



[12] 发明专利申请公开说明书

[21] 申请号 01811791.0

[43] 公开日 2003 年 8 月 27 日

[11] 公开号 CN 1439123A

[22] 申请日 2001.5.9 [21] 申请号 01811791.0

[30] 优先权

[32] 2000. 5. 10 [33] US [31] 60/203,277

[86] 国际申请 PCT/CA01/00648 2001. 5. 9

[87] 国际公布 WO01/86386 英 2001. 11. 15

[85] 进入国家阶段日期 2002. 12. 26

[71] 申请人 泰克林克国际娱乐有限公司

地址 加拿大新斯科舍

[72] 发明人 维克托·Y·曹 约翰·西多斯

[74] 专利代理机构 北京市柳沈律师事务所

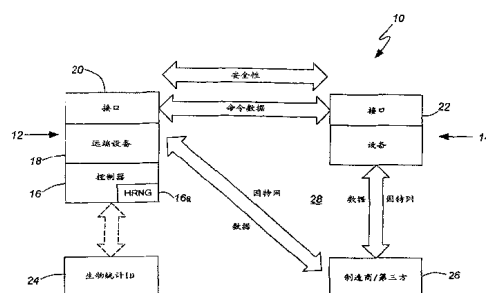
代理人 黄小临 王志森

权利要求书 5 页 说明书 30 页 附图 11 页

[54] 发明名称 用于在设备之间进行高级交易的安全系统

[57] 摘要

本发明提供了用于在设备之间进行高级交易 (transaction) 的安全系统和方法。该系统包括在远端设备与主机设备 (host device) 之间提供多级加密的非确定性硬件随机数发生器。



1. 一种用于保护远端设备与主机设备之间的数据交易（transaction）的系统，该远端设备包括：

5 适合于主机设备与远端设备之间操作性连接的接口；

操作性地连接到接口的管理控制器，所述的管理控制器用于控制远端设备与主机设备之间的数据交易；以及

操作性地连接到管理控制器的硬件随机数发生器（HRNG）控制器，用于把供数据加密用的非确定性随机数数据提供给管理控制器。

10 2. 如权利要求 1 的系统，其中，硬件随机数发生器控制器包括提供流式（streaming）随机数比特的硬件随机数发生器，并且硬件随机数发生器控制器把随机数比特格式化至少一种预定的字节格式。

3. 如权利要求 1 的系统，其中，硬件随机数发生器控制器包括受保护的存储区。

15 4. 如权利要求 3 的系统，其中，硬件随机数发生器控制器产生存储在受保护的存储区中的身份识别（ID）号。

5. 如权利要求 4 的系统，其中，用身份识别解密密钥把身份识别号加密到第一级。

20 6. 如权利要求 5 的系统，其中，为了用主机设备注册远端设备，用公开密钥把加密的身份识别号加密到第二级。

7. 如权利要求 5 的系统，其中，主机设备用公开密钥把身份识别号解密到第一级，并且主机设备存储第一级加密的身份识别号。

8. 如权利要求 6 的系统，其中，公开密钥由系统管理员来改变。

25 9. 如权利要求 6 的系统，其中，在注册后，硬件随机数发生器控制器在主机设备与远端设备之间交换应用专用数据之前，检验第一级加密身份识别号的有效性。

10. 如权利要求 9 的系统，其中，一旦检验第一级加密身份识别号，硬件随机数发生器控制器就产生用于把应用专用数据加密到第一数据加密级的数据解密密钥。

30 11. 如权利要求 10 的系统，其中，硬件随机数发生器控制器产生用于把身份识别号加密到第一级的新的身份识别解密密钥。

12. 如权利要求 11 的系统, 其中, 把加密到第一数据加密级的应用专用数据和加密到第一级的身份识别号以及数据解密密钥相互附加在一起, 以形成附加的数据分组。
13. 如权利要求 12 的系统, 其中, 用公开密钥加密附加的数据分组。
- 5 14. 如权利要求 1 的系统, 其中, 接口是穿过 (pass through) 接口。
15. 如权利要求 1 的系统, 其中, 接口是无线的。
16. 如权利要求 1 的系统, 其中, 至少一种预定的格式包括至少一种机会对策 (game-of-chance) 格式。
17. 如权利要求 1 的系统, 其中, 硬件随机数发生器控制器能够进行物理和电侵入检测, 并且响应物理或电侵入而自毁内部存储器。
- 10 18. 如权利要求 1 的系统, 还包括与远端设备操作性地连接的生物统计识别系统。
19. 如权利要求 18 的系统, 其中, 生物统计识别系统是从语音识别系统、面部识别系统或语音指纹识别系统的任何一种或它们的组合中选择出来的。
- 15 20. 如权利要求 1 的系统, 其中, 远端设备关于主机设备是秘密 (stealth) 的。
21. 一种用于控制和管理主机设备与软件保护器 (dongle) 之间的数据通信的软件保护器, 该软件保护器包括:
- 适合于主机设备与软件保护器之间的操作性连接的接口;
- 20 操作性地连接到接口的管理控制器, 所述的管理控制器, 用于从主机设备接收数据、和向主机设备提供数据, 以及, 用于从与管理控制器操作性地连接的硬件随机数发生器控制器接收数据、和向与管理控制器操作性地连接的硬件随机数发生器控制器提供数据, 所述的硬件随机数发生器控制器用于把非确定性随机数数据提供给管理控制器。
- 25 22. 如权利要求 21 的软件保护器, 其中, 硬件随机数发生器控制器包括用于提供流式随机数比特的硬件随机数发生器, 并且, 硬件随机数发生器控制器把随机数比特格式化至少一种预定的字节格式。
23. 如权利要求 21 的软件保护器, 其中, 硬件随机数发生器控制器包括受保护的存储区。
- 30 24. 如权利要求 23 的软件保护器, 其中, 硬件随机数发生器控制器产生存储在受保护的存储区中的身份识别号。

25. 如权利要求 24 的软件保护器, 其中, 硬件随机数发生器控制器用身份识别解密密钥把身份识别号加密到第一级。

26. 如权利要求 25 的软件保护器, 其中, 在用主机设备注册远端设备期间, 硬件随机数发生器控制器用公开密钥把加密的身份识别号加密到第二级。

5 27. 如权利要求 26 的软件保护器, 其中, 在注册后, 硬件随机数发生器控制器在主机设备与远端设备之间交换应用专用数据之前, 检验第一级加密身份识别号的有效性。

28. 如权利要求 27 的软件保护器, 其中, 一旦检验第一级加密身份识别号, 硬件随机数发生器控制器就产生用于把应用专用数据加密到第一数据加密级的数据解密密钥。

29. 如权利要求 25 的软件保护器, 其中, 对于应用专用数据的每一次交换, 硬件随机数发生器控制器产生用于把身份识别号加密到第一级的新的身份识别解密密钥。

30. 如权利要求 28 的软件保护器, 其中, 把加密到第一数据加密级的应用专用数据和加密到第一级的身份识别号以及数据解密密钥相互附加在一起, 以形成附加的数据分组。

31. 如权利要求 30 的软件保护器, 其中, 用公开密钥加密附加数据分组。

32. 如权利要求 21 的软件保护器, 其中, 接口是穿过接口。

33. 如权利要求 21 的软件保护器, 其中, 接口是无线的。

20 34. 如权利要求 21 的软件保护器, 其中, 至少一种预定的格式包括至少一种机会对策格式。

35. 如权利要求 21 的软件保护器, 其中, 硬件随机数发生器控制器能够进行物理和电侵入检测, 并且响应物理或电侵入而自毁内部存储器。

25 36. 如权利要求 21 的软件保护器, 还包括与远端设备操作性地连接的生物统计识别系统。

37. 如权利要求 36 的软件保护器, 其中, 生物统计识别系统是从语音识别系统、面部识别系统或语音指纹识别系统的任何一种或它们的组合中选择出来的。

38. 如权利要求 21 的软件保护器, 其中, 软件保护器关于主机设备是秘密的。

39. 一种用主机设备注册特定的远端设备的方法, 该方法包括步骤:

- a. 产生非确定性身份识别号，并将其存储在远端设备中；
- b. 用非确定性身份识别解密密钥把身份识别号加密到第一级；
- c. 用公开密钥把第一级加密的身份识别号加密到第二级；
- d. 把第二级加密的身份识别号传递给主机设备；以及
- 5 e. 用公开密钥把主机设备中的第二级加密的身份识别号解密到第一级，并把第一级加密的身份识别号存储到主机设备中。

40. 一种用主机设备检验特定的远端设备的注册的方法，该方法包括步骤：

- a. 通过远端设备从主机设备请求第一级加密的非确定性身份识别号；
- 10 b. 接收第一级加密的非确定性身份识别号，并且用先前产生并存储的非确定性身份识别解密密钥来解密第一级加密的非确定性身份识别号；以及
- c. 检验步骤 b) 的解密的非确定性身份识别号与远端设备中先前产生并存储的非确定性身份识别号之间的等效性。

41. 一种在先前注册的远端设备与主机设备之间传送数据的方法，该方法包括步骤：

- a. 用非确定性数据解密密钥来加密数据分组；
- b. 用非确定性身份识别解密密钥来加密身份识别号；
- c. 用步骤 b) 的身份识别解密密钥，把步骤 a) 的加密的数据分组附加到步骤 b) 的加密的身份识别号上，以形成加密的数据分组；
- 20 d. 用公开密钥来加密步骤 c) 的加密的数据分组，以形成第二级加密的数据分组；
- e. 把第二级加密的数据分组传递给主机设备；以及
- f. 用公开密钥和数据解密密钥来解密步骤 e) 的第二级加密的数据分组，以检索数据分组。

25 42. 如权利要求 41 的方法，其中，用步骤 b) 的加密的身份识别号更新先前存储在主机设备中的加密的身份识别号。

43. 一种用服务提供商 (service provider) 注册用户而使得可以从非安全场所访问服务提供商的系统，该系统包括步骤：

- 在用于注册用户的安全或非安全场所，
- 30 a) 把字符个人身份识别号 (PIN) 提供给用户；
- b) 把语音个人身份识别号提供给用户；

c) 让用户说出语音个人身份识别号到语音指纹处理器中, 以产生语音个人身份识别号的安全场所语音指纹文件; 以及

d) 把字符个人身份识别号和语音指纹文件存储在授权的用户的数据库中。

5 44. 如权利要求 43 的系统, 还包括步骤:

在具有计算机、和与授权的用户的数据库操作性地连接的第二语音指纹处理器的安全场所,

a) 提示用户输入字符个人身份识别号;

10 b) 提示用户把语音个人身份识别号输入到第二语音指纹处理器中, 以产生非安全场所语音指纹文件;

c) 把字符个人身份识别号和非安全场所语音指纹文件提交给授权的用户的数据库; 以及

在授权的用户的数据库中,

15 d) 在授权的用户的数据库中的字符个人身份识别号中搜索相似的字符个人身份识别号; 以及

e) 根据所记录的语音指纹文件, 在非安全场所语音指纹文件中搜索相似的字符个人身份识别号, 以确定非安全场所语音指纹文件是否与所记录的语音指纹文件相对应。

20 45. 如权利要求 44 的系统, 还包括通知用户他们是授权的用户还是未授权的用户的步骤。

46. 如权利要求 45 的系统, 还包括步骤: 如果用户是授权的用户, 并且已经得到对服务提供商的服务的访问, 那么, 就周期性地请求重新输入字符个人身份识别号和语音个人身份识别号, 以便被重新授权。

25 47. 如权利要求 43 的系统, 其中, 用户在注册时, 在步骤 a) 之前, 声明他们是否满足用于访问服务提供商的特定的注册标准。

48. 一种用于注册和保护每一个都具有如权利要求 21 的软件保护器和中央注册数据库的主机设备之间的交易的方法, 该方法包括步骤:

a) 用中央注册数据库把加密的身份识别号(ID#)注册在软件保护器中; 以及

30 b) 在允许主机设备之间的公开密钥加密的交易之前, 检验每一个主机设备是否已经完成了步骤 a) 的注册。

用于在设备之间进行高级交易的安全系统

5 技术领域

本发明提供了一种用于在设备之间进行高级交易的安全系统和方法。该系统包括在远端设备与主机设备之间提供多级加密的非确定性硬件随机数发生器 (HRNG)。

10 背景技术

在因特网和电子交易逐渐普及的世界里，交易安全性是交易所涉及的各方最关心的问题。为了使不必要的第三方获得关于交易的信息和/或获得以后能够访问特定的设备或系统的信息的风险最小化，这种安全性是必须的。在当今的繁忙的电子世界里，所有类型的交易，包括个人之间的交易、个人与商家/机构之间的交易、也包括商家或机构之间的交易，都需要交易安全性。另外，在某些企业中，还需要：由本身也可能需要复杂的安全级别的第三方管理者和/或许可的代理机构选择地监视的特定的交易。

