



## [12] 发明专利说明书

专利号 ZL 99816560.3

[45] 授权公告日 2007 年 3 月 7 日

[11] 授权公告号 CN 1303778C

[22] 申请日 1999.11.19 [21] 申请号 99816560.3

[30] 优先权

[32] 1998.11.19 [33] US [31] 09/196,430

[86] 国际申请 PCT/US1999/027621 1999.11.19

[87] 国际公布 WO2000/030285 英 2000.5.25

[85] 进入国家阶段日期 2001.5.18

[73] 专利权人 阿科特系统公司

地址 美国加利福尼亚

[72] 发明人 巴拉斯·N·考斯克

拉莫汉·瓦拉达拉简

[56] 参考文献

US5491752 1996.2.13

US5668876 1997.9.16

US5778065 1998.7.7

审查员 刘剑波

[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 付建军

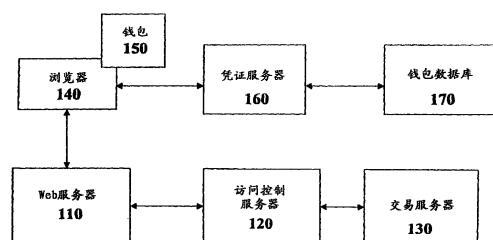
权利要求书 8 页 说明书 10 页 附图 3 页

[54] 发明名称

用于向漫游用户安全分发认证凭证的方法和设备

[57] 摘要

一个需要一份认证凭证(如私钥)(230)来访问一台计算机服务器(110)以执行一个电子交易的漫游用户(150)可以以一种按需提供的方式通过计算机从一台用户可访问的凭证服务器获得认证凭证(230)。在这种方式下，用户可以自由地在网络中漫游而不必实际携带其认证凭证(230)。可以通过一个或多个询问-响应协议来保护对凭证(230)的访问，该协议涉及简单共享密文、带有一对一散列(210)的共享密文或生物测量学方法如指纹识别。如果使用伪装来保护认证凭证(230)，可以在服务器(160)或用户计算机(160)上进行去除伪装的处理。



1.一种计算机可实施的用于在一个网络环境中获得一个可用来进行一个电子交易的认证凭证的方法，包括：

(a)通过一个网络访问一个服务器，来请求一个预定的认证凭证，所述认证凭证：

(i)在产生所述请求之前就已经存在于所述服务器中，

(ii)唯一标识其请求者，并且

(iii)在进行一个电子交易中使用；

(b)从所述服务器接收一个要求预定响应的询问，该预定响应与所述认证凭证的持有者相关联；

(c)发送一个对所述询问的回答；并且

(d)当所述回答经判断为正确时，从所述服务器接收所述认证凭证；

所述方法可以由所述请求者从多个请求地点以可重复的、在要求时提供的方式来操作。

2.权利要求1的方法，其中所述认证凭证包括一个所述请求者的秘密凭证。

3.权利要求2的方法，其中所述秘密凭证是一个私钥。

4.权利要求2的方法，还包括：

(e)使用所述认证凭证来进行所述电子交易；以及

(f)从所述请求者的计算设备中删除所述认证凭证。

5.权利要求2的方法，其中所述请求者的计算设备安装有一个Web浏览器，并且所述网络是一种分布式的计算机网络。

6.权利要求2的方法，其中所述请求者的计算设备配置有一个数字钱

包。

7. 权利要求 2 的方法，其中所述响应包括一个在所述服务器和所述请求者之间的共享密文。

8. 权利要求 1 的方法，还包括：

- (e) 使用所述认证凭证来进行所述电子交易；以及
- (f) 从所述请求者的计算设备中删除所述凭证。

9. 权利要求 8 的方法，其中所述认证凭证包括一个所述请求者的私钥。

10. 权利要求 1 的方法，其中所述接收的认证凭证采用密码伪装的形式。

11. 权利要求 10 的方法，其中所述认证凭证是用一个访问代码来加密的，并且还包括：

- (i) 所述请求者提供一个候选访问代码；
- (ii) 验证所述候选访问代码属于一族伪合法响应；  
以及
- (iii) 如果所述候选访问代码属于所述伪合法响应族，使用所述候选访问代码来对所述储存的认证凭证进行解密。

