[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 19/00 (2006.01)
A63F 13/12 (2006.01)

[12] 发明专利说明书

专利号 ZL 00817166.1

[45] 授权公告日 2007 年 7 月 4 日

[11] 授权公告号 CN 1324513C

[22] 申请日 2000.12.5 [21] 申请号 00817166.1
[30] 优先权
[32] 1999.12.17 [33] FR [31] 99/15950
[86] 国际申请 PCT/FR2000/003382 2000.12.5
[87] 国际公布 WO2001/045025 法 2001.6.21
[85] 进入国家阶段日期 2002.6.14
[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 斯特凡妮·利翁 燕梅·唐－塔尔皮
[56] 参考文献
US5643086A 1997.7.1
US5850447A 1998.12.15
US5768382A 1998.6.16
审查员 徐 春

[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

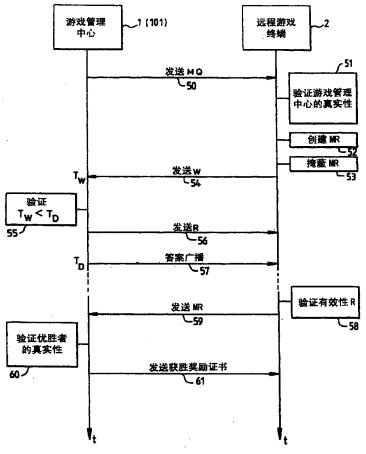
权利要求书 4 页 说明书 11 页 附图 3 页

[54] 发明名称

远程游戏管理的保密方法

[57] 摘要

与至少一个远程游戏终端链接的游戏管理中心，向它所链接的终端发送一个包含游戏标识符和问题的消息。游戏者通过远程游戏终端输入的应答，以用秘密掩蔽的形式向游戏管理中心发送，从而保证用户匿名。如果被掩蔽的应答消息，在答案广播的瞬时之前被收到，游戏管理中心就向所述游戏终端发送确认回执。继而向所有远程游戏终端广播对问题的答案。如果游戏者已给出正确答案，为获取其奖品，终端必须发送一个消息，这个消息包含确认回执和证明它是用来掩蔽应答的秘密的所有者的一个项目。



1．一种游戏管理中心（1，101）和至少一个远程游戏终端（21-23；121-123；2）之间的远程游戏管理的保密方法，其特征在于：它包括与远程游戏终端有关的步骤：

a）从所述游戏管理中心（1，101）接收包含游戏标识符 ID_GAME 以及问题的第一消息 MQ；

b）构造应答消息 MR，其包含游戏标识符 ID_GAME 以及利用所述游戏终端的游戏者的应答；

c）以只有游戏终端知道的密码 y，K_y 掩蔽应答消息 MR；

d）向游戏管理中心发送掩蔽的应答消息 W；和

e）当在步骤 d）中发送的游戏者的应答被游戏管理中心考虑时，从所述游戏管理中心（1，101）接收一个确认收妥回执 R。

2．如权利要求 1 所述的方法，其特征在于：步骤 c）包括：

产生秘密随机数 x；

在这个秘密数 x 上应用单向函数（f），从而产生公开掩蔽数 y；

利用所述公开掩蔽数 y，掩蔽应答消息 MR。

3．如权利要求 2 所述的方法，其特征在于：单向函数（f）是基于下列关系定义的离散对数函数：

$y=g^x \bmod p$

这里 p 和 g 是已知数值，p 是最小 512 位的最大的质数，g 是 Z/pZ 产生器，Z 是有理整数组，mod 是模函数。

4．如权利要求 1 所述的方法，其特征在于：步骤 c）包括借助所述远程游戏终端产生的对称保密密钥 K_y，对应答消息 MR 加密。

5．如权利要求 2 所述的方法，其特征在于：在步骤 a）中接收的第一消息 MQ 还包括：

游戏管理中心的标识符 ID_CJ；

证书，所述证书是由认证当局核发给游戏管理中心的，通过认证当局的公开密钥解密辨认，提供游戏管理中心的公开密钥，其与所述游戏

管理中心的标识符相对应；

借助于与游戏管理中心的公开密钥关联的专用密钥，整体或部分的签署所述消息。

6．如权利要求 5 所述的方法，所述远程游戏终端存有认证当局的公开密钥，其特征在于：在步骤 b）中，远程游戏终端在构成应答消息 MR 之前，借助于由认证当局核发的证书，验证游戏管理中心的真实性。

7．如权利要求 1 所述的方法，其特征在于：在步骤 b）中构建的应答消息还包含辅助定制数据。

8．如权利要求 5 所述的方法，其特征在于：掩蔽的应答消息 W 在步骤 d）中以游戏管理中心的公开密钥的加密的形式发送。

9．如权利要求 5 所述的方法，其特征在于：在步骤 e）中的确认回执 R 中，包括借助于专用密钥的数字署名，所述数字署名由游戏标识符 ID_GAME 和掩蔽的应答消息 W 链接而成。