在安全交易领域中，加密/解密技术的使用是众所周知的。也就是说，众所周知，可以将不同方之间发送的数据加密，然后，由第二方，在接收到加密数据后，用包括加密/解密密钥的各种方法将其解码。典型地，加密/解密密钥是基于伪随机（确定性）的算法，并因此局限于：它们具有循环长度有限的重复模式。一个熟练的程序员在数小时之内，或者，甚至在数分钟之内就可以创建一个这种伪随机数发生器的数学模型，并从而破坏设备的安全性。毁坏安全系统的能力常常既可以借助于关于安全协议的内部信息而造成，也可以不借助于关于安全协议的内部信息而造成。

相比之下，非确定性随机数发生器因预测结果或影响结果的风险更加困难，而本质上更安全。这种非确定性或基于硬件的随机数发生器 (RNG) 已经经受了各种各样的统计随机数发生器的测试，例如，由 InfoGard 实验室 (由美国商业部的标准技术国家研究院 (NIST)、加拿大政府的通信安全机构 (CSE) 和由 NVLAP 授权的密码测试实验室，密码模块测试实验室 (授权号 100432-2)) 在联邦信息处理标准 (FIPS) 出版物 140-1 中规定的那些测试，

并且,已经证实,这种非确定性或基于硬件的随机数发生器能够提供非确定性结果。

硬件随机数发生器基于自然发生的随机现象而产生真正随机的比特。一个例子是从微米尺寸的热耗散陶瓷电阻中产生的 Johnson(约翰逊)或白噪声。

5 噪声的放大、A/D 转换和数字处理能够产生循环长度无限的随机位流。这种随机性是真正随机的,因为,它是由于在加热的电阻内的电子的随机运动保证在所有频率上具有相等噪声密度的宽带噪声源的热噪声的函数。当前的硬件随机数发生器不需要初始值或种子(seed),并且,可以以通常不小于 20 千比特/秒和通常只受系统的速度限制的速度进行操作。

10 目前,为提供高的安全级别,设备之间的敏感的交易是通过硬件和软件两者的解决方案而提供的。这些设备包括蜂窝电话、网络设备、电缆调制解调器、机顶盒、网络计算机、卫星接收器、掌上电脑和博弈机。当把高价值内容的电影、博弈、金融信息、电子商务、合作信息、保密电子邮件和语音通信转移到这些设备中时,强壮的数据安全性仍然是所有各类平台所需要的。

15 更具体地说,博弈产业需要极高级别的安全性,以确保保持支持机会对策的机器的诚实性(integrity)。为授权博弈许可证,博弈管理者必须对每一个博弈机的诚实性满意,以确保博弈的公正性并防止可能决定博弈结果的任何非法的攻击。目前,博弈设备内的随机数发生器是基于软件的,本质上是确定性的,因此,易遭受富有经验的黑客的攻击。

20 在软件产业中,普遍使用软件保护器(dongle)(一种硬件和软件安全设备)。软件保护器用于确保单个用户在任何特定的时间、在特定的机器上受限地使用许可软件的特定的拷贝,以防止在许可协议之外非法使用软件。现有软件保护器通常连接到设备的 I/O 端口,并且,在主机程序周期地询问时进行操作,以提供有效代码。如果没有提供代码,主机程序就终止。

25 在金融交易产业中,金融和其它数据的交换,要求在交易期间经常使用基于软件的加密/解密系统具有高级别的安全性。

由于对交易诚实性的要求,人们需要一种在不同设备之间进行电子交易时提供更高级别的安全性的系统。尤其是,需要一种安全系统,能够产生非确定性的基于硬件的随机数,以供在设备之间创建加密/解密密钥之用,以便
30 减小从第三方进行非法攻击的可能性。尤其是,需要防备可能拥有特权信息的设计者和开发者。

另外,在这种安全系统内,需要使现有主机设备的功能随着非确定性随机数发生器的安全特点的增加而增强的增加的智能。

再者,随着对来自许多不同设备的交易安全性的要求的不断提高,需要一种系统,可以容易地改进现有设备,否则,不与设备及其相关的外围设备的常规操作相互干扰。还要求安全系统对设备的常规操作是透明的,以便使系统的主要功能的性能损失降到最低。

再者,随着密码、个人身份识别号(PIN)、卡和令牌越来越多地用于访问远端帐户,与用户拥有和管理许多不同安全设备相联系的安全风险也不断增加。相应地,需要一种包括生物统计识别系统的高级用户识别系统,包括与其它安全系统耦合在一起的电子指纹、语音和面部识别系统。

发明内容

根据本发明,提供了一种用于保护远端设备与主机设备之间的数据交易的系统,所述的远端设备包括:

15 适合于主机设备与远端设备之间的操作性连接的接口;

操作性地连接到接口上的管理控制器,所述的管理控制器用于控制远端设备与主机设备之间的数据交易;以及

操作性地连接到管理控制器的硬件随机数发生器控制器,用于把供数据加密用的非确定性随机数数据提供给管理控制器。

20 根据再一个实施例,本发明提供了一种用于控制和管理主机设备与远端设备之间的数据通信的系统,包括:

适合于主机设备与远端设备之间的操作性连接的接口;以及

操作性地连接到接口的管理控制器,所述的管理控制器,用于从主机设备接收数据、和向主机设备提供数据,以及,用于从与管理控制器操作性地连接的硬件随机数发生器控制器接收数据、和向与管理控制器操作性地连接的硬件随机数发生器控制器提供数据,所述的硬件随机数发生器控制器用于把非确定性随机数数据提供给管理控制器。

根据又再一个实施例,本发明提供了一种用主机设备注册特定的远端设备的方法,包括步骤:

- 30 a. 产生非确定性身份识别(ID)号,并且将其存储在远端设备中;
b. 用非确定性身份识别解密密钥把身份识别号加密到第一级;

- c. 用公开密钥把第一级加密的身份识别号加密到第二级;
- d. 把第二级加密的身份识别号传递给主机设备;
- e. 用公开密钥把主机设备中的第二级加密的身份识别号解密到第一级,并且把第一级加密的身份识别号存储到主机设备中。

5 在又一个实施例中, 本发明提供了一种用主机设备来检验特定的远端设备的注册的方法, 包括步骤:

- a. 通过远端设备从主机设备请求第一级加密的非确定性身份识别号;
- b. 接收第一级加密的非确定性身份识别号, 并且用先前产生并存储的非确定性身份识别解密密钥来解密第一级加密的非确定性身份识别号; 以及
- 10 c. 检验步骤 b 的解密的非确定性身份识别号与远端设备中先前产生并存储的非确定性身份识别号之间的等效性。

在又一个实施例中, 本发明提供了一种在先前注册的远端设备与主机设备之间传送数据的方法, 包括步骤:

- a) 用非确定性数据解密密钥来加密数据分组;
- 15 b) 用非确定性身份识别解密密钥来加密身份识别号;
- c) 用步骤 b) 的身份识别解密密钥, 把步骤 a) 的加密的数据分组附加到步骤 b) 的加密的身份识别号上, 以形成加密的数据分组;
- d) 用公开密钥来加密步骤 c) 的加密的数据分组, 以形成第二级加密的数据分组;
- 20 e) 把第二级加密的数据分组传递给主机设备; 以及
- f) 用公开密钥和数据解密密钥来解密步骤 e) 的第二级加密的数据分组, 以检索数据分组。

本发明也可以提供一种用远端设备和主机设备的用于特定的用户识别的生物统计识别系统。

25 在又一个实施例中, 提供了一种系统, 该系统用服务提供商来注册用户, 使得可以从非安全场所访问服务提供商, 包括步骤:

在用于注册用户的安全或非安全场所,

- a) 把字符个人身份识别号提供给用户;
- b) 把语音个人身份识别号提供给用户;
- 30 c) 让用户说出语音个人身份识别号到语音指纹处理器中, 以产生语音个人身份识别号的安全场所语音指纹文件

d) 把字符个人身份识别号和语音指纹文件存储在授权的用户数据库中。

本发明还又提供了一种系统，其中，在具有计算机、和与授权的用户数据库操作性地连接的第二语音指纹处理器的安全场所，一种方法是：

5 a) 提示用户输入字符个人身份识别号；

b) 提示用户把语音个人身份识别号输入到第二语音指纹处理器中，以产生非安全语音指纹文件；

c) 把字符个人身份识别号和非安全场所语音指纹文件提交给授权的用户数据库；以及

10 在授权的用户数据库中，

d) 在授权的用户数据库中的字符个人身份识别号中搜索相似的字符个人身份识别号；以及

e) 根据记录的语音指纹文件，在非安全场所语音指纹文件中搜索相似的字符个人身份识别号，以确定非安全场所语音指纹文件是否与记录的语音指纹文件相对应。

15

在又一个实施例中，提供了一种用于注册和保护每一个都具有软件保护器和中央注册数据库的主机设备之间的交易的方法，包括步骤：

a) 用中央注册数据库把加密的身份识别号(ID #)注册在软件保护器中；以及

20 b) 在允许主机设备之间的公开密钥加密的交易之前，检验每一个主机设备是否已经完成了步骤a)的注册。

附图说明

从参考附图的如下描述中，本发明的这些和其它特征将会更加清楚，其中：

25

图 1 是根据本发明的安全系统的总体图；

图 2 是根据本发明的一个实施例的基于硬件随机数的远端设备的整体图；

图 3 是根据本发明的一个实施例的安全协议的整体图；

30 图 3a 是根据本发明的一个实施例的两部分身份识别号的整体图；

图 3b 是根据本发明的一个实施例的、与数据一起发送的两部分身份识别

号的整体图；

图 4 是根据本发明的一个实施例的并行端口专用软件保护器的概略图；

图 5 是根据本发明的一个实施例的含有生物统计语音身份识别的串行端口专用软件保护器的电路图；

5 图 6 是根据本发明的一个实施例的用含有生物统计识别系统的服务提供商来注册用户和给用户授权的概略图；

图 7 是具有读卡机的安全系统的概略图；以及

图 8 是用中心站点来注册远端设备并认证交易的安全系统的概略图。

10

具体实施方式

本发明的一般性描述

根据本发明，并且参照图 1，提供了能够在电子设备之间，具体地说，是在远端设备 12 与本地设备 14（主机设备）之间进行安全数据交易的安全系统 10。远端设备 12 包括与管理微控制器 18 和接口 20 操作性地连接的、

15 含有硬件随机数发生器 16a 的硬件随机数发生器控制器 16。远端设备 12 通过有线或无线链接与本地设备 14 通信，以便在设备之间交换数据，或者把单向命令数据提供给在各自接口 20 和 22 之间的本地设备 14。在本发明的各种实施例中，远端设备 12 可以包括生物统计身份识别功能块 24。远端设备 12 与本地设备 14 均可以通过诸如因特网之类的网络链接 28 与制造商或第三方 26

20 通信，以便在各设备之间发送和接收数据。

远端设备的硬件随机数发生器 16，建立和管理远端设备 12 与本地设备 14 之间的安全措施，从而能够在远端设备 12 与本地设备 14 之间进行高安全性的数据交易。远端和本地设备的例子的非穷举（non-exhaustive）列表和它们的基本功能列于表 1 中。

25

表 1 - 远端/本地设备的例子

远端设备	远端设备的功能	接口	本地设备	本地设备的功能
用于博弈产业的软件保护器	-硬件随机数发生器安全 -硬件随机数发生器格式化的博弈数据	穿过（pass-through）接口（例如，串行或并行）	博弈设备（VLT）	-用户参与博弈
用于点对点/因特网交易的软件保护器	-硬件随机数发生器安全	穿过接口（例如，串行或并行）	金融业务（例如，银行服务器）	-会计管理 -金融交易

远端控制设备	-硬件随机数发生器安全 -命令数据	有线或无线	消费者产品（例如，汽车、家用电器）	-执行远端命令数据
--------	----------------------	-------	-------------------	-----------

远端设备硬件操作整体图

参照图 1 和图 2，在远端设备 12 的每一个实施例中，远端设备 12 包括与管理微处理器 18 和接口 20 操作性地连接的硬件随机数发生器控制器 16。

管理控制器 18 通常提供硬件随机数发生器控制器 16 与本地设备 14 之间的物理和硬安全保护墙，也管理与硬件随机数发生器控制器 16 的所有保密通信。

硬件随机数发生器控制器 16 包括：产生非确定性流式随机数比特的硬件随机数发生器 16a。硬件随机数发生器控制器 16 捕获来自硬件随机数发生器 16a 的随机数比特流，并把该随机数比特流格式化应用敏感字节（如果需要的话）或用于加密数据的前后关系。另外，管理控制器 18 管理硬件随机数发生器控制器 16 与主机设备 14 之间的受保护的（加密的）通信。

