(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1689297 B
(45)授权公告日 2014.01.08

(21)申请号 03816358.6
(22)申请日 2003.07.08
(30)优先权数据
10/192,920 2002.07.10 US
(85)PCT国际申请进入国家阶段日
2005.01.10
(86)PCT国际申请的申请数据
PCT/US2003/021088 2003.07.08
(87)PCT国际申请的公布数据
WO2004/006536 EN 2004.01.15
(73)专利权人 摩托罗拉移动有限责任公司
地址 美国伊利诺伊州
(72)发明人 亚历山大·迈德温斯基
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 黄启行 谢丽娜
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/30(2006.01)
H04L 9/08(2006.01)

(56)对比文件
GB 2355905 A,2001.05.02, 权利要求 1.
CN 1276659 A,2000.12.13, 全文.
US 6292893 B1,2001.09.18, 全文.
CN 1283827 A,2001.02.14, 全文.
Adi Shamir. IDENTITY--BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES. LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG. 1998, 第 47 页至第 53 页.

审查员 陈昇

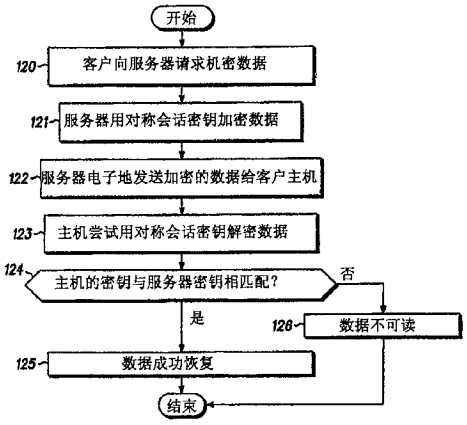
权利要求书2页 说明书9页 附图6页

(54)发明名称

使用密钥基防止未经授权分发和使用电子密钥的方法

(57)摘要

一种用于产生在电子交易中使用的电子密钥的方法和系统，可以通过在主机上执行单向函数来产生，所述函数从保存在该主机的非易失性存储单元中的一个密钥基和一个驻留该主机的唯一主机标识来导出电子密钥。优选地在每次进行需要使用该电子密钥的电子交易时执行该函数。



CN 1689297 B

1. 一种产生在电子交易中使用的电子密钥的方法，所述方法包括：在主机上执行单向函数，该函数从保存在所述主机的非易失性存储单元中的密钥基和唯一主机标识导出所述电子密钥，其中所述密钥基和所述单向函数是从密钥分发中心接收的，在每次进行需要使用所述电子密钥的电子交易时执行所述函数以导出所述电子密钥。

2. 如权利要求 1 的方法，进一步包括：用所述保存的密钥基和所述唯一主机标识作为输入执行所述单向函数，以产生在所述主机和电子装置之间的所述电子交易中使用的所述电子密钥，所述电子装置在所述电子交易中使用登记的公共密钥。

3. 如权利要求 2 的方法，进一步包括；只有在所述电子密钥与所述公共密钥正确相关时才允许所述电子交易成功完成。

4. 如权利要求 1 的方法，进一步包括：

从密钥分发中心接收所述密钥基；以及

把所述密钥基保存在所述主机的所述非易失性存储单元以产生保存的密钥基。

5. 如权利要求 4 的方法，进一步包括：用所述保存的密钥基和所述唯一主机标识作为输入执行所述单向函数，以产生在所述主机和电子装置之间的所述电子交易中使用的所述电子密钥，所述电子装置在所述电子交易中使用对称会话密钥。

6. 如权利要求 5 的方法，进一步包括：只有在所述电子密钥与所述对称会话密钥正确相关时才允许所述电子交易成功完成。

7. 如权利要求 1 的方法，进一步包括：不把所述电子密钥保存在所述主机的非易失性存储单元中。

8. 如权利要求 1 的方法，进一步包括：在所述交易后从所述主机装置中删除所述电子密钥。

9. 一种用于产生在电子交易中使用的电子密钥的系统，所述系统包括：

用于在主机上执行单向函数的装置，所述用于在主机上执行单向函数的装置从保存在所述主机的非易失性存储单元中的密钥基和唯一主机标识导出所述电子密钥；以及

用于从密钥分发中心接收所述密钥基和所述单向函数的装置，

其中所述用于在主机上执行单向函数的装置在每次进行需要使用所述电子密钥的电子交易时执行所述函数以导出所述电子密钥。

10. 如权利要求 9 的系统，其中，所述用于在主机上执行单向函数的装置使用所述保存的密钥基和所述唯一主机标识作为输入，以产生在所述主机和电子装置之间的所述电子交易中使用的所述电子密钥，所述电子装置在所述电子交易中使用登记的公共密钥。

