1 和要证明的数据一起发送。然而由于发现任一密钥是不可能的，所以考虑第二次应用算法 DES。正如图 3 所示，发送合格消息的信段的游戏卡要求接收机例如主计算机 1 提供第二随机数 Rnd2。

通过卡的微处理器，算法 DES 重新用于对话密钥 kt'和第二随机数 Rnd2 以便计算证明 C。

数据消息同由卡计算的随机数 Rnd1 和证明 C 一起发送给接收机构。因此所用密钥尤其是秘密识别密钥 kt 和对话密钥 kt'不交换。

通过基于相同数据再计算认证 C'进行数据消息鉴别。中央管理计算机 1 把其秘密识别密钥 kt 安排在其安全模块 MSO 内。这样安全模块 MSO 能根据识别密钥 kt 和随机数 Rnd1 计算对话密钥 kt'。

安全模块 MSO 还具有预先提供给游戏卡的随机数 Rnd2。根据这两数 Rnd2 和 kt'通过第二次用算法 DES，安全模块 MSO 重新计算认证 C'。

通过检查由卡计算的认证 C 与由其安全模块重新计算的认证 C'相符，主计算机能鉴别接收的数据的消息。

让我们注意到，对于每一个要求的消息证明重新计算一新对话密钥 kt'和新认证 C。该过程通过对前述认证的复制确保在网络上无私设的机器可存

取数据库或卡的存储器。

在执行了一次或多次这种检查之后，中央管理计算机 1 发送能加密或译码的协调信号。

在这两最初的实施例，我们已看到：卡执行识别功能，其号码允许主计算机 1 或游戏机上辨认出它，甚至在引导发展忠实顾客的某些应用里辨认出游戏人。此外，卡有小钱包的功能，价值单元余额贮存在卡内，通过卡基本上知道其余额，因此复制中央构构 1 内的余额用于检查目的。

根据第三实施方式，小钱包的功能不再由卡保证而是通过中央管理计算机本身保证。卡不包含任何有关游戏人余额的数据而只包含识别数据，例如识别号 Id，多个鉴别密钥 kta，ktb，ktc 以及也有关于游戏人的信息。这时价值单元的余额 S1 的数据是唯一贮存在中央管理计算机 1 的数据库 BD 内。该价值单元数目依靠识别号码 Id1 例如在数据库内找到。

在游戏运作期间，卡 CJ1 的识别号码 Id 经网络的耦合装置 123 发送到中央管理计算机 1。如果识别号码被机器或其转录器储存则它能直接通过游戏机 200 或其转录器发送。识别号码 Id 也能在卡上读出或在每次游戏运作时通过转录器 210 发送给中央管理计算机 1。

在检查了识别号码 Id 之后中央管理计算机 1，浏览数据库 BD 并且把规定分派于卡 CJ1 的数值单元余额 S1 送往游戏机 200。

根据上述数据交换的安全协议，价值单元余额的数据最好随认证传输。

第三实施方式的优点是：投入游戏的总数额贮存在中央管理计算机 1 内，这避免游戏卡上任何价值记忆。

根据第三实施例，考虑把记入贷方和/或记入借方的价值余额有有效数据贮存在集中管理装置的数据库内，以避免作用智能卡的任何舞弊。

在第三实施例中控制简单地在于用在中央管理计算机 1 的数据库 BD 内读出的识别密钥 kt1 检查识别号码 Id 以控制卡的完整性。

应用本发明第三实施例可以看到：在游戏机上使用的游戏卡能有益地用于检查完整性。

此外，通过实施保护数据交换方式，本发明允许有益地检验由游戏卡、

游戏机网络、中央管理计算机的数据库形成的系统的完整性，因此，系统三元素之一或卡、或网络或数据库被检查用于完整性。

事实上本发明提供一个有能力实施本发明处理的系统。

这样一种系统包含多台游戏机，每一台机器装备有能力将游戏卡价值单元记入借方的转录器，机器通过耦合装置在网内与中央管理计算机连接。

根据本发明用智能卡在游戏机上执行的游戏运作的有效数据贮存在游戏卡的存储器内以及并行地存储在中央管理计算机提供的数据库内。

贮存的数据是由卡的识别数据和余额或用卡记入借方和/或记入贷方的价值单元的相继的余额组成。

提供一些控制方法例如对卡的识别号码进行鉴别和对贮存在卡上或数据库内的余额值进行比较，还对交换的数据进行证明的计算机程序，以便检查系统的完整性。

为了使网上的数据交换安全，最好考虑：安全模块应基于贮存在模块存储器内秘密数据计算识别认证以及控制方法应确保由安全模块计算的鉴别认证与由游戏卡或另一安全模块计算的鉴别认证一致。

这样一些安全模块 MS0，SM1 可提供在游戏卡 CJ1，CJ2，…，上或在转录器 10，110，210，210'，210''，210'''，310 上，游戏机 200，200'，200''，200'''上，中央管理计算机 1 上，或甚至在网络的耦合装置 123 上。