12. 权利要求 11 的方法，其中所述伪合法响应具有与所述访问代码的散列输出相同的特性。

13. 权利要求 12 的方法，其中所述认证凭证包括一个所述请求者的私钥。

14. 权利要求 10 的方法，其中所述认证凭证包括一个所述请求者的秘密凭证。

15. 权利要求 10 的方法，还包括以下步骤：

- (e) 使用所述认证凭证来进行所述电子交易；以及
- (f) 从所述请求者的计算设备中删除所述凭证。

16. 权利要求 1 的方法，其中所述询问及所述响应是零知晓证明协议的组成部分。

17. 权利要求 1 的方法，其中所述步骤(b)和(c)是密码伪装询问-响应协议的一部分。

18. 权利要求 1 的方法，还包括从所述服务器上连同所述认证凭证一起下载一个数字货币。

19. 一种用于在一个网络环境中获取一个可以用来进行一个电子交易的认证凭证的设备，包括：

(a) 一个用于网络通信的第一接口，配置为：

(i) 通过网络访问一个服务器来从中请求一个预定的认证凭证，所述认证凭证：

(A) 在所述请求之前就存在于所述服务器，

(B) 唯一标识其请求者，并且

(C) 用来进行一个电子交易，并且

(ii) 从服务器接收一个询问，这个询问要求与所述认证凭证的所述请求者相关联的预定响应；

(b) 一个用于用户对网络的访问的第二接口，配置为接收来自所述请求者的对所述询问的回答；

(c) 当所述回答经判断为正确时，所述用于网络通信的第一接口从所

述报服务器接收所述认证凭证；以及

(d)一个存储器，配置为在所述请求者的计算设备上储存所述认证凭证；

所述设备可以被所述请求者所使用，来从多个请求者地点获取可重复的、在要求时提供的访问。

20.权利要求 19 的设备，其中所述认证凭证包括一个所述请求者的秘密凭证。

21.权利要求 20 的设备，其中所述秘密凭证是一个私钥。

22.权利要求 19 的设备，其中安装有一个 Web 浏览器，并且其中，所述网络是一个分布式的计算机网络。

23.权利要求 19 的设备，其中配置有一个数字钱包。

24.权利要求 19 的设备，其中所述服务器配置为以密码伪装的形式储存所述认证凭证。

25.权利要求 24 的设备，其中：

(i)所述认证凭证是用一个访问代码加密的；

(ii)所述用于用户对网络的访问的第二接口配置为接收来自所述请求者的一个候选访问代码；并且

(iii)还包含加密逻辑单元，配置为：

(iv)如果所述候选访问代码属于所述伪合法响应族，验证所述候选访问代码属于一族伪合法响应；以及

(v)使用所述伪合法候选访问代码来解密所述储存的认证凭证。

26.权利要求 25 的设备，其中所述伪合法响应具有与所述访问代码的

散列输出相同的特性。

27. 权利要求 26 的设备，其中所述认证凭证包括一个所述请求者的私钥。

28. 权利要求 19 的设备，其中所述询问和所述预定响应是密码伪装询问-响应协议的一部分。

29. 权利要求 24 的设备，其中所述认证凭证包括一个所述请求者的秘密凭证。

30. 一种计算机可实施的用于在一个网络环境中提供一个可以用来进行电子交易的认证凭证的方法，包括：

(a) 通过网络接收一个来自请求者的对预定认证凭证的请求，所述认证凭证：

(i) 在所述请求之前就存在于所述服务器，

(ii) 唯一标识其请求者，并且

(iii) 在进行一个电子交易中使用；

(b) 向所述请求者发送一个询问，要求与所述请求者相关联的预定响应；

(c) 接收对所述询问的回答；

(d) 判断所述回答是否满足所述询问的判断，仅当判断正确时执行步骤 e；并且

(e) 为所述请求者发送所述认证凭证；

所述方法可以由所述请求者在多个请求者地点来操作，以处理可重复的、在要求时提供的认证凭证请求。

31. 权利要求 30 的方法，其中所述认证凭证包括一个所述请求者的秘密凭证。

32. 权利要求 31 的方法，其中所述秘密凭证是一个私钥。

33. 权利要求 31 的方法，其中所述请求者通过一个 Web 浏览器来请求预定的认证凭证，而所述网络是一个分布式计算机网络。

34. 权利要求 31 的方法，其中所述发送所述请求者的秘密凭证的目标是所述请求者的数字钱包。

35. 权利要求 31 的方法，其中所述响应包括一个在所述服务器和者之间的共享密文。

36. 权利要求 30 的方法，其中所述服务器配置为以密码伪装的形式储存所述认证凭证。

37. 权利要求 36 的方法，其中所述认证凭证是用一个访问代码加密的，并且其中所述判断所述回答满足所述询问包括：

- (i) 验证所述回答属于一族伪合法响应；并且
- (ii) 如果所述回答属于所述伪合法响应族，使用所述响应来对所述储存的认证凭证进行解密。

38. 权利要求 37 的方法，其中所述伪合法响应具有与所述访问代码散列输出相同的特性。

39. 权利要求 38 的方法，其中所述认证凭证包括一个所述请求者的私钥。

40. 权利要求 36 的方法，其中所述认证凭证包括一个所述请求者的秘密凭证。