远端设备与本地设备之间的通信协议整体图。

远端设备与本地设备之间的通信要求：在数据交易之前，在远端设备与本地设备之间进行初始化。初始化由远端设备控制。

在远端设备与本地设备之间进行初始化之后，远端设备与本地设备之间的进一步通信，在某些应用中可以由本地设备来初始化，或者，可靠地，可选地由远端设备来初始化。

正如下面将更详细地说明的那样，硬件随机数发生器控制器 16 包含受保护的存储区，该受保护的存储区含有只可以在工厂安装的特殊身份识别功能。不能反过来设计存储器的这个区域，并且，存储器的这个区域包括将防止对这个存储区的任何非法访问的各种篡改检测机制。

硬件随机数发生器控制器 16 的随机加密功能块只在初始化期间产生公开密钥，并将其传递到主机设备，然后，传递含有加密的部分和永久分配的可读部分的两部分身份识别号。可读部分是由制造商或由诸如监督权限（monitoring jurisdiction）之类的第三方来分配指定。加密的部分是由硬件随机数发生器随机地产生的，并被永久地分配给特定的远端设备，且被存储在硬件随机数发生器控制器的受保护的存储区中。然后，把两部分身份识别号发送到用公开密钥加密的主机设备。硬件随机数发生器控制器 16 将随后改变用于远端设备与本地设备之间的每一次交易的公开密钥。这种随机关系只为

硬件随机数发生器控制器所知，而不为其它方所知，相应地，一旦主机设备把远端设备注册到服务中，该远端设备就只与那个主机设备一起工作。身份识别号的加密的部分，只为硬件随机数发生器控制器所知，因为，它是由通过改变随机公开密钥而密封起来的、它自己的人工智能（AI）创建的。由于

5 在受保护的存储区中，身份识别号的加密的部分，只为硬件随机数发生器控制器所知，因此，这种方法可以防止拥有内部信息的那些个人的非法入侵。

远端设备与主机设备之间的通信协议

参照图 3，描述了远端设备与主机设备之间的操作和安全协议。

1. 在注册或初始化时

10 1a) 在注册时，也就是说，在第一次着手使用远端设备和主机设备时，硬件随机数发生器控制器 16 产生随机身份识别号。身份识别号是所产生并存储在硬件随机数发生器控制器的受保护的存储区内的秘密数字。它的产生是为了在初始化之后，使远端设备成为主机设备专用的，这样，只有专用的主机设备可以与专用的硬件随机数发生器控制器一起使用。

15 身份识别号从不会不加密就从硬件随机数发生器控制器输出。如此，主机设备从不会知道由硬件随机数发生器控制器所指定的真实身份识别号。

1b) 在产生身份识别号之后，硬件随机数发生器控制器用随机产生的身份识别解密密钥来加密身份识别号，以便产生身份识别号/身份识别解密密钥分组（单级加密）。

20 1c) 然后，通过公开密钥进一步加密身份识别号/身份识别解密密钥分组，以便产生身份识别号/身份识别解密密钥/公开密钥分组（双层加密），并将其发送到主机设备。公开密钥可以由硬件随机数发生器控制器来设置和改变，或者，可以由系统管理员适当地（例如，每天一次）设置和改变。公开密钥为远端设备和主机设备两者所知。相应地，取决于公开密钥的产生场所，按

25 照要求，公开密钥被转发给主机设备或远端设备。

1d) 主机设备接收身份识别号/身份识别解密密钥/公开密钥分组。公开密钥用于把身份识别号/身份识别解密密钥/公开密钥分组解密成随后存储在主机设备存储器中的身份识别号/身份识别解密密钥分组。

1e) 到此为止，用主机设备注册远端设备的过程就完成了。

30 2. 注册后的数据交易

如下的数据交易协议是专用于来自博弈设备的随机数请求的。但是，应

该明白，依赖于具体应用，数据交易可以由远端设备或主机设备来初始化，相应地，通信协议可以容易地适用于特定的方向的数据流。

2a) 主机设备请求应用专用随机数。

2b) 一旦接收到随机数请求，硬件随机数发生器控制器就从主机设备请求所存储的身份识别号/身份识别解密密钥分组，并且，一旦接收到，就用只为硬件随机数发生器控制器所知的身份识别解密密钥来认证身份识别号。

如果认证成功，

2c) 那么，硬件随机数发生器控制器就产生随机数，并根据由主机设备请求的应用格式来处理它，且随机地产生数据解密密钥。数据解密密钥用于产生随机数/数据解密密钥分组。

2d) 然后，硬件随机数发生器控制器产生用于身份识别号的加密的新的身份识别解密密钥。身份识别解密密钥用于产生新的身份识别号/身份识别解密密钥分组。

2e) 把身份识别号/身份识别解密密钥分组、随机数/数据解密密钥分组和数据解密密钥相互附加在一起，以产生一个身份识别号/身份识别解密密钥/随机数/数据解密密钥/数据解密密钥分组。

2f) 用公开密钥来加密身份识别号/身份识别解密密钥/随机数/数据解密密钥/数据解密密钥，以产生一个身份识别号/身份识别解密密钥/随机数/数据解密密钥/数据解密密钥/公开密钥分组。

2g) 把身份识别号/身份识别解密密钥/随机数/数据解密密钥/数据解密密钥/公开密钥分组发送到主机设备。

2h) 主机设备接收身份识别号/身份识别解密密钥/随机数/数据解密密钥/数据解密密钥/公开密钥分组，并且，用公开密钥将身份识别号/身份识别解密密钥/随机数/数据解密密钥/数据解密密钥/公开密钥分组解密成身份识别号/身份识别解密密钥/随机数/数据解密密钥/数据解密密钥分组。

2i) 主机设备从身份识别号/身份识别解密密钥/随机数/数据解密密钥/数据解密密钥分组中提取随机数解密密钥。然后，将随机数解密密钥用于解密随机数/数据解密密钥分组，以便提取供用于主机设备的随机数。

2j) 用身份识别号/身份识别解密密钥分组替换先前存储在主机设备中的身份识别号/身份识别解密密钥分组。

2k) 对于由硬件随机数发生器控制器接收的每一个随机数请求，都重复

步骤 2a-2j。

注：

a) 用硬件随机数发生器控制器接收的每一个随机数请求，来改变和更新的身份识别解密密钥。

5 b) 最好是，由合法的管理员或由硬件随机数发生器控制器，以适合于特定的安装的有规律的方式，来改变公开密钥。

c) 身份识别号从不以未加密的方式泄露到硬件随机数发生器控制器的外面。

d) 随机数解密密钥随每一个随机数请求而改变。

10 e) 一旦一个主机设备已经存储了一个加密的身份识别号，就不可以再将另一个远端设备注册到其上。更确切地说，远端设备将检测到某个秘密身份识别号的存在，并且将不允许注册继续进行。

在如图 3a 和图 3b 所示并如上面介绍的另一个实施例中，身份识别号是能够独立审查软件保护器/主机设备的两部分身份识别号。在这个实施例中，
15 第一部分是使用身份识别解密密钥来加密的，而第二部分是不由身份识别解密密钥来加密的可读的 tax/许可身份识别信息。然而，每当可读 tax/许可身份识别信息在主机设备与软件保护器之间传输时，就用公开密钥将其加密。

为了确保远端设备是秘密的，如果需要的话，当主机设备发送数据请求时，就只开始传送数据。在通过握手（handshake）协议建立发送与接收关系
20 （握手）之后，远端设备就发送随机加密密钥。主机设备接收并处理随机加密密钥，以使将每一个帧内的后续消息解密。这个过程防止了敌意的窃听、以及黑客/窃贼把伪造的远端设备安装到主机设备上的可能性。

远端设备 12

远端设备与独立微处理器、管理控制器和硬件随机数发生器控制器一起
25 工作，它们都包含具有闪存（flash）能力的它们自己的一组集成的存储器，以供电路内程序下载用。

硬件随机数发生器控制器 16

硬件随机数发生器控制器 16 包括硬件随机数发生器 16a，并且，产生和管理用于保护和用于应用专用功能的随机数数据。

30 管理控制器 18

管理控制器 18 控制接口与硬件随机数发生器控制器 16 之间的操作。管

理控制器起着应用接口之间的数据安全缓冲器的作用，并且被安排成能非常秘密地与硬件随机数发生器控制器 16 进行通信。管理控制器，对于其主机设备的具体软件实现来说，最好是透明的。

远端设备与本地设备接口

- 5 远端设备与本地设备之间的接口可以是有线的或无线的。

有线的接口可以是利用主机设备上的现有的接口的穿过接口，诸如：简单 2 线双向接口 (I²L、SMBus、Access Bus)、RS232 串行端口、并行端口、以太网、数字用户线 (DSL)、非对称数字用户线 (ADSL) 或普通老式电话 (POT)，即，模拟电话。

- 10 最好是，远端设备可以：不与主机设备的接口的常规使用相冲突地，且不把任何冲突引入主机设备与任何外围设备之间的现有的工作关系中地，与主机设备与任何连接的外围设备之间的主机设备相连接。在这种情况下，最好是，远端设备与主机设备之间具有秘密的关系。

- 15 例如，主机设备可以具有与调制解调器相连接的串行端口、以及与打印机相连接的并行端口。适合于通过串行端口与主机设备相连接的远端设备可以连接在主机设备与调制解调器之间，或者，适合于通过并行端口与主机设备相连接的远端设备可以通过穿过接口相连接。进行这种连接是为了使远端设备对于调制解调器是秘密的，且对于打印机也是秘密的，以允许在主机设备与外围设备之间进行常规的通信。

- 20 相应地，通过提供可适合于现有的设备的串行或并行端口的系统，无需在主机设备上附加任何物理端口，就可以把远端设备的功能加入到主机设备中，从而增加了系统对现有的设备的使用性和适用性。

无线接口

- 25 在主机设备和远端设备的候补实施例中，通信可以是利用诸如射频 (RF) 电缆装置 (即，有线电视 (CATV)、DIRECTV)、电气电子工程师学会 (IEEE) 802.11、或蓝牙 (Bluetooth) 射频之类的标准无线通信硬件/软件的无线通信。

- 30 有线的和无线的实施例均可以是“线内 (inline)”的或“网络”的，或者是它们的组合。“线内”的例子包括串行、并行、数字用户线、非对称数字用户线、普通老式电话、有线电视 (即，DIRECTV)、电气电子工程师学会 802.11、和蓝牙射频接口，而“网络”的例子包括射频电缆装置 (即，电缆调制解调器)、以太网、电气电子工程师学会 802.11、和蓝牙射频接口。

博弈专用硬件随机数发生器控制器整体图

在博弈产业中的软件保护器的特定的应用中，硬件随机数发生器控制器 16 能够产生用于包括扑克、21 点、叠纸牌博弈 (keno)、排五点博弈 (bingo)、8-way slot (一种投币老虎机)、3-reel slot (一种老虎机)、5-reel slot (一种老虎机) 等的著名机会对策用的真正随机数格式。软件保护器使用下面更加详细描述

5 的通信协议来发送和接收加密的但简单的字节宽 (byte-wide) 的分组。

硬件随机数发生器微控制器最好含有有限数目的到外部的物理连接 (在一个实施例中，只个五个物理连接)。另外，硬件随机数发生器控制器 16 最好拥有诸如具有自毁 (存储器) 能力的敌意侵入检测之类的功能，以便阻止 10 包括拥有特权信息的黑客获得对硬件随机数发生器微控制器的受保护的存储区的访问。硬件随机数发生器微控制器包含硬件加密引擎。

最好是，远端设备具有为每种类型的机会对策同时产生几种随机字格式的处理带宽，使得博弈设备主机处理器可以方便地同时运行几种类型的机会对策。

15 用于穿过连接到并行端口的软件保护器的电路图的例子显示在图 4 中。

其它特征

电源供应

对远端设备的供电可以是独立的 (最好是电池)，或通过主机设备。本领域的普通技术人员应该明白，远端设备可以通过现有的端口从主机设备获取 20 电能，或从分离的主机电源系统获取电能。

生物统计识别

为了增强根据本发明的安全系统的应用，可以把附加功能加入到远端设备中，以便为用户提供专门的保护。包括指纹识别系统、语音识别系统和面部识别系统的生物统计识别系统可以在远端设备中实现，或者对于远端设备 25 是可配置的。

