[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 17/60

[12]发明专利申请公开说明书

[21]申请号 00805438.X

[43]公开日 2002年4月10日

[11]公开号 CN 1344396A

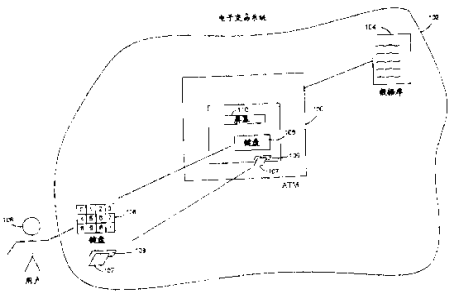
[22]申请日 2000.2.25 [21]申请号 00805438.X
[30]优先权
[32]1999.3.2 [33]US [31]09/260,384
[86]国际申请 PCT/US00/04819 2000.2.25
[87]国际公布 WO00/52866 英 2000.9.8
[85]进入国家阶段日期 2001.9.24
[71]申请人 艾斯格尼克斯公司
地址 美国加利福尼亚
[72]发明人 王殷军
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 罗亚川

权利要求书13页 说明书25页 附图页数14页

[54]发明名称 便携式电子的付费与授权装置及其方法

[57]摘要

一种便携式交易装置,它允许用户面对电子交易系统的一个付费卡终 端进行付费卡交易。所述付费卡终端被这样配置:为了进行所述付费卡 交易的目的而跟一张付费卡进行通信。付费卡是磁条卡和电子智能卡二者当中的一种,便携式交易装置包括一张仿真卡,它具有仿真卡接口。该仿真卡接口对所述付费卡的接口进行仿真。付费卡的接口便于在付费 卡以及付费卡终端之间进行通信。还包括一个便携式仿真卡配置装置,它被安排跟所述仿真卡配合使用,上述装置又包括一个存储器,它被配 置去存储属于该用户的第1付费卡的第1付费卡数据,以及一种验证机 制。便携式仿真卡配置装置被配置成这样:若该用户通过所述验证机制 已被验证,则将第1付费卡数据从存储器写入到仿真卡中去,由此允许 所述仿真卡通过所述仿真卡接口而出现,经过写入之后,并且为了进行 所述交易的目的,像所述第1付费卡与所述付费卡终端(的关系)那样,并且使付费卡终端从仿真卡读入第1付费卡数据,以便进行付费卡交易。



ISSN1008-4274

权 利 要 求 书

1．一种便携式交易装置，它允许用户面对电子交易系统的一个付费卡终端进行付费卡交易，所述付费卡终端被配置成这样：为了进行所述付费卡交易的目的而跟一张付费卡进行通信，所述付费卡是磁条卡和电子智能卡二者当中的一种，包括：

一张仿真卡，它具有仿真卡接口，所述仿真卡接口对所述付费卡的接口进行仿真，所述付费卡的所述接口便于在所述付费卡以及所述付费卡终端之间进行通信；

一个便携式仿真卡配置装置，它被安排跟所述仿真卡配合使用，包括

一个存储器，它被配置去存储属于所述用户的第 1 付费卡的第 1 付费卡数据，以及

一种验证机制，所述便携式仿真卡配置装置被配置成这样：若所述用户通过所述验证机制已被验证，则将所述第 1 付费卡数据从所述存储器写入到所述仿真卡，由此允许所述仿真卡通过所述仿真卡接口而出现，经过写入之后，并且为了进行所述交易的目的，像所述第 1 付费卡与所述付费卡终端的关系那样，并且使所述付费卡终端从所述仿真卡读入所述第 1 付费卡数据，以便进行所述付费卡交易。

2．根据权利要求 1 所述的便携式交易装置，其中，所述仿真卡包括一个唯一的标识标志，其用途是基本上唯一地将所述仿真卡跟所述便携式仿真卡配置装置联系在一起。

3．根据权利要求 1 所述的便携式交易装置，其中，所述付费卡是一种磁条式自动柜员机（ATM）卡，所述付费卡终端是一个自动柜员机（ATM）终端。

4．根据权利要求 1 所述的便携式交易装置，其中，所述付费卡是一种磁条卡，所述付费卡终端是一个自动柜员机（ATM）终端和一个销售点终端二者中的一种。

5．根据权利要求 1 所述的便携式交易装置，其中，所述付费卡是一种电子智能卡。

6．根据权利要求 1 所述的便携式交易装置，其中，所述便携式仿真卡配置装置被配置成这样：在完成所述付费卡交易之后，从所述仿真卡中擦掉所述第 1 付费卡数据。

7．根据权利要求 1 所述的便携式交易装置，其中，所述便携式仿真卡配置装置还包括被安排在所述仿真卡接口以及所述存储器之间的加密逻辑，所述加密逻辑在所述仿真卡接口以及所述存储器之间提供能保证安全的访问。

8．根据权利要求 7 所述的便携式交易装置，其中，所述仿真卡配置装置包括一种付费卡选择机制，所述付费卡选择机制使所述用户能从所述多种付费卡（其付费卡数据也被存储在所述存储器之中）中选择所述用户的所述第 1 付费卡。

9．根据权利要求 8 所述的便携式交易装置，其中，所述存储器为一个单独的个人仅存储付费卡数据。

10．根据权利要求 1 所述的便携式交易装置，其中，所述验证机制包括一个用以接受一组口令字的输入机制，上述口令字包括来自所述用户的、用于验证目的的一组字母数字串。

11．根据权利要求 1 所述的便携式交易装置，其中，所述验证机制为了验证而使用生物测量学。

12．根据权利要求 1 所述的便携式交易装置，其中，所述验证机制为了验证而使用指纹。

13．根据权利要求 7 所述的便携式交易装置，其中，所述仿真卡配置装置被进一步地配置为：将一个加密的交易号码写入所述仿真卡，并且用所述私人密钥对所述加密的交易号码进行加密。

14. 根据权利要求 7 所述的便携式交易装置，其中，所述存储器被配置成这样：存储一组私人密钥，以便按照一种公共密钥/私人密钥加密方案，对数据进行加密，不能从所述便携式仿真卡配置装置的外面访问所述私人密钥，除了通过所述加密逻辑以外。

15．根据权利要求 14 所述的便携式交易装置，其中，所述仿真卡配置装置被进一步地配置为：将加密的交易信息写入所述仿真卡，用所述

私人密钥对所述加密的交易信息进行加密，并且加密的交易信息至少包括属于所述付费卡交易的一个交易时间以及一个交易金额，所述加密的交易信息可以被所述付费卡终端读出，并且使所述仿真卡仅在所述付费卡交易中有效。

16．根据权利要求 15 所述的便携式交易装置，其中，所述加密的交易信息包括所述的交易时间，若所述给定的付费卡交易不能在所述交易时间的一个预定的时间周期之内完成，则所述仿真卡在用于完成一项给定的付费卡交易中是无效的。

17．一种方法，它允许用户面对电子交易系统的一个付费卡终端进行付费卡交易，所述付费卡终端被配置成跟一张付费卡建立接口关系，其目的是进行所述付费卡交易，所述付费卡是磁条卡和电子智能卡二者当中的一种，包括:

提供一种仿真卡，它具有一个仿真卡接口，所述仿真卡接口对所述付费卡的接口进行仿真，所述付费卡的接口便于在所述付费卡以及所述付费卡终端之间进行通信;

提供一个便携式仿真卡配置装置，它被安排跟所述仿真卡配合使用，包括

一个存储器，它被配置去存储属于所述用户的第 1 付费卡的第 1 付费卡数据，以及

一种验证机制，所述便携式仿真卡配置装置被配置成这样：若所述用户通过验证机制已被验证，则将所述第 1 付费卡数据从存储器写入到所述仿真卡，由此允许所述仿真卡通过所述仿真卡接口而出现，经过写入之后，并且为了进行交易的目的，像所述第 1 付费卡与所述付费卡终端（的关系）那样，使所述付费卡终端从所述仿真卡读入所述第 1 付费卡数据，以便进行所述付费卡交易。

18．根据权利要求 17 所述的方法，其中，所述付费卡是一种磁条式自动柜员机（ATM）卡，所述付费卡终端是一个自动柜员机（ATM）终端。

19．根据权利要求 17 所述的方法，其中，所述付费卡是一种磁条卡，

所述付费卡终端是一个自动柜员机（ATM）终端和一个销售点终端二者中的一种。

20．根据权利要求 17 所述的方法，其中，所述付费卡是一张电子智能卡。

21．根据权利要求 17 所述的方法，其中，所述便携式仿真卡配置装置被配置成这样：在完成所述付费卡交易之后，从所述仿真卡中擦掉所述第 1 付费卡数据。

22．根据权利要求 17 所述的方法，其中，所述便携式仿真卡配置装置还包括被安排在所述仿真卡接口以及所述存储器之间的加密逻辑，所述加密逻辑在所述仿真卡接口以及所述存储器之间提供能保证安全的访问。

23．根据权利要求 22 所述的方法，其中，所述存储器被配置成这样：存储一组私人密钥，以便按照一种公共密钥/私人密钥加密方案，对数据进行加密，不能从所述便携式仿真卡配置装置的外面访问所述私人密钥，除了通过所述加密逻辑以外。

24．根据权利要求 17 所述的方法，其中，所述仿真卡配置装置被进一步地配置成这样：不能将付费卡数据写入另一张卡，所述另一张卡指的是这样一张仿真卡，它基本上不是唯一地将所述便携式仿真卡配置装置跟一张付费卡联系在一起。

25．根据权利要求 17 所述的方法，其中，所述仿真卡包括一个唯一的标识标志，其用途是基本上唯一地将所述仿真卡跟所述便携式仿真卡配置装置联系在一起。

26．根据权利要求 23 所述的方法，其中，所述仿真卡配置装置包括一种付费卡选择机制，所述付费卡选择机制使所述用户能从所述多种付费卡（其付费卡数据也被存储在所述存储器之中）中选择所述用户的所述第 1 付费卡。

27．根据权利要求 26 所述的方法，其中，所述存储器为一个单独的个人仅存储付费卡数据。

28．根据权利要求 17 所述的方法，其中，所述验证机制包括一种用

以接受一组口令字的输入机制，上述口令字包括来自所述用户的、用于验证的一组字母数字串。

29．根据权利要求 17 所述的方法，其中，所述验证机制为了验证而使用生物测量学。

30．根据权利要求 17 所述的方法，其中，所述验证机制为了验证而使用指纹。

31．根据权利要求 23 所述的方法，其中，所述仿真卡配置装置被进一步地配置为：将一个加密的交易号码写入所述仿真卡，并且用所述私人密钥对所述加密的交易号码进行加密。

32．根据权利要求 23 所述的方法，其中，所述便携式仿真卡配置装置被进一步地配置为：将加密的交易信息写入所述仿真卡，用所述私人密钥对所述加密的交易信息进行加密，并且加密的交易信息至少包括属于所述付费卡交易的一个交易时间以及一个交易金额，所述加密的交易信息可以被所述付费卡终端读出，并且使所述仿真卡仅在所述付费卡交易中有效。

33．根据权利要求 23 所述的方法，其中，所述加密的交易信息包括所述的交易时间，若所述给定的付费卡交易不能在所述交易时间的一个预定的时间周期之内完成，则所述仿真卡在用于完成一项给定的付费卡交易中是无效的。

34．根据权利要求 23 所述的方法还包括从一个可信任的第三方获得一组公共密钥，用以对从所述仿真卡读出的数据进行解密，所述数据被所述便携式仿真卡配置装置用所述私人密钥进行加密。

35．一个便携式交易装置，它允许用户面对电子交易系统的一个付费卡终端进行付费卡交易，包括：

便携式仿真卡配置装置，它被配置跟所述仿真卡配合使用，并且具有对所述仿真卡进行写入的功能，包括

存储器装置，它被配置去存储属于所述用户的第 1 付费卡的第 1 付费卡数据，所述仿真卡具有仿真卡接口，所述仿真卡接口对所述付费卡的接口进行仿真，所述付费卡终端被配置成通过所述第 1 付费卡的所述接

口跟所述第 1 付费卡进行通信，所述付费卡是磁条卡和电子智能卡二者当中的一种，以及

验证装置，它被这样安排：使用被存储在所述存储器装置里面的所述验证数据来验证所述用户，所述便携式仿真卡配置装置被配置成这样：若所述用户通过所述验证机制已被验证，则将属于所述第 1 付费卡的所述第 1 付费卡数据从所述存储器装置写入到所述仿真卡，由此允许所述仿真卡通过所述仿真卡接口而出现，经过写入之后，并且为了进行所述交易的目的，像所述第 1 付费卡与所述付费卡终端（的关系）那样，并且使所述付费卡终端从所述仿真卡读入所述第 1 付费卡数据，以便进行所述交易。

36．根据权利要求 35 所述的便携式交易装置还包括，被安排在所述仿真卡接口以及所述存储器装置之间的加密逻辑，所述加密逻辑在所述仿真卡接口以及所述存储器装置之间提供能保证安全的访问。

37．根据权利要求 35 所述的便携式交易装置，其中，所述付费卡是一种磁条式自动柜员机（ATM）卡，所述付费卡终端是一个自动柜员机（ATM）终端。

38．根据权利要求 35 所述的便携式交易装置，其中，所述付费卡是一种磁条卡，所述付费卡终端是一个自动柜员机（ATM）终端和一个销售点终端二者当中的一种。

39．根据权利要求 35 所述的便携式交易装置，其中，所述付费卡是一种电子智能卡。

40．根据权利要求 35 所述的便携式交易装置，其中，所述便携式仿真卡配置装置被配置成这样：在完成所述付费卡交易之后，从所述仿真卡中擦掉所述第 1 付费卡数据。

41．根据权利要求 35 所述的便携式交易装置，其中，所述便携式仿真卡配置装置还包括被连接到所述存储器装置的加密逻辑，所述加密逻辑被安排向所述存储器装置提供能保证安全的访问。

42．根据权利要求 41 所述的便携式交易装置，其中，所述存储器装置被配置成这样：存储一组私人密钥，以便按照一种公共密钥/私人密钥

加密方案，对数据进行加密，不能从所述便携式仿真卡配置装置的外面访问所述私人密钥，除了通过所述加密逻辑以外。

43．根据权利要求 42 所述的便携式交易装置，其中，所述仿真卡配置装置被配置成这样：不能将付费卡数据写入另一张仿真卡，所述另一张仿真卡指的是这样一张仿真卡，它基本上不是唯一地联系于所述便携式仿真卡配置装置。

44．根据权利要求 43 所述的便携式交易装置，其中，所述仿真卡包括一个唯一的标识标志，其用途是基本上唯一地将所述仿真卡跟所述便携式仿真卡配置装置联系在一起。

45．根据权利要求 35 所述的便携式交易装置，其中，所述仿真卡配置装置包括一种付费卡选择机制，所述付费卡选择机制使所述用户能从所述多种付费卡（其付费卡数据也被存储在所述存储器之中）中选择所述第 1 付费卡。

46．根据权利要求 45 所述的便携式交易装置，其中，所述存储器装置为一个单独的个人仅存储付费卡数据。

47．根据权利要求 35 所述的便携式交易装置，其中，所述验证机制包括一种用以接受一组口令字的输入机制，上述口令字包括来自所述用户的、用于验证的一组字母数字串。

48．根据权利要求 42 所述的便携式交易装置，其中，所述仿真卡配置装置被进一步地配置为：将一个加密的交易号码写入所述仿真卡，

所述加密的交易号码可以被所述付费卡终端读出，并且用所述私人密钥对所述加密的交易号码进行加密。

49．根据权利要求 42 所述的便携式交易装置，其中，所述便携式仿真卡配置装置被进一步地配置为：将加密的交易信息写入所述仿真卡，用所述私人密钥对所述加密的交易信息进行加密，并且加密的交易信息至少包括属于所述付费卡交易的一个交易时间以及一个交易金额，所述加密的交易信息可以被所述付费卡终端读出，并且使所述仿真卡仅在所述付费卡交易中有效。