10．如权利要求 5 所述的方法，其特征在于包括附加步骤：当在步骤 d）中发送的游戏者的应答是在步骤 a）中收到的第一消息 MQ 中所含问题的正确答案时，游戏者要求所赢得的奖品，所述附加步骤包括：

f）向游戏管理中心发送要求奖品 MP 的消息，至少包含：

在步骤 e）从游戏管理中心收到的确认回执 R；

一个项证明所述游戏终端拥有在步骤 c）中用来掩蔽应答消息 MR 的密码；

游戏管理中心接受来自获胜游戏者使用的终端要求奖品的消息。

11．如权利要求 10 所述的方法，其特征在于：在步骤 f）中由远程游戏终端（2）向游戏管理中心发送的，以证明所述终端拥有密码的项包括：

公开掩蔽数 y，

秘密随机数 x，

它们是早先在步骤 c）中产生的。

12．如权利要求 10 所述的方法，其特征在于：在步骤 f）中由远程游戏终端（2）向游戏管理中心发送的，以证明所述终端拥有密码的项包括：

—公开掩蔽数 y；

—证明，其通过零知识规约，证明所述终端也是拥有用于产生所述公开掩蔽数 y 的秘密随机数 x。

13．如权利要求 4 所述的方法，其特征在于包括：当在步骤 d)中发送游戏者的响应是对包含在步骤 a)中接收的第一消息 MQ 的问题的正确回答时，游戏者要求赢得的奖金的附加步骤，所述附加步骤由获胜者使用的远程游戏终端（2）执行，并包括：

f）向游戏管理中心发送要求奖金的消息，至少包括：

在步骤 e)中从游戏管理中心接收的确认回执 R；

对称保密密钥 K_y。

14．如权利要求 10 至 13 之一所述的方法，其特征在于：在步骤 f）中，远程游戏终端（2）在发送要求奖品 MP 的消息之前，验证步骤 e）中的游戏管理中心收到的确认回执 R 的真实性。

15．如权利要求 10 所述的方法，其特征在于：任何在步骤 f）过程中由远程游戏终端向游戏管理中心发送的消息以用游戏管理中心的公开密钥加密的形式发送。

16．如权利要求 12 所述的方法，其特征在于：在零知识规约范围内，由远程游戏终端从游戏管理中心收到的消息以用游戏管理中心的公开密钥所关联的专用密钥加密的形式发送。

17．一种游戏管理中心（1，101）和至少一个远程游戏终端（21-23；121-123；2）之间的远程游戏管理的保密方法，其特征在于：它包括与游戏管理中心有关的步骤：

i)向远程游戏终端(21-23；121-123；2)发送包含游戏标识符 ID_GAME 以及问题的消息 MQ；

j）从所述远程游戏终端（21-23；121-123；2）接收应答消息 MR 中的游戏者的应答，这个消息是被以只有远程游戏终端知道的密码（y，K_y）掩蔽 W 的；

k）验证：掩蔽的应答消息 W，是在对步骤 i）中所提问题的应答广播的瞬时 T_D 之前的瞬时 T_W 收到的；

l）在步骤 k）中得到确证的情况下，向所述远程游戏终端发送确认

回执 R；

m）向所述远程游戏终端广播在步骤 i）中所提问题的回答。

18．如权利要求 17 所述的方法，其特征在于包括向获胜游戏者分派奖品的附加步骤：

n）接收来自获胜游戏者使用的终端要求奖品 MP 的消息，这个消息至少包含：

在步骤 l）中发送的确认回执 R；

一个项证明所述远程游戏终端拥有在步骤 j）中收到的掩蔽应答消息使用的密码；

o）核验在所述要求奖品的消息中所收到的应答的真实性；

p）在步骤 o）中得到确证的情况下，在实施装置中向获胜游戏者分派奖品。

远程游戏管理的保密方法

技术领域

本发明涉及游戏管理中心和远程游戏终端之间的远程游戏管理的保密方法。

背景技术

游戏的组织者日益注重利用开放式网络，例如互联网或交互式电视提供的可能性，来组织远程游戏。

US－A－5 850 477特别描述了一种用于参加交互电视游戏的系统，其中采用与游戏有关事件的（年月日）时间顺序进行核验的方法。

远程游戏提出的主要问题是：

—对组织者来说，要确信优胜者的真实性，

—对游戏者来说，要确信他们的答案在游戏结束之前一直保密，并且，如果它们获胜，能收到他们的奖品。

关于在远程游戏中保护机密，通常建议解决方法的要点是在游戏之前，游戏者向游戏的组织者登记。在这种情况下，他们收到一个标识符和有关的密码，然后，任何时候他们想玩游戏都必须使用它们。

在游戏之前必须登记意味着游戏者不能即兴地参与游戏。这个系统的另一个缺点是，游戏者匿名不能被保证，因为他总是在标识符之下游戏。

发明内容

本发明的目的是提出一种新颖的方法，以解决上述问题，这种新颖的远程游戏管理方法使游戏者能即兴地游戏，而不需要任何事先登记手续，并且，在保证机密性的同时，从游戏组织者和游戏者双方看来，都是匿名的。