41. 权利要求 36 的方法，其中所述步骤(e)包括向所述请求者以密码伪装形式发送所述认证凭证，以便由所述请求者进行加密去伪操作。

42. 权利要求 30 的方法，还包括向所述请求者连同所述认证凭证发送一个数字货币。

43. 一种用于在一个网络环境中提供一个可以用来进行一个电子交易的认证凭证的设备，包括：

(a) 一个用于网络通信的第一接口，配置为：

(i) 通过网络接收来自一个请求者的对一个预定认证凭证的请求，所述认证凭证：

(A) 在所述请求之前就存在于所述设备中；

(B) 唯一标识其请求者；并且

(C) 在进行一个电子交易中使用，

(ii) 发送一个询问，要求一个与所述请求者相关联的预定响应，并且

(iii) 从所述所有者处接收一个对所述询问的回答；

(b) 逻辑单元，配置为判断所述回答是否满足所述询问，仅当判断正确时为请求者发放认证凭证；并且

(c) 一个存储器，配置为储存将发放给所述请求者的所述认证凭证；

所述设备可以由所述请求者在多个请求者地点进行操作，以处理重复的、在要求时提供的认证凭证请求。

44. 权利要求 43 的设备，其中所述认证凭证包括一个所述请求者的秘密凭证。

45. 权利要求 44 的设备，其中所述秘密凭证是一个私钥。

46. 权利要求 44 的设备，其中所述响应包括一个所述服务器和所述请

求者之间的共享密文。

47. 权利要求 43 的设备，其中所述服务器配置为以密码伪装形式储存所述认证凭证。

48. 权利要求 47 的设备，其中所述认证凭证是用一个访问代码加密的，并且其中所述用于判断所述回答是否满足所述询问的逻辑包括：

(i) 第一密码逻辑单元，用于验证所述回答属于一族伪合法响应；以及

(ii) 第二密码逻辑单元，用于当所述回答属于所述伪合法响应族时使用所述回答来对所述储存的认证凭证进行解密。

49. 权利要求 48 的设备，其中所述伪合法响应具有与所述访问代码散列输出相同的特性。

50. 权利要求 49 的设备，其中所述认证凭证包括一个所述请求者的私钥。

51. 权利要求 47 的设备，其中所述用于网络通信的第一接口配置为，向所述请求者以密码伪装形式发放所述认证凭证，以便所述请求者进行加密去伪操作。

52. 权利要求 47 的设备，其中所述认证凭证包括一个所述用户的秘密凭证。

## 用于向漫游用户安全分发认证凭证的方法和设备

交叉参见相关申请

本申请是未决的美国专利申请 No.08/996,758 的部分继续申请。

### 发明背景

在网络化的计算机配置(deployments)中，要求客户机的用户向服务器认证自己的身份，用于如电子邮件之类的应用程序、访问特许的或机密的信息、购买商品或服务，以及其他许多电子商务交易。当有关信息的价值比较低时，对用户来说，使用一个简单的口令来认证自己也就足够了。但是，当信息的价值很高时，或者当数据网络不安全时，简单的口令对于有效地控制访问是不够的。例如，当经过因特网访问计算机时，在包穿过网络时对其进行过滤，很容易捕捉到口令。或者，可以通过智能性的尝试来猜出或”破译”出口令，因为口令经常是 6 个或者更少的字符。简单地说，口令的方便性也使它们容易被破解—如果它们对用户来说足够易于记住，那么它们对黑客来说也就足够易于猜出。

为了克服口令的不安全性，又开发出了替代技术。一种这样的技术是不对称密钥密码技术。在这种技术中，每个用户具有两个密钥，一个私钥和一个公钥。用户使用其私钥在一个数字量上执行一个密码操作（如，加密或数字签名），以便由一个只能访问用户公钥的验证者对该数字量进行认证。因此私钥是作为用户的认证凭证来使用的。也就是说，验证者不需要为了对用户进行认证而知道用户的私钥。因为公钥可以广泛地散布而私钥却保持机密，所以可以提供带有增强安全性的强有力的认识。对于用户记忆来说，私钥一般都过于长而复杂，并且，因而通常储存在软件或硬件标记 (token) 中，并在使用之前与计算机连接 (interfaced)。

一个这样的软件标记就是所谓的软件钱包，其中私钥用一个口令或

其他控制访问的数据加密。在这种软件钱包中，不能制止一个入侵者无一遗漏地不断重复尝试口令，直到他恢复出私钥。这种状态类似于上述的简单口令方案的安全性风险。另外，软件钱包储存在用户的计算机中，如果用户需要自由地从一个地点漫游到另一个地点，这可能会带来不便。

与软件钱包相对照，硬件标记如智能卡更安全，而且在用户漫游时能够方便地携带。在一个典型的硬件智能卡中，私钥被储存在硬件中，并由监视芯片（watchdog chip）进行保护，只有用户输入了解锁智能卡的正确口令，监视芯片才允许他访问私钥。智能卡甚至能够按这样设置，如果一个黑客企图猜测口令，在次数很少的连续尝试错误之后，卡片将会锁上。硬件标记的缺点是：(1)漫游限制在安装了合适的标记阅读器硬件的地点；(2)与软件标记相比，硬件标记是昂贵的；(3)硬件标记必须实际携带，不论用户想去什么地方漫游；以及(4)硬件标记经常丢失、误置或被窃取。