适当的生物统计系统可以实现，例如，通过细 3 线 (电缆和插座) 连接，来与一个生物统计系统进行通信。在这个实施例中，远端设备检测生物识别系统是否存在，并将请求生物统计识别输入。如果接收到适当的生物统计信息，就启动远端设备。

30 在语音身份识别系统的具体例子中，提示用户说出他/她的名字和/或 4 到 8 个字符的个人身份识别号。如果语音指纹与注册的用户语音相匹配，就

启动远端设备。下面更详细地描述用于注册的系统。

具有生物统计语音识别的软件保护器的例子显示在图 5 中。

物理形式

远端设备的硬件随机数发生器控制器 16 最好是小型多层印刷电路板的形式。远端设备也可以被进一步集成并制造在一片定制设计的应用专用的集成电路 (ASIC) 芯片上。

物理保护

为了确保设备专用的身份识别号得到保护,远端设备的受保护的存储区包括篡改检测。篡改检测系统将最好包括物理和电特性检测设备的组合,如果硬件随机数发生器控制器遭到破坏,所述的物理和电特性检测设备的组合将使远端设备的内部闪存存储器被擦除。检测系统可以包括用于感测温度、电阻、静电、功率尖峰和电源故障等的快速变化的检测器。

用于博弈具体应用的通信协议的例子

下面是远端设备(软件保护器)和本地设备(设备)之间的通信协议的一个例子,并且是专用于博弈应用的。应该明白,按照本发明,也可以执行其它通信协议和命令序列。

硬件随机数发生器控制器与管理控制器之间的通信最好是遵从国际标准化组织(ISO) 7816,并通过“U5”(图 4),且对于主机设备是透明的。使国际标准化组织 7816 标准建立到硬件随机数发生器控制器和“U5”之中。不需要其它外部硬件来实现这个目的。安全性是通过由硬件随机数发生器控制器产生的两部分身份识别号的秘密部分来控制的。主机设备从硬件随机数发生器控制器接收随机产生的加密的密钥,以便解密数据分组,以及用于秘密身份识别号检验。无需知道管理控制器 18(U4)与硬件随机数发生器控制器 16(U5)之间的秘密关系,主机设备(最终用户)通过其端口请求随机数发生器遵从来自硬件随机数发生器控制器 16 的、下面描绘的软件协议。下面是事件的顺序:

1. 硬件随机数发生器控制器取出两部分身份识别号的秘密加密的部分,并检验其真实性。秘密身份识别只为硬件随机数发生器控制器所知,而不为其它方所知。在注册期间,随机地产生一次,但对于每一个主机设备的随机数发生器请求解密密钥改变的。

2. 对于每一个请求的随机数发生器,主机设备从硬件随机数发生器控制

器接收持续变化的随机解密密钥。

3. 在随机数发生器到主机设备的每一次传送末尾，硬件随机数发生器控制器用新的随机密钥来加密秘密身份识别号，并且，当主机设备请求另一个随机数发生器时，将其再次取出用于检验。

5 I. 数据分组

所有数据传输都是以一帧 8 个字节的数据分组的形式。

帧 1 = 数据分组 0、偏移 0

数据分组 1、偏移 1

...

10 ...

数据分组 7、偏移 7

每一个数据分组都以头字节（02H）开始，后面接着是命令字节、和 4 个数据字节。然后，以检验和与尾字节（03H）结束该分组。

数据分组 0,...,7 = 02H，正文开始

15 xxH，命令字节

??H，数据字节 0

??H，数据字节 1

??H，数据字节 2

??H，数据字节 3

20 yyH，数据分组检验和

03H，正文结束

a) 命令字节

命令字节不仅标识命令，而且标识分组的来源。

其格式如下：

位	7	6	5	4	3	2	1	0
	1	0 设备	00 数据			命令身份识别		
	1	1 软件保护器	01 保留			命令身份识别		
			10 保留			命令身份识别		
			11 保留			命令身份识别		

b) 检验和

检验和是在包括头和尾字节的整个分组之上计算的。计算出检验和作为所有分组字节的和的二者之和。

II. 肯定应答 (ACK)

- 5 肯定应答是 8 个字节数据分组的唯一例外。设备和软件保护器均返回其值为 A0H 的单字节肯定应答。

III. 数据流

- 10 设备开始最多数量的数据传送。设备将把数据发送到软件保护器，或者从软件保护器请求数据。特殊情况是自动响应模式。使用这种模式，软件保护器可以把数据发送到可能需要立刻关注的设备。例如，软件保护器状态、非法侵入、和/或失败的自检。自动响应模式由设备来启用或禁用。一旦加电，就禁用自动响应模式。如果自动响应被禁用，设备将需要为状态改变而轮询软件保护器。

这些模式被概括如下：

- 15 1. 发送数据（握手和产生数据的指令）

开始

设备发送数据分组到软件保护器

软件保护器接收数据分组

如果（无通信错误）

- 20 开始

软件保护器返回肯定应答

软件保护器执行数据分组

（准备产生一个 keno 号,等等）

结束

- 25 结束

肯定应答响应将在 50 毫秒内返回。如果在 50 毫秒之前没有接收到肯定应答，那么，设备应该重新发送数据。

2. 请求数据

开始

- 30 设备发送数据请求分组到软件保护器

软件保护器接收数据分组请求

- 如果（无通信错误）
开始
软件保护器发送请求的数据分组
设备接收数据分组
- 5 如果（无通信错误）
开始
设备发送肯定应答
或
设备发送s数据请求分组
- 10 或
设备发送数据分组
结束
结束
结束
- 15 肯定应答响应应该在 50 毫秒内返回。如果在 50 毫秒之前没有接收到肯定应答，那么，软件保护器将重新发送数据，直到接收到肯定应答为止。
3. 自动响应
软件保护器条件需要立刻动作（即，检测到非法入侵）
如果（自动响应启用）
- 20 开始
软件保护器发送数据分组
设备接收数据分组
如果（无通信错误）
开始
- 25 设备发送肯定应答分组
或
设备发送数据请求分组
或
设备发送数据分组
- 30 结束
结束

结束

肯定应答响应应该在 50 毫秒之内返回。

如果在 50 毫秒之前没有接收到肯定应答，那么，软件保护器将重新发送数据，直到接收到肯定应答为止。

5 4. 通信错误检测

协议也提供了通信错误检测。错误条件是如下之一：

- 1) 分组没有以头字节 02H 开始。
- 2) 分组没有以尾字节 03H 结束。
- 3) 检验和无效。
- 4) 字节间延迟大于 20 毫秒。

10

当将数据分组从软件保护器发送到设备时，如果被无错误地接收到，则设备应该用肯定应答来响应。如果检测到错误，那么，就无响应从设备返回到软件保护器，而软件保护器将重新发送数据，直到从设备接收到肯定应答为止。当将数据分组从设备发送到软件保护器时，如果被无错误地接收到，

15

则软件保护器用肯定应答来响应。如果检测到错误，那么，就无响应从软件保护器返回到设备。然后，设备可以选择重新发送数据。当将数据请求从设备发送到软件保护器时，如果被无错误地接收到，则软件保护器用请求的数据来响应。如果检测到错误，那么，就无响应从软件保护器返回到设备。然后，设备将重新发送数据请求，直到接收到数据为止。一旦已经无错误地接

20

收到数据，设备最后将用肯定应答来响应。

IV. 从设备发送到软件保护器的数据分组的细节

请求数据

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	80H	命令字节
2	字节	??H	请求的数据
			C0H 软件保护器序号
			C1H 版本（即，身份识别号）
			C2H 只读存储器（ROM）（闪存）检验和
			C3H 电可擦除可编程只读存储器（EEPROM）检验和
			C4H 随机存取存储器（RAM）检验和
			C5H 随机加密密钥 0-3
			C6H 随机加密密钥 4-7
			C7H 随机加密密钥 8-B

			C8H 随机加密密钥 C-F
			C9H 保留
			CAH 保留
			CBH 保留
			CCH 保留
			CDH 保留
			CEH 保留
			CFH 保留
3	字节	??H	C0H 的随机字返回的类型
			00H 自动响应状态
			01H 重新洗一副纸牌
			02H 发一副纸牌当中的一张牌
			03H 重新洗两副纸牌
			04H 发两副纸牌当中的一张牌
			05H 重新洗 4 副纸牌
			06H 发 4 副纸牌当中的一张牌
			07H 重新洗 6 副纸牌
			08H 发 6 副纸牌当中的一张牌
			09H 重新开始 keno 序列
			0AH 发一个 keno 号
			0BH 重新开始 Bingo 序列
			0CH 发一个 Bingo 号
			0DH Slot Reel-Stop 范围 (0-255)
			0EH 根据“0DH”范围发送 Reel-Stop 数
			OFH 百搭 (Joker) 选项 例如: 发送这个字节的前述的纸牌请求, 将返回一副带百搭的牌。
4	字节	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

自动响应模式

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	81H	命令字节
2	字节	??H	自动响应 0 禁止 1 允许
3	字节	00H	保留
4	字节	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

杂项输出请求 (把“事件”打开/关闭)

偏移	类型	值	说明
----	----	---	----

0	字节	02H	正文开始
1	字节	82H	命令字节
2	字节	??H	输出状态 0 关闭 1 打开 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
3	字节	??H	输出状态 0 关闭 1 打开 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
4	字节	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

闪存只读存储器检验和种子

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	83H	命令字节
2	二进制 2	????H	检验和种子 LSByte 第一
4	二进制 2	????H	检验和除数 LSByte 第一 =0 igt 检验和
6	字节	??H	检验和
7	字节	03H	正文结束

电可擦除可编程只读存储器检验和种子

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	84H	命令字节
2	二进制 2	????H	检验和种子 LSByte 第一
4	二进制 2	????H	检验和除数 LSByte 第一 =0 igt 检验和
6	字节	??H	检验和

7	字节	03H	正文结束
---	----	-----	------

静态随机存取存储器 (SRAM) 检验和种子

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	85H	命令字节
2	二进制 2	???H	检验和种子 LSByte 第一
4	二进制 2	???H	检验和除数 LSByte 第一 =0 igt 检验和
6	字节	??H	检验和
7	字节	03H	正文结束

输出单脉冲命令

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	86H	命令字节
2	二进制 2	??H	设备号 0 设备 1 1 设备 2 2 设备 3 3 设备 4 4 设备 5 5 设备 6 6 设备 7
3	字节	00H	保留
4	二进制 2	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

随机字序列计数

例子: 52 张纸牌当中的第 14 张纸牌

10 个 keno 点当中的第 4 个 keno 点

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	87H	命令字节
2	字节	??H	随机字 / 博弈的类型 0 单副 (52 张) 纸牌 1 一副带百搭的牌 2 双副纸牌 3 4 副纸牌 4 6 副纸牌 5 keno 6 bingo
3	二进制 2	???H	号计数 LSByte 第一
5	字节	00H	保留
6	字节	??H	检验和

7	字节	03H	正文结束
---	----	-----	------

清除错误

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	88H	命令字节
2	字节	??H	错误类型 0 清除所有错误 1 清除通信错误 2 无效循环冗余码校验 (CRC) 3 闪存只读存储器检验和 4 电可擦除可编程只读存储器检验和 5 静态随机存取存储器检验和 6 保留 7 保留 FF 清除侵入错误
3	字节	00H	保留
4	字节	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

逆逻辑运算

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	89H	命令字节
2	字节	??H	逆逻辑非运算 0 标准 1 逆的 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留 位 8 保留
3	字节	00H	保留
4	字节	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

设备肯定应答

响应来自软件保护器的有效数据分组，发送设备肯定应答。

偏移	类型	值	说明
----	----	---	----

0	字节	A0H	命令字节
---	----	-----	------

V. 从软件保护器发送到设备的数据分组的细节

在自动响应模式中，当条件满足时，自动发送分组 C0 到 C5。

软件保护器状态

偏移	类型	值	说明
1	字节	02H	正文开始
1	字节	C0H	命令字节
2	字节	??H	状态字节 0 均很好 1 完成检验和 2 完成从单副纸牌中选出单张纸牌 3 完成从一副带百搭的牌中选出一张百搭牌 4 完成从双副纸牌中选出一张纸牌 5 完成从 4 副纸牌中选出一张纸牌 6 完成从 6 副纸牌中选出一张纸牌 7 完成 keno 号 8 完成 bingo 号 9 完成 slot reel-stop 号 10 静态随机存取存储器恶化 11 闪存只读存储器恶化 12 电可擦除可编程只读存储器恶化 13 检测到侵入 14 保留 15 保留 16 保留 17 保留 18 保留 19 保留 20 保留 21 保留
3	字节	??H	辅助状态类型 0 没有辅助状态 1 自动响应状态 2 保留 3 保留 4 字节??H 辅助状态 5 没有辅助状态 0 1 自动响应状态 1 启用 2 保留 01H 保留的损坏 (bad) 02H 保留的损坏 04H 保留的损坏 08H 保留的损坏