50．根据权利要求 42 所述的便携式交易装置，其中，所述加密的交

易信息包括所述的交易时间，若所述给定的付费卡交易不能在所述交易时间的一个预定的时间周期之内完成，则所述仿真卡在用于完成一项给定的付费卡交易中是无效的。

51．一个便携式交易装置，它允许用户面对电子交易系统进行交易，包括:

一个付费卡终端接口子系统，包括

一张仿真卡，它具有仿真卡接口，所述仿真卡接口对一张付费卡的接口进行仿真，所述付费卡是磁条卡和电子智能卡二者当中的一种，所述付费卡的所述接口便于在所述付费卡以及所述电子交易系统的一个付费卡终端之间进行通信；以及

一个便携式仿真卡配置装置，它被安排跟所述仿真卡配合使用，包括

一个第 1 存储器部分，它被配置去存储属于所述用户的一张付费卡的付费卡数据，以及

一种验证机制，所述便携式仿真卡配置装置被配置成这样：若所述用户通过所述验证机制已被验证，则将属于所述用户的所述付费卡的付费卡数据从所述存储器写入到所述仿真卡，由此允许所述仿真卡通过所述仿真卡接口而出现，经过写入之后，并且为了进行所述交易的目的，像所述用户的所述付费卡与所述付费卡终端（的关系）那样，并且使所述付费卡终端从所述仿真卡读入所述付费卡数据，以便进行所述交易；以及

一个电子授权接口子系统，包括

第 1 逻辑电路，它被配置从所述电子交易系统接收第 1 数字数据，该数据代表属于所述交易的一项交易请求，

第 2 逻辑电路，它被这样配置：响应于由所述第 1 逻辑电路接收的所述交易请求，若所述交易请求被所述用户认可，则形成第 2 数字数据，代表已加密数据的所述第 2 数字数据表示所述用户对所述交易请求的认可；以及

被连接到所述第 2 逻辑电路的发送电路，所述发送电路被这样配置：若所述用户认可所述交易请求，则将所述第 2 数字数据从所述的便携式

交易装置发送到所述电子交易系统。

52．根据权利要求 51 所述的便携式交易装置，其中所述便携式仿真卡配置装置还包括被安排在所述仿真卡接口以及所述第 1 存储器部分之间的加密逻辑，所述加密逻辑在所述仿真卡接口以及所述第 1 存储器部分之间提供能保证安全的访问。

53．根据权利要求 51 所述的便携式交易装置，其中，所述仿真卡包括一个唯一的标识标志，其用途是基本上唯一地将所述仿真卡跟所述便携式仿真卡配置装置联系在一起。

54．根据权利要求 51 所述的便携式交易装置，其中，所述便携式仿真卡配置装置还包括被连接到所述第 1 存储器部分的加密逻辑，所述加密逻辑被安排向所述第 1 存储器部分提供能保证安全的访问。

55．根据权利要求 54 所述的便携式交易装置，其中，所述便携式仿真卡配置装置还包括被连接到所述加密逻辑的第 2 存储器部分，所述第 2 存储器部分被配置去存储一组私人密钥，以便按照一种公共密钥/私人密钥加密方案，对数据进行加密，所述加密逻辑被安排向所述第 1 存储器部分提供能保证安全的访问。

56．根据权利要求 55 所述的便携式交易装置，其中，所述仿真卡配置装置包括一种付费卡选择机制，所述付费卡选择机制使所述用户能从所述多种付费卡（其付费卡数据也被存储在所述第 1 存储器部分之中）中选择所述用户的所述付费卡。

57．根据权利要求 55 所述的便携式交易装置法，其中，所述验证机制包括一种用以接受一组口令字的输入机制，上述口令字包括来自所述用户的、用于验证的一组字母数字串。

58．根据权利要求 55 所述的方法，其中，所述验证机制为了验证而使用生物测量学。

59．根据权利要求 55 所述的便携式交易装置，其中，所述仿真卡配置装置被进一步地配置为：将一个加密的交易号码写入所述仿真卡，

并且用所述私人密钥对所述加密的交易号码进行加密。

60．根据权利要求 55 所述的便携式交易装置，其中，所述便携式仿

真卡配置装置被进一步地配置为：将加密的交易信息写入所述仿真卡，用所述私人密钥对所述加密的交易信息进行加密，并且加密的交易信息至少包括属于所述付费卡交易的一个交易时间以及一个交易金额，所述加密的交易信息可以被所述付费卡终端读出，并且使所述仿真卡仅在所述付费卡交易中有效。

61．根据权利要求 60 所述的便携式交易装置，其中，所述加密的交易信息包括所述的交易时间，若所述给定的付费卡交易不能在所述交易时间的一个预定的时间周期之内完成，则所述仿真卡在用于完成一项给定的付费卡交易中是无效的。

62．根据权利要求 51 所述的便携式交易装置，其中，所述付费卡是一种磁条式自动柜员机（ATM）卡，所述付费卡终端是一个自动柜员机（ATM）终端。

63．根据权利要求 51 所述的便携式交易装置，其中，所述付费卡是一种磁条卡，所述付费卡终端是一个销售点终端。

64．根据权利要求 51 所述的便携式交易装置，其中，所述付费卡是一种电子智能卡。

65．根据权利要求 51 所述的便携式交易装置，其中，所述便携式仿真卡配置装置被配置成这样：在完成所述付费卡交易之后，从所述仿真卡中擦掉所述第 1 付费卡数据。

66．一种方法，它允许用户面对被连接到因特网的一部用户计算机终端去认可一项因特网交易请求，通过被连接到因特网的一部第 1 计算机来产生所述因特网交易请求，包括：

将所述第 1 数字数据从所述第 1 计算机送往所述用户计算机终端，所述第 1 数字数据表示所述因特网交易请求；

在被连接到因特网的一部第 2 计算机接收第 2 数字数据，所述用户经由所述用户计算机终端以手工方式输入所述第 2 数字数据，所述第 2 数字数据表示用户可读的、已加密的交易认可数据，表示所述用户对所述因特网交易请求的认可，所述用户通过便携式电子授权装置（PEAD）以及便携式电子付费与授权装置（PECAD）二者其中之一，使用所述用户

的私人密钥对所述第 2 数字数据进行加密，并且所述第 2 数字数据是来自由所述用户输入到便携式电子授权装置（PEAD）以及便携式电子付费与授权装置（PECAD）二者其中之一的信息；以及

在进行所述接收之后，使用所述用户的公共密钥对第 2 数字数据进行解密。

67．根据权利要求 66 所述方法还包括从一个可信任的第三方接收所述公共密钥。

68．根据权利要求 66 所述方法，其中，由所述用户向所述便携式电子授权装置（PEAD）以及便携式电子付费与授权装置（PECAD）二者其中之一输入的信息包括与所述因特网交易请求有关的交易金额。

69．根据权利要求 66 所述方法，其中，由所述用户向所述便携式电子授权装置（PEAD）以及便携式电子付费与授权装置（PECAD）二者其中之一输入的信息还包括用于付费的一个信用卡号码。

70．根据权利要求 66 所述方法，其中，使用所述便携式电子授权装置（PEAD）对所述第 2 数字数据进行加密。

71．根据权利要求 66 所述方法，其中，使用所述便携式电子付费与授权装置（PECAD）对所述第 2 数字数据进行加密。

72．根据权利要求 66 所述方法，其中，所述第 1 计算机和所述第 2 计算机是相同的计算机。

73．根据权利要求 66 所述方法，其中，所述第 1 计算机和所述第 2 计算机是不同的计算机。

74．一种由计算机实现的、用以对专门的电子加密装置的用户进行注册的方法，上述装置被配置成按照一种公共密钥加密方案对数据进行加密，包括：

在一个计算机数据库中，提供一份属于多个电子加密装置的公共密钥和标识信息的列表，所述公共密钥列表中的各具体成员跟多个电子加密装置的各具体成员有关；

接收来自所述用户的装置标识数据，所述装置标识数据对所述专门的电子加密装置加以标识；

接收已加密的用户标识数据，以证实所述用户的身份；

在所述数据库中，将所述装置标识数据跟所述专门的电子加密装置联系在一起，由此从数据库中证实一组专门的公共密钥跟所述专门的电子加密装置有关；

使用所述专门的公共密钥对所述已加密的用户标识数据进行解密；以及

若所述解密是成功的话，在所述数据库中将所述用户跟所述专门的电子加密装置联系在一起。

75．根据权利要求 74 所述方法，其中，所述专门的电子加密装置表示一个便携式电子授权装置。

76．根据权利要求 74 所述方法，其中，所述专门的电子加密装置表示一个便携式电子付费与授权装置。

77．根据权利要求 74 所述方法还包括在所述数据库中，向所述用户分配一个有效性等级，根据与所述用户标识数据有关的信用等级来分配所述有效性等级。

78．根据权利要求 77 所述方法，其中，所述有效性等级表示一个高级和一个低级，若所述用户出示其个人的所述用户标识数据，并能通过所述用户身份与所述用户标识数据的验证，则在所述数据库中，向所述用户分配所述高级。

79．根据权利要求 78 所述方法，其中，若所述用户未能出示其个人的所述用户标识数据，以通过所述用户身份与所述用户标识数据的验证，则在所述数据库中，向所述用户分配所述低级。

80．根据权利要求 77 所述方法，其中，所述有效性等级跟一项保险政策所提供的保险覆盖金额挂钩，配置此项保险政策是为了保护所述专门的电子加密装置免受欺骗性的注册。

81．一种由计算机实现的、用以对专门的电子加密装置的用户进行注册的装置，上述装置被配置成按照一种公共密钥加密方案对数据进行加密，包括：

用于存储属于多个电子加密装置的公共密钥和标识信息的一份列表，

在所述各公共密钥的列表中，具体的各公共密钥跟所述多个电子加密装置的各具体成员有关；

用于从已加密的、用户提供的装置标识数据来确定所述标识信息以及所述各公共密钥的列表的装置，一组专门的公共密钥跟所述专门的电子加密装置有关，由此，所述已加密的、用户提供的装置标识数据对所述专门的电子加密装置加以标识；

使用所述专门的公共密钥，对从所述用户那里接收的所述已加密的、用户提供的装置标识数据进行解密的装置；以及

若所述解密是成功的话，将所述用户跟所述专门的电子加密装置联系在一起的装置。

82．根据权利要求 81 所述的由计算机实现的装置，其中，所述专门的电子加密装置表示一部便携式电子授权装置。

83．根据权利要求 81 所述的由计算机实现的装置，其中，所述专门的电子加密装置表示一部便携式电子付费与授权装置。

84．根据权利要求 81 所述的由计算机实现的装置还包括，在所述数据库中，向所述用户分配一种有效性等级的装置，根据与所述用户的身份有关的信用等级来分配所述有效性等级。

说　　明　　书

便携式电子的付费与授权装置及其方法

发明背景

本发明涉及用于进行电子交易的方法和装置。 特别是，本发明涉及便携式电子授权装置（ PEADs），它基本上排除了使用现有技术在用户和电子交易系统之间认可交易时的安全风险，这是非常有利的。

电子交易系统是人所共知的。 电子交易系统允许用户用电子的方式进行指定的交易，这大大地提高了效率，为用户提供了很大的方便。 电子交易的实例包括，通过计算机网络、自动柜员机（ ATM’ s ）、自动销售点系统、自动化图书馆系统等进行的交易。 通过计算机网络进行的交易可能包括各种各样的交易，包括通过计算机网络进行的信息和数据的交换，例如，在网上向卖方进行购买，这个计算机网络通常被称为因特网。 ATM’s 允许用户以电子的方式在金融机构进行金融交易（例如，提款、转帐、存款等等）。 商人可能使用自动销售点系统，让用户利用自己的电子帐号购买产品或服务，自动化图书馆系统可能被用来让图书馆读者进行结帐以及归还图书馆的资料。 其他的电子交易系统的实例在文献中很容易找到，为了简便起见，这里就不再枚举。

为了提高用户帐号的安全性，电子交易系统一般要求用户提供标识数据，以证明他自己就是被授权去认可意向中的交易或各项交易的那个用户。 若用户不能提供所要求的标识数据，则意向中的交易或各项交易就得不到授权，并且将不会被处理。 可能每一笔交易都要求有标识数据。 举例来说，自动销售点系统可能要求用户认可一笔购买交易，并且只有当认可交易的那个人能够提供足够的识别数据，证明他自己是被授权进行交易认可的那个人时，才接受这条认可信息。 可选地，用户可以在交易开始时输入标识数据来认证他自己，使用户随后可以进行任何数量的交易而不必进一步地进行认证。

使用现有技术，一般要求用户手工地将标识数据输入电子交易系统进行认证。 输入标识数据一般涉及使用数字小键盘或键盘键入一个口令字。 然后标识数据连同预先存储在电子交易系统里面的数据进行比较，当二者匹配时，认证得以通过。 如前所述，如果不匹配，意向中的交易或各项交易将不被允许进行。

虽然现有技术的电子交易系统能够对未被授权的访问以及用户帐号的使用提供一定的防护，但是还有不利之处。 为了举例说明现有技术的电子交易系统的某些不利之处，这里可能需要参照图 1 。 图 1 表示自动柜员机（ATM）100 ，是电子交易系统 102 的请求装置。 例如，电子交易系统 102 可能包括一个中央数据库 104 ，其中含有预先存储的用户 106 的标识数据和帐号数据。

为了开始进行与 ATM 100 的一笔典型的交易，用户 106 首先将数据卡 107，例如银行卡或信用卡，插入读卡机 109。 数据卡 107 一般包括一条磁带，其中包含与该用户有关的帐号及其他信息，然后这些信息可能被读卡机 109 读出。 数据卡 107 中存储的数据使电子交易系统 102 能够确定用户 106 希望同数据库 104 中的哪个帐号进行商务交易。

通过 ATM 100 上的键盘 108，用户 106 就能够输入他的标识数据，例如，他的个人标识号码（PIN），以认证他自己。 如果输入的标识数据，与通过数据卡 107 从数据库 104 中识别出来的帐号中存储的标识数据相匹配，那么用户就通过认证，并且被授权访问他的帐号。 如果不匹配，认证就失败。 认证后，例如，用户 106 就能综合使用键盘 108 和屏幕 110 从他的帐号中提取现金，这样就导致现金从 ATM 100 中向外发放，数据库 104 里面他的帐号余额也相应地减少。

从理论上说，输入 ATM 100 的标识数据应当是安全的。 实际上，使用现有技术的认证方法，标识数据存在许多潜在的安全风险。 因为在输入 ATM 100 之前标识数据没有经过加密，未加密的标识数据容易受到未经授权的访问或被他人获得。在现有技术中，对标识数据进行加密是不实际的，因为用户进行加密或记住加密的标识数据会非常复杂和/或不方便。 使用现有技术时，可能发生未经授权而获得标识数据，例如，输

入时被另一方无意中看到，比如用户 106 后面的任何人，或者在屏幕 110 上，或者更可能在键盘 108 上看到。

即使在现有技术中对标识数据进行了加密，例如，在从 ATM 100 发送到数据库 104 之前，但是加密一般发生在 ATM 100 内部，仍然要求用户 106 输入非加密的标识数据，而且标识数据还会在 ATM 100 里面存在一段时间。如果未经授权的一方能够进入 ATM 100，并且在那里，例如通 ATM 100 安装的软件或硬件，截获了未加密的标识数据，那么对标识数据的未经授权的访问就可能发生。

此外，如果 ATM 100 里面使用公共密钥的加密方法，那么用户的私人密钥存储在 ATM 100 里面，使得私人密钥易于被盗，更进一步地将用户的帐号暴露于风险之中。被盗的口令字和/或私人密钥可能会被用来让未经授权的人访问用户的帐号，从而给用户带来损害。