因此，虽然硬件标记系统提高了安全性，但它们与基于软件的系统相比，还有几个缺点。人们因而希望有一种系统能够将基于硬件和基于软件的系统的优点结合在一起。

### 发明内容

本发明公开了一种用于按需向漫游用户发放验证凭证的方法与设备。凭证在软件中储存、发放并传送，避免了额外的硬件。在该系统的一个基本实施方案中，当一个用户以他事先交给凭证服务器保存的共享密文（shared secret）的形式提供了身份证明时，他就能够根据意愿要求他的凭证。共享密文可以由用户选择，并且可以是易于记忆的密文，如：母亲未婚时的姓名，三年级的老师等。用户将通过一个询问-响应协议（challenge-response protocol）来响应服务器的询问，在发放用户凭证之前先要给出对此类问题服务器所要求的正确答案。在本发明的另一个实施方案中，一个用户认证凭证可以储存在由简单共享密文方案保护的服务器上，简单共享密文方案可以是如口令、基于指纹或视网膜图像

的生物测量学认证方案、或一对散列的共享密文。在本发明的另一个实施方案中，用户与服务器通过一个密码伪装的询问-响应协议进行交互操作。特别是，如果用户正确地响应了服务器的询问，用户将接收到他的认证凭证。然而，如果用户的响应不正确，比如可能在一个黑客试图突破系统时，用户将接收似是而非且形式很好却无效的凭证。进而，可以用一个只有用户知道的附加密文对认证凭证本身加密或伪装。当一个认证凭证被嵌入许多相似（伪合法）的数据中时，它是密码伪装的形式。这些数据有足够的区域，用户能够没有任何困难地使用一个他能记住的共享密文来查出正确的数据。然而，数据又有足够的相似之处，入侵者会发现所有数据都是那么似是而非。可以以伪装的或去伪的形式来提供这样一个密码伪装的认证凭证，即，可以在凭证服务器或用户计算机上进行去伪操作。上面所述的本发明的各种实施方案提供了一个或多个或以下优点：

根据本发明的第一方面，提供了一种计算机可实施的用于在一个网络环境中获得一个可用来进行一个电子交易的认证凭证的方法包括：(a)通过一个网络访问一个服务器，来请求一个预定的认证凭证，所述认证凭证：(i) 在产生所述请求之前就已经存在于所述服务器中，(ii) 唯一标识其请求者，并且 (iii) 适于在进行一个电子交易中使用；(b) 从所述服务器接收一个要求预定响应的询问，该预定响应与所述认证凭证持有者相关联；(c) 向所述询问发送一个回答；并且 (d) 响应所述服务器对所述回答是否满足所述询问的判断，从所述服务器接收所述认证凭证；所述方法可以由所述请求者从多个请求地点以可重复的、按需提供的方式来操作。

根据本发明的第二方面，提供了一种用于在一个网络环境中获取一个可用来进行一个电子交易的认证凭证的设备，包括：(a) 一个网络接口，配置为：(i) 通过网络访问一个服务器来从中请求一个预定的认证凭证，所述认证凭证：(A) 在所述请求之前就存在于所述服务器，(B) 唯一标识其请求者，并且 (C) 适于用来进行一个电子交易，并且 (ii) 从服务器接收一个询问，这个询问要求与所述认证凭证的所述请求者相关联的预定响应；(b) 一个用户接口，配置为接收来自所述请求者的对所述询问的回答；(c) 所述网络接口配置为根据一个由所述服务器所作的对所述回答是否满足所述询问的判断来接收所述认证凭证；以及 (d) 一个存储器，配置为在所述请求者的计算设备上储存所述认证凭证；所述设备可以被所述请求者所使用，来从多个请求者地点获取可重复的、按需提供的访问。

根据本发明的第三方面，提供了一种计算机可实施的用于在一个网络环境中提供一个可以用来进行电子交易的认证凭证的方法，包括：

(a) 通过网络接收一个来自请求者的对预定认证凭证的请求，所述认证凭证：(ii) 在所述请求之前就存在于所述服务器，(ii) 唯一标识其请求者，并且(iii) 适于用来进行一个电子交易；(b) 向所述请求者发送一个询问，要求与所述请求者相关联的预定响应；(c) 接收对所述询问的回答；(d) 判断所述回答满足询问；并且(e) 为所述请求者发送所述认证凭证；所述方法可以由所述请求者在多个请求者地点来操作，以处理可重复的、按需提供的认证凭证请求。