6	字节	??H	检验和
7	字节	03H	正文结束

保留 I/O

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C5H	命令字节
2	字节	??H	I/O 状态 1 0 不变 1 改变 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
3	字节	??H	I/O 状态 2 0 不变 1 改变 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
4	字节	??H	I/O 状态 3 0 不变 1 改变 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
5	字节	??H	I/O 状态 4 0 不变 1 改变 位 0 保留 位 1 保留 位 2 保留

			位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
6	字节	??H	检验和
7	字节	03H	正文结束

保留状态

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C6H	命令字节
2	字节	??H	状态 1 0 (关闭) 1 (打开) 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
3	字节	??H	状态 2 0 (关闭) 1 (打开) 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
4	字节	??H	状态 3 0 (关闭) 1 (打开) 位 0 保留 位 1 保留 位 2 保留 位 3 保留 位 4 保留 位 5 保留 位 6 保留 位 7 保留
5	字节	00H	保留

			10H 保留的损坏 20H 保留的损坏 40H 保留损坏 3 保留的状态 1 保留的故障
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

闪存只读存储器检验和

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C1H	命令字节
2	二进制 2	????H	闪存只读存储器检验和值 LSByte 第一
4	字节	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

电可擦除可编程只读存储器检验和

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C2H	命令字节
2	二进制 2	????H	电可擦除可编程只读存储器检验和值 LSByte 第一
4	字节	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

静态随机存取存储器检验和

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C3H	命令字节
2	二进制 2	????H	静态随机存取存储器检验和值 LSByte 第一
4	字节	00H	保留
5	字节	00H	保留
6	字节	??H	检验和
7	字节	03H	正文结束

保留

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C4H	命令字节
2	二进制 2	??H	静态随机存取存储器检验和值 LSByte 第一
3	字节	??H	保留
4	字节	??H	保留
5	字节	00H	保留

3	字节	??H	数据字节 2
4	字节	??H	数据字节 3
5	字节	??H	数据字节 4
6	字节	??H	检验和
7	字节	03H	正文结束

随机密钥数据字节 5-8

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	CBH	命令字节
2	字节	??H	数据字节 5
3	字节	??H	数据字节 6
4	字节	??H	数据字节 7
5	字节	??H	数据字节 8
6	字节	??H	检验和
7	字节	03H	正文结束

密码字节 1-4

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	CCH	命令字节
2	字节	??H	数据字节 1
3	字节	??H	数据字节 2
4	字节	??H	数据字节 3
5	字节	??H	数据字节 4
6	字节	??H	检验和
7	字节	03H	正文结束

密码字节 5-8

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	CDH	命令字节
2	字节	??H	数据字节 5
3	字节	??H	数据字节 6
4	字节	??H	数据字节 7
5	字节	??H	数据字节 8
6	字节	??H	检验和
7	字节	03H	正文结束

安全数据字节 1-4

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	CEH	命令字节
2	字节	??H	数据字节 9
3	字节	??H	数据字节 10
4	字节	??H	数据字节 11
5	字节	??H	数据字节 12
6	字节	??H	检验和

6	字节	??H	检验和
7	字节	03H	正文结束

保留 I/O 输出

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C7H	命令字节
2	二进制 2	????H	值 LSByte 第一
4	字节	??H	I/O 模式 0 关闭 1 打开
5	字节	??H	安装 I/O 0 没有安装 1 安装
6	字节	??H	检验和
7	字节	03H	正文结束

保留 I/O 状态

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C8H	命令字节
2	二进制 2	????H	I/O 状态值 LSByte 第一
4	字节	??H	I/O 模式 0 关闭 1 打开
5	字节	??H	安装 I/O 0 没有安装 1 安装
6	字节	??H	检验和
7	字节	03H	正文结束

版本

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	C9H	命令字节
2	字节	??H	月代码（二进制编码的十进制（BCD））
3	字节	??H	日代码（二进制编码的十进制）
4	字节	??H	年代码（二进制编码的十进制）
5	字节	??H	序号（二进制）
6	字节	??H	检验和
7	字节	03H	正文结束

随机密钥数据字节 1-4

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	CAH	命令字节
2	字节	??H	数据字节 1

7	字节	03H	正文结束
---	----	-----	------

安全数据字节 5-8

偏移	类型	值	说明
0	字节	02H	正文开始
1	字节	CEH	命令字节
2	字节	??H	数据字节 13
3	字节	??H	数据字节 14
4	字节	??H	数据字节 15
5	字节	??H	数据字节 16
6	字节	??H	检验和
7	字节	03H	正文结束

软件保护器设备肯定应答（响应来自设备的有效数据分组而发送的）

偏移类型值说明

0 字节 A0H 命令字节

5 博弈应用例子

例 1

在使用 52 张纸牌的纸牌博弈中，主机系统请求这副纸牌当中的一张牌。如主机系统所请求的，硬件随机数发生器控制器获取一组随机比特流，并构造一副纸牌，且管理这副纸牌的分发。如果纸牌博弈需要多副纸牌，硬件随机数发生器控制器就按要求构造将要提供给主机系统的纸牌。

例 2

一种使用 80 个号的 keno 博弈。主机系统请求一个 keno 号，硬件随机数发生器控制器就获取一组随机比特流，并构造一个 80 个数的集合，且如主机系统所请求地管理其分配。

15 使用生物统计身份识别的授权系统

根据图 6 中所示的本发明的另一个实施例，提供了用于检验打算访问服务提供商的安全系统的用户的身份的系统和方法。这种系统的例子是因特网或无监督的博弈场所或现场，在那里，用户的年龄是用于操作涉及到个人财务数据的场所和 / 或金融机构的网站的合法的重要参数。

20 为了访问这种安全系统，可以进行如下的注册：

1. 打算用服务提供商 52 注册的潜在用户 50，将使其自然外貌出现在注册中心 54 或安全场所，在那里，服务提供商工作人员 56，将通过检验包括照片身份识别和诸如驾驶执照、护照等之类的其它合法的身份识别的传统的识别物 58，来检验潜在的用户的身分和资格。

2. 在服务提供商工作人员确信潜在的用户是合法的消费者之后，将赋予用户 50 一个典型地为四到八个数字或字母的数字的和 / 或字母（字符）的个人身份识别号 60，并且，将请求用户 50 说出个人身份识别号到语音身份识别盒 62 中，以产生一个安全场所语音指纹文件 64。在系统的不同的实施例中，可以要求用户记住他们的个人身份识别号，或者，可选地，把具有在卡上可视地或电子地编码的个人身份识别号字符细节的卡发给用户。在电子地编码的个人身份识别号的实施例中，在授权期间，可以把卡插入到与远端设备操作性地连接的读卡机中（下面所述的），以便把字符个人身份识别号信息提供给服务提供商。

10 3. 把用户的姓名、字符个人身份识别号和安全场所语音指纹文件输入到服务提供商的授权的用户的数据库 52a 中。

4. 注册之后，用户 50a 可以从具有能进行因特网访问的主机设备 14、如上所述的远端设备 18 和语音身份识别盒 24 的非安全站点 66，来访问服务提供商站点 52。

15 5. 在获得初步访问服务提供商的安全站点 52 之后，将提示用户 50a 输入他们的字符个人身份识别号（通过键盘或读卡机），并说出他们的语音指纹个人身份识别号到语音身份识别盒 24 中。通过提供字符个人身份识别号和语音指纹个人身份识别号，授权的用户的数据库 52a 能够通过首先识别具有相同的个人身份识别号的授权的用户之中的每一个，然后，通过比较文件上的语音指纹（安全场所语音指纹）和新说出的个人身份识别号来确定它们的真实身份，来更快速地检验用户 50a 的身份。用这种方式，随着正在被搜索的文件的子集（subset）变小，可以比根据它们的语音指纹严格地识别用户更快速地，识别出注册在包含成千上万的用户的授权的用户数据库中的授权的用户。也就是说，这种系统，使形成个人身份识别号所需的号码的个数的复杂性最小，测试个人身份识别号，被用作相对应的语音指纹文件的分类和搜索指标。

语音指纹检验软件的准确性，能够区分出真正说出的个人身份识别号、与可能已经记录在记录机器上并由未授权的用户回放（play back）的个人身份识别号。

30 在某些服务提供商应用中，系统在整个交易过程中将周期性地提示用户重新说出他们的个人身份识别号，以确保实际用户是授权的用户。

在进一步的实施例 5 中，如上所述的注册阶段可以要求由潜在的用户在安全的或非安全的站点上作出声明或“软”宣誓，在那里，用户陈述他们满足用于访问服务提供商的站点的合法的或选择的要求。在这个实施例中，用户可以联系服务提供商的站点来进行注册，并得到一份合法的声明文件，该合法的声明文件用于确认他们满足合法的注册标准，所述的合法的注册标准是诸如年龄、和/或不存在包括先前曾经从那个站点开除过的任何禁止标准。应该认识到，虽然这种形式的注册不及如上所述的安全场所注册安全，但对于某些应用或服务来说是足够的。

一旦做出声明，将可以请求用户用如上所述的系统来进行生物统计注册。
10 读卡机

在进一步的实施例中，远端设备包括如图 7 中所示的读卡机 80，读卡机使得诸如用户身份信息、借方、贷方或智能卡数据之类的数据能够通过设备 12 而被访问。

点对点通信

15 在安全系统的进一步的应用中，提供了不同的本地计算机之间的安全交易。也就是说，在其中每一台计算机都具有其自己的远端设备 190 和 192 的系统中，起始协议将建立每台计算机之间的基本联系，其中，在设备之间交换加密的秘密身份识别号。一旦接收到一个加密的秘密身份识别号，每台计算机将识别：使各用户进一步选择对任何后续交易进行加密的级别的安全环境是否存在。也就是说，在如上所述的随机地改变的公开密钥的控制下，每一个用户可以选择对交易进行加密的单个或双个级别（潜在地更高）。
20

再进一步，并参照图 8，也提供了其中用中央站点来注册各远端设备 190、192 的系统。中央站点包括含有远端设备 12 和注册数据库 204 的中央服务器 202。注册数据库 204 包含：含有名称、设备号和当前因特网协议（IP）地址的设备专用信息。在注册时，用户（在设备 190 或 192 上）登录到中央服务器 202 中，并把加密的身份识别号提供给与用户的因特网协议地址和其它标识符一起存储在注册数据库中的中央服务器 202。
25

如果拥有设备 190 的用户想开始与拥有设备 192 的用户交易，用户 190 从注册数据库 204 请求设备 192 的设备号和因特网协议地址。如果可获得注册信息，即，如果用户 192 已注册，就通知这两个用户这两个设备都已注册了，从而，能够使用如上所述的随机地改变的公开密钥来进行进一步的交易。
30