因此，根据其第一方面，本发明涉及游戏管理中心和至少一个远程游戏终端之间的远程游戏管理方法，所述方法包括下列远程游戏

终端实现的步骤。

第一步骤是，从所述游戏管理中心接收包含游戏标识符以及问题的第一消息。

第二步骤是，构造应答消息，其包含游戏标识符和使用所述游戏终端的游戏者对所述问题的应答。

第三步骤是，以秘密掩蔽应答消息；

第四步骤是，向游戏管理中心发送掩蔽的应答消息。

第五步骤是，当在第四步骤中发送的游戏者应答已被游戏管理中心考虑时，从所述游戏管理中心接收确认回执的消息。

凭借本发明的方法，游戏者能即兴地游戏，因为他不需要向游戏管理中心预先登记。因此，以掩蔽的形式发送他的应答，能保证他匿名，同时保证他的应答传输的安全。

根据本发明的第一实施例，第三步骤的要点是：产生保密随机数；在这个保密随机数上应用一个单向函数，从而产生一个公开掩蔽数码，并利用这个公开掩蔽数码，掩蔽应答消息。

根据本发明第二实施例，第三步骤是借助所述远程游戏终端产生的对称保密密钥，对应答消息加密。

根据一个特定的实施例，在第一步骤发送的第一消息中进一步包括：游戏管理中心的标识符；由认证当局发给游戏管理中心的证书，可借助于认证当局的公开密钥对其解密，可产生与所述游戏管理中心的标识符相对应的游戏管理中心公开密钥；所述消息的整体或部分的署名，这个署名要借助于游戏管理中心关联的专用密钥。

其优点是能够验证游戏管理中心，特别是，保证所提出的问题确实来源于认证当局认可的游戏组织者，并且在传输中不曾被黑客改造。

根据这个特定实施例的另一方面，每个远程游戏终端含有认证当局的公开密钥，在第二步骤中，远程游戏终端在构成应答消息之前，借助于认证当局的公开密钥验证游戏管理中心的真实性。

根据本发明的另一个特定的实施例，由远程游戏终端在第二步骤中构成的应答消息，包括辅助定制数据。这可包括游戏者的姓名，他的地址，他的电话号码等等。当然，这些数据借助于公开掩蔽的数据以隐藏

的形式被发送，以便保证游戏者匿名，除非在游戏者获胜并希望得到他的奖品的情况下，他将不被公开。

根据本发明的另一个优选实施例，掩蔽的应答消息在第四步骤中以用游戏管理中心的公开密钥加密的形式发送。除了掩蔽应答以外，这提供了第二级保密性。

根据本发明的另一个实施例，在第五步骤发送的确认回执包括消息的署名，借助于与游戏管理中心的公开密钥关联的专用密钥，这个署名由游戏标识符和远程游戏终端所发送的掩蔽应答消息链接而成。

根据本发明的另一个方面，方法包括一个随后的附加步骤，当在第五步骤中发送的游戏者的应答，是在第一步收到的包含在第一消息中问题的正确答案时，游戏者要求所赢得的奖品。

第六步骤是获胜游戏者所使用的远程游戏终端，向游戏管理中心发送要求奖品的消息，至少包括：在第五步骤中从游戏管理中心收到的确认回执；一个项证明所述游戏终端是在第三步骤中用来掩蔽应答消息秘密的所有者。

在第一变型中，如果应答消息在本发明的第一实施例第三步骤中已被掩蔽，则在第六步骤发送的项包括，曾在第三步骤产生的公开掩蔽数和秘密随机数。

在第二变型中，在第六步骤发送的项包括公开掩蔽数和通过零知识规约的证明装置，即终端也是用于产生所述公开掩蔽数的秘密的所有者。

根据本发明的第二实施例，如果应答消息在第三步骤已被掩蔽，则在第六步骤发送的项包括对称秘密密钥。

本发明也涉及远程游戏终端，它能够实现上述方法的步骤 1 至 6 中至少一个。

根据第二方面，本发明也涉及在游戏管理中心和至少一个远程游戏终端之间的远程游戏管理的安全方法，该方法包括游戏管理中心执行的下列步骤。

第一步骤是，向远程游戏终端发送包括游戏标识符以及问题的第一消息。

第二步骤是，从所述远程游戏终端接收游戏者的应答，这个应答消

息只有远程游戏终端才知道秘密掩蔽。

第三步骤是，验证接收到掩蔽应答消息先于在第一步骤中提出问题的应答的广播。

第四步骤是，在第三步骤中验证确实的情况下，向所述远程游戏终端发送确认回执。

第五步骤是，向所述远程游戏终端广播对第一步骤中提出的问题的回答。

在本发明的这一方面的特定实施例中，游戏管理中心通过第一双向通信路径和通过从管理中心至终端的第二单向通信路径，与所有的远程游戏终端链接。根据这个实施例，第一消息通过所述单向通信路径在第一步骤发送。例如，它可以是利用电缆或卫星的无线电波广播路径。

根据这个实施例的另一方面，第五步骤中应答的广播通过单向路径进行。

根据本发明的这个第二方面的另一特定实施例，方法包括一些附加步骤，它们是由游戏管理中心执行，向获胜的游戏者分派奖品。

第六步骤是，接收来自获胜游戏者所使用的远程游戏终端要求奖品的消息，该消息至少包括：在第四步骤中发送的确认回执；和一个项证明所述远程游戏终端是第二步骤中收到的掩蔽应答所用的秘密的所有者。