鉴于前述各点，理想的装置和方法是在电子交易系统中进行交易的同时，能够大体上排除对用户帐号的未经授权的访问以及未经授权地取得用户标识数据的风险。这种装置应当尽可能地便于携带，以允许用户在任何地方都能方便而舒适地进行交易认证。

本发明在一个实施例中涉及一个便携式交易装置，它允许用户面对电子交易系统的一个付费卡终端进行付费卡交易。付费卡终端被这样配置：为了进行付费卡交易的目的而跟一张付费卡进行通信。付费卡是磁条卡和电子智能卡二者当中的一种。便携式交易装置包括一张仿真卡，它具有仿真卡接口。仿真卡接口对付费卡的接口进行仿真。付费卡的接口便于在付费卡以及付费卡终端之间进行通信。还包括一个便携式仿真卡配置装置，它被安排跟仿真卡配合使用，仿真卡又包括一个存储器，它被配置去存储属于该用户的第 1 付费卡的第 1 付费卡数据，以及一种验证机制。便携式仿真卡配置装置被这样配置：若该用户通过验证机制已被验证，则将第 1 付费卡数据从存储器写入到仿真卡，由此允许该仿真卡通过仿真卡接口而出现，经过写入之后，并且为了进行交易的目的，像第 1 付费卡与付费卡终端（的关系）那样，并且使付费卡终端从仿真卡读入第 1 付费卡数据，以便进行付费卡交易。

在另一个实施例中，本发明涉及一种方法，它允许用户面对电子交易系统的一个付费卡终端进行付费卡交易。该付费卡终端被配置成跟一张付费卡建立接口关系，其目的是进行付费卡交易。付费卡是磁条卡和电子智能卡二者当中的一种。本方法包括提供一种仿真卡，它具有一个仿真卡接口。仿真卡接口对付费卡的接口进行仿真。付费卡的接口便于在付费卡以及付费卡终端之间进行通信。还包括一个便携式仿真卡配置装置，它被安排跟仿真卡配合使用，仿真卡包括一个存储器，它被配置去存储属于该用户的第 1 付费卡的第 1 付费卡数据，以及一种验证机制。便携式仿真卡配置装置被这样配置：若该用户通过验证机制已被验证，则将第 1 付费卡数据从存储器写入到仿真卡，由此允许该仿真卡通过仿真卡接口而出现，经过写入之后，并且为了进行交易的目的，像第 1 付费卡与付费卡终端（的关系）那样，并且使付费卡终端从仿真卡读入第 1 付费卡数据，以便进行付费卡交易。

在又一个实施例中，本发明涉及一种方法，它允许用户面对被连接到因特网的一部用户计算机终端去认可一项因特网交易。通过被连接到因特网的一部第 1 计算机产生因特网交易请求。本方法包括将第 1 数字数据从第 1 计算机送往用户计算机终端，第 1 数字数据表示因特网交易请求。本方法还包括在被连接到因特网的一部第 2 计算机中接收第 2 数字数据。用户经由用户计算机终端以手工方式输入第 2 数字数据。第 2 数字数据表示用户可读的、已加密的交易认可数据，表示该用户对因特网交易请求的认可，上述交易认可数据来自用户向便携式电子授权装置（PEAD）以及便携式电子付费与授权装置（PECAD）二者其中之一输入的信息，并且通过便携式电子授权装置（PEAD）以及便携式电子付费与授权装置（PECAD）二者其中之一，使用用户的私人密钥对上述因特网交易请求进行加密。本方法还包括，在接收之后，使用用户的公共密钥对第 2 数字数据进行解密。

在再一个实施例中，本发明涉及一种由计算机实现的、用以对专门的电子加密装置的用户进行注册的方法，上述装置被配置成按照一种公共密钥加密方案对数据进行加密。本方法包括在一个计算机数据库中，提

供属于多个电子加密装置的一份公共密钥和标识信息的列表，该公共密钥列表中的各具体成员跟多个电子加密装置的各具体成员有关。本方法还包括从用户那里接收装置标识数据。该装置标识数据对专门的电子加密装置加以标识。还包括接收已加密的用户标识数据，以证实该用户的身份。此外，在数据库中还包括将装置标识数据跟专门的电子加密装置联系在一起，由此从数据库中证实一组专门的公共密钥跟专门的电子加密装置有关。还有，这里还包括使用专门的公共密钥对已加密的用户标识数据进行解密，并且若解密是成功的话，在数据库中将该用户跟专门的电子加密装置联系在一起。

通过阅读以下的详细说明以及研究诸附图，本发明的这些和其他优点将变得更加明显。

诸附图的简要说明

为了便于讨论，图 1 表示一种现有技术的电子交易系统，包括一个自动柜员机（ATM）。

图 2 根据本发明的一个实施例，说明一种便携式电子授权装置（PEAD），它表示用于安全地认可在电子交易系统中进行的交易的装置。

图 3A 表示，在本发明的一个实施例中，图 2 的 PEAD 的简化的简图。

图 3B 表示，在一个实施例中，代表性的交易认可数据的格式。

图 4 表示，根据本发明的一个实施例的 PEAD 的一个逻辑的方框图。

图 5A 表示，根据本发明的一个实施例的 PEAD 的一种高级硬件实施方案。

图 5B 表示 PEAD 的一种实施方案，其中，PEAD 电路在一块集成电路上实现。

图 5C 表示图 5B 的 PEAD 在嵌入到卡状壳内后的外观图。

图 6A 表示，根据本发明的一个优选实施例的 PEAD 的外观。

图 6B 根据本发明的一个方面，并且以简化的方式，表示用于实现图 6A 的 PEAD 的硬件。

图 7 是一份流程图，根据本发明的一个方面，表示使用创新性的 PEAD 的认可技术。

图 8 是一份流程图，根据本发明的一个方面，表示在使用公共密钥加密方法对交易认可数据进行加密时所涉及的各步骤。

图 9 表示，根据本发明的一个方面的一种便携式电子支付与授权装置（PECAD）的一份简化的方框图。

图 10 是 PECAD 的一份简化图，包括根据本发明的一个实施例而安置在其中的一张仿真卡。

图 11 是一份简化的流程图，表示根据一个实施例，如何结合一个 PECAD 系统来使用一个交易号码，以改进交易的安全性。

各优选实施例的详细说明

图 2 根据本发明的一个实施例，说明一种便携式电子授权装置（PEAD）200，它表示用于安全地认可在电子交易系统中进行的交易的装置。参照图 2，经由通信端口 204，通过向 PEAD 200 发送属于一项意向中的交易的交易请求，请求装置 202 就能用 PEAD 200 来启动一个交易认可过程。请求装置 202 可以代表例如一部自动柜员机（ATM），在网络中的一个计算机终端，一个自动化图书馆的结帐终端，或者允许用户跟电子交易系统进行商务交易的各种类似的装置。意向中的交易可以是，例如，针对一定金额的一个特定项目的销售交易。交易请求本身可以包括，例如，交易标识（ID），商人的姓名，商人的标识（ID），意向中的购买时间，等等。在一个实施例中，来自请求装置 202 的交易请求可以被加密，以便增加安全性，但是不要求这样做。属于意向中的交易的数据经由图 2 的路径 206 到达 PEAD 200。

端口 204 表示便于跟 PEAD 200 进行红外通信的红外端口。可供选择地，端口 204 也可以表示用以实现无线通信的无线端口。端口 204 甚至可以表示一个接触型连接端口，例如一个磁读/写机构，或者一个具有电触点的插头，用于将 PEAD 200 直接插入端口 204 以实现通信。在请求装置 202 与 PEAD 200 之间用以实现通信的其他技术也都是专业人士早已熟知的。

用户可以在请求装置 202 的屏幕 208，或者可选地在备有 PEAD 200 的显示屏幕（在图 2 中未示出）上察看属于意向中的（各项）交易的数据。若用户认可该项交易，例如，一项给定的金额的购买项目，则该用户通过按压在 PEAD 200 上的一个开关，来表示他的认可，由此导致一项认可消息，连同该用户的标识数据一起被生成，该消息经加密后经由路径 212 送回请求装置 202。若此项交易没有被认可，则该用户可以什么也不做，并且经过一段时间之后，让该项交易请求过时，或者可以按压在 PEAD 200 上的另一个开关（在图 1 中未示出），由此导致一条拒绝消息，可能是已加密的或未加密的，经由路径 212 被送回请求装置 202。

本发明不同于图 1 所示的现有技术，在现有技术中，用户被要求将其标识数据输入到电子交易系统，例如，输入到 ATM 100 中去，以验证他本身。与此相对照，本发明在所有的时间内都在 PEAD 200 中保证涉及该用户的标识数据的安全。交易认可在 PEAD 200 中发生，并且，在发送到电子交易系统，例如图 2 的请求装置 202 之前，表示此种认可的数据再次在 PEAD 200 中被加密。

相应地，即使认可数据被截获，它的密码也能防止未经授权的用户出于不正当的目的来使用该项标识数据。若使用公共密钥加密方法来加密认可数据，则该用户的私人密钥经常被保存在 PEAD 200 之中。由于在加密过程中需要用户的私人密钥，并且不为他人所知，就连电子交易系统也不知道，所以，在一个实施例中，若加密的认可数据被他人所截获，虽然使用该用户的公共密钥能对该项认可数据进行解密，但是对未经授权的第三方来说，仍然是无用的。再有，这也不同于现有技术中的验证技术，在现有技术中，加密过程在电子交易系统中发生，并且要求输入标识数据和/或从 ID 卡，例如 ATM 卡，信用卡等，读入该用户的私人密钥。如上所述，现有技术的电子交易系统需要这样的标识数据和/或用户的私人密钥，就将这些数据暴露于风险之中，例如，若请求装置不安全，或者经由软件或硬件，使其对数据截获者开放。

作为另一项不同之处，本发明使用在便携式电子授权装置（PEAD）里面的电路，在 PEAD 本身的内部进行交易认可数据的认可和加密。与

此相对照，现有技术的数据卡基本上都是无源装置。例如，现有技术的各种 ATM 卡或各种信用卡仅有一个磁条用以存储帐号信息，并且不具备任何用于进行交易认可数据的认可和/或加密的装置。而当前正在开发的各种智能卡或 IC 卡，可能含有电子电路，其实施方案的现行标准仍然需要一个与请求装置相关联的读出器去读出标识数据和/或用户的私人密钥，以便请求装置进行任何认可和/或加密。如上所述，将这些数据送往请求装置，一旦被发送，就不必要地将这些数据暴露于被盗和/或未经授权的截获的风险之中。

在这一点上，应当记住的是，虽然在此次公开中，为了便于理解以及为了强调本发明的一个特殊方面，讨论了公共密钥的加密方法，但是整个的发明不局限于任何特定的加密算法，并且可以使用任何常规的加密技术来实现，上述常规的加密技术包括公共密钥加密算法，诸如 RSA，Diffie-Hellman，其他各种离散算法系统，各种椭圆曲线系统，等等。关于某些不同的公共密钥的加密方法的附加的信息，可参考例如，1998 年 10 月 5 日发布的《用于公共密钥的加密方法的 IEEE P1363/D8 标准说明书》，该文献可以从纽约州 10017-2349，纽约市，东 7 街 345 号，国际电气与电子工程师学会标准部获得。

正如前面提到，使用现有技术时，交易的认可发生在电子交易系统内部。相比之下，本发明允许交易认可发生在 PEAD 200 内部。交易认可完全发生在 PEAD200 内部有许多好处。举例来说，在一个实施例中，该特点使得请求装置中不需要标识数据和/或用户的私人密钥。交易认可完全发生在 PEAD 200 内部（使用用户标识数据和／或用户的私人密钥，它们在 PEAD 200 内部通常是安全的），大大加强了用户标识数据和用户私人密钥的保密性，以及交易认可过程的完整性。

因为认可完全发生在 PEAD 200 内部，所以用来认证交易的用户标识数据可能是更复杂和精细的，能够确保更高的安全性。举例来说，用户标识数据可能比一个简单的口令字更加精细，并且可能会包括用户姓名、出生日期、社会保障号码、或者其它的诸如指纹、DNA 编码序列、声纹等生物测量学或独一无二的识别数据中的任何一种。 相比之下，现有技

术的认证方法将用户标识数据局限为简单的模式，例如，由少数几个字符组成的简单口令字，它们可以容易地被用户记住，因为更精细的标识数据可能难以记住，或者手动输入太麻烦。此外，即使复杂的标识数据可能存储在使用现有技术的数据卡中，仍然要求将它读入电子交易系统的请求装置，一旦读入，又会使这个数据暴露于被截获或者被盗的危险之中。

也可以提供额外的防范措施，防止接触 PEAD 200 内部的用户标识数据和/或用户私人密钥，无论是用电子手段还是物理手段都一样，这里将详细进行描述。因为标识数据和/或用户私人密钥从来没有被暴露，因此这些数据的安全风险实质上得以最小化。

图 3A 表示，在本发明的一个实施例中，图 2 中包括开关 210 的 PEAD 200 的一个简化的概略图。数据通路 206 是用来接收来自电子交易系统的交易请求的，数据通路 212 将交易认可数据送回电子交易系统。必须记住，虽然在这里讨论两个数据通路是为了易于理解，但是在一个实施例中，这些数据通路和这里其他的数据通路可能代表逻辑的数据通路，并且可能是通过一个单一的物理的数据连接来实现的。同样地，在一个实施例中，为了便于理解，这里不同的端口可能代表逻辑的数据端口，并且可能事实上用一个物理的端口来实现。

当提出交易要求时，例如，从 ATM 中取出金额为$200.00 的交易，通过数据通路 206 传输到 PEAD 200，该交易由加密逻辑 300 接收到。这时，用户可以核对意向中的交易，例如，通过电子交易系统和/或 PEAD 200 拥有的显示屏，可选择认可或者不认可意向中的交易。 如果用户认可该项交易，在一个实施例中，他可以触发开关 210，这就使得交易认可数据产生出来，由加密逻辑 300 加密后，通过路径 212 送回电子交易系统。

注意用于交易认可过程的用户标识数据块 302，它不是直接连接到路径 206 和 212。换句话说，存储用户标识数据的存储区有意地从 PEAD 200 的输入和输出端口脱离连接，以防止从这里直接进行访问。

如果要求访问用户标识数据 302，例如，认可一项交易，访问只能通过加密逻辑块 300 进行。同样地，不能直接访问存储用户的私人密钥的

存储器部分 304。如果要求访问用户的私人密钥，例如，为交易认可数据加密，访问只能通过加密逻辑块 300 进行。必须记住，虽然用户标识 302 和用户的私人密钥 304 保存在不同的存贮器部分，但是这样的说明只是为了便于理解，在一个实施例中，两者可能事实上是存储在同一个存储器模块的不同地址。

在有些情况下，交易认可数据要求包含标识数据 302 的某些部分。例如，包含在电子交易系统的交易请求中的一项交易可能附加表示“电子签名”的数据，之后才被加密和送回电子交易系统。图 3B 表示，在一个实施例中，代表性的交易认可数据 350 的格式。参照图 3B，交易数据 352 代表来自电子交易系统的交易请求的一部分或者全部，它附加有某位用户的标识数据 354 和一个可选的时间戳记 356。只有当交易请求被用户认可后，交易认可数据 350 才形成。一旦附加上去，交易认可数据 350 就被加密，然送回电子交易系统。

在有些情况下，需要在传输到 PEAD 之前对交易请求进行加密，以进一步提高安全性。例如，某些交易伙伴，比如，计算机网络上的卖主或其他的用户，可能希望为交易请求中的信息保密，并且可能喜欢在发送到 PEAD 以前对交易请求加密。数据加密也是合乎需要的，例如当用户标识数据和用户的私人密钥第一次写入空白的 PEAD，以配置某位用户的 PEAD 时。 关于用户标识数据和用户的私人密钥的配置数据，必须是由 PEAD 200 的发行者一次写入 PEAD 200，最好是进行加密以减少被盗的弱点。例如，PEAD 200 的发行者可能是信用卡发行者、政府、或用户用以保持其帐号的任何其他机构。