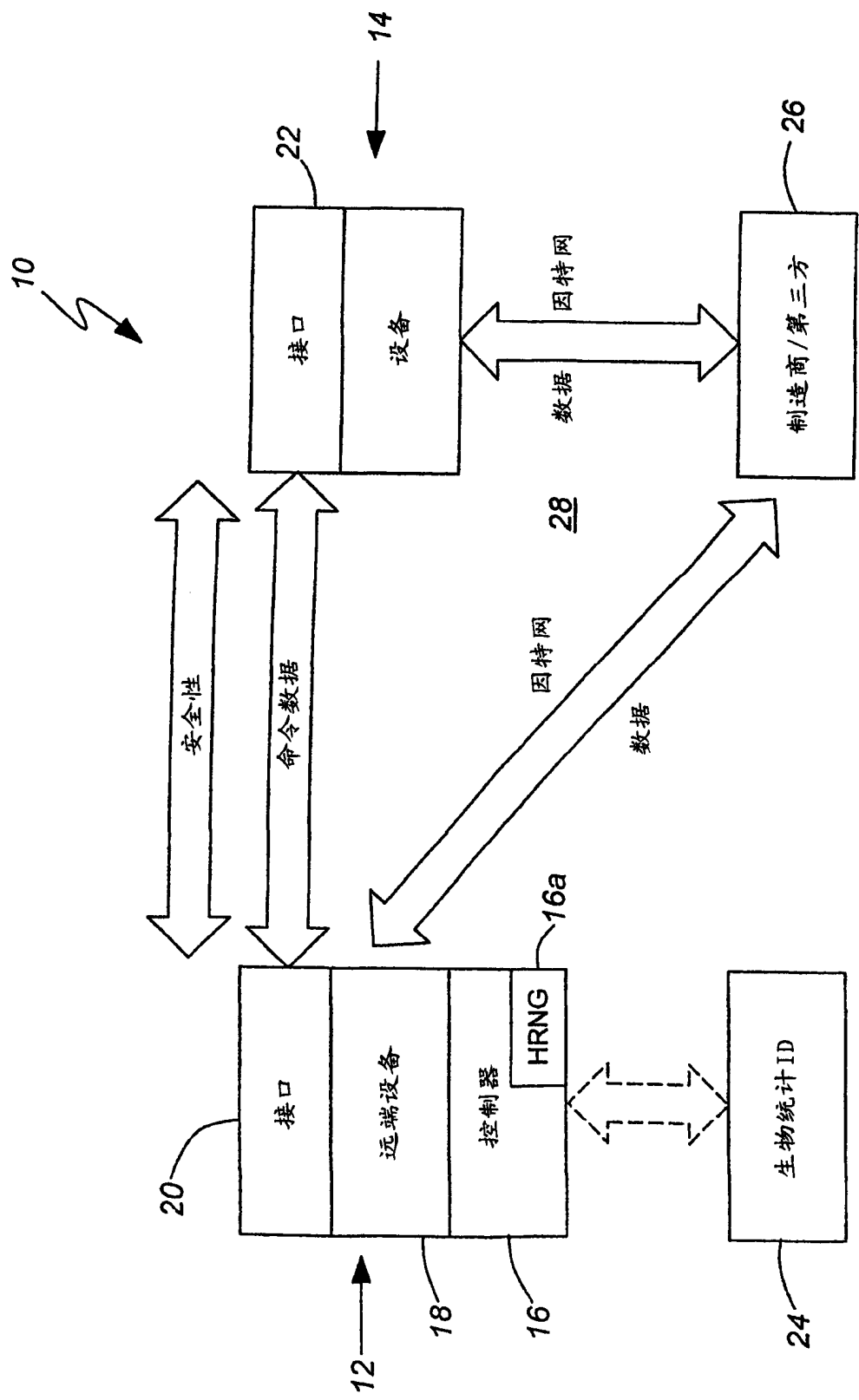


图 1

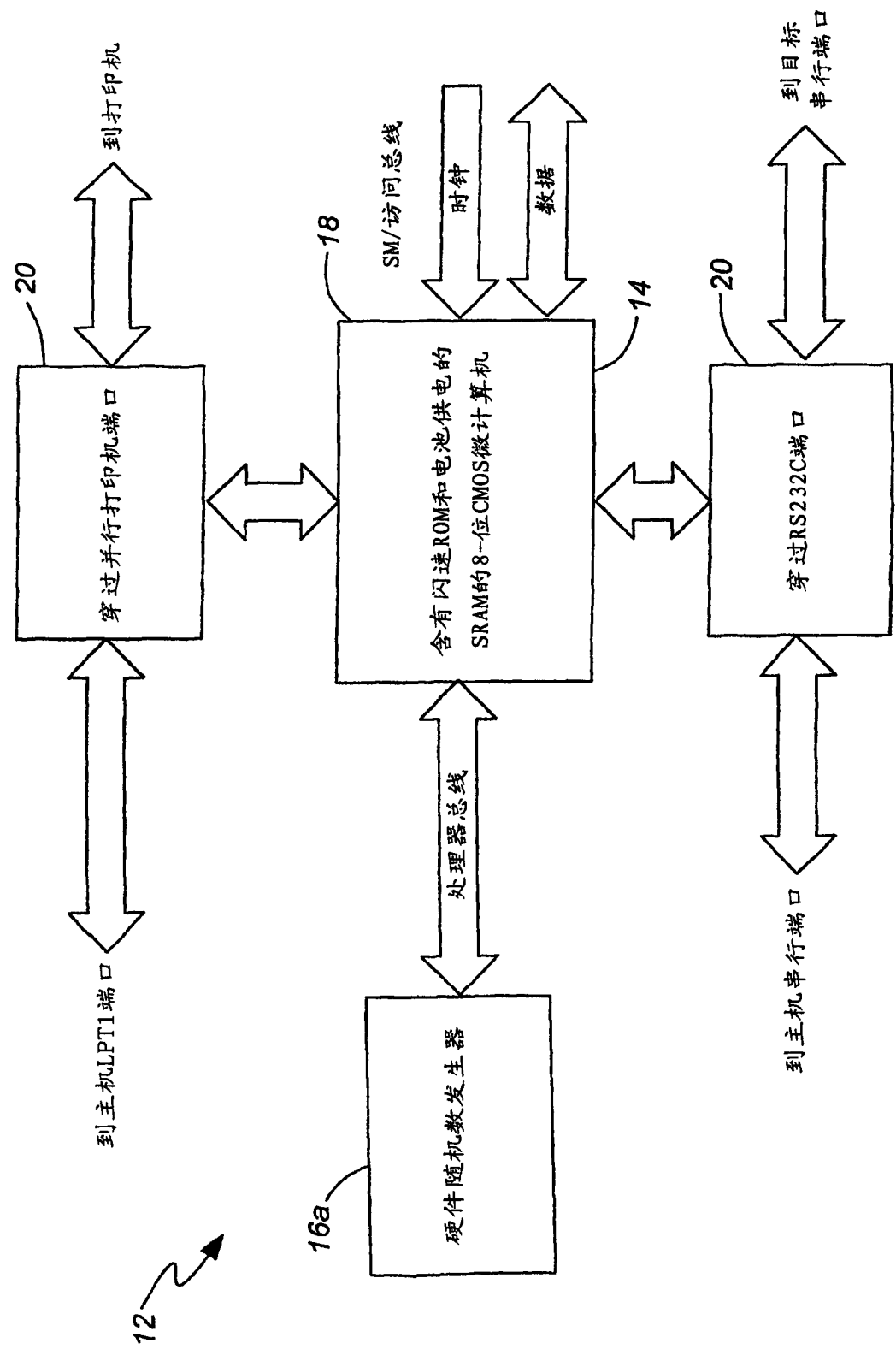


图 2

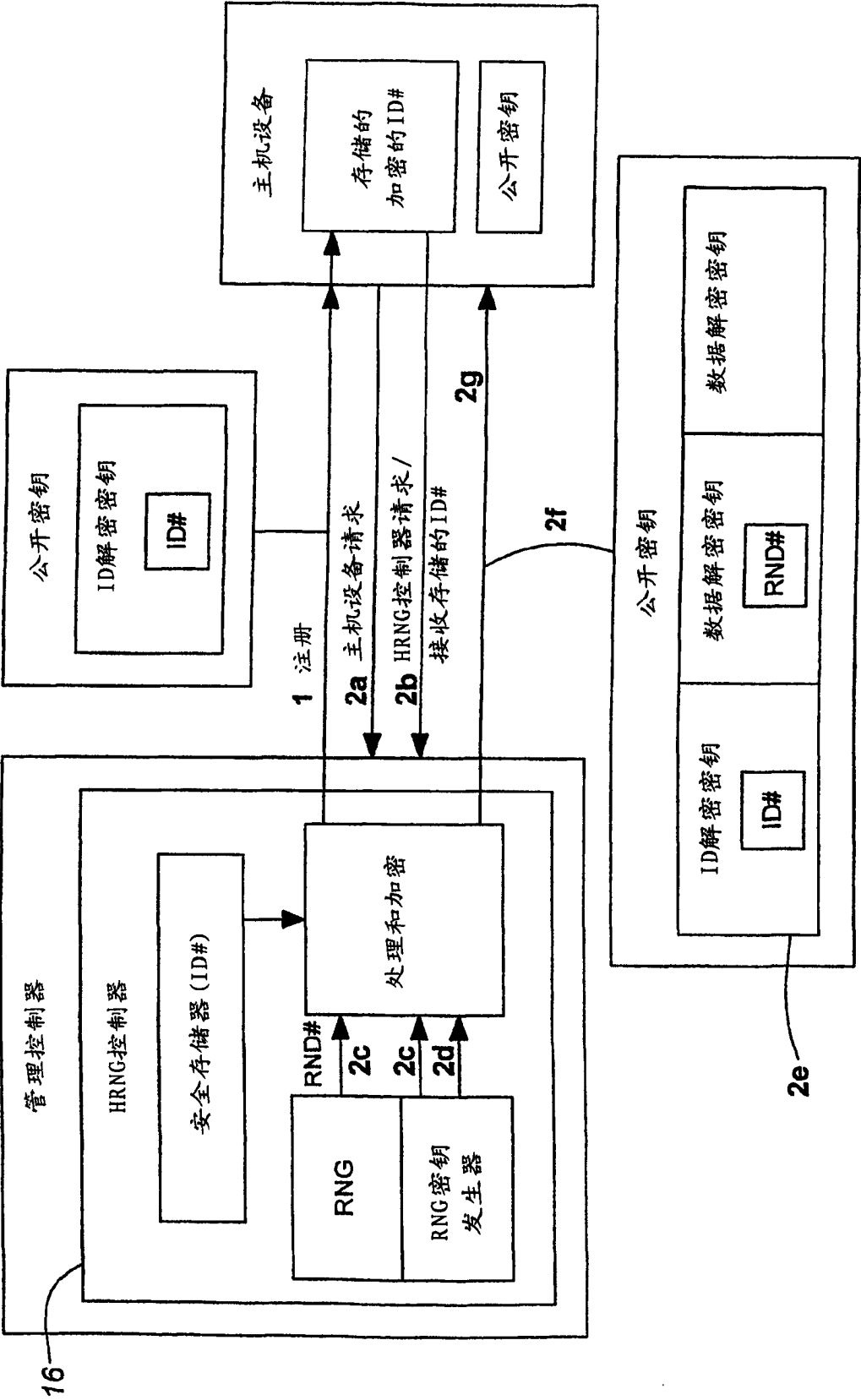
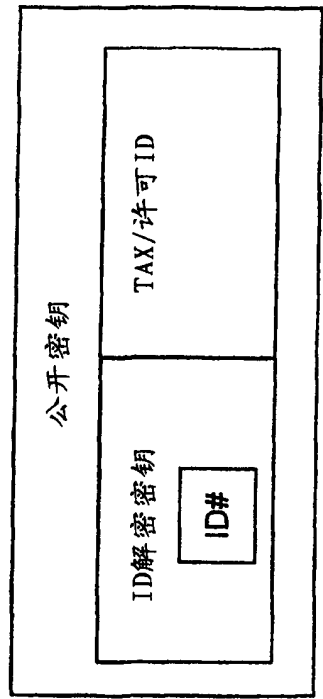
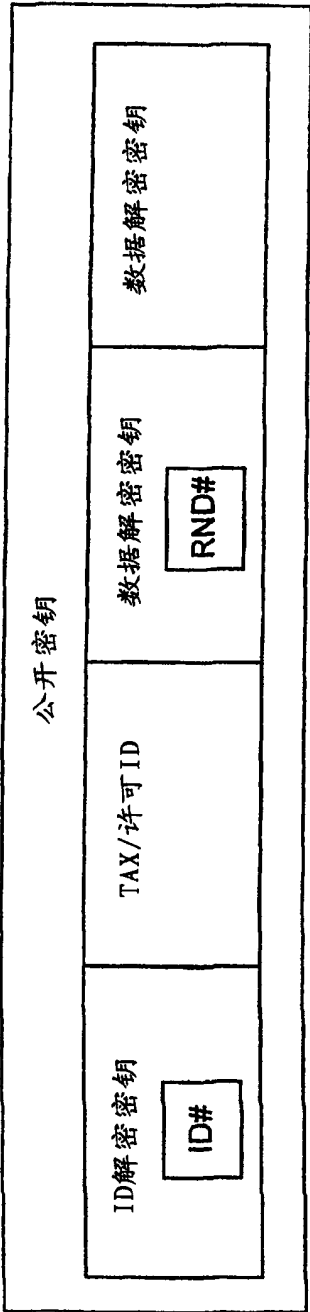