第七步骤是，验证在所述要求奖品的消息中收到的应答的有效性。

第八步骤是，在第七步骤中验证确实的情况下，向获胜游戏者分派奖品的执行装置。

发明还涉及游戏管理中心，它能够执行上述步骤 1 至 8 中的至少一个。

附图说明

本发明的其他特征和优点，通过参考附图对非限定实施例的详细描述将会显露出来，附图中：

图 1 表示本发明第一实施例的与若干远程游戏终端链接的游戏管理中心；

图 2 表示本发明第二实施例的与若干远程游戏终端链接的游戏管理

中心；

图 3 表示本发明的远程游戏管理的方法；

图 4 和 5 表示本发明方法中使用的消息内容。

具体实施方式

下面将详细描述游戏管理中心管理的方法，它能在不同类型的环境中实现，特别是更适用于互联网或交互电视结构内。

图 1 中所表示的是适用本发明方法的第一典型环境。例如，位于游戏组织者的游戏管理中心 1 是一个服务器，游戏应用程序在其中执行。它通过第一双向网络 30 链接至用户那里的远程游戏终端 21，22，23。

例如，远程游戏终端可以是配有微处理器模块的电视接收机，与服务器 1 中执行的游戏应用程序相应的程序在微处理器中执行。它们也可以是通过电缆或通过卫星甚至游戏操纵台发送的数字或模拟电视信号的解码器。远程游戏终端包括特别是由显示屏构成的用户界面，它能够描述游戏组织者提出的问题；键盘或任何其他装置能够输入答案，以响应所提问题（尤其是遥控）。

在图 1 的例子中，游戏管理中心 1 与广播中心 11 协同工作，广播中心 11 通过第二单向网络 31 与远程游戏终端通信。

例如，在游戏的组织者是电视节目的分销商的情况下，广播中心 11 是他用来广播节目的地方。例如，单向网络 31 是用电缆或用卫星以无线电波广播数字和模拟电视信号。它可以从游戏管理中心 1 同时向与它链接的所有远程游戏终端 21，22，23 发送信息项目。

例如，第一双向网络 30 是由交换型电话网的电话线或其余的较高速专用数字线形成的。在游戏方法实现于交互式电视结构之内的情况下，双向网络 30 构成交互式节目的返回通路。这个网络 30 能够在每个远程游戏终端和游戏管理中心之间在两个方向上建立各自的通信。

如图 2 所示，实现本发明游戏方法的第二类环境中，游戏管理中心 101 通过双向链路 40 与互联网链接，每个远程游戏终端 121，122，123 通过双向链路 41，42，43 也与互联网链接。

在这个典型的应用中，这些远程游戏终端由形成潜在游戏者的用户

那里的个人计算机形成。

现在，我们将适当地结合图 3 至 5，描述游戏管理方法。

本发明的游戏管理方法特别适用于这样的游戏，在其中向游戏者提出问题，给他们一定的时间应答。它可包含一个有意思的问题，需要有专门的知识才能回答。在彩票的情况下，问题可以是请游戏者为未来的随机翻牌打睹。在这种情况下，期望的应答是彩票翻牌的结果。

图 3 中图解说明的是本发明的游戏管理的方法，这个方法用在游戏管理中心 1 或 101 与所有链接至游戏管理中心的终端中给定的远程游戏终端 2 之间。游戏管理方法的各种步骤，已沿时间轴 t 表示出来，时间轴 t 分为两个，以便说明两个设备之间所进行的交换。

下面将描述的游戏管理方法的第一部分，涉及实际的游戏，就是说，提出问题的动作和匿名回答它的方式。

在第一步骤 50 中，游戏管理中心向与它链接的所有远程游戏终端发送问题。如上面已看到的，这个问题可能在电视游戏中（例如，将消息显现在屏幕上的形式）或其他互联网站上提出。问题提出的实际方式不构成本发明的主题，所以在下面不做进一步描述。

实际上，所提的问题以消息 MQ 的形式，游戏管理中心向每个远程游戏终端发送，这个消息最好通过单同通信路径 31（图 1）发送，如果它存在的话，在相反的情况下，则通过双向通信路径 40—43（图 2）发送。如果游戏在交互式电视传输结构中进行，这个消息尤其能在视频信号流中发送。

消息 MQ，它的内容在图 4 中以图形表示，包含一个游戏识别数据 ID_GAME，这个数码对于每个游戏（就是说对于每个新提出的问题）是不同的，它唯一地识别所提出的问题。这个游戏识别数码在与消息 MQ 中的问题本身（“QUESTION”—图 4）相同的时间被发送。

游戏管理中心也能在消息中发送验证元素，这个验证元素使远程游戏终端能检验所提问题发源于由认证当局认可的游戏管理中心，并且，在传输期间不曾被改变。

为些，消息 MQ 最好包含一个识别游戏管理中心数码 ID_CJ，这个数码对于每个游戏管理中心是不同的，并且它是由认证当局唯一地分配

给每个游戏管理中心的。认证当局也分配给每个游戏管理中心一个证书，这个证书使得游戏管理中心的标识符 ID_CJ 和与保密方式有关的公开密钥 K_{PVB_CJ}。特别是，已知的信息保密方法是利用公开密钥密码系统，其中每个部分占有只让他自己知道的专用密钥，和让其他部分知道的公开密钥。认证当局本身占有它签署证书的专用密钥和公开密钥，公开密钥包含在远程游戏终端中，如下面将看到的，使他们能检验证书的有效性。