11. 如权利要求 10 的系统，进一步包括；用于只有在所述电子密钥与所述公共密钥正确相关时才允许所述电子交易成功完成的装置。

12. 如权利要求 9 的系统，进一步包括：

用于把所述密钥基保存在所述主机的所述非易失性存储单元以产生保存的密钥基的装置。

13. 如权利要求 9 的系统，其中，所述用于在主机上执行单向函数的装置使用所述保存的密钥基和所述唯一主机标识作为输入，以产生在所述主机和电子装置之间的所述电子交易中使用的所述电子密钥，所述电子装置在所述电子交易中使用对称会话密钥。

14. 如权利要求 13 的系统，进一步包括：用于只有在所述电子密钥与所述对称会话密

钥正确相关时才允许所述电子交易成功完成的装置。

15. 如权利要求 9 的系统，进一步包括 :用于不把所述电子密钥保存在所述主机的非易失性存储单元中的装置。

16. 如权利要求 9 的系统，进一步包括 :用于在所述交易后从所述主机装置中删除所述电子密钥的装置。

17. 如权利要求 13 的系统，其中，所述主机执行所述单向函数以产生在所述主机和电子装置之间的所述电子交易中使用的私有密钥，所述电子装置在所述电子交易中使用登记的公共密钥。

18. 如权利要求 17 的系统，其中，只有在所述私有密钥与所述公共密钥正确相关时所述电子交易才成功完成。

19. 如权利要求 9 的系统，其中，所述密钥基包括对称会话密钥基。

20. 如权利要求 19 的系统，所述系统进一步包括密钥分发中心，用于发送所述对称会话密钥基给所述主机，所述主机把所述对称会话密钥基保存在所述非易失性存储单元中。

21. 如权利要求 20 的系统，其中，所述主机执行所述单向函数以产生在所述主机和电子装置之间的所述电子交易中使用的对称会话密钥，所述电子装置还在所述电子交易中使用对称会话密钥。

22. 如权利要求 21 的系统，其中，只有在所述主机使用的所述对称会话密钥与所述电子装置使用的所述对称会话密钥匹配时所述电子交易才成功完成。

23. 如权利要求 9 的系统，其中，所述非易失性存储单元包括硬盘驱动器。

24. 如权利要求 9 的系统，其中，所述主机包括个人计算机。

25. 如权利要求 9 的系统，其中，所述主机包括机顶盒。

26. 如权利要求 9 的系统，其中，所述电子密钥没有保存在所述非易失性存储单元中。

使用密钥基防止未经授权分发和使用电子密钥的方法

技术领域

[0001] 本发明涉及电子交互密码学领域。更具体地，本发明涉及要求使用电子密钥的电子交互领域。

背景技术

[0002] 每天有成千上万的人进行电子交互。例如，人们使用电子邮件 (e-mail) 与其他人通信或发送信息。人们和商业严重依赖于计算机网络或其它电子装置来管理、保护和传递重要信息。每天经银行网络和自动取款机 (ATM) 电子转账上百万美元。人们使用蜂窝电话和其它无线个人数字助理 (PDA) 交流和传递日常信息。

[0003] 由几百万个互联的计算机组成的互联网的出现急剧加速了电子交互。互联网几乎允许即时交流和传递信息到世界上几乎任何地方。万维网 (WWW) 用于在线业务、数据分发、营销、证券交易、在线银行业务、游戏、研究、学习以及无数其他活动。

[0004] 当参与方面对面或使用诸如纸张这样的物理媒介交互时，相对地较容易鉴定正在交互的人的证书。例如，如果一个人走进一家银行并且试图取钱时，银行出纳员在给予所请求的现款时可能要求并且核对他或她的身份。一个人在合同上的签名可以被认为能充分保证他或她承认合同。类似地，如果一个人进入一个商店并且用信用卡买一件物品，那么收银员很容易采取措施以致可以适度确保这个人是该信用卡的拥有人。