图 4 表示，根据本发明的一个实施例，图 2 中 PEAD 200 的一份逻辑方框图。图 4 的 PEAD 200 更进一步地使用了一个解密逻辑，用来接受加密的配置数据以及可选的加密交易请求。在图 4 中，加密逻辑 300、用户的私人密钥 304、以及数据通路 206 和 212 排列在一起，并且大体上发挥着类似于图 3A 相关论述的功能。

交易请求通常是非加密的，也就是说，它们的接收和处理的方式就像是图 3A 的相关论述一样。然而对于高度敏感的交易来说，交易请求可能

被加密，然后通过数据通路206传输到PEAD 200，最后输入到解密逻辑402进行解密。若使用的是公共密钥加密方法，则加密的交易请求可能要用交易伙伴的公共密钥404解密。

一旦解密，交易请求就显示出来让用户去认可。如果得到认可，交易认可数据可以通过路径406传送到加密逻辑300进行加密，例如，对开关210的按下作出响应。如果使用公共密钥加密方法，加密最好以用户的私人密钥304完成，然后加密的交易认可数据通过数据通路212送回电子交易系统。

因为配置数据一般包括敏感的用户标识数据和用户的私人密钥，因此它在通过数据通路408被传输到PEAD 200之前，常常被加密。加密的配置数据由解密逻辑402接收，然后，在被写入用户标识数据块410和用户的私人密钥块304之前，在那里解密。如果使用的是公共密钥加密方法，加密的配置数据可能在传输之前，在电子交易系统中由发行者的私人密钥加密；一旦被PEAD 200接收，就用发行者的公共密钥412解密。

注意，一旦配置数据被解密并且被写入用户标识数据块410和用户的私人密钥块304之后，用户标识数据和用户的私人密钥只能通过加密逻辑300访问。注意，从任何I/O数据通路，例如，数据通路206，212或408，都没有通往用户标识数据块410以及用户的私人密钥块304的直接连接。有利地，敏感的用户标识数据和用户的私人密钥一旦写入各自的块410和304之后，在那里就不易从外面进行访问(在一个实施例中，这可能仅仅代表PEAD 200存储器中的存储块)。

另外，用户标识数据和用户的私人密钥不能由那些没有发行者私人密钥的人进行更新。正如图4所示，数据只有通过解密逻辑402，用发行者公开密钥412解密后才能写入用户的私人密钥块304和用户标识块410。因此，除非更新的配置数据已经使用发行者私人密钥加密(这被认为是非常安全的)，否则更新的配置数据不会被解密或者被写入相应的块304和410。当然，如果块304和410内部的配置数据不能物理地被更新，例如，它们使用只能一次写入的存储器来存储，如PROM (可编程只读存储器)，

WORM (一次写入多次读出的存储器)，等等，这样与未经授权的配置数据更改相关的安全性考虑就可以基本上被排除。

如果要求更高水平的安全性，用户的私人密钥可以在写入用户的私人密钥块 304 之前，由可选择的加扰器／解扰器逻辑 413 进行选择性地加扰或者随机化。在一个实施例中，加扰器／解扰器逻辑 413 可以，接收由 PEAD 200 的发行机构提供给用户的私人密钥，然后对它进行加扰和／或随机化，以生成另一个用户的私人密钥和相应的用户公共密钥。然后这个被加扰／随机化的用户的私人密钥保存在用户的私人密钥块 304 之中，现在甚至 PEAD 200 的发行者也不知道，而对应的用户公共密钥则可能公布给发行者和／或交易伙伴以便于交易。 有利地，除了用户的私人密钥块 304 以外，在别的什么地方都没有已加扰／随机化的用户的私人密钥的拷贝。

在另一个实施例中，可能使用可选择的密钥生成逻辑 414，它响应于来自发行机构的请求，产生用户的私人密钥和用户的公开密钥，换言之，不用首先要求从发行机构收到用户的私人密钥或者对它随机化。然后，产生的用户的私人密钥保存在私人密钥块 304 之中，并且公共密钥公布给发行机构和／或交易伙伴以便于交易。这样一来，用户的私人密钥的任何版本无论是否随机化，都没有在 PEAD 外面存在。 正如专业人士所懂得的那样，通过利用密钥生成逻辑 414 可更进一步地提高用户的私人密钥的保密性。

图 5A 表示，根据本发明的一个实施例的 PEAD 200 的一种高级硬件实施方案。如图 5A 所示，PEAD 200 包括逻辑电路 502，它可能代表中央处理器，如微处理器或微控制器，离散逻辑，可编程序逻辑，专用集成电路(ASIC)等等，用于实现图 2 中的加密逻辑 300，以及图 4 中可选的解密逻辑 402。

程序/数据存储器 504 还存储操作 PEAD 200 以及用户标识数据和用户的私人密钥的代码。程序/数据存储器 504 最好使用某种形式的非易失性存储器(NVM)来实现，例如闪烁存储器，电可编程只读存储器(EPROM)，电可擦拭可编程只读存储器(EEPROM)等。暂时存储器 506

充当便笺式存储器，用于计算目的以及用于数据的暂存，并且可能使用某种形式的随机存取存储器(RAM)，例如静态随机存取存储器或动态随机存储器来实现，这些在业界中都是已知的。可供选择地，或者光存储器，磁存储器，或其他类型的存储器都可能用来实现程序/数据存储器 504 和／或暂时存储器 506。

总线 508 通过逻辑电路 502 将程序/数据存储器 504 和暂存器 506 连接起来。通信端口 510 表示 PEAD 200 和电子交易系统之间通信网关，它可以使用红外技术、无线的射频技术、磁读／写头、触点式插头来实现，以便于串行的或并行的数据传输等等。在一个实施例中，通信端口可能也表示一个 PC 卡端口(一般业内人士称为 PCMCIA 卡)。 数据通路 206 将交易请求输入逻辑电路 502，而数据通路 212 将交易认可数据从逻辑电路 502 输出到电子交易系统。可选的数据通路 408 在图 4 中已经进行了描述，它将配置数据输入 PEAD 200，将用户标识数据和用户的私人密钥写入程序/数据存储器 504，这样给特定的用户配置唯一的 PEAD 200。

另外，要注意的是，当访问程序／数据存储器 504 和在那里的数据时（例如，用户标识数据和用户的私人密钥），只能通过逻辑电路 502 进行。例如，如果用户标识数据和用户的私人密钥已经用发行者私人密钥适当地加密，那么这个数据只能写入程序/数据存储器 504。 在适当的软件和/或固件控制下，为了在这里写入数据而对这些存储块进行访问时，可能也会受到逻辑电路 502 的限制。

同样地，读取用户标识数据和访问用户的私人密钥只能通过逻辑电路 502 的加密逻辑来完成。这个方面对安全方面的优越性已经结合图 3A 和图 4 进行了讨论，这里最重要的一点是，从外部不能直接访问敏感的用户标识数据和用户的私人密钥。因此，本发明的设计使这些数据项目的保密性和安全性大大地提高了。

也可以提供一些类型的电源，例如电池。如果 PEAD 200 通过单片设计来实现，也就是说，图 5A 所示的几乎所有组件都在一个单片上集成，那么电源就存在于该单片之外。如果使用接触式通信，例如，如果 PEAD

200 必须插入电子交易系统才能进行交易，那么当插上插头进行交易认可时，可以使用完全在 PEAD 以外的电源，从而排除便携式交易装置配有电池时所带来的尺寸、重量、和成本的负担。

在一个实施例中，PEAD 200 可以使用通用的便携式计算装置来实现，例如，任何小型化便携式计算机或当前流行的个人数字助理(PDA)。例如可能使用 Apple Newton®这样的 PDA 来实现 PEAD 200。

图 5B 表示 PEAD 的一种实施方案，其中，PEAD 的电路在一块集成电路上实现。在图 5B 中，与图 5A 中的元件有着同样的参照号码的元件也有着类似的功能。数据通路 408, 206 和 212 已经在图 5A 中作了相关的描述，它们被连接到一个串行的的 I / O 电路 520，这便于 PEAD 200 和电子交易系统之间在数据通路 522 上以串行的的方式进行数据发送和接收。也显示了为图 5B 中 PEAD 200 提供电源的 Vcc 引脚 524 和地线引脚 526。

图 5C 是图 5B 中 PEAD 的外观图，它被嵌入一个像卡一样的包装，以便于携带和插入电子交易系统的串行的 I /O 端口。在一个实施例中，卡 550 嵌入集成电路以实现本发明的 PEAD，它包括 4 个外部触点。外部的串行触点 552 和 554 分别连接数据线和地线，以便于利用电子交易系统的串行装置进行串行通信。外部的 Vcc 触点 524 和外部接地触点 526 也被显示出来，它们为 PEAD 提供电源，就像图 5A 中相关的论述那样。当卡 550 被插入电子交易系统时，它通过外部触点 524 和 526 来提供电源，从而使在那里的 PEAD 电路通过外部的串行的触点 552 和 554 接受交易请求，如果合适的话，就在 PEAD 内部认可交易请求，在电路内部对交易认可数据进行加密，并且通过外部串行的触点 552 和 554 向电子交易系统以串行的的方式传送加密的交易认可数据。

图 6A 表示，根据本发明的一个优选实施例的 PEAD 的外观。图 6A 的 PEAD 200 最好是被实现为一个小的、整套装在一起的封装，它足够在该领域中进行日常使用。最好是，图 6A 的 PEAD 200 足够小，用户可以随时方便地携带，例如，作为钥匙链的一件饰物，或一个可以轻易地装进钱包或钱袋的物件。PEAD 200 的物理外壳安排合理，使得其内容是

防干扰的（即，如果以未经授权的方式打开，那么用户的私人密钥和/或用户标识数据将被销毁，或者 PEAD 将不再认可交易)。举例来说，外壳的布置方式可能是，如果它被打开，那么在电流通路中就会有电流变化，例如，或者现有的电流被切断，或者是本来处于等待状态的电流通路开始流动。电流的变化可能会迫使 RE。

这里有一个红外通信端口 602 用于接收和发送关于电子交易系统的数据。一个小的通/断开关 604 允许用户在不使用时关掉 PEAD 以节省电源。认可按钮 606 允许用户表示认可意向中的交易。可选的跳过按钮 608 允许用户拒绝一项特定的交易。跳过按钮 608 可以被省略，因为在一些实施例中，如果在接受请求一定时间后仍然没有触发认可按钮 606，交易请求就被视为没有被认可。

可选的显示器 610 可以使用任何显示技术来实现，如液晶技术。 显示器 610 显示被建议以供认可的交易。如果需要，显示器 610 也可以省略，而在这样情况下，交易可以在电子交易系统本身的显示器上查看。可选的的用户认证装置 612 可保证，只有当用户能向 PEAD 200 证明自己是合法的和被授权的用户时，PEAD 200 才能用于认可交易。 可选的用户认证装置 612，可能要求用户在启动 PEAD 200 以及认可交易之前输入一个口令字，提供指纹、或声纹、或其他的生物测量学的和/或被授权用户特有的识别特征。

图 6B 根据本发明的一个方面，并且以简化的方式，表示用于实现图 6A 中的 PEAD 200 的硬件。电池 652 为 PEAD 200 的电路提供电源。微控制器 654 执行存储在闪烁存储器 656 中的代码，并且使用随机存取存储器 658 来执行。在一个实施例中，微控制器 654、闪烁存储器 656、甚至随机存取存储器 658 可能在一个单片上实现,例如，来自伊利诺斯州 Schaumberg 的摩托罗拉公司的 NC68HC05SCXX 系列芯片 NC68HC05SC28。认可按钮 606 和可选择的跳过按钮 608 与微控制器 654 连接在一起，允许用户使用显示电路 660 表明认可或拒绝所显示的特定交易。往返于电子交易系统的通信，通过红外线收发信机 662 在微控制器 654 的控制下完成。电源开关 664 允许用户在不用的时候关闭 PEAD

200，以节省电源，并防止意外的认可。

图 7 是根据本发明的一个方面的一份流程图，表示在创新性的 PEAD 中使用的认可技术。在步骤 702，PEAD 接收到来自电子交易系统的请求装置的交易请求。在步骤 704，用户可以选择是认可还是拒绝意向中的交易。如果不认可，例如，或者可以启动 PEAD 的跳过按钮或者只是让请求超时，这将不会发生任何事情。

另一方面，如果认可意向中的交易，用户可以激活认可按钮来生成交易认可数据。然后，在步骤 708，交易认可数据在 PEAD 内部进行加密。在步骤 710，加密的交易认可数据在加密后被发送到电子交易系统的请求装置。

图 8 是根据本发明的一个方面的一份流程图，表示在使用公共密钥加密方法对交易认可数据进行加密所涉及的步骤。在步骤 802，生成交易认可数据包。正如前面关于图 3B 的论述的那样，交易认可数据，可以通过给交易请求的一部分或全部附加任何必需的用户标识数据来生成。可供选择地，该处也可以附加一个时间戳记。 在步骤 804，交易认可数据使用用户的私人密钥进行加密，用户的私人密钥最好是一直保存在 PEAD 内部，非常安全。此后，加密的交易认可数据被送回电子交易系统。

根据本发明的一个方面，即使加密的交易认可数据被第三方截获并且进行解密分析，只要用户的私人密钥或用户标识数据是安全的，就不可能绕过本发明的安全特性。如前所述，因为不能从外部访问用户标识数据，所以它在 PEAD 内部总是安全的。这与现有技术的不同之处在于，使用现有技术时，要求用户向电子交易系统输入标识数据，例如，口令字，这样就有暴露这些敏感数据的风险。

即使用户标识数据被泄露，但是只有当拥有用户的私人密钥后才能对交易进行认可。即使可以使用用户的公共密钥对截获的加密交易认可数据进行解密，也是无用的。因为交易伙伴，比如请求交易认可的那个商人，不会接受任何没有使用用户的私人密钥进行加密的交易认可数据。又因为从外部不可能访问私人密钥，因此它在 PEAD 内部总是安全的。本发明的这个方面在完成在线交易方面有很大的优势，因为用户的私人密

钥不必保存在工作站中有弱点的计算机文件里，那样可能易于被其他人访问，并且难以方便地用于其它的认证工作。

将 PEAD 实现为一个小的、便携式封装，这使得它变得非常方便和舒适，并使它经常处于用户的掌握之中。然而即使 PEAD 本身被物理地偷走，可选择的用户认证机制，例如，图 6A 中的用户认证装置 612，提供了额外的防护层次，使 PEAD 只对被正确地授权的用户有用。当然如果 PEAD 被盗或丢失，用户总是可以通知 PEAD 的发行者，发行者就可以通知交易伙伴，拒绝所有使用被盗的 PEAD 中用户的私人密钥进行加密的交易认可数据。

交易认可数据包括时间戳记、商人的姓名、认可的金额以及其他有关数据，这也提高了交易认可过程的完整性。如果商人无意中或故意向发行者提交多次交易认可，发行者也许能从这些数据项目中发现提交是重复的，从而忽略任何重复的交易认可数据。例如，发行者可能注意到，用户不太可能在某一个日期和时间在同一家饭店多次购买完全相同的晚餐。

发明者在这里注意到，虽然 PEAD 和基于 PEAD 的销售点终端为认可交易提供了非常安全的系统，但是存在一个牢固建立起来的和广泛地可用的付费卡基础设施，它包括无数现有的付费卡销售点终端，并在世界范围内使用(例如，付费卡读卡器或 ATM 终端）。还应认识到，即使没有基于 PEAD 的销售点终端，某些 PEAD 功能也可能向现有付费卡基础设施提供更好的交易保密性。