在本申请中，优选使用根据 ITU-T 标准，推荐 X.509/ISO/IEC 9594-8，建立证书，本文将进一步参考其细节。

证书在消息 MQ（“CERTIFICATE”—图 4）中被发送，这个消息还包含一个借助于与游戏管理中心的公开密钥 K_{PUB_CJ} 有关的专用密钥 K_{PRI_CJ} 的署名消息（“SIGNATURE”）。例如，署名被定义如下：

$$Sign_{KPRI\_CJ}（ID\_CJ||QUESTION）\qquad（1）$$

这里“||”表示链接算子，“Sigh“是已知的数学函数，例如散列函数，它有一个对应的函数“Verif”存在，满足：

$$Verif_{KPUB\_CJ}（Sign_{KPRI\_CJ}（M1），M2）=\text{true if } M1=M2\qquad（2）$$

$$Verif_{KPUB\_CJ}（Sign_{KPRI\_CJ}（M1），M2）=\text{true if } M1\neq M2$$

这里，M1、M2 是任意消息。

这使得有可能检验消息确实发源于游戏管理中心，并在它的传输期间不曾被改变。

就远程游戏终端 2 来说，方法的一下步骤 51 是检验游戏管理中心的真实性。

为此，如上述看到的，分配给用户的每个游戏终端包含认证当局的公开密钥。借助于这个公开密钥，游戏终端检验 CERTIFICATE 的内容，并恢复游戏管理中心的公开密钥 K_{PUB_CJ}。因此，能确保包含在消息中的游戏中的识别号数 ID_CJ 确实与证书上的一致。借助于公开密钥 K_{PUB_CJ}，游戏终端还有利用上文提出的验证函数，验证包含在消息 MQ 中的

SIGNATURE 确实与消息的内容一致。

在下一步骤 52 中，假定使用远程游戏终端 2 的游戏者已经回答了包含在消息 MQ 中的问题，并通过游戏终端的用户界面将它输入。这样，游戏终端就建构一个消息 MR，它的内容如图 5 中所示，它包含游戏者给出的答案（“ANSWER”），游戏标识号数 ID_GAME，最好还有辅助（AUXILIARY）定制数据（DATA），例如游戏者的姓名或名字，他的地址，他的电话号码等。

根据本发明的原理，这个消息然后在步骤 53 中被用秘密掩蔽，为的是在游戏者发送他的答案时，确保游戏者匿名。

因此，根据一个优选实施例，远程游戏终端产生一个随机数 x。例如，这个数能从技术人员熟知的伪随机数据产生器发送出来。这个数必须保持机密，不能往游戏终端散发。当他以后在游戏中获胜时，它将被用作他确实给出过正确答案的证明。

然后，游戏终端 2 用这个秘密的随机数 x 创建公开掩蔽数 y，它将形成用来掩蔽应答消息 MR 的秘密。这个公开掩蔽数 y 必须以这样的方法从秘密 x 创建，即已知 y 以及以 x 形成 y 所用的函数，也不可能提取出 x。

所以，用一个单向函数 f 从 x 计算 y。

基于离散对数的函数将被优选用作函数 f，并特别地被描述于 ISO 9796 标准第 4 部分中，它以下列关系（3）定义：

$$y=g^x \bmod p \qquad (3)$$

这里 p 和 g 是已知数值，p 是最大的质数（最小 512 位），g 是产生器 Z/pZ（Z 是有理整数组），“mod”是模函数。

然后，远程游戏终端（2）借助于公开掩蔽数 y 进行下列计算（4），以创建掩蔽的应答消息 W：

$$W=y \oplus MR \qquad (4)$$

这里，⊕表示“异或”函数（或“XOR”）。

其他算法显然也可以用于借助数 y 对应答消息 MR 进行掩蔽，特别是有可能进行两项相乘，模 p。

在本发明的第二实施例中，消息 MR 的掩蔽是利用远程游戏终端产

生的对称保密密钥 K_y 加密而实现的，优选地根据 DES 标准（Data Encryption Standard（数据加密标准））。

在下一步骤 54 中，远程游戏终端 2 向游戏管理中心发送掩蔽的应答消息 W。

根据本发明的目的，游戏者的应答是秘密的和匿名的，因为除非知道 y 和 K_y，是不可能从消息 W 中单独提取出游戏者的应答的。

尽管如此，仍有可能在变型实施例中，通过以用游戏管理中心的公开密钥 K_{PUB_CJ}（在步骤 51 中，终端已将它恢复）加密的形式发送消息 W 的方法，使保密水平添加一级。

游戏管理中心在瞬时 T_W 接收消息 W。在下一步骤 55 中，它验证这个瞬时 T_W 确实先于对步骤 50 中所提问题的答案的广播瞬时 T_D。这样就能保证游戏者不致欺骗，他的答案不会是在游戏的组织者广播正确答案之后发送的。

然后，在步骤 56，游戏管理中心向游戏终端发送一个确认回执 R，向游戏者担保他的掩蔽的应答确实已经被游戏的组织者登记。根据这一个优选实施例，确认回执由下式计算：

$$R=Sign_{KPRI\_CJ}（ID\_GAME||w） \qquad （5）$$

这就是说，借助于与游戏管理中心的公开密钥 K_{PUB_CJ} 关联的专用密钥计算数字署名，它是由游戏标识符 ID_GAME 和掩蔽的应答消息 W 的链接而成的。