[0005] 但是，在电子交互领域，不能使用这样的物理验证手段。如果人们和企业感觉他们的电子交互是不保密和不安全的，那么他们就不在互联网上转移资金、买东西或使用任何电子装置管理和传递机密信息。因此，在电子传送决定和协议的领域中，需要用于提供验证、安全和保密的电子技术。

[0006] 密码使用术是可以用于保护敏感信息、维护通信中的保密性、验证交易中的用户以及在信息传递中执行其他安全措施的技术和应用的研究。密码分析是研究如何使密码机制泄密、失效。例如，黑客是研究和实践密码分析的人。密码学是组合的密码使用术和密码分析的学科。

[0007] 密码使用术允许人们把在物理世界中找到的信任转入电子世界，从而允许人们电子地进行交易而不过度担心欺骗、私密性的破坏或缺少安全性。电子传输的信息的持续增长导致对密码使用术的更大依赖。

[0008] 例如，密码使用技术有助于站点保密和电子传输安全。这允许人们用他们的信用卡进行在线银行业务、在线贸易以及进行在线购买而不需担心他们的帐户信息被泄密。密码使用术对于互联网和电子商务的持续增长是非常重要的。

[0009] 密码使用术还用在电话、电视以及各种普通的家庭项目。没有密码使用术，黑客将能够更容易地访问其他人的私人 e-mail、窃听电话交谈、接进电缆公司获取免费电缆服务或侵入银行帐户。

[0010] 在密码使用术中的一个主要重点包括加密和解密。加密是把数据转换为一种表面上难以理解并且在没有例如密钥这样的相应知识的情况下极难（虽然不是不可能）在合理

的适量时间内访问的形式。密钥将在下面进一步解释。加密的目的是为了通过把信息对没有预定的人、甚至那些可以访问加密数据的人隐藏起来以便确保私密性。解密是加密的相反过程；它是把加密数据反过来转换为可理解的形式。为了站点安全，例如，在存储数据和接收数据的计算机之间传送的所有数据必须加密。接收计算机必须能够解密该数据。

[0011] 尽管现代密码使用术逐渐变得各种各样，密码使用术根本上基于很难解的问题。一个问题可能是因为它的解需要使用一些秘密知识而很难。一个问题也可能是因为它本身难以完成而很难，例如找到一个极大数的因子。

[0012] 如上面所解释的，成功地加密和解密依赖于仅有执行该加密和解密的各方在理论上已知的一些种类的秘密知识。该项知识称为密钥。密钥通常是一串随机或伪随机比特。因此，没有正确密钥的人不能发送、接收或解释其他人的敏感信息。密钥还用于电子验证、数字签名、数字时间标记以及用于其他电子安全目的。如后面以及在附随的权利要求中使用的，如果不另外特别说明，术语“电子交易”将用于泛指要求使用一个或多个密钥的所有可能电子通信。

[0013] 当前，有两类密码系统：秘密密钥和公共密钥密码使用术。在秘密密钥密码使用术（也称为对称会话密码使用术）中，同样的密钥既用于加密也用于解密。对称会话密码使用术的主要问题在于使发送方和接收方约定对称会话密钥而不让其他人发现该对称会话密钥。例如，如果他们在不同的物理位置，他们必须信赖信使、电话系统或一些其他传输媒介以便防止对称会话密钥的公开。窃听或解释传送中的密钥的人可以在稍后使用该密钥读取、修改并且伪造所有加密和验证信息。密钥的产生、传输和存储称为密钥管理。所有密码系统必须处理密钥管理问题。因为在对称系统的密码系统中的所有密钥最好必须保持秘密，因此对称会话密码使用术通常有提供秘密密钥管理的困难，尤其是在具有大量用户的开放系统中。

[0014] 由于与对称会话密码使用术相关的密钥管理问题，发展了公共密钥密码使用术系统。在公共密钥密码使用术中，每个用户有一个公共密钥和一个私有密钥。公共密钥是公开的而私有密钥保持秘密。用公共密钥执行加密而只能用私有密钥执行解密。在公共密钥密码使用术中，消除了对发送方和接收方共享秘密信息的需要；所有通信只涉及公共密钥，而私有密钥不发送或共享。因而，不需要信任传送对称会话密钥的一些手段的安全性。任何人可以通过只使用公共信息发送机密消息。该消息只能使用私有密钥解密，而该私有密钥只有预定接收方单独持有。