根据本发明的另一个方面，提供了一种便携式的电子付费/认可装置(PECAD)，它不但提供上述的 PEAD 功能，允许用户认可基于 PEAD 的销售点终端的交易，而且还允许用户在现有付费卡基础设施中进行交易。特别是，完整的 PECAD 系统包括 PECAD 和相关的仿真卡，从与现有的付费卡读卡器接口方面来看，该仿真卡符合现行的付费卡标准。仿真卡可以被 PECAD 灵活地配置，对于现有的付费卡读卡器来说就像是普通的付费卡。PEACD 和仿真卡一起，形成了在现有付费卡基础设施中进行交易的安全系统。

注意，因为这些术语用在这个实施例的语境中，所以付费卡包括磁条卡和电子智能卡。付费卡本身可能是信用卡(例如维萨卡或万事达卡)、ATM 卡、皇室卡、折扣卡，以及用户能用以在销售点终端获得现金、货物、和/或服务的任何其他类型的卡。

在进行交易之前，PECAD 在它的存储器中已经存有属于用户的一张或多张付费卡的付费卡数据。为了实现 PECAD 的功能，存储器可能也包括其他的数据项目，这在前面的 PEAD 中已经论述。付费卡数据可以通过适当的输入端口预先输入 PECAD.或者可以预先使用适当的 PECAD 读/写装置从实际的付费卡中读入。

因为 PECAD 包含 PEAD 的功能，它当然能用于认可基于 PEAD 的销售点终端的交易，其方式类似于前面对 PEAD 的论述。但是如果没有基于 PEAD 的销售点终端，就可用仿真卡代替，在现有付费卡基础设施中进行交易。

为了使用仿真卡进行交易，用户首先要求 PECAD 将属于一张被选定的付费卡的付费卡数据写入仿真卡。被选定的付费卡可能在写之前就被用户选定。因为一张仿真卡可以仿真任意数目的付费卡，所以它可以代替现今用户必须携带的各种付费卡。在允许用户使用 PECAD 将付费卡的数据写入仿真卡之前，最好使用与 PECAD 相关的适当的验证装置，首先对用户进行认证。

将与用户选定的付费卡有关的付费卡数据写入仿真卡之后，用户就可以像使用付费卡一样来使用仿真卡，完成交易。简而言之，因为仿真卡符合现有付费卡和付费卡读卡器的 I / O 要求，它就可以象付费卡一样由现有的付费卡读卡器读出。

一旦交易完成，用户可以选择性地使用 PECAD 从仿真卡中擦掉付费卡数据，从而使仿真卡失效，这样只有恰当地被认证过的用户，再一次授权 PECAD 将付费卡数据写入仿真卡后，才能进一步进行交易。 若仿真卡仿真一张电子智能卡，则可以通过例如，适当地配置仿真卡内的寄存器或标志，将仿真卡设置为不能用于进行其他的交易。 这样，即使仿真卡被盗，它对于未经授权的使用者来说也是无用的。 此外，即使仿

真卡和 PECAD 一起被窃，仿真卡本身也不能使付费卡的数据写入，除非该使用者已被恰当地认证过。 这与现有的情况形成了鲜明的对照，例如，一张被盗的信用卡在它的磁条中，仍然包含着进行一笔交易所需的全部信息。 为了更加安全，仿真卡本身可能在物理上，由真正被授权的用户签名，并且可能包含被授权用户的个人照片，这样可以让商人在视觉上确认进行交易的那个人是否真的是仿真卡的合法所有者。

在一个优选实施例中，每一张仿真卡都大体上以一种唯一的方式，与特定的 PECAD 相匹配，进一步提高了安全性。 在这种情况下，一个给定的 PECAD 只能将付费卡的数据写入与它唯一匹配的仿真卡中。 举例来说，仿真卡可能具有恰当的用光学方法加密的标记（例如全息图）、用磁性方法加密的标记（例如磁性存储的各比特）或者用机械方法加密的标记（例如随机地定位的孔），使得它只能由特定的 PECAD 写入数据。

每一张仿真卡最好与一个唯一的 PECAD 相匹配。 然而应当指出，这个唯一匹配的特征并不要求是数学上的绝对（虽然这样可能更好）。 专业人士会都懂得，当发行的仿真卡和 PECAD 的数量足够大时，可能会发生一些重叠，使得一张给定的仿真卡被不止一个 PECAD 识别成为可能（虽然在现实生活中很少见）。 事实上，发行者或制造商可能拥有万能 PECAD，可以识别大量的已发行的仿真卡。这样，仿真卡和 PECAD 之间的关联只是基本上的唯一，类似于一把门钥匙对于每一把门锁也是基本上唯一那样，不能排除某个制造商可能愿意制造对应于给定的 PECAD 的绝对唯一的仿真卡，或者在无数制造出来的门锁中，一把给定的钥匙可能打开不止一把门锁的这种极小的可能性。仿真卡／PECAD 的加密标记和地理分布模式（例如，在同一个城市或州内）的安排，最好能使这种极小的可能性最小化。

因为每张仿真卡基本上与特定的 PECAD 唯一地相匹配，即使 PECAD 被盗，打算进行欺诈的人也成功地绕过验证装置，被盗的 PECAD 仍然不能被用来将付费卡的数据写入任何任意的空白仿真卡之中，以进行欺诈的交易。 另外一个优点是，一张给定的 PECAD 只能写入（经

过正确的认证后）基本上与它唯一地匹配的仿真卡中，这个条件基本上排除了 PECAD 意外地冲掉现有的付费卡。

图 9 表示根据本发明的一个方面的 PECAD 902 的一份简化方框图。 在图 9 中，存储器 904 最好是非易失性的、防干扰的存储器，与 PEAD 中的存储器电路发挥同样的功能，只是存储器 904 也可用来存储用户的一张或和多张付费卡的加密数据。加密逻辑 906 发挥着加密／解密／安全功能，这与 PECAD 中加密逻辑的相关论述一样。 简而言之，对存储在存储器 904 中的数据进行访问，包括用户的私人密钥、用户的个人数据、以及付费卡数据，最好是只通过加密逻辑 906 进行。

认证装置 908 发挥着如同前面结合 PEAD 来讨论拿样的用户认证功能。当能够用于认可交易的用途时，I/O 电路 910 代表的电路，允许 PECAD 同基于 PEAD 的销售点终端进行通信。交易认可的这个方面，在前面结合 PEAD 的相关论述中已经进行了说明，这里将不再重复。 如果某些型号的 PECAD 不与 PEAD 通信，仅仅用来配置仿真卡，以便在现有付费卡基础设施中进行交易，那么，在这些 PEAD 型号中就可以省略 I/O 电路 910。

卡读/写装置 912 表示这样一种装置，它被用来将选定的付费卡数据写入仿真卡，并且在交易完成之后擦掉仿真卡上的数据。 如果通过读取现有付费卡来获得付费卡数据，那末卡读/写装置 912 也能够读入现有付费卡，以便将付费卡的数据存储到存储器 904 (通过加密逻辑 906）。 请注意，通过卡读／写装置 912 读出的数据，在被存储到存储器 904 之前，被加密逻辑 906 进行了加密。 同样地，存储在存储器 904 中的数据（例如付费卡数据），在通过卡读/写装置 912 写入仿真卡之前，首先由加密逻辑 906 进行加密。

图 10 是 PECAD 1002 的一份简图，包括安置在其中的仿真卡 1004。仿真卡 1004 可以从插槽 1006 中取出，以便在现有付费卡读卡器中完成交易。在图 10 的实例中，仿真卡 1004 包括一条磁条 1008 ，以仿真磁条式付费卡。 然而，如上所述，仿真卡 1004 配置后可以仿真任何类型的付费卡接口，包括接触式 IC 卡接口。卡读/写装置 1010 被表示

为一种轮廓的形式，以说明它是 PECAD 1002 的一部分。卡读/写装置 1010 可以从现有付费卡中读出数据或向仿真卡写入数据。 键盘 1015 可以被用作认证装置，就像对 612 和 908 所作的描述一样。 用户可以键入口令字或 PIN 以激活 PECAD，以便将付费卡的数据写入仿真卡 1004。

认可按钮 1012 基本上类似于图 6A 中的认可按钮 606 ，也可以用来通过基于 PEAD 的销售点终端来认可一笔交易。另一方面，卡按钮 1014 表示用户通过仿真卡完成交易的愿望。卡选择器按钮 1016(a)—(b) 是示例性的选择，用户可以选择哪一种付费卡用来进行交易。 显示器 1018 可以用来显示付费卡的数据，例如被选定的付费卡的付费卡号码、有效期、持有者的姓名等，以便商人在必要时能够记录这些信息以完成交易。

根据本发明的另一个方面，通过使用 PECAD 将已经用用户的私人密钥（安全地保存在 PECAD 的非易失性存储器中）加密的交易号码或其他已加密的数据写入仿真卡，这更进一步地提高了交易的安全性。 图 11 根据一个实施例来说明本发明的这个方面。在步骤 1102，每次交易都生成唯一的交易号码，并且用用户的私人密钥进行加密。在步骤 1104，加密的交易号码从 PECAD 写入到仿真卡中。 例如，若仿真卡仿真一张磁条卡，则已加密的交易号码可能写入空磁道或保留磁道二者之一，比如，磁条上的磁 3。 在步骤 1106，付费卡读卡器中的软件可能指示付费卡读卡器去接收已加密的交易号码，然后使用从可信任的第三方获得的公共密钥进行认证（步骤 1108）；或者在步骤 1106，付费卡读卡器读入已加密的交易号码，然后发送给例如万事达卡或维萨卡的信用卡结算中心，该信用卡结算中心通过使用从可信任的第三方获得的一个用户的公共密钥，对用户进行认证（步骤 1108）。一般地，可能需要向可信任的第三方发送某种形式的用户标识，以便获得公共密钥。 举例来说，付费卡读卡器读出用户的 ID 或公共密钥 ID，然后将其发送到可信任的第三方以获得公共密钥。 例如，公共密钥 ID 可能表示在公共密钥中各比特的独特模式（例如，最低的 32 位或 64 位），该模式可能被发送到接收一侧，用于公共密钥的检索和解密。如果通过认证，那么交易就被认可，让商人向用户提供货物/服务（步骤 1110）。

从以上所述可以理解，本发明基本上不需要对现有的付费卡读卡器和现有的付费卡基础设施进行硬件的更改。更改仅仅涉及软件修改，这些软件指示现有的付费卡读卡器读入已加密的交易号码，使用从可信任的第三方获得的一个用户的公共密钥来认证已加密的交易号码。

此外，付费卡读卡器可能完全不用更改。但是，信用卡结算中心的软件可能需要改动，以便使用从可信任的第三方获得的一个用户的公共密钥来认证已加密的交易号码。付费卡读卡器仅读入付费卡或仿真卡的全部数据，然后原封不动地将全部信息发送到信用卡结算中心进行认可。这样一来，该实施例使得对现有付费卡基础设施的改动最小化（即，只需在信用卡结算中心一个地方进行更改，而不用更改现有的无数的付费卡读卡器）。

如果希望更加安全，用户可以向 PECAD 键入交易的金额和/或交易的时间。还可以用用户的私人密钥对这些数据进行加密，然后写入仿真卡中，由付费卡读卡器接收并且用用户的公共密钥在信用卡结算中心进行解密，当然用户的公共密钥最好是从可信任的第三方获得。在这种情况下，只有当交易的金额符合加密和接收的交易金额和/或当交易发生的时间处于加密和接收的交易时间的预定的时间周期（预先从 PECAD 写到仿真卡）以内时，交易才能被认可。这样，即使仿真卡被盗，并且仿真卡也没有被擦掉或者被重新配置，它对于后来的其他交易也是无用的。

在因特网交易中，用户通过存储在 PEAD 和 PECAD 中的自己的私人密钥，对认可的金额进行加密，从而使用 PEAD 或 PECAD 认可交易。此后，他可以通过键盘键入信息，将 PEAD 显示器 610 或 PECAD 显示器 1002 上显示的已加密的信息拷贝到因特网。显示在 PEAD 显示器 610 或 PECAD 显示器 1002 之中的已加密的信息最好是一种人可读的格式，例如字母数字串，这样使用户易于读出，便于人工地输入到连接在因特网上的计算机（例如键入或者通过语音命令），以便进行因特网交易。必要时，你还可以使用 PEAD 或 PECAD 将交易信息和信用卡号码一起加密，进行安全的因特网交易。当然，人们在希望手工的输入/键入技术向后兼容的同时，它也可能同等地被其他的数据输入形式所代替，

例如，通过计算机和 PECAD（或 PEAD）适当的端口进行无线或红外通信，使数据发送到因特网。

如上所述，最好是使用保存在可信任的第三方的用户公共密钥来进行用户的身份认证。例如，可信任的第三方可能是公众很信赖的任何实体，例如，被认为拥有可信赖的声誉的、具有自身利益的组织。其实例包括政府组织、银行、大公司，等等。

可信任的第三方提供 PECAD 公共密钥目录服务，将制造商提供的公共密钥目录跟用户联系起来。当用户第一次获得（例如，用户通过购买或发行）PECAD 时，他可以通过可信任的第三方注册自己对 PECAD 的所有权。 根据注册过程的完整程度，用户被分配一个有效性等级，这个等级表示完成注册的那个人事实上就是他所说的那个人的可信程度。

举例来说，用户注册时，可能只是通过电子邮件、电话、或普通邮件提供个人的信息，例如社会安全号码、家庭地址和家庭电话号码，连同 PECAD 序列号码和公共密钥签名（它是制造商分配给特定的 PECAD 的唯一的序列号码，通过按压指定的键序列就能从 PECAD 中读出）。 然后，PECAD 公共密钥目录中心将用户提供的 PECAD 序列号码，作为唯一的检索标识符去查找数据库中的公共密钥，一旦找到公共密钥，它就使用用户提供的公共密钥签名来核实数据库中的公共密钥。 如果核对成功，那么用户就可以注册了。否则用户就被拒绝。公共密钥最好是唯一的。

对用户所有权进行注册，更加安全的的方法如下（这种过程通常发生在购买 PECAD/PEAD 的地方或在发行者那里，例如银行）。 发行者首先利用制造商提供的口令字激活 PEAD/PECAD。 此后， PEAD/PECAD 用户用自己的口令字或其他的（各）认证装置来冲掉制造商提供的口令字。 然后用户指示 PEAD/PECAD 在 PEAD/PECAD 内部生成一对新的私人/公共密钥（称为用户私人密钥和用户公共密钥）。 用户也可以指示 PEAD/PECAD 利用制造商提供的私人密钥对个人信息（例如社会保障信息、家庭地址等等)和新的用户公共密钥进行加密，制造商提供的私人密钥事先存储在 PEAD/PECAD 中以生成用户注册信息。当 PEAD/PECAD

被制造时， PEAD/PECAD 就能生成制造商提供的私人/公共密钥对。

发行者然后利用公共密钥目录服务中心的公共密钥对 PEAD/PECAD 序列号码和用户注册信息进行加密，以生成注册信息，然后将注册信息发送到公共密钥目录服务中心。接收到注册信息后，公共密钥目录服务中心就用它自己的私人密钥对注册信息进行解密。 此后，公共密钥目录服务中心可以使用 PEAD/PECAD 的序列号码在数据库中查找制造商提供的公共密钥。 如果解密成功，那么就在目录服务数据库中用新的用户公共密钥更新制造商提供的公共密钥，并且在目录服务数据库中更新个人信息，使用例如个人姓名+电话号码或公共密钥的最低的 32 位（或者 64 位）来生成公共密钥的 ID，以便将来参照之用。另一方面，如果解密失败，用户就被拒绝。

这种注册过程通常符合低的有效性等级，因为除了用户本人以外还可能有其他人以欺诈方式获得用户的个人信息，用于注册所有权（一旦注册完成并且激活 PECAD，就使得该用户对随后的欺诈性付费承担责任）。

除了为了获得低的有效性等级需要提供的信息外，通过提供更高置信度的信息，证明提供信息的那个人就是他自己所说的那个人，这样就可以获得中级的有效性等级。举例来说，这些附加的信息可以采取照片、签名、公证印章的形式，或者上述各项的组合。通过提供甚至更高的置信度的信息来证明提供信息的那个人就是他自己所说的那个人，就可以获得高级的有效性等级。 举例来说，注册人可以亲自出现在 PECAD 公共密钥目录中心，提供一张照片、一份签名、一份生物测量学的样品（例如指纹、视网膜扫描图、DNA 打印图形等）或上述各项的组合。