最后，游戏管理方法的第一部分终止于游戏管理中心在瞬时 T_D 广播正确答案（步骤 57）。比较好的是，答案的广播通过单向网络 31（图 1）进行，如果它存在的话，特别是交互式电视游戏的情况下。如果游戏建在互联网上，答案可在游戏组织者的互联网位置上表明。答案的实际广播方式不是本发明的主题，所以在下面将不做进一步描述。

刚才描述的步骤当中，步骤 51 至 56 显然可由与管理中心链接的每个远程游戏终端完成。

游戏管理方法的第二部分，涉及游戏者已给出对所提问题的正确答

案，并要求获得他的奖品的情况。假定第二部分开始时，游戏者已经证实在步骤 57 中的广播答案与他在步骤 52 中给出过的答案符合，并且，他已经通过游戏终端 2 的用户界面发出通知，向游戏组织者要求他的奖品。

这时候，游戏终端 2 必须向游戏管理中心证明，游戏者在游戏时（在步骤 52 至 54）确实给出过正确答案。它还必须证明，它知道用来掩蔽应答的秘密。这样就能保证只有真实的获胜者才能收到奖品。

为此，游戏终端 2 将用游戏管理中心曾在步骤 56 发送给它的确认回执 R，作为游戏者的答案向游戏组织者登记过的证明。

在第一步 58 中，远程游戏终端 2 首先利用例如在上文中提出的验证函数组，借助于游戏管理中心的公开密钥 K_{PUB_CJ}，检验确认回执 R 的有效性。

当验证确实，从而证明确认回执没有被第三者修改时，游戏终端向游戏管理中心发送（步骤 59）消息 MP，证明游戏者已经给出正确答案，并且信函数确实是由他发出的。

如果应答消息 MR 已经在本发明的第一优选实施例的步骤 53 中被掩蔽，消息 MP 就会包含确认回执 R 以及作为掩蔽消息 MR 的数 y 以形成消息 W。确认回执能够证明，游戏终端确实已在步骤 54 中发送过掩蔽的消息 W。

为证明掩蔽的应答消息 W 确实曾发自远程游戏终端 2，还需要证明后者曾知道用来计算 y 的秘密数 x。仍然在这个第一实施例中，根据第一变型，消息 MP 因此还包含秘密随机数 x。

在第一实施例的第二变型中，消息 MP 包含确认回执 R 和公开掩蔽数 y，但它不包含秘密数 x。在这个优选变型实施例中，零知识规约被用来向游戏管理中心证明，远程游戏终端 2 知道秘密数 x，但不直接显露这个数 x。

当上文中关系式（3）所定义的单向函数已被用于从 x 计算 y 时，Schnorr 验证规约将被优选用来证明知道 x 而不直接发送 x。

这个规约运行如下：

1．远程游戏终端 2 产生一个随机数 r_1，通过它按下文关系式（6）

计算一个 z_1，并在消息 MP 中发送这个数 z_1；

$$z1=g^{r1} \bmod p \qquad (6)$$

2. 游戏管理中心在应答中向远程游戏终端 2 发送一个二进制数 b_1（等于 0 或 1）；

3. 游戏终端 2 按照下文关系式（7）计算数值 u_1，并将它发往游戏管理中心；

$$u_1=r_1-b_1\times x \qquad (7)$$

4. 游戏管理中心验证下文关系式（8）为真；

$$g^{u1}=y^{b1}\times z_1 \qquad (8)$$

这些步骤 1 至 4 必须以不同的数 r_1，z_1，b_1 和 u_1 重复几次，以使游戏管理中心确信游戏终端 2 知道 x。

如果应答消息 MR 已经在本发明的第二实施例的步骤 53 中被掩蔽，在步骤 59 中发送的消息 MP 就会包含确认回执 R 以及秘密密钥 K_y。确认回执能够证明，游戏终端确认在步骤 54 中发送过掩蔽的应答 W，密钥 K_y 能够证明，终端知道用来掩蔽应答信号的秘密。

有利的是，为进一步改善交换的保密性，所有在游戏管理中心和远程游戏终端 2 之间交换的消息都加密。因此，在第一实施例（或第二实施例）的第一变型中发送的消息 MP 以用游戏管理中心的公开密钥 K_{PUB_CJ} 加密的形式发送。在第一实施例的第二变型中，从游戏终端 2 向游戏管理中心发送的消息消息 MP，和发送的数 u_1，以公开密钥 K_{PUB_CJ} 加密，而从游戏管理中心向远程游戏终端发送的消息，以游戏管理中心的专用密钥 K_{PRI_CJ} 加密。

在步骤 60 中，游戏管理中心验证获胜者的真实性，这就是说，它要查看只在第一实施例（或在第二实施例）的第一变型中才有的消息 MP，或者其余的在第一实施例的第二变型中按照 Schnorr 验证规约被交换的消息，验证游戏者的应答是正确的答案，并且确实是从他那里发送过来的。