[0015] 但是，当前公共密钥密码使用术的一个缺点在于：私有密钥数学上与公共密钥相联系。因此，通过从公共密钥导出私有密钥来攻击公共密钥系统是可能的。但是，这典型地需要极大量的时间或其他资源。

[0016] 当前，对称会话密钥和私有密钥可以存储在用户计算机或其他电子装置的硬盘或其他非易失性存储单元，其他电子装置例如是电缆机顶盒(STB)。用户然后可以使用这些密钥安全地进行电子通信。但是，在用户的控制下在用户计算机或其他装置上存储密钥有各种问题。首先，例如，用户可能复制在他或她的计算机或其他装置上的密钥，并且把复制的密钥分发给其他人。这些人然后可以假冒用户的电子身份并发送和接收预定只供初始用户使用的信息。这种情况可能发生在一个人支付按月预定收费率以在互联网或有线电视系统上接收内容的情况。如果这个人把允许接入付费内容的密钥分发，那么就有多个用户可以

接收该内容而不负担它的费用。

[0017] 在用户计算机或其他电子装置上存储密钥的第二个问题涉及篡改和窃取。如果用户偶然中离开他或她的无人照管或没有电子保护的计算机或其他电子装置，那么未经授权的人可能复制用户的密钥。未经授权的用户然后就可能发送或接收预定给初始用户的私人信息。

[0018] 因此，在本领域中需要一种在安全电子通信中防止未经授权分发和使用密钥的方法和系统，密钥包括对称会话密钥和私有密钥。如后面和附随权利要求中所使用的，如果不另外特别说明，那么术语“密钥”用于泛指所有可能的电子通信密钥，包括对称会话密钥和私有密钥。

[0019] 有几种防止未经授权分发和使用密钥的方法。一种方法是使用欺骗管理 (fraud management)。欺骗管理是检测采取同一身份的多个活动主机。主机例如可能是连接到互联网的计算机或连接到电缆网络的STB。如后面和附随的权利要求所使用的，如果没有另外特别说明，术语“主机”用于泛指用户用来电子通信的任何电子装置。

[0020] 欺骗管理有几个缺点。首先，欺骗管理是在欺骗已经发生之后才检测并且不能首先防止非法使用密钥发生。欺骗管理还要求额外的成本和开销并且也不简单。

[0021] 另一种防止非法分发和使用密钥的方法是使用抗干扰 (tamper-resistant) 的密钥存储装置，这种装置最好使得黑客不可能析取和复制密钥。如果这种装置被打开，它宁可毁坏它自己，并且这种装置可以屏蔽使用电磁辐射的攻击。有多种可能的抗干扰密钥存储器的设计，包括包含密钥的主机，它可以通过使用特殊的物理密钥或通过检测授权用户的唯一物理特性激活。

[0022] 但是，要求每个想要发送和接收敏感信息的用户具有抗干扰密钥存储装置不是经济可行的。因此，这种保护方法不适宜于大量用户。

[0023] 事实在于防止未经授权的分发和使用密钥的安全措施都不是完全十分简单的。这在密码学领域中被普遍接受。因此，实现多于一种的防止未经授权的分发和使用密钥的安全措施应该能提供比只使用一种安全方法更好的保护。

发明内容

[0024] 在多种可能实施例的一种实施例中，本发明提供一种产生在电子交易中使用的电子密钥的方法。该方法包括，在主机上执行单向函数，该单向函数可以从该主机的非易失性存储单元中保存的密钥基 (keyseed) 和驻留在该主机上的唯一主机标识中导出电子密钥。优选地在每次进行要求使用该密钥的电子交易时执行该函数。

[0025] 本发明的另一个实施例提供一种用于产生在电子交易中使用的电子密钥的系统。该系统包括，一个用于进行该电子交易的主机，具有驻留在该主机上的唯一主机标识；一个用于存储密钥基的该主机的非易失性存储单元；以及一个用于从该密钥基和该主机标识导出该电子密钥的单向函数。该主机优选地在每次进行要求使用该密钥的电子交易时执行该函数。