图 3



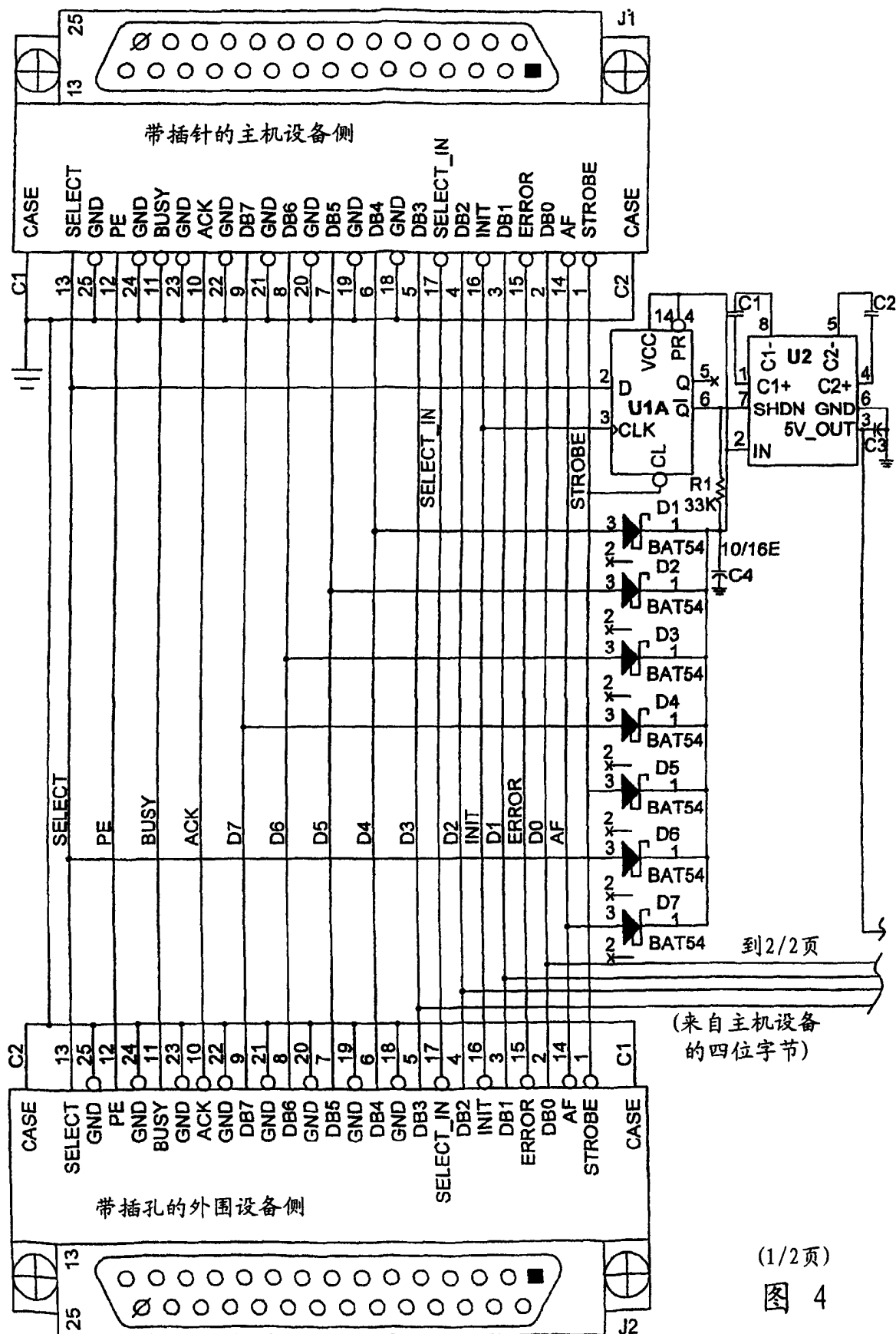
Two-part ID#

Figure 3a



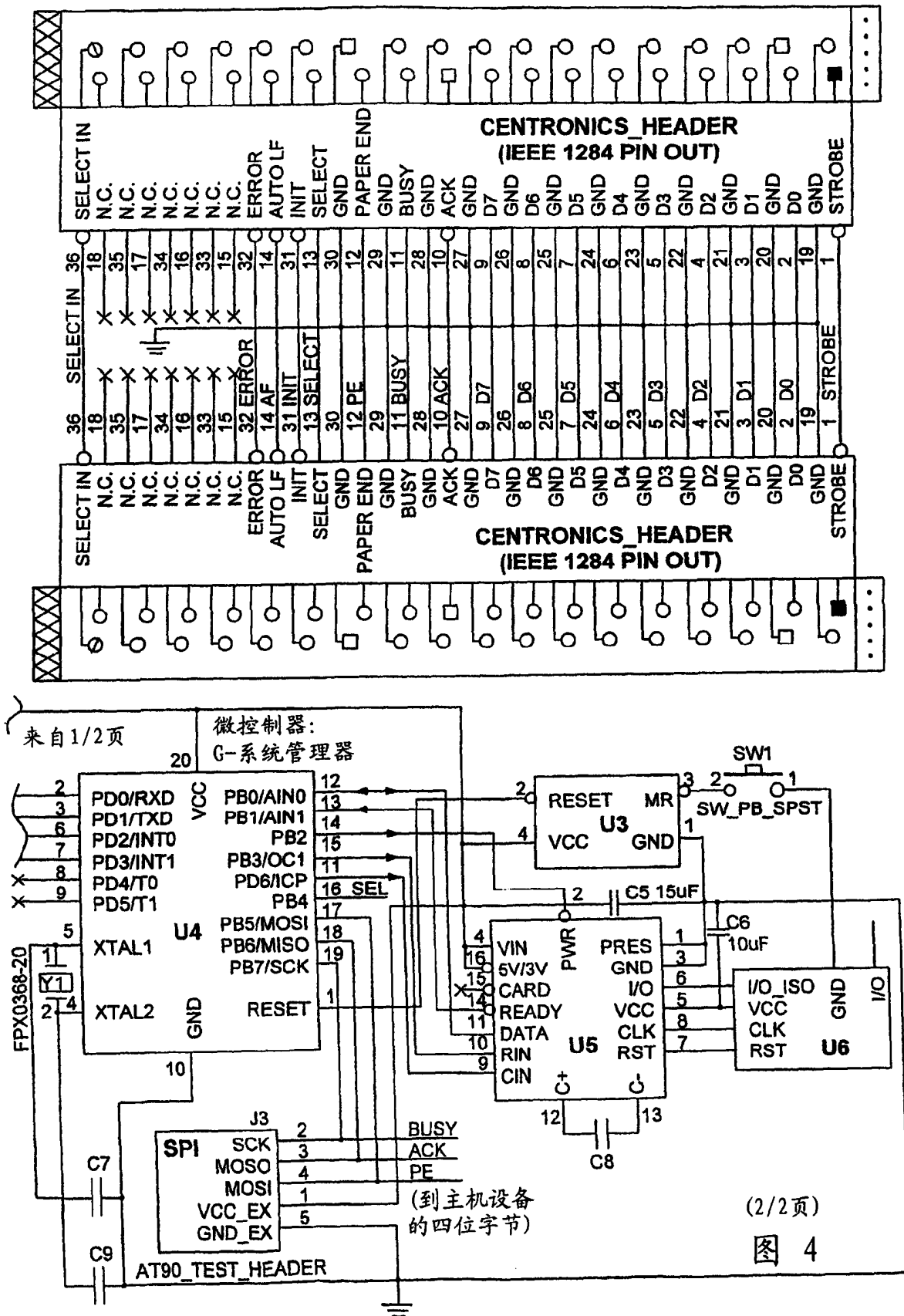
With data sent together in two-part ID#

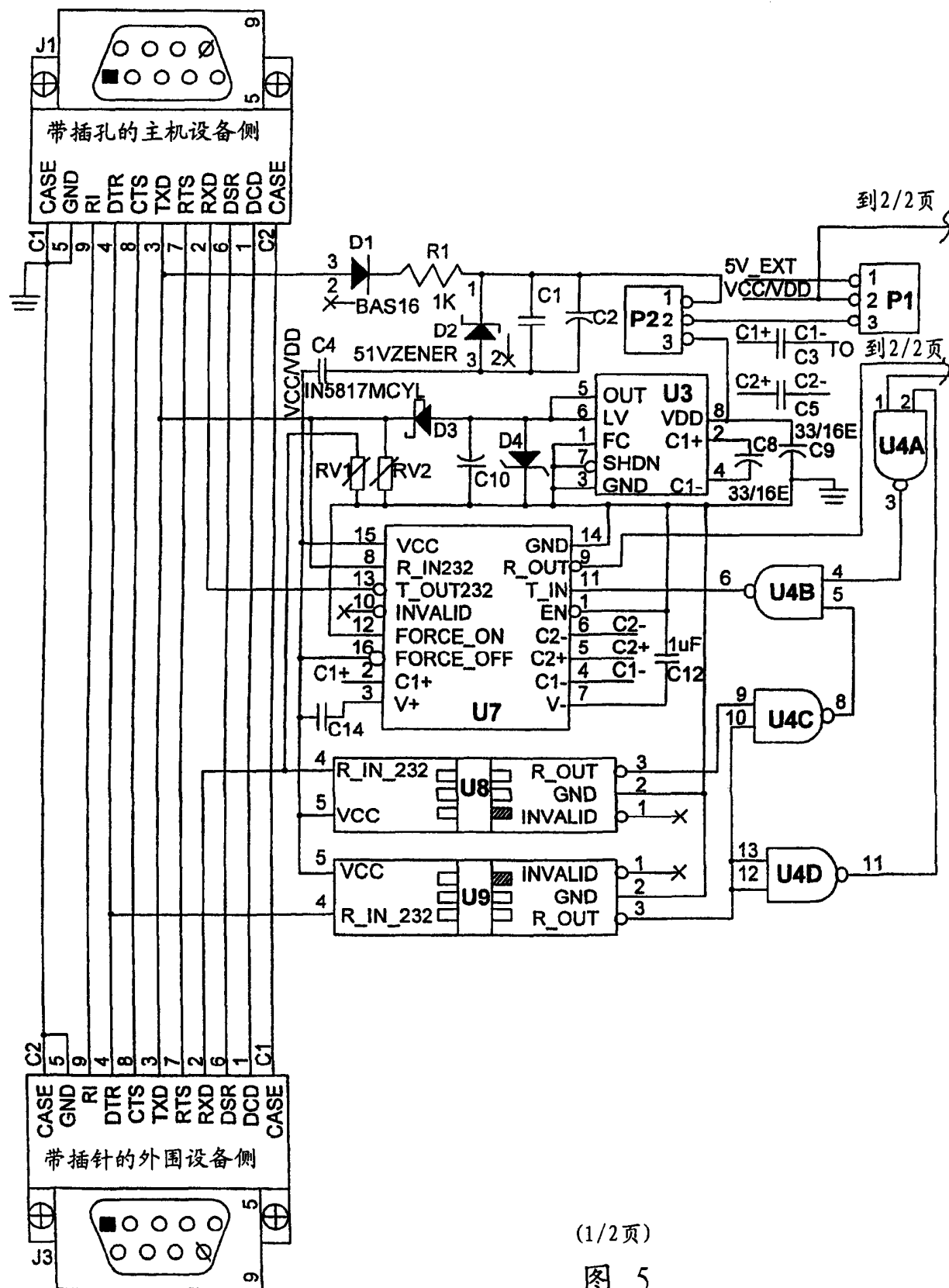
Figure 3b

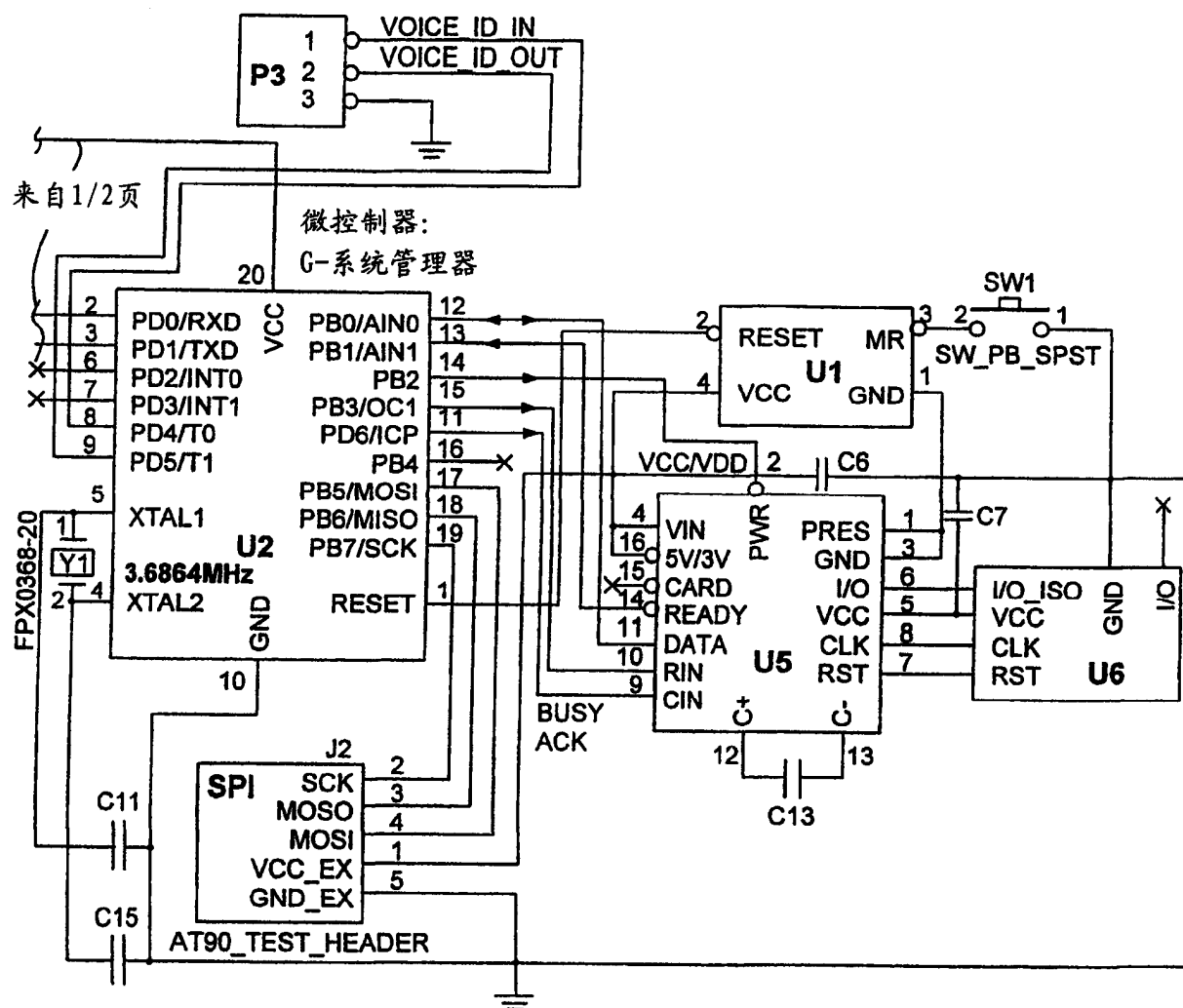


(1/2页)