特别是在网内能提供若干安全模块或分散的安全装置。每一转录器 10，210，210'，210''，210'''或每一接口 11，120，120'，120''，120'''例如包含一安全模块，使得在耦合装置 123 上的数据交换包括鉴别认证，例如发射器 10 将其由接收转录器 210 鉴别的认证在发送到相应机器 200 之前加到其消息上。

本发明的其他实施例方案，优点和特点对专业人员看来是清楚的且不超出所附权利要求的范围。

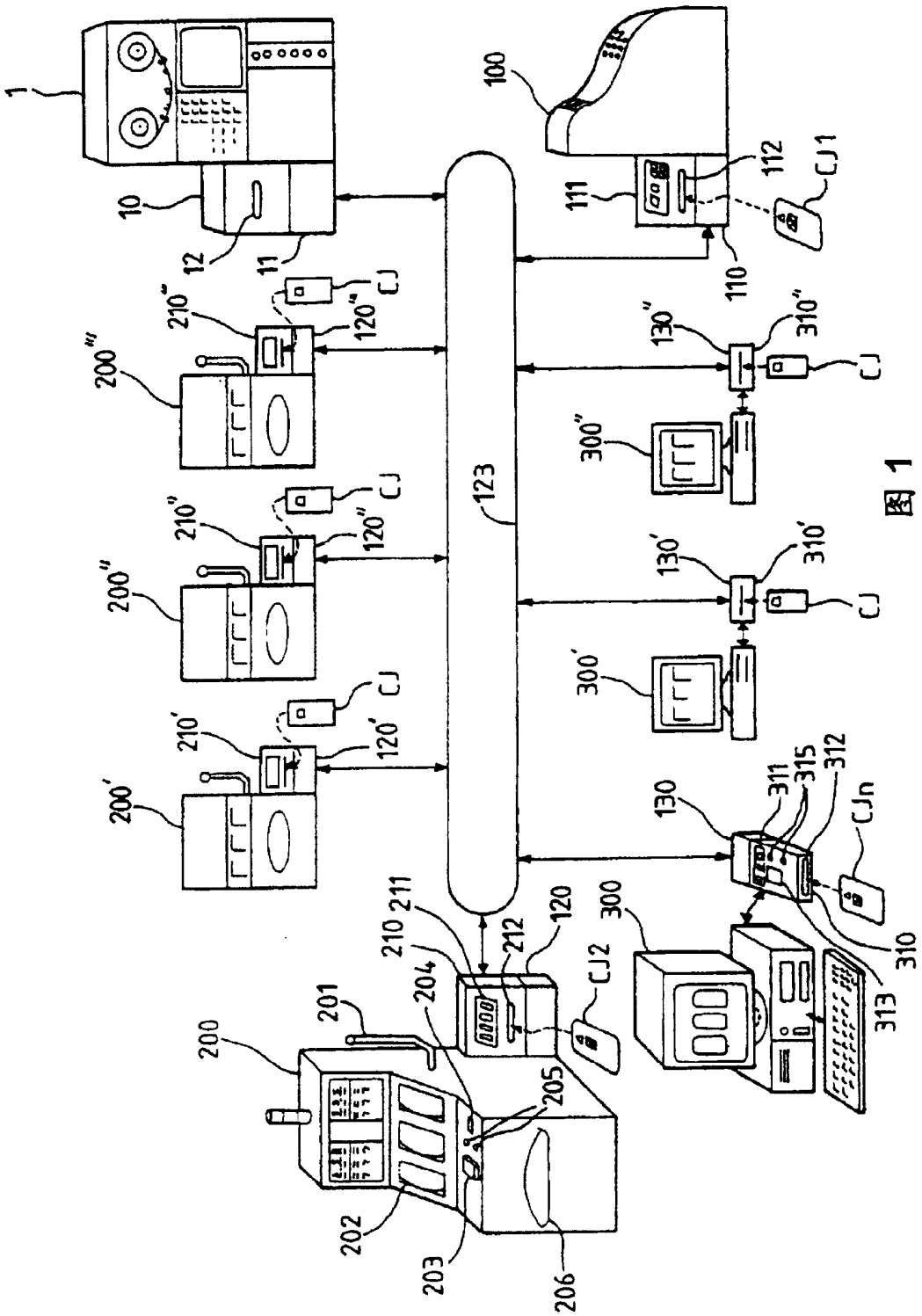

1
10
12
11
100
111
112
CJ1
110
210"
120"
CJ
200"'
130"
310"
300"
123
210"
120"
200"
130'
310'
300'
210'
120'
200'
311
315
312
CJn
310
313
211
210
212
120
CJ2
300
201
204
200
205
202
203
206