[0026] 本发明的其他优点和新颖特点将在后面的说明中阐述，或者本领域技术人员通过读取这些材料或实践本发明可以认识到。本发明的优点可以通过在附随的权利要求中所列举的装置来实现。

附图说明

[0027] 附图描述了本发明的优选实施例并且是说明书的一部分。附图与下面的说明一起论证和揭示了本发明的原理。所说明的实施例是本发明的例子而不限制本发明的范围。

[0028] 图 1 是可以用于实现本发明的一个实施例的示范性电子交互配置的框图；

[0029] 图 2 是说明可以实现本发明的一种对称会话密码使用术的示范方法的流程图；

[0030] 图 3 是说明可以实现本发明的一种公共密钥密码使用术的示范方法的流程图；

[0031] 图 4 是说明本发明的一种方法的流程图，该方法需要在主机的非易失性存储单元中存储一个代替密钥的密钥基，然后基于该密钥基和该主机唯一标识导出密钥。

[0032] 图 5 是说明当应用于公共密钥密码使用术时本发明的一种示范方法的流程图；

[0033] 图 6 是说明当应用于公共密钥密码使用术时本发明的第二示范方法的流程图；

[0034] 图 7 是说明当应用于对称会话密码使用术时本发明的一种示范方法的流程图。

[0035] 所有的附图中，同样的参考号表示类似的（但不需要是同样的）元件。

具体实施方式

[0036] 本发明提供一种方法和系统，借此主机在非易失性存储器中保存一个代替密钥的密钥基。该密钥基将在下面结合附图 4 进行更详细的解释。为了得到期望的密钥，用户在主机上运行一个单向函数，其中使用密钥基和主机标识（主机 ID）作为对该函数输入。这样，该单向函数只在预定使用该密钥的主机上产生一个有效密钥。因为该密钥本身没有存储在该主机的非易失性存储单元中，因此该密钥不能被复制并分发给其他人。本发明的另一个优点是它相对较低的经济实现成本。

[0037] 使用这些附图，现在描述本发明的优选实施例。

[0038] 图 1 是可以用于实现本发明的一个实施例的示范电子交互配置的框图。如图 1 所示，主机 (100) 由期望与服务器 (101) 电子交互的客户或用户使用。该主机 (100) 可以是个人计算机、服务器、自动取款机 (ATM)、蜂窝电话、有线或卫星机顶盒 (STB) 或任何其他能够电子通信的装置。服务器 (101) 也可以是个人计算机、服务器、ATM、蜂窝电话、有线头端或任何其他能够电子通信的装置。如在后面和附随的权利要求中所使用的，如果没有另外特别说明，术语“主机”用于泛指客户使用的所有可能的电子通信装置，并且术语“服务器”用于泛指客户期望与之通信的所有可能的电子通信装置。

[0039] 如图 1 所示，主机 (100) 优选地包含一个被设计为与主机 (100) 一起运行或在主机 (100) 内运行的非易失性存储单元 (103)。该非易失性存储单元 (103)，如在后面和附随的权利要求中所指的，例如可以是硬盘、软盘、光盘 (CD)、闪存单元或任何其他能够非易失性存储的存储单元 (103)。根据本发明的一个实施例以及如图 1 所示，密钥基 (106) 可以存储在非易失性存储单元 (103) 中。

[0040] 主机 (100) 优选地还包含用于暂时存储信息的随机访问存储器 (RAM)(104)。RAM(104) 例如可以暂时存储通过该函数产生的密钥。该主机优选地还包含一个处理器 (105)，例如 CPU，用于运行产生密钥的函数。

[0041] 如图 1 所示，服务器 (101) 也可以具有非易失性存储单元 (103)、RAM(104) 以及可以在完成与主机 (100) 的电子交易中使用的处理器 (105)。

[0042] 因为主机 (100) 和服务器 (101) 可以是不同的系统，因此如图 1 所示，使用一个协议 (102) 便于在主机 (100) 和服务器 (101) 之间的电子通信。协议 (102) 是一组管理在电子通信装置之间交互的格式和控制的协定。换句话说明，协议 (102) 是一种方法和系统，通过它两个不同或不一样的电子系统可以通信。