根据本发明的第四方面，提供了一种用于在一个网络环境中提供一个可以用来进行一个电子交易的认证凭证的设备，包括：(a) 一个网络接口，配置为：(i) 通过网络接收来自一个请求者的对一个预定认证凭证的请求，所述认证凭证：(A) 在所述请求之前就存在于所述设备中；(B) 唯一标识其请求者；并且(C) 适于在进行一个电子交易中使用，(ii) 发送一个询问，要求一个与所述请求者相关联的预定响应，并且(iii) 从所述所有者处接收一个对所述询问的回答；(b) 逻辑，配置为判断所述回答是否满足所述询问；并且(c) 一个存储器，配置为储存将发放给所述请求者的所述认证凭证；所述设备可以由所述请求者在多个请求者地点进行操作，以处理重复的、按需提供的认证凭证请求。

布置中不需要额外的硬件。这是与硬件标记如需要广泛布置卡片及读卡器的智能卡对照而言的。

(1) 高度的用户方便性。漫游用户不需要携带标记，却能够在需要时要求它们。

(2) 低管理费用。丢失、误置或忘记标记的用户不需要管理介入。

(3) 快速的分发速度。带漫游访问的软凭证可以迅速布置，因为它们可以直接使用并且几乎不需要用户/管理者培训。

(4) 对纯单一因素系统增强的安全性。

#### 附图说明

图 1 描绘了一个本发明的示范实施方案，其中一个用户访问一台 web 服务器来与一台访问控制服务器保护的交易服务器进行一个电子交易。

图 2 描绘了一个钱包的示范实施方案，其中一个私钥由一个 PIN(个人身份号码) 来保护。

图 3 描绘了一个示范实施方案，其中图 2 的钱包以一个密码伪装的形式来保护。

### 具体实施方式

我们现在使用一个操作 web 浏览器来访问一个或多个远程服务器的用户的示范环境来叙述本发明的多个示范实施方案，借助该方案，用户能够自由地在因特网中漫游而仍然保持对其认证凭证的访问。熟悉技术的人员会认识到本发明也适用于其他客户机-服务器环境，包括但不限于数据库、医疗客户工作站及财务交易工作站。而且，网络环境不一定是因特网，而可以是一个内联网或实际上的任何分布式计算机网络。

现在参照图 1，一个在浏览器 140 的用户希望访问一个 Web 服务器 110 来进行一个电子交易。Web 服务器 110 被访问控制服务器 120 保护起来，访问控制服务器 120 防止对交易服务器 130 未经认证的访问。例如，Web 服务器 110 可以是一个公司的主页，访问控制服务器 120 可以是一个防火墙，而交易服务器 130 可以包含用户希望访问的专有公司数据。在另一个示例中，访问控制服务器 120 可以是一个会员资格或者信用/支付验证系统，而交易服务器 130 可以是一个后端装运/发货系统。熟悉技术的人员会意识到任何或所有服务器 110、120 和 130 可以合成在一个服务器中，可以有多个附加服务器实现其他专门的功能，任何这些服务器可以是集中的或者广泛分布的。同样地，电子交易可以是几乎任何类型的，包括但不限于安全电子邮件、访问特许的或机密的信息以及购买电子或实物商品或服务。

在访问交易服务器 130 进行电子交易之前，用户首先需要向访问控制服务器 120 验证自己。正如在发明背景中所提到的，用户通常使用其私钥执行一个密码操作来验证自己，该操作是关于一个访问控制服务器 120 发送的询问。这个加密的操作可以是一个简单加密，一个伴随加密的散列（通常指一个数字签名），或者熟悉技术的人员熟知的其他协议。当然，在安全性较低的应用程序中，认证凭证可以是一个简单口令。私钥、口令和其他认证凭证对那些熟悉技术的人员来说都是熟知的，并且不需要在这里进行详细的描述。例如，读者可以参考知名的标准文本如 Applied Cryptography(Bruce Schneier, 第二版, 1996, 101-112 页及

548-549 页)来了解详细内容。

不管是何种认证凭证或协议，如果访问控制服务器 120 验证了用户，用户接着就被允许访问交易服务器 130。本发明提供了一种方法与设备，用于根据需要向希望能够访问服务器 110、120 与/或 130 的来自各种浏览器 140 的用户(所谓的”漫游用户”)提供认证凭证。

这种按需提供的漫游能力是由一个凭证服务器 160 来提供的，该服务器 160 通过一个软件钱包 150 向在浏览器 140 的用户下载认证凭证(如私钥)。如此处所用的，钱包 150 只需要作为一个认证凭证的基本容器来使用。这样，就可以认为它只是其中体现了认证凭证的数据结构，或者它可以是多个复杂的具有处理其他用户拥有的项目如数字证书或数字货币(包括而不局限于，电子现金或单据)能力的容器。在本发明的一个基本实施方案中，凭证服务器 160 体现为一个 web 服务器。用户向凭证服务器指出其浏览器 140，该凭证服务器以在设置阶段事先与用户相关联的共享密文的形式向用户发出一条询问。这个共享密文可以是以下的示范形式：