图 4







(2/2页)

图 5

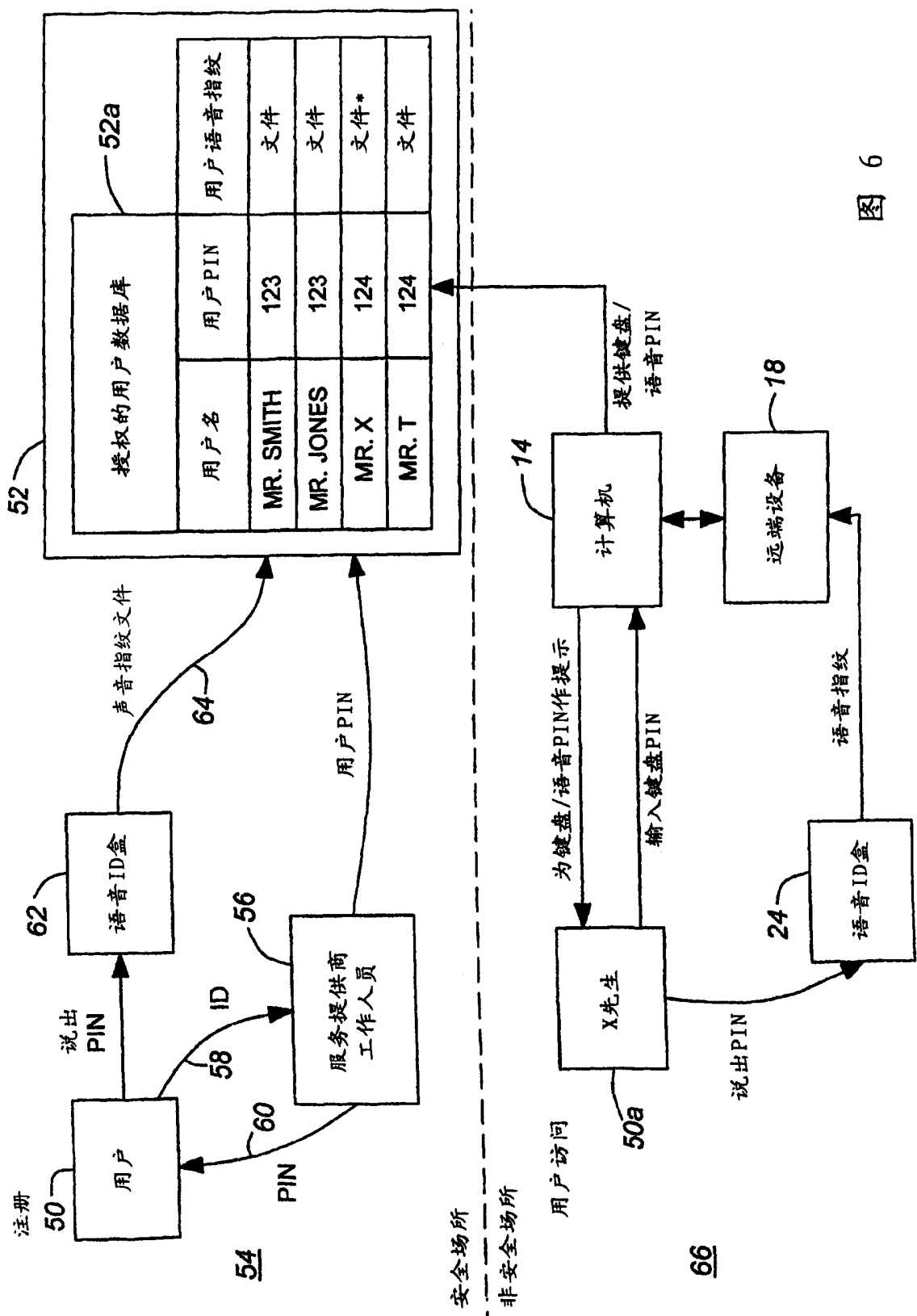


图 6

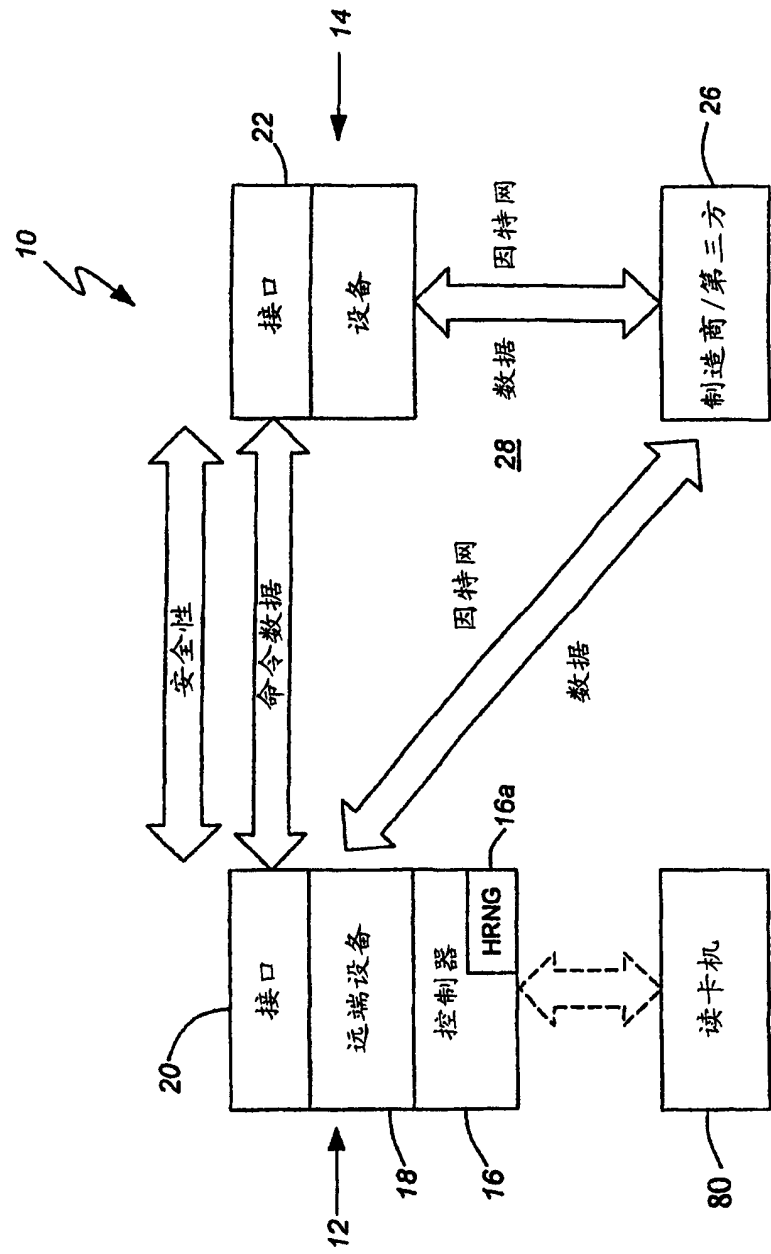


图 7

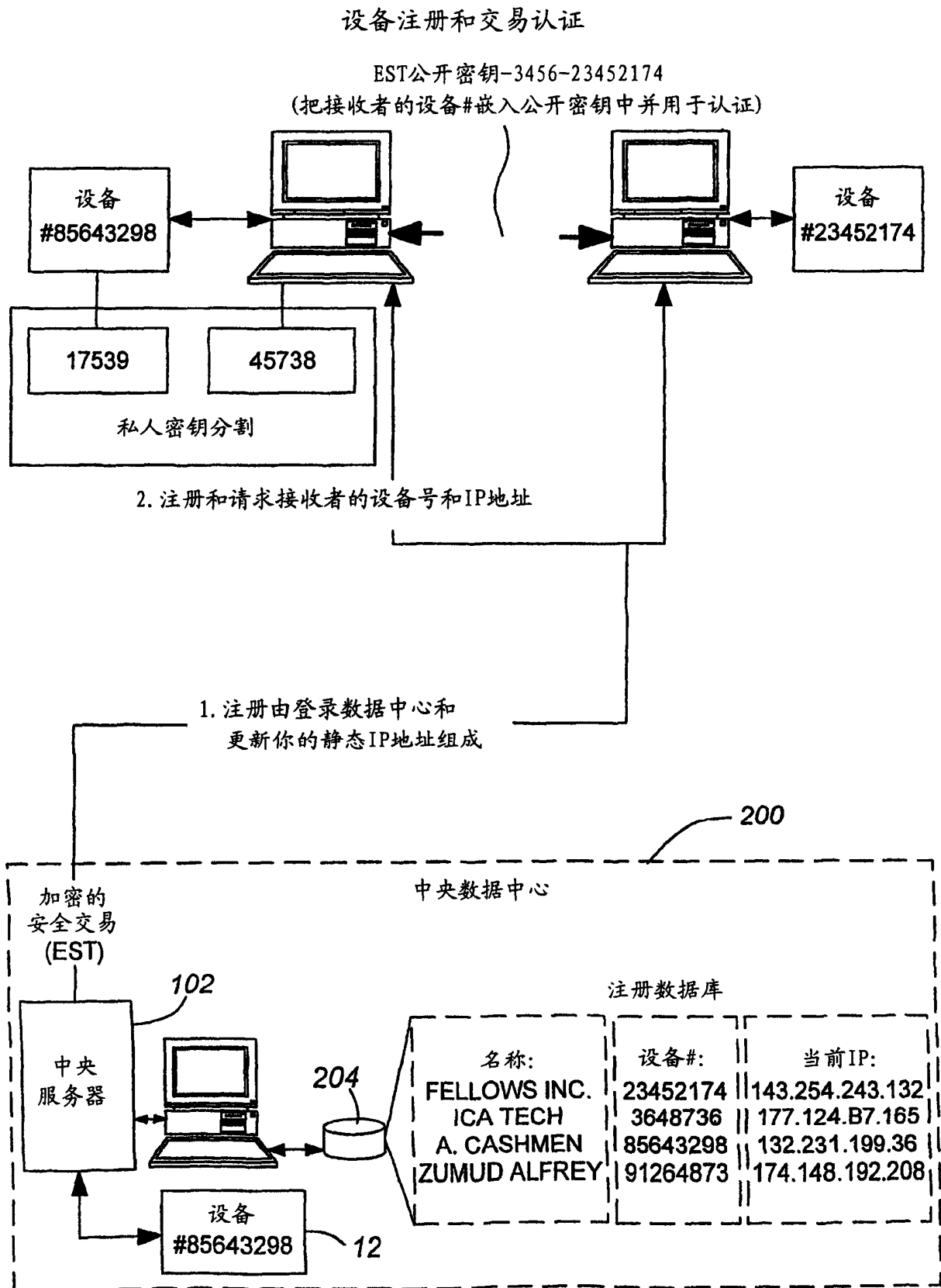


图 8