在验证确实的情况下，在步骤 61 中向远程游戏终端 2 发送获胜奖品证书，使游戏者能收到证书上的指明的奖品。

任何适当的方法都可以用来向获胜者分派奖品。

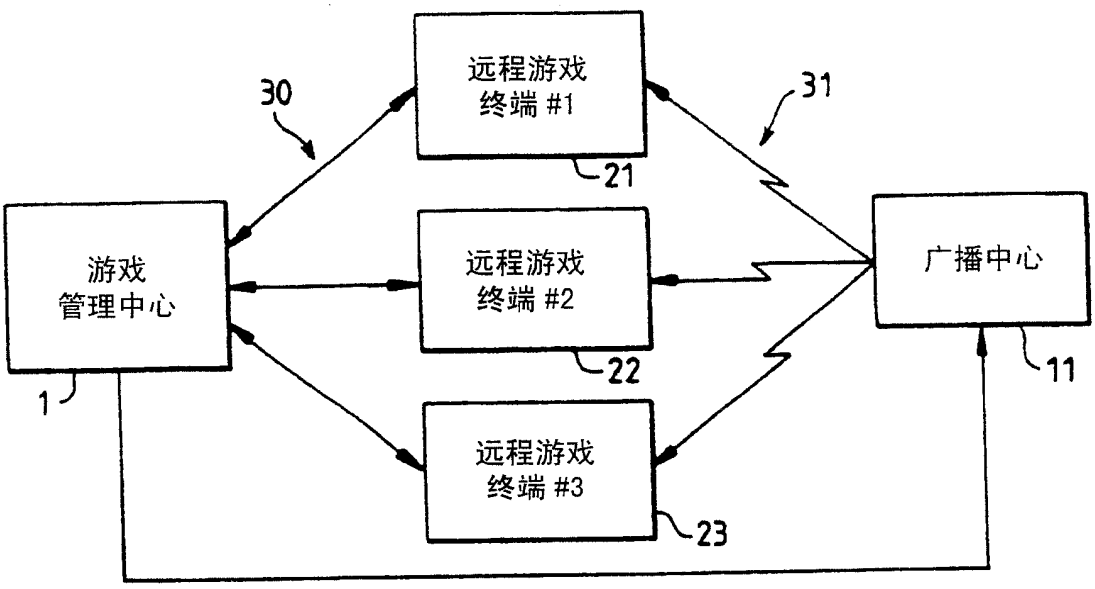

远程游戏
终端 #1
30
31
21
游戏
管理中心
远程游戏
终端 #2
广播中心
22
11
1
远程游戏
终端 #3
23

图 1

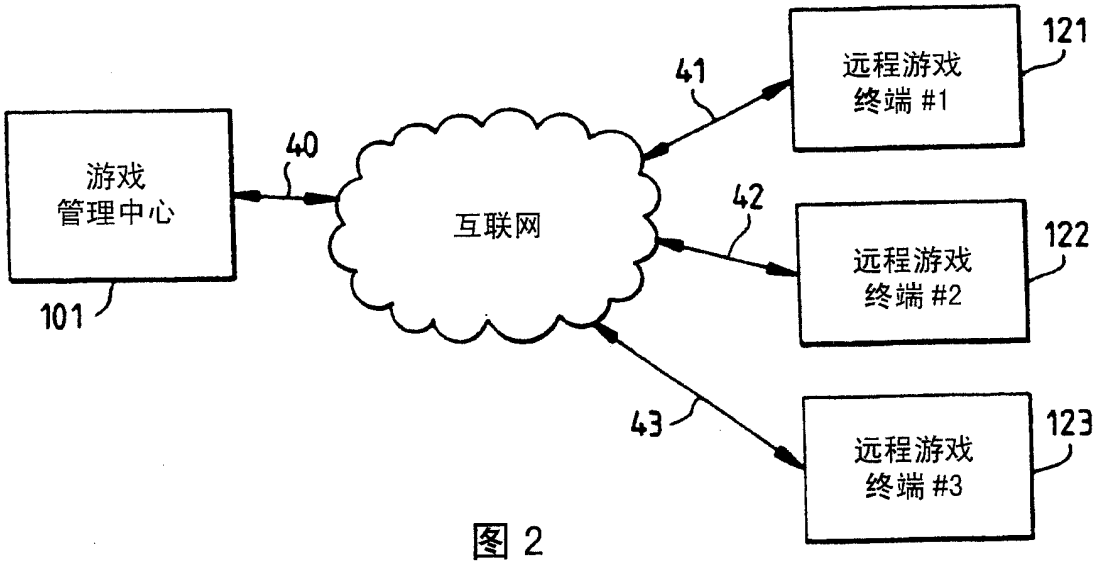

121
41
远程游戏
终端 #1
游戏
管理中心
40
互联网
42
远程游戏
终端 #2
122
101
43
远程游戏
终端 #3
123