问题：母亲未婚时的姓名？ 答案：Jones

问题：狗的名字 答案：Lucky

问题：喜欢的运动 答案：足球

问题：PIN? 答案：PIN

实际的问题数目从凭证服务器到凭证服务器，根据它们各自的安全策略，可以有多种变化。如果用户提供了正确的答案，凭证服务器 160 从一个钱包数据库 170(它可以是或不是凭证服务器 160 的一部分)获得用户的钱包，并将钱包提供给在浏览器 140 端的用户。在一个替代实施方案中，钱包或它的一部分可以直接提供给任何服务器 110、120 和 130。

上述的任何一个方案中，1)或者钱包可以安装在软件程序的存储器空间，与/或接着 2)或者钱包可以安装到硬件驱动器或计算机的其他物理存储器上。如果仅仅是前者的话，在会话结束时，认证凭证将被毁掉。如果是后者的话，在那台特定的计算机上，认证凭证可以跨多个会话而

为用户所用。在任何一种情况下，当用户漫游到另一台计算机上时，可以重复该进程来按需提供对所需认证凭证的访问，而不需要实物标记（尽管，如果想要的话，本发明还能够与一个实物标记一起使用）。

上面描绘了所谓共享密文的使用，借助它，用户和服务器都共享访问系统所需的信息的复印件。当然，本发明不局限于这种简单协议，这种协议由于其自身特点，会被欺骗服务器滥用。例如，也可以使用零知晓证明（zero knowledge proofs），用户使用它能够向服务器证明他知道其母亲未婚时的姓名（或其他密文信息），而不用实际向服务器告知该姓名。作为一个简单的例子，对一个只需要知道相关公钥来验证私钥的验证者来说，用户的私钥自身就能够以这种方式来使用。零知晓证明的原理与实施对熟悉技术的人员来说是熟知的，并且不需要在这里叙述。读者可以参考知名的标准文本如前面提过的 Applied Cryptography 来获得详细内容。

在本发明的一个实施方案中，钱包自身可以被一个共享密文保护。例如，图 2 显示了一个钱包的示范实施方案，其中由一个 PIN 来保护一个私钥。如前所述，PIN（更普遍地是一个共享密文）可以是由用户向凭证服务器 160 传送的共享密文，而在钱包中的私钥（更普遍地是认证凭证）可以被凭证服务器 160 解密并以明码提供给在浏览器 140 端的用户。或者，对在浏览器 140 端本地解密的用户，整个钱包（包括加密形式的认证凭证）都可以提供给用户。不论使用哪种方法，对 PIN 保护的认证凭证进行解密的进程如下所述。用户输入一个 PIN200（更普遍地是一个访问代码）来对钱包解锁，而 PIN 通过一个一对一散列函数 210。散列函数还包括一个盐值（salt value）或者其他加强安全性的特征，对于熟悉技术的人员是可以理解的。所输入的 PIN 的散列值 215 被与储存的散列值 220 进行比较，储存的散列值 220 是正确的 PIN 的散列值。如果两个散列值一致，PIN 被送到解密模块 240。加密并储存在区域 230 中的私钥（以正确的 PIN 作为加密密钥）被解密模块 240 解密，解密模块 240 代表性地是 DES（数据加密标准）或某些其他加密函数如三重 DES、IDEA 或 BLOWFISH。此后，发放经过解密的私钥 250 以供使用。

计算散列并对储存的散列解密的密操作可以使用一个或多个密码逻辑（如软件或硬件）模块来实施，而正确的散列值和私钥可以被储存 在受保护的数据区域或其他存储形式（如从 ROM 中读取，从计算机可 读介质中读取等）中。一个典型的密钥钱包也可以包括用于接收候选 PIN 的输入与输出逻辑和用于输出经解密的私钥，也包括用于管理、查看、 复制和处理密钥和其他数据的逻辑。

散列函数的一对一特性确保正确的 PIN 且只有正确的 PIN 将会对 密钥钱包解锁。不幸的是，它也允许一个恶意的黑客通过强制搜索来猜 测完整的 PIN。例如，他可以写一段程序，简单地在密钥钱包上检验所 有 6 位 PIN 代码。如果他得到了密钥钱包的复印件，他就能够在他的计 算机上以完全检测不到而且是自动化的方式只花几分钟的时间来进行这 种攻击。

为了抵御 PIN 散列攻击，本发明的另一个实施方案使用一种称为 密码伪装的技术来提供与认证凭证有关的更好的安全性。下面对照图 3 简要地叙述密码伪装；对于全部详细内容，读者可以参考这里相结合的 同样未决的美国专利申请 No. 08/996,758。