图 1

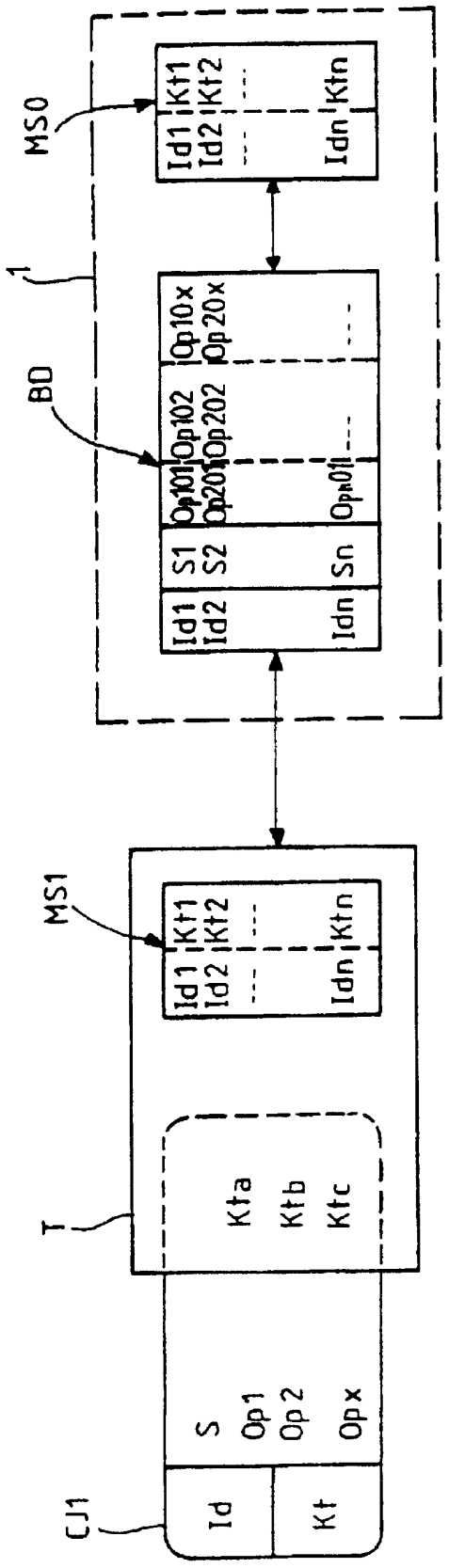

MS0
Id1 Id2 Idn
Kt1 Kt2 Ktn
1
BD
Op10x Op20x
Op101 Op102 Op201 Op202 Op(n)01
S1 S2 Sn
Id1 Id2 Idn
MS1
Id1 Id2 Idn
Kt1 Kt2 Ktn
T
Kta Ktb Ktc
CJ1
Id
Kt
S Op1 Op2 Opx

图 2

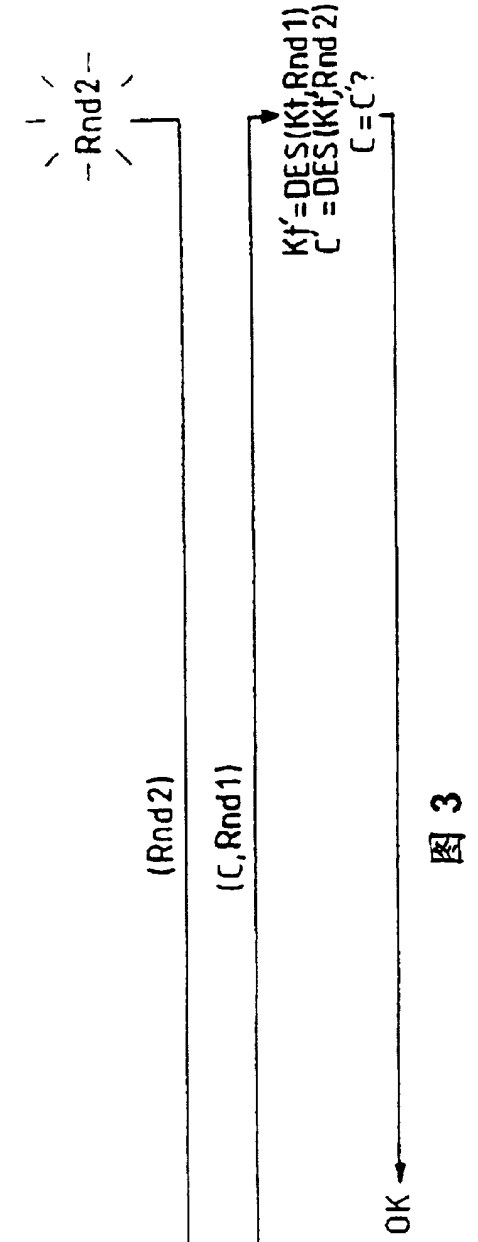

Rnd2
(Rnd2)
Kt'=DES(Kt,Rnd1)
C'=DES(Kt',Rnd2)
C=C'?
(C,Rnd1)
Rnd1
Kt'=DES(Kt,Rnd1)
C=DES(Kt',Rnd2)
OK

图 3