一旦注册完成，由可信任的第三方提供的 PECAD 公共密钥目录就可以被信用卡结算中心或商人查阅，以认证用户并认可交易。

通过设立保险单也可以使 PECAD 公共密钥目录得以进一步地强化，这些保险单可以保护商人或信用卡结算中心，使之避免由于例如有问题的注册过程中的欺诈所带来的经济损失。 保险单提供的保险总额可能按照有效性等级进行划分，较高的有效性等级享有较高的的保险总额。

尽管已经按照几个优选实施例对本发明进行了说明，但是也有一些更

改、置换和等价物也属于本发明的范围。应当注意的是，在实现本发明的过程中，存在着许多可供选择的方法和装置。举例来说，虽然这里的讨论集中在对交易的认可，但是专业人士可以很容易看出，任何时候希望从用户向电子交易系统安全地发送数据，都可以使用 PEAD 在电子交易系统中进行任何种类的交易。例如， PEAD 可以被用来登录到高度敏感的计算机系统或设备。当这样实现时，与 PEAD 通信的计算机终端可能装备有红外端口、磁性读出器端口、或接触式插头，以便跟 PEAD 进行通信。这样用户就可以使用 PEAD 在线进行任何类型的认证工作。

作为另外一个实例，PEAD 可以被用来“签署”任何用于认证目的的计算机文件（例如，认证日期或用户）。这样交易认可数据可以连同待认证的文件一起存储，以备将来参考。要注意的是，由于任何没有使用用户的私人密钥进行加密的交易认证数据都被看成是不可信的，所以交易认证数据也要防干扰。 同样，很显然，如果 PEAD 只是用来认可预先确定的交易，那么交易数据就可以预先保存在 PEAD 内部，而不需要由 PEAD 从外部接收。 因此，作者指望以下所附的权利要求书将被解释为，所有这样的更改、置换和等价物都属于本发明的精神实质和范围之内。

说 明 书 附 图

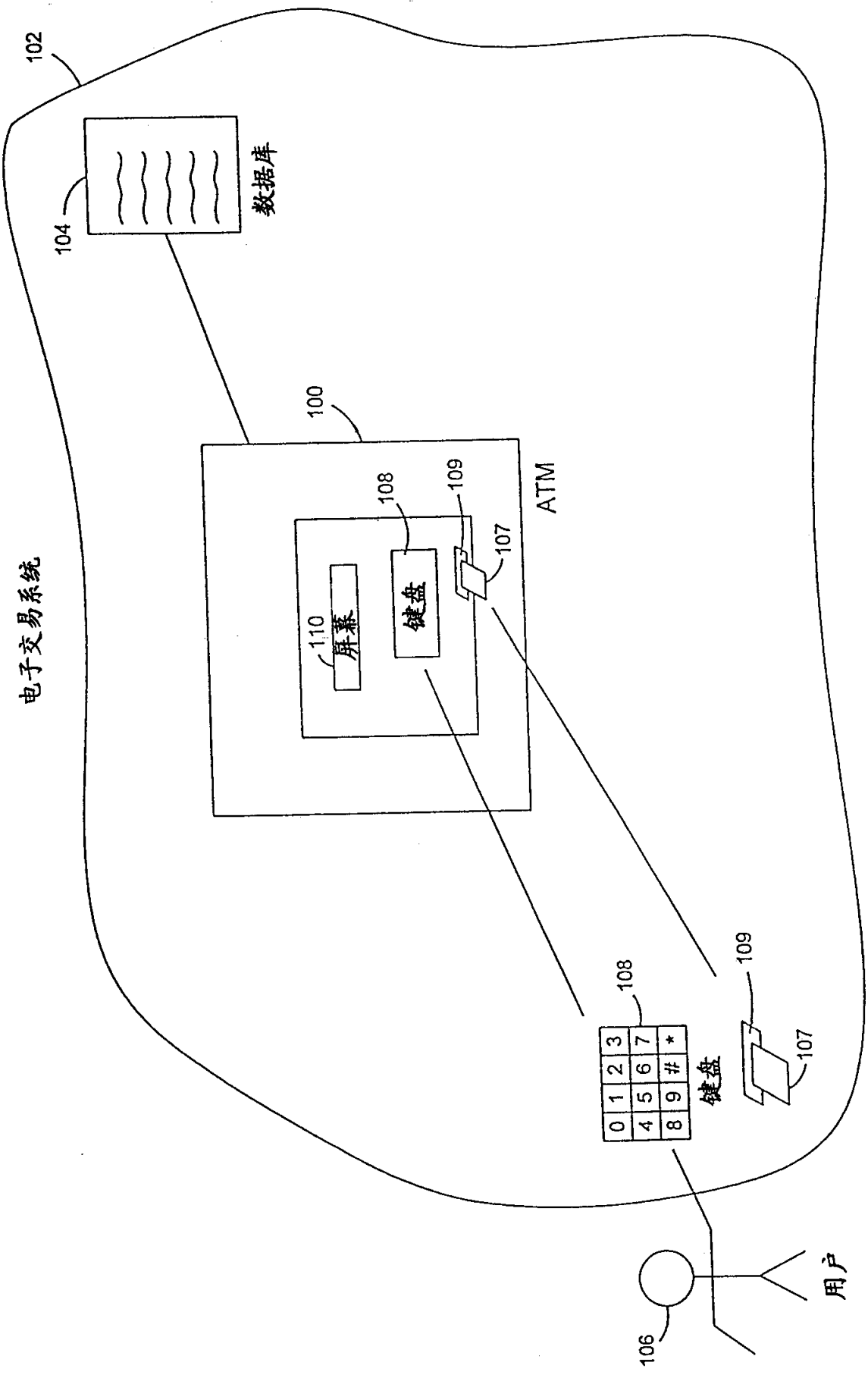


图 1（现有技术）

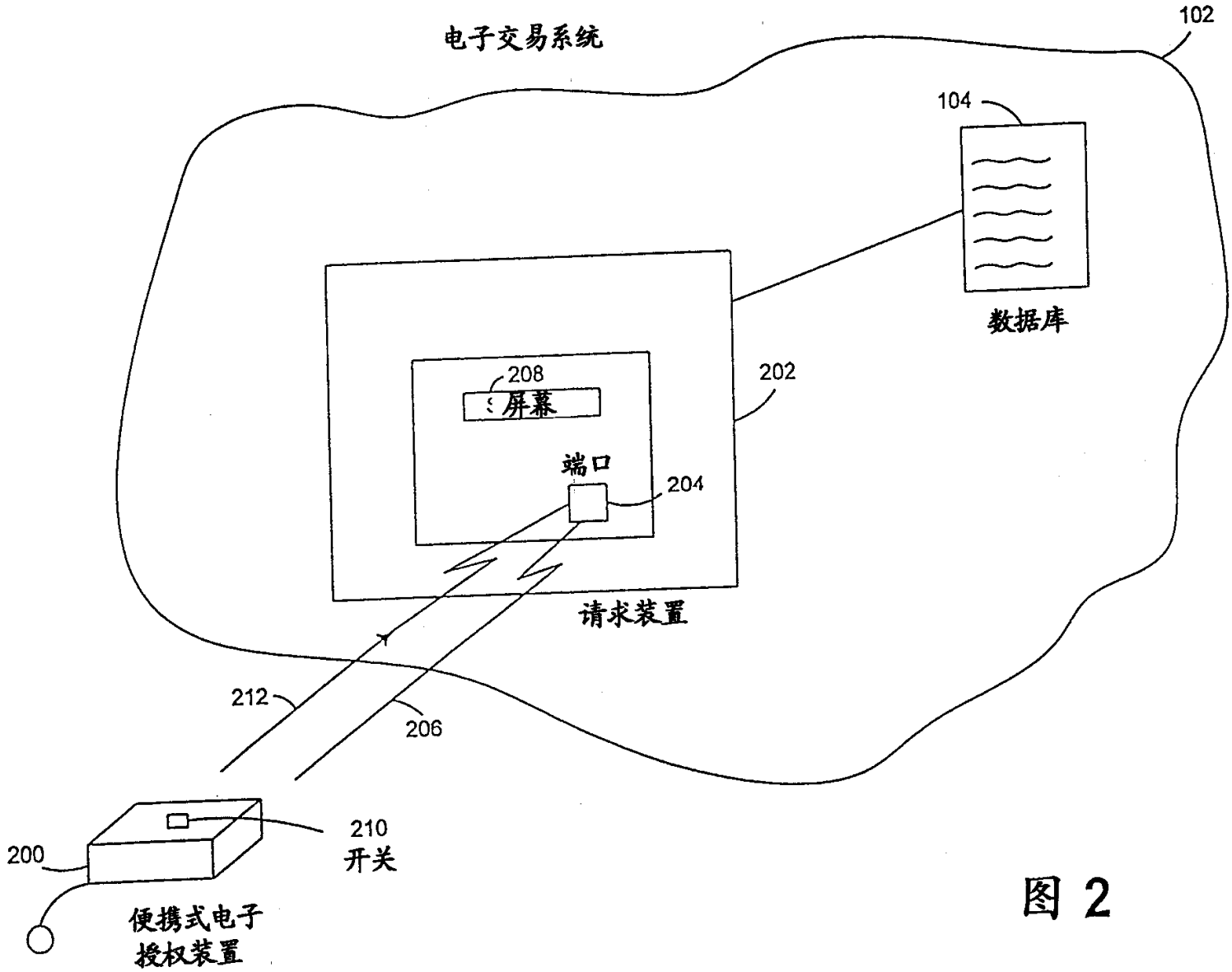

电子交易系统
102
104
数据库
208
屏幕
202
端口
204
请求装置
212
206
200
210
开关
便携式电子
授权装置

图 2

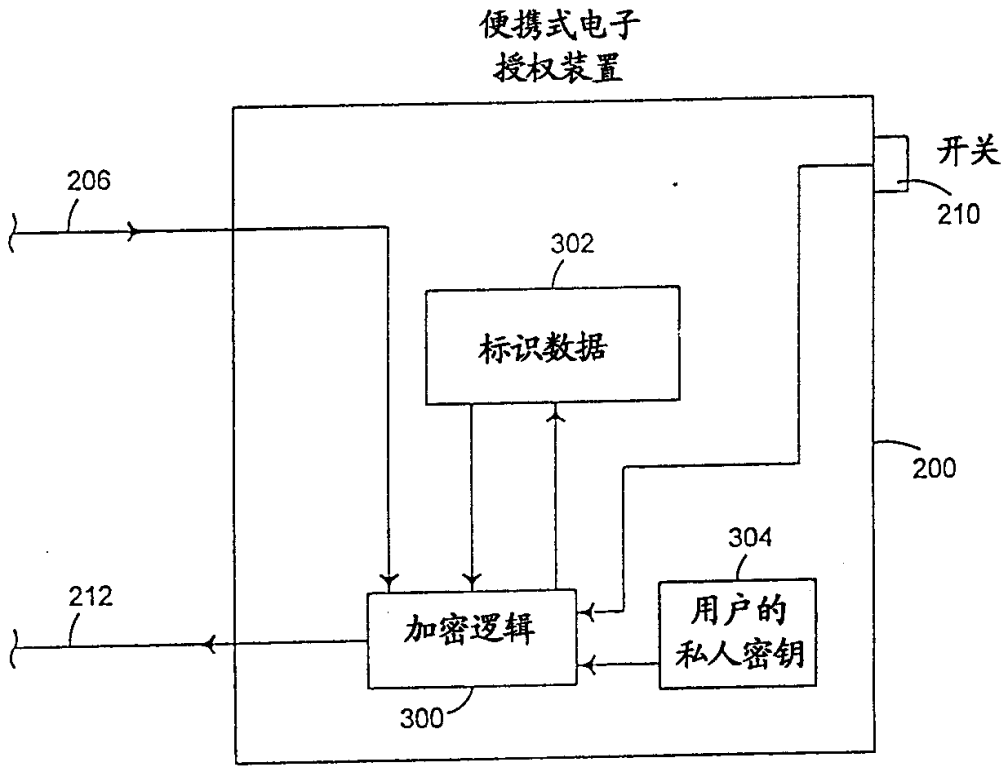

便携式电子
授权装置
开关
210
206
302
标识数据
200
304
212
加密逻辑
用户的
私人密钥
300

图 3A

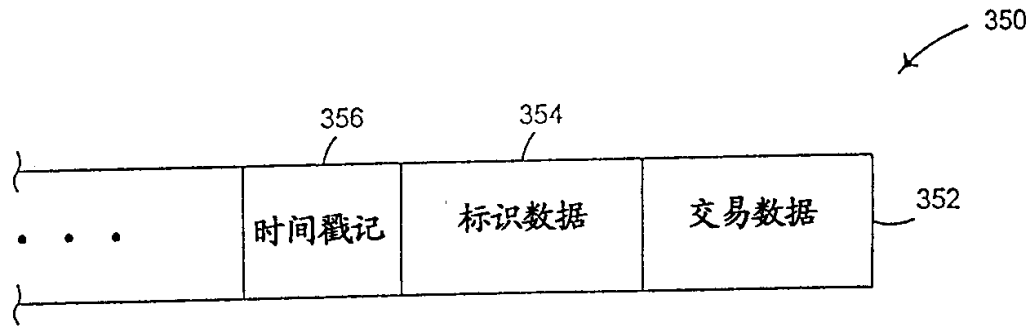

350
356
354
时间戳记
标识数据
交易数据
352

图 3B

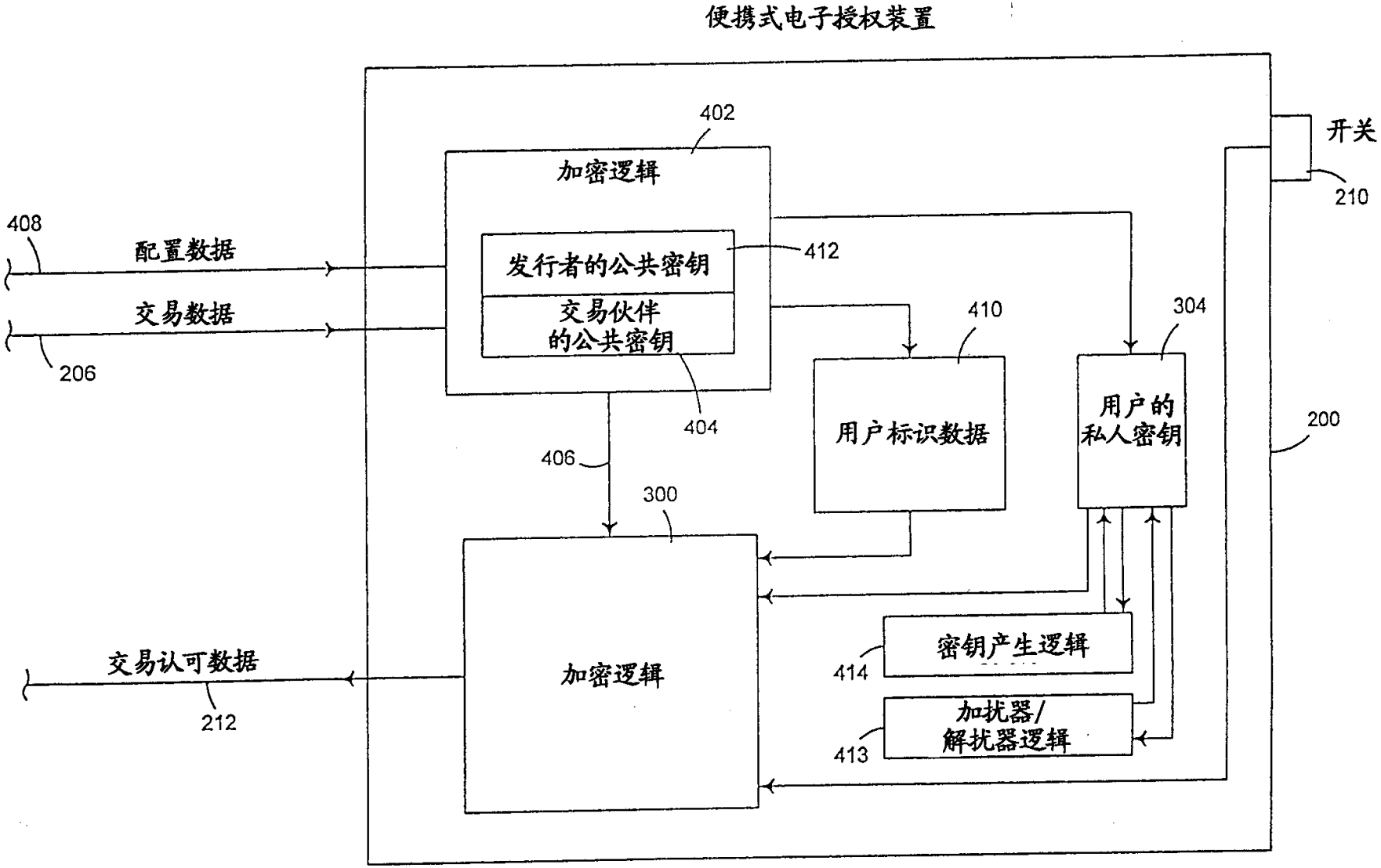

便携式电子授权装置
402
加密逻辑
开关
210
408
配置数据
发行者的公共密钥
412
交易数据
交易伙伴
的公共密钥
206
404
410
304
用户标识数据
用户的
私人密钥
200
406
300
加密逻辑
密钥产生逻辑
414
加扰器/
解扰器逻辑
413
交易认可数据
212