现在参考图 3，认证凭证（如私钥）通过如图 2 中所示的一个访问 代码来保护。但是，用一个多对一散列来替代一对一散列，多对一散列 即一个散列，其中多个输入产生（即再生）相同的散列输出。在一个示 范实施中，多对一散列函数 310 可以将 6 位代码散列为 2 位散列值。在 常规的密钥钱包中，输入的 PIN300 的散列值 315 与储存的散列值 320 进行比较，储存的散列值 320 是正确的 PIN 的散列值。如果两个散列值 相同，密钥钱包打开。私钥再次被加密储存到密钥钱包的区域 330 中， 以正确的 PIN 作为加密密钥。当正确的 PIN 被输入时，储存的加密的 密钥被解密并发放正确的私钥 350 以供使用。然而，因为散列函数是 多对一的，将会有许多不同的输入 PIN 能够满足散列询问来打开密钥钱 包。（散列值与正确的 PIN 的散列值相同的 PIN，包括正确的 PIN，在 这里称为伪合法 PIN）。例如，如果散列函数将 6 位代码散列为 2 位散 列代码值，从总共可能的 1000000 个 6 位代码中，将会有 10000 个能

打开密钥钱包的 6 位伪合法 PIN。伪合法 PIN 将全部被送入解密模块 340 来对所储存的加密的密钥进行解密，以产生一个候选的私钥。但是，除了一个之外，其他所有这些候选的私钥都将是所储存的（正确的）私钥的非正确解密结果。只有当输入的 PIN 是那个正确的 PIN 时，正确的私钥才能被恢复。

更适宜地，应该将上述多对一散列函数选为一个优质散列(good hash)。例如且不局限于此，MD5 和 SHA 是为人熟知的优质散列函数。优质散列函数是一种在所有可能 PIN 的空间中充分均匀地分布伪合法 PIN 的方法。例如，考虑一个从 6 位代码到 2 位散列值的散列函数。如果散列函数是一个优质散列，这些值将被充分均匀地分布。特别地，在一百个 PIN 中会有一个是伪合法的，并且这些将是有效地随机分布。尤其是，如果用户在输入正确 PIN 时出现打字错误，其结果 PIN 将是一个伪合法 PIN 的机会是 1/100。

另一个可能的实施方案使用一个弱散列 (weak hash)，即一个散列，它产生伪合法 PIN 的群集，这使一个猜到一个伪合法 PIN 的入侵者更容易找到其他的伪合法 PIN。一个出现一系列 1 位打字错误的合法用户也可以得到一个伪合法 PIN 序列，而如果接受由此加密的私钥或者消息的系统有一个针对重复失败报警或禁用的特性，这将会不经意地把合法用户关在外面。因此，相对于优质散列，弱散列通常是不受欢迎的。不过，有一些应用程序，其中弱散列提供某种特性，如计算的效率和易于实现，对专门的应用程序是有利的。

上述段落叙述了进一步保护钱包的技术，或者带有一个一对一散列，或者带有一个多对一散列。熟悉技术的人员将意识到解密进程 200-250 和 300-350 (如密码伪装) 可以在用户计算机或凭证服务器 160 进行。在前一种情况下，钱包以解密的形式被下载到用户端，而在后一种情况下，在下载到用户端之前，钱包在凭证服务器 160 上进行解密。

更普遍地，也可以认识到，对这一点所述的各种询问-响应协议 (如简单共享密文；生物测量学方法如指纹识别；图 2 的一对一散列密文；以及图 3 的多对一散列密文) 能够在凭证服务器 160 或浏览器 140 端使

用，并且这种使用可以发生在任何组合或排列中。例如，对最小安全性来说，凭证服务器 160 可以通过一个简单共享密文被访问，钱包可以以明码方式下载到用户端。或者，钱包可以被一个一对一或多对一（即加密地伪装的）散列共享密文进一步保护，并且根据用户对适当询问-响应协议的响应在凭证服务器上对钱包进行解密。解密的（或者，在多对一散列的情况下，去伪的）钱包则会以明码形式被下载到用户端。对更好的安全性来说，钱包可以以伪装形式下载到用户端，在用户计算机上进行去伪操作。还要求更好的安全性的话，可以用一个一对一或多对一散列进程来代替简单共享密文，用于初始的服务器访问。通常，一对一散列或多对一散列可以在初始服务器访问阶段布置，而任何简单共享密文、一对一散列、多对一散列技术可以在后续的钱包下载阶段使用。