图 2

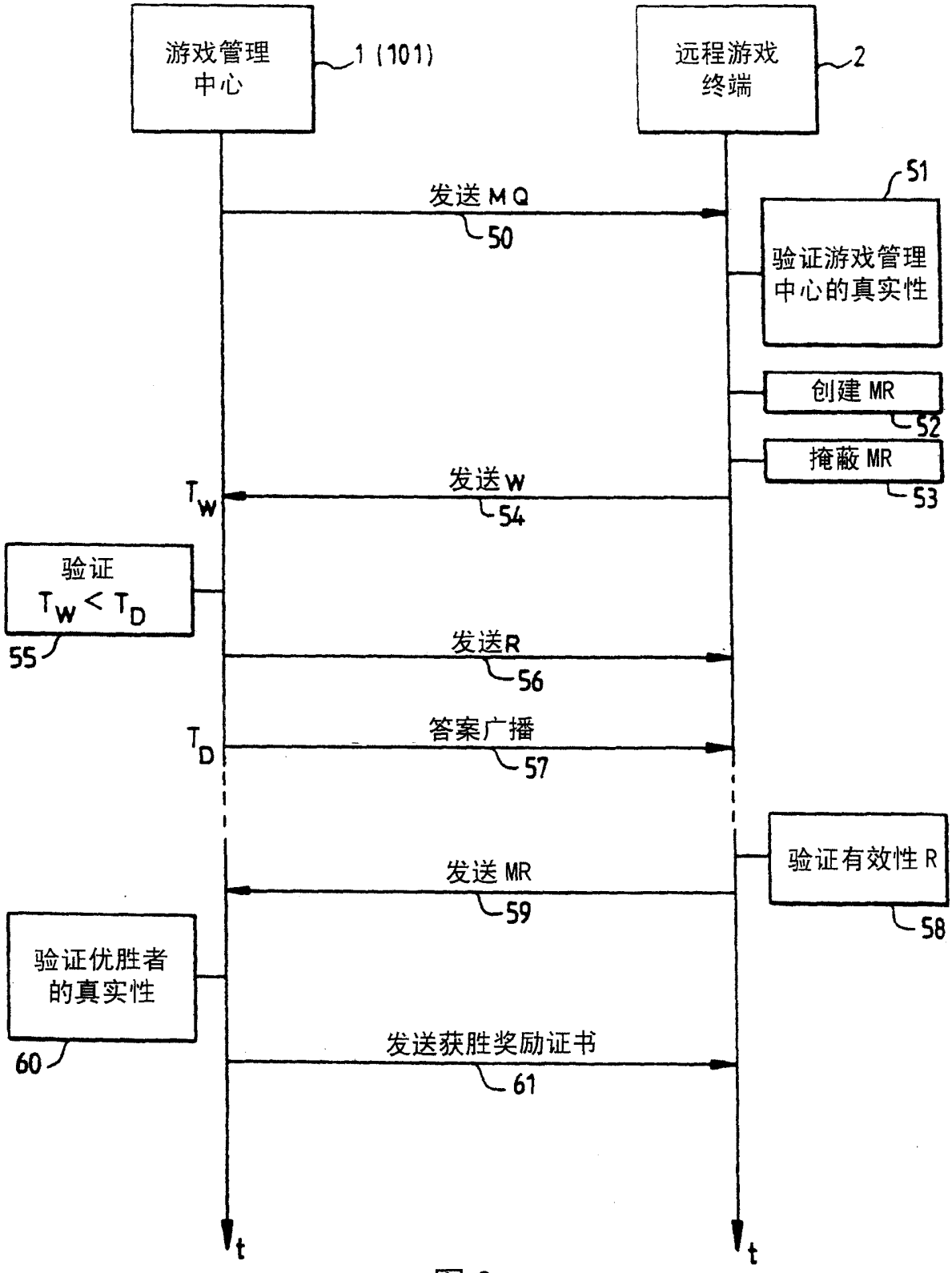

游戏管理中心
1 (101)
远程游戏终端
2
51
发送 MQ
50
验证游戏管理中心的真实性
创建 MR
52
掩蔽 MR
53
T_W
发送W
54
验证
$T_W < T_D$
55
发送R
56
T_D
答案广播
57
验证有效性 R
58
发送 MR
59
验证优胜者的真实性
60
发送获胜奖励证书
61
t
t

图 3

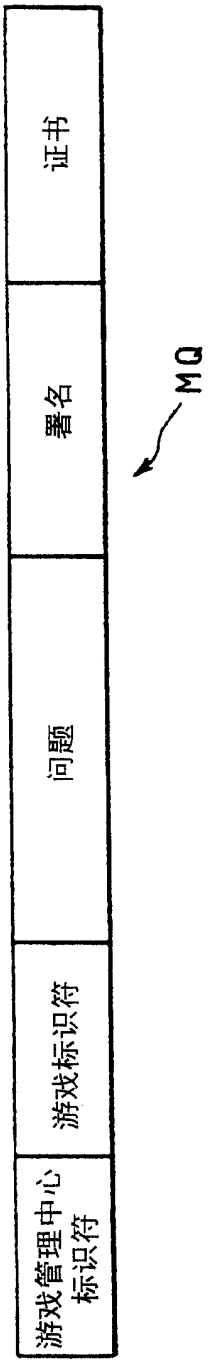


图 4

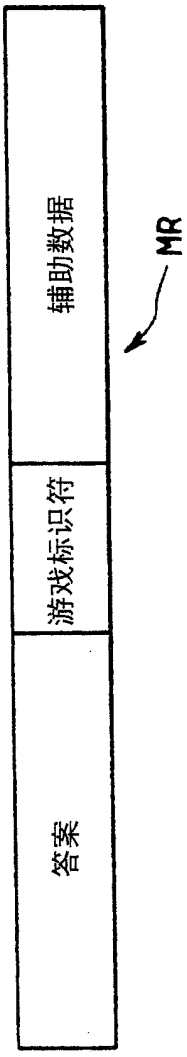


图 5