图 4

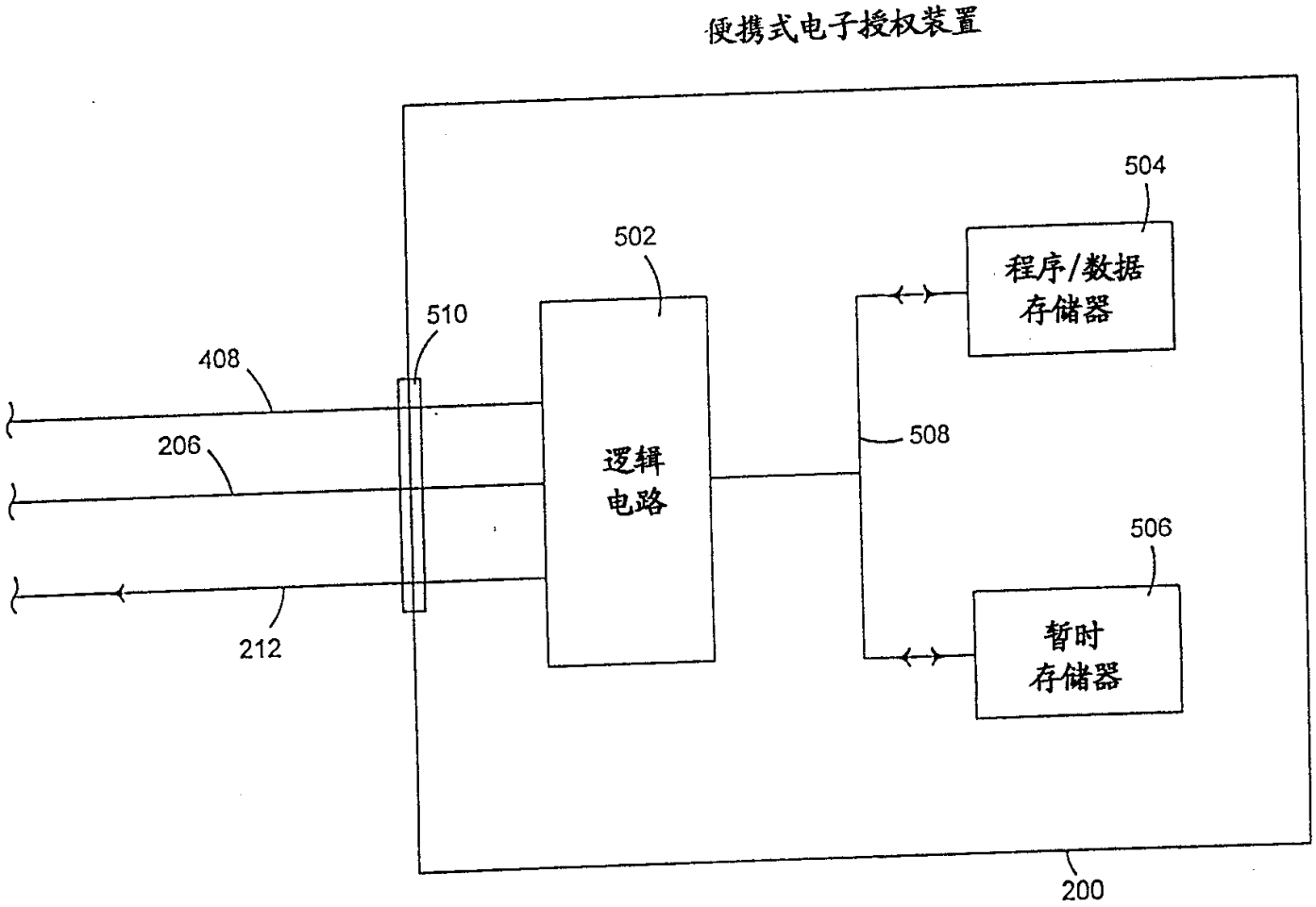

便携式电子授权装置
504
502
程序/数据
存储器
510
408
206
逻辑
电路
508
506
暂时
存储器
212
200

图 5A

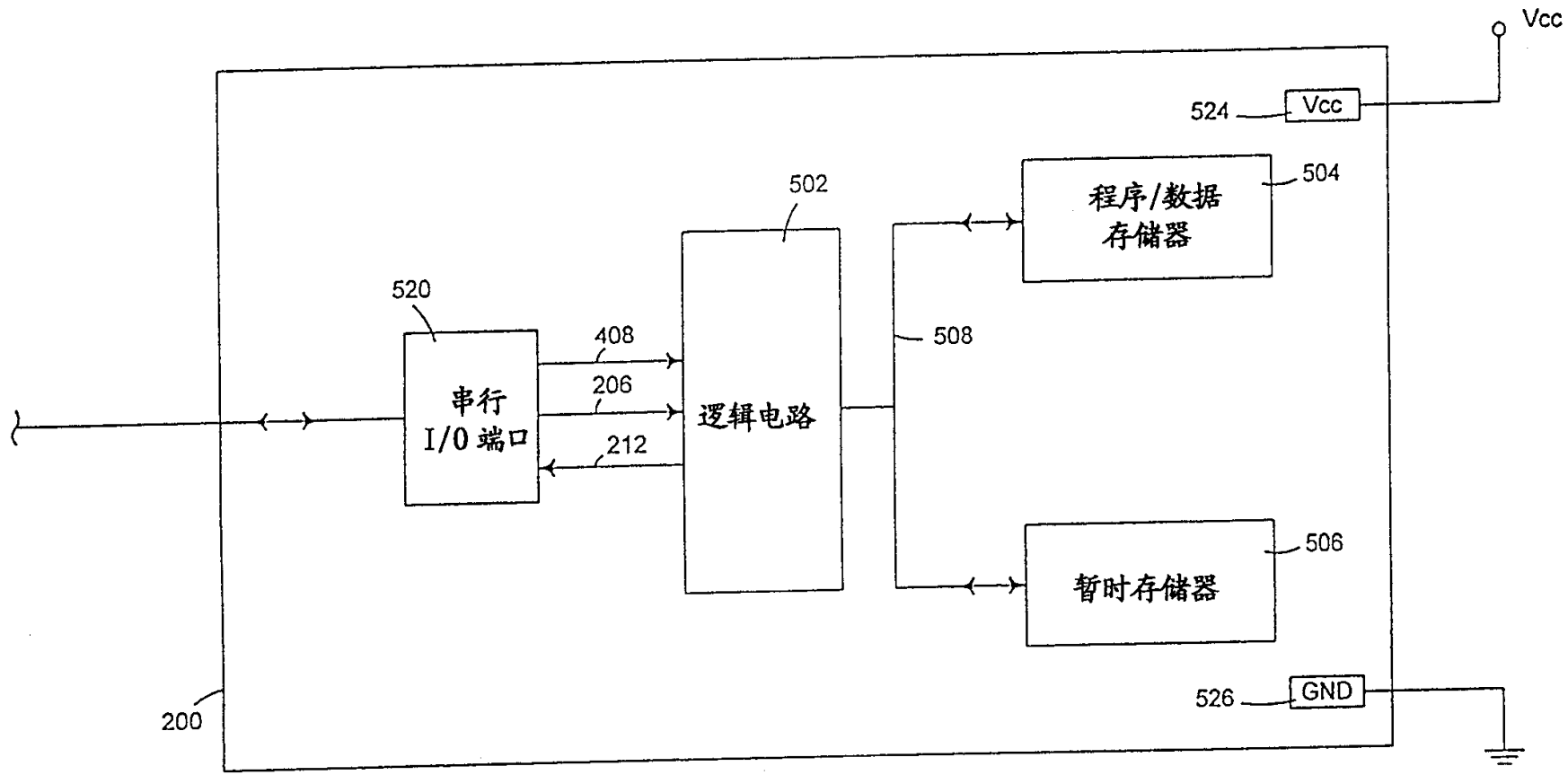

便携式电子授权装置
Vcc
524
Vcc
502
程序/数据
存储器
504
520
408
206
212
串行
I/O 端口
逻辑电路
508
506
暂时存储器
200
526
GND