由于这些及其他可以被熟悉技术的人员理解的变化，因此，本发明的范围不局限于在此公开的特定实施方案，但受限于所附权利要求的全部范围。

图 1

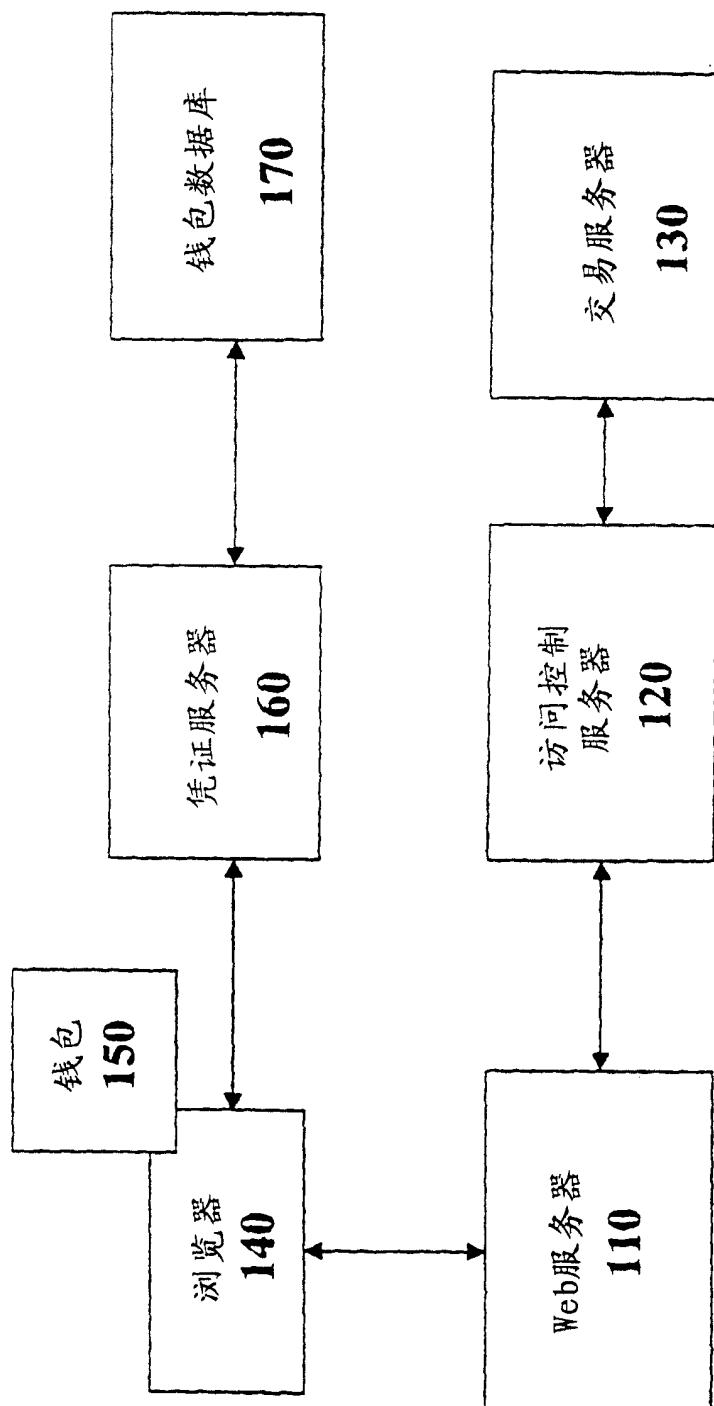


图 2

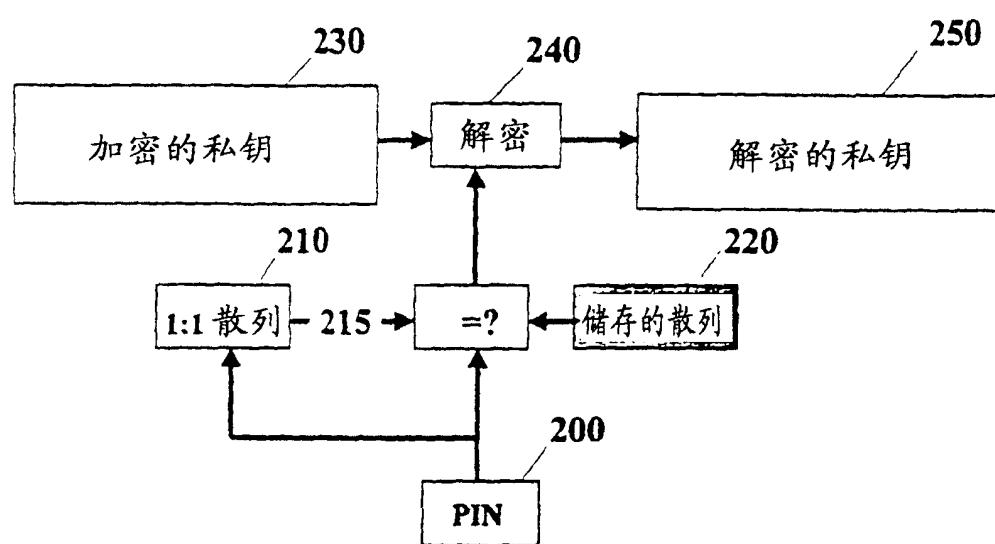


图 3