图 5B

图 5C

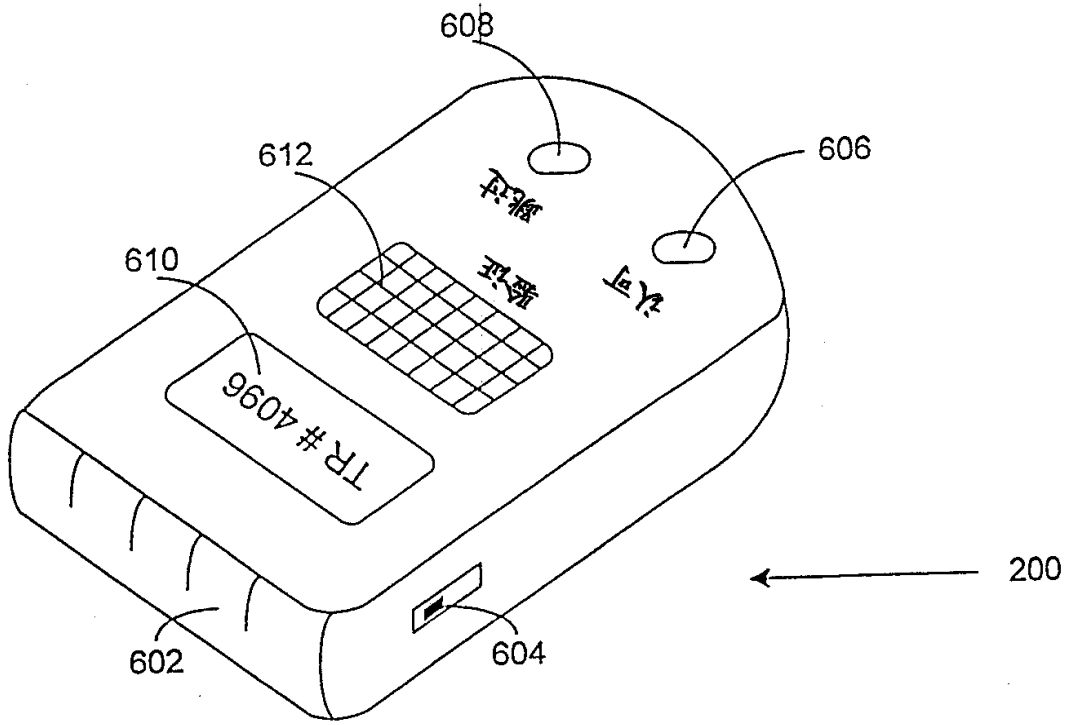


图 6A

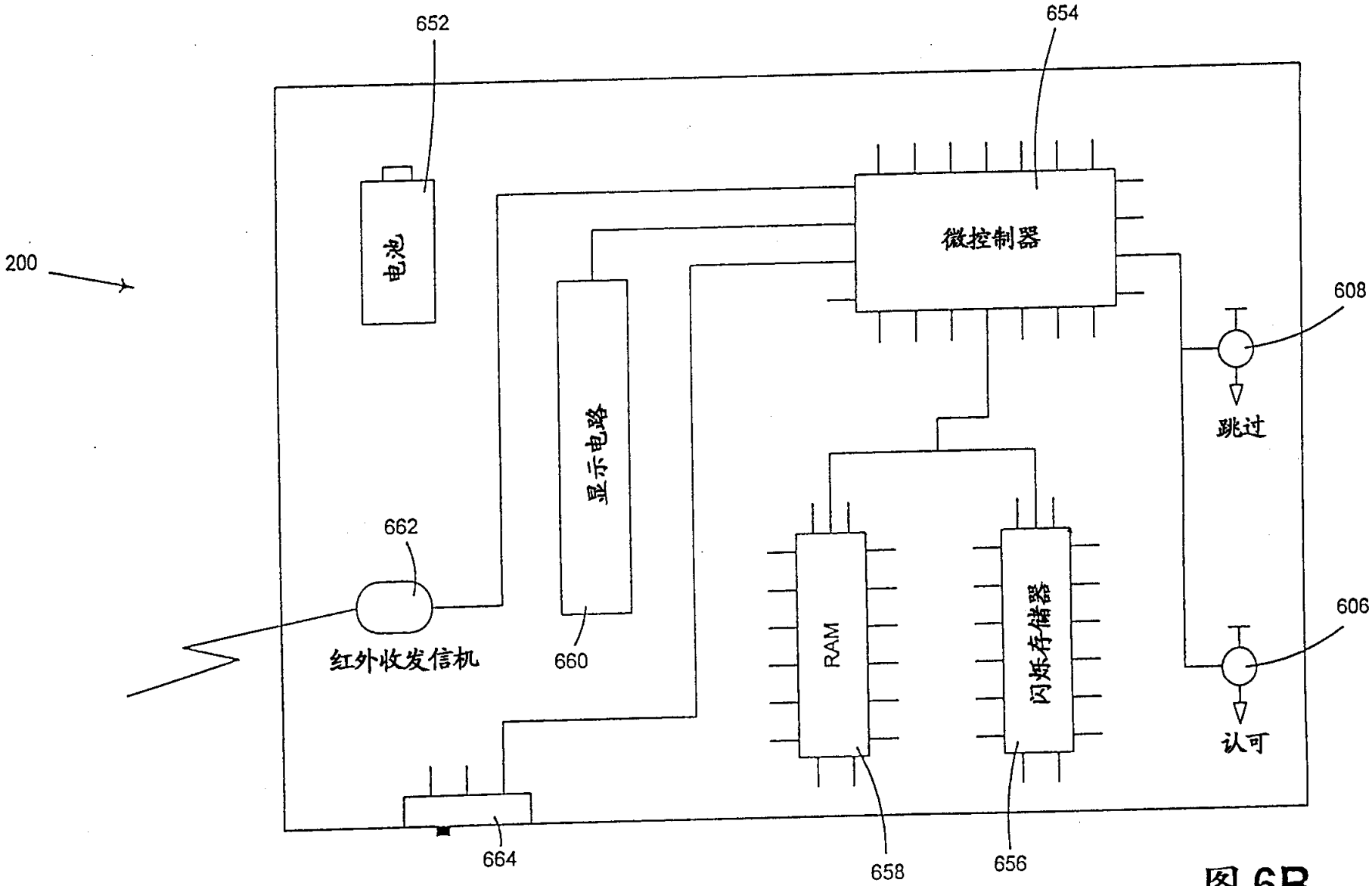

200
652
654
电池
微控制器
608
跳过
显示电路
662
红外收发信机
660
RAM
闪烁存储器
606
认可
664
658
656

图 6B

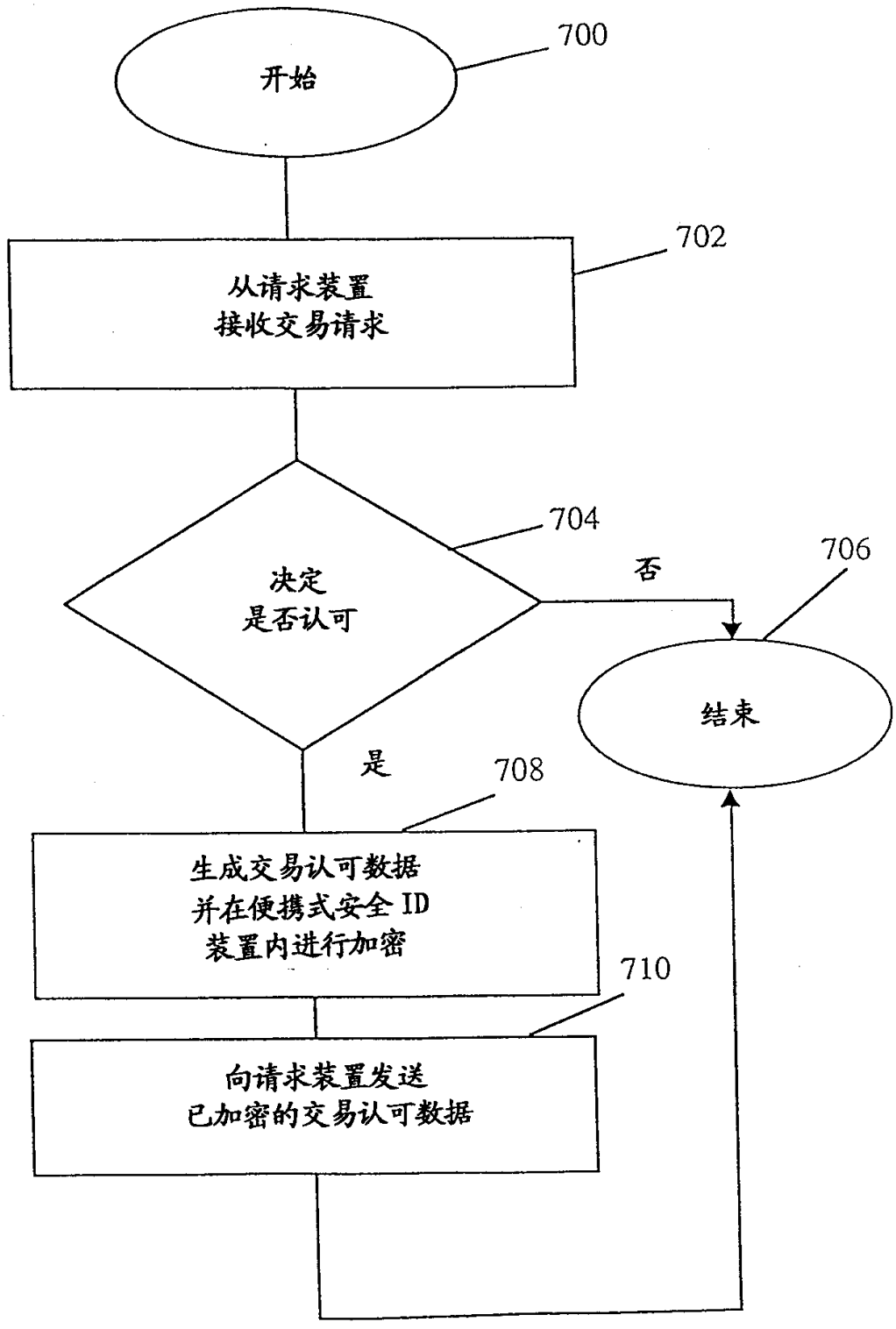

开始
700
从请求装置
接收交易请求
702
决定
是否认可
704
否
706
结束
是
708
生成交易认可数据
并在便携式安全 ID
装置内进行加密
710
向请求装置发送
已加密的交易认可数据

图 7

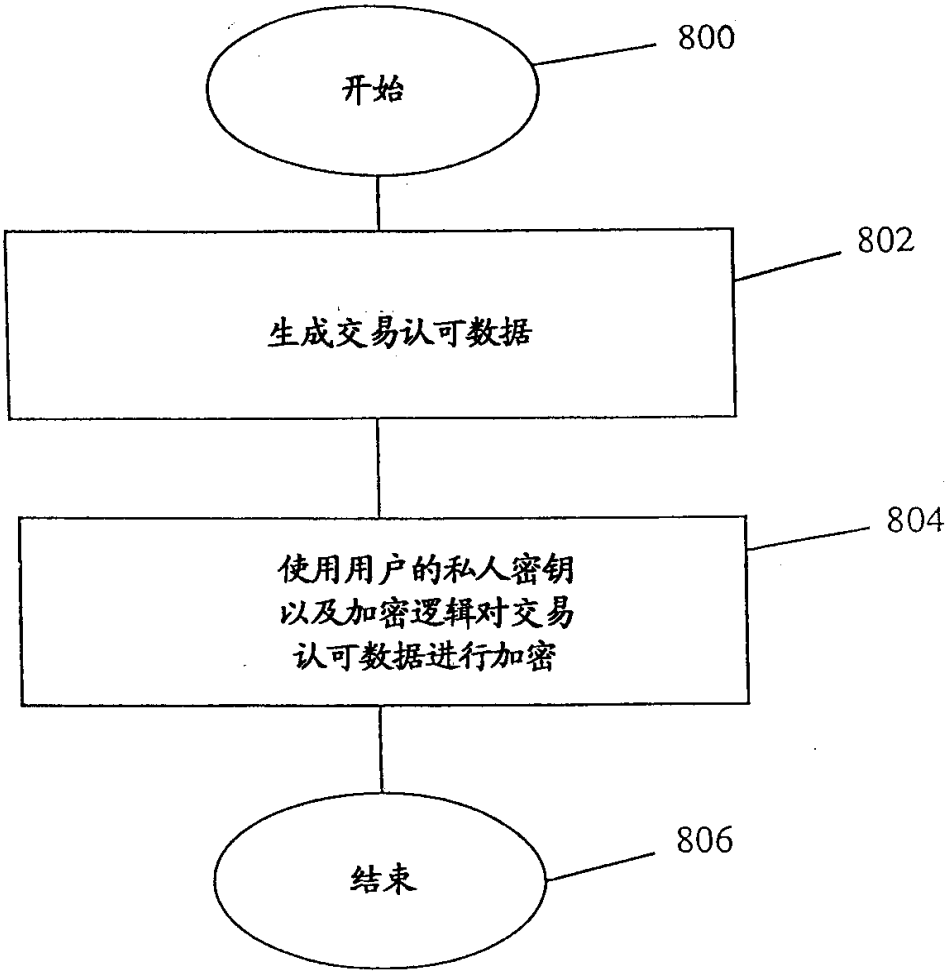

开始
800
生成交易认可数据
802
使用用户的私人密钥
以及加密逻辑对交易
认可数据进行加密
804
结束
806

图 8

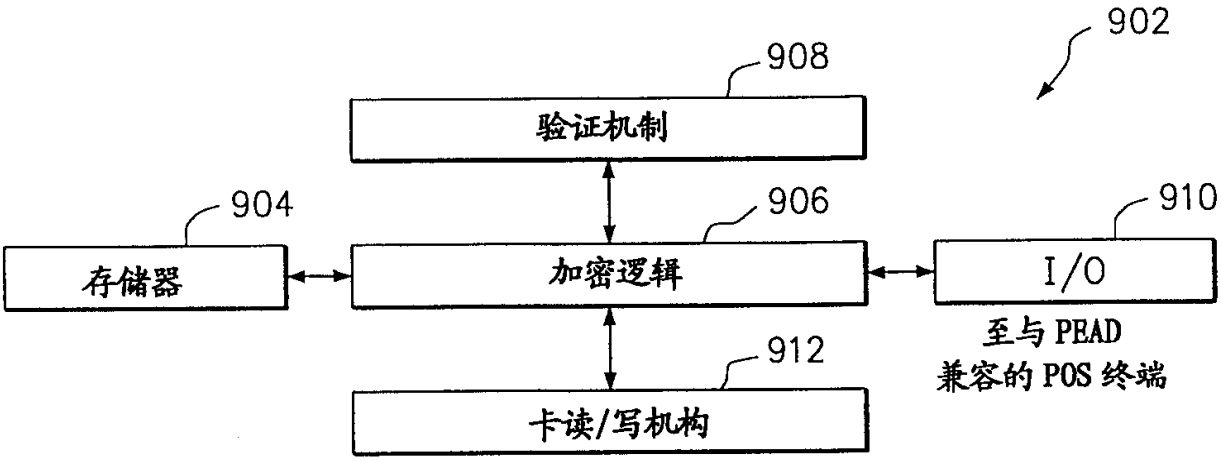

902
908
验证机制
904
906
910
存储器
加密逻辑
I/O
至与 PEAD
兼容的 POS 终端
912
卡读/写机构

图 9

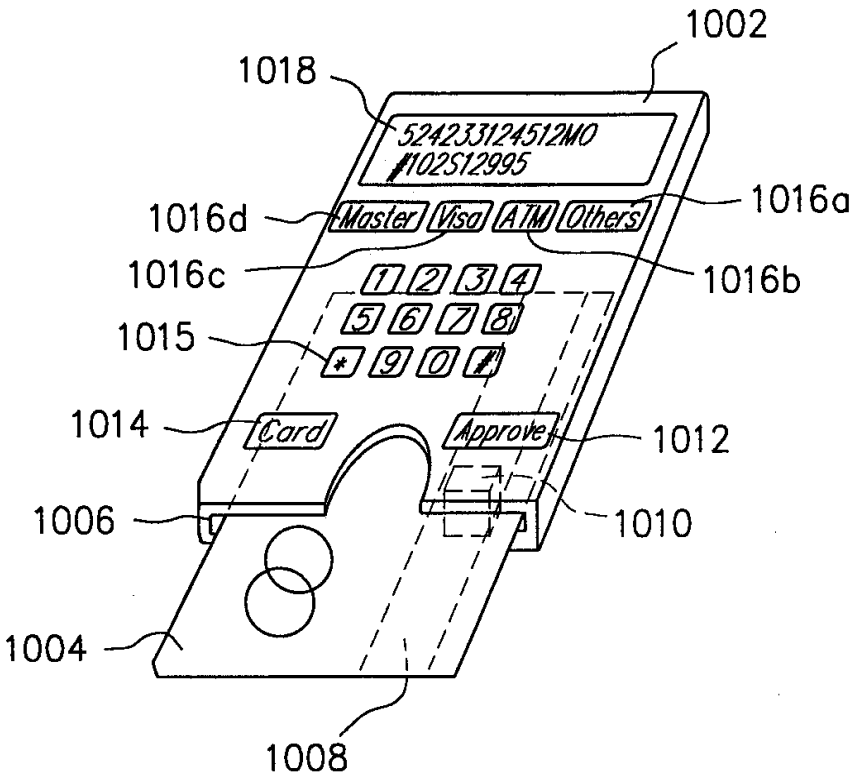

1002
1018
5242331245 12MO
#102512995
1016d
Master
Visa
ATM
Others
1016a
1016c
1016b
1 2 3 4
5 6 7 8
1015
* 9 0 #
1014
Card
Approve
1012
1006
1010
1004
1008

图 10

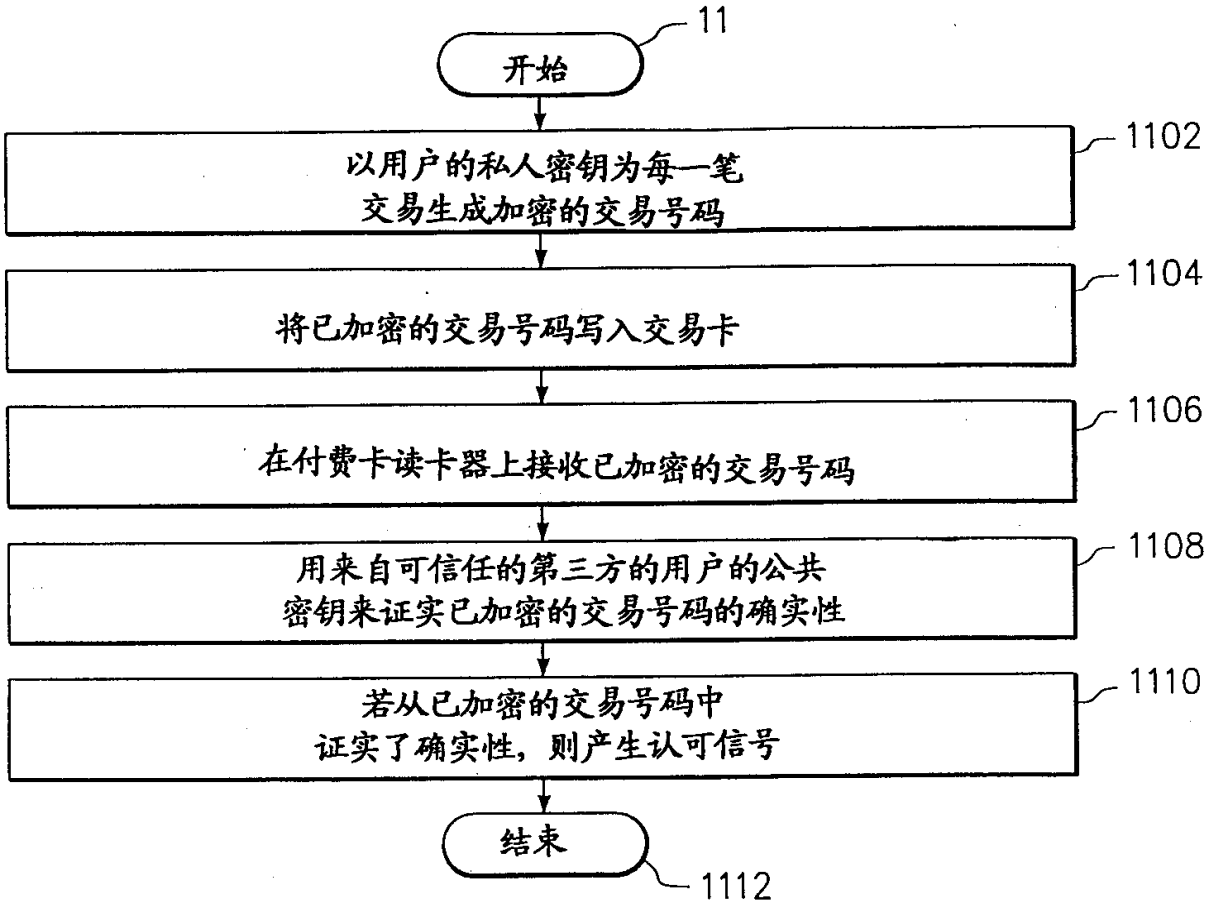

11
开始
1102
以用户的私人密钥为每一笔
交易生成加密的交易号码
1104
将已加密的交易号码写入交易卡
1106
在付费卡读卡器上接收已加密的交易号码
1108
用来自可信任的第三方的用户的公共
密钥来证实已加密的交易号码的确实性
1110
若从已加密的交易号码中
证实了确实性，则产生认可信号
结束
1112

图 11