[0043] 在密码学领域，有许多不同的协议 (102) 可以用于确保在主机 (100) 和服务器 (101) 之间信息交换中的安全性和私密性。无论交换基于一个密钥或多个密钥，这些用于确保在电子装置之间信息交换中的安全性和私密性的协议 (102) 都可以称为密钥管理协议 (102)。当前使用的可能的密钥管理协议 (102) 的例子是 Kerberos、DOCSISBPI+、互联网密钥交换 (IKE)。本发明可以使用这些协议 (102) 中的任一个以及涉及在非易失性存储单元上存储密钥的任何其他协议 (102) 来实现。在公共密钥密码使用术的情况中，本发明可以使用允许私有密钥基随机产生并且公共密钥可以从私有密钥导出的协议 (102) 来实现。

[0044] 图 2 是说明对称会话密码使用术的示范方法的流程图，使用该方法可以实现本发明。尽管图 2 的方法说明了机密数据的加密和解密，但是该方法还可以应用于其他任何类型的使用对称会话密码学的电子交易。

[0045] 如图 2 所示，处理从客户向服务器请求机密数据开始 (120)。该请求可以以各种方式执行，包括（但不限于）在网页上选择一个选项、发送 e-mail、从 STB 发送请求、进行电话呼叫或发送书面形式的信。

[0046] 在进行对机密数据的请求后，服务器使用一个对称会话密钥加密要发送给客户的数据 (121)。该服务器然后电子地把加密的数据发送给客户主机 (122)。

[0047] 一旦客户主机接收该加密的数据，它就尝试使用一个密钥解密该加密的数据 (121)。成功的解密取决于主机用于解密该数据的密钥。在对称会话密码系统中，主机将使用一个与服务器用来加密该数据相同的密钥。因此，如果该主机的密钥与服务器使用的密钥相匹配 (124)，那么所请求的数据的成功解密和恢复 (125) 都是可能的。但是，如果一个主机没有或不使用与服务器使用的密钥相一致的密钥对该加密数据解密，那么该加密数据就不能被解密并且不可读 (126)。

[0048] 图 3 是说明公共密钥密码使用术的示范方法的流程图，使用该方法可以实现本发明。尽管图 3 的方法说明机密数据的加密和解密，但是该方法可以应用于使用公共密钥密码学的任何其他类型的电子交易。

[0049] 如图 3 所示，处理从一个客户向服务器请求机密数据开始 (120)。该请求可以以各种方式执行，包括（但不限于）在网页上选择一个选项、发送 e-mail、从 STB 发送请求、进行电话呼叫或发送书面形式的信。

[0050] 在进行对机密数据的请求后，服务器使用一个与请求该机密数据的客户相关联的公共密钥加密要发送给客户的数据 (130)。该服务器然后电子地把加密的数据发送给客户主机 (122)。

[0051] 一旦客户主机接收该加密的数据，它就尝试使用相应于用来加密该机密数据的公共密钥的一个私有密钥对该加密的数据解密 (131)。成功的解密取决于主机用来解密该数据的私有密钥。在公共密钥密码系统中，主机使用一个与服务器用来加密该数据的公共密钥数学地相关的私有密钥。因此，如果该主机的私有密钥与服务器使用的公共密钥正确相关 (132)，那么所请求数据的成功解密和恢复 (125) 都是可能的。但是，如果一个主机没有

或不使用正确的私有密钥对加密数据解密，那么优选地该加密数据不能被解密并且不可读(126)。

[0052] 但是，如上所述，如果一个用于对称会话密码系统的对称会话密钥或用于公共密钥密码系统的私有密钥存储在用户的主机上，那么那个用户就可以尝试共享那个秘密或私有密钥以允许其他人访问来自该服务器的通信。此外，如果一个用于对称会话密码系统的对称会话密钥或用于公共密钥密码系统的私有密钥存储在用户主机上，那么未经该用户同意的人就可以找到访问该用户主机并得到秘密或私有密钥的途径，从而获得对服务器发送给该授权用户的机密数据的访问。图 4 是说明根据本发明的一个实施例的方法，其中需要在主机的非易失性存储单元上存储一个代替密钥的密钥基，以便减少在用户合作或没有用户合作的情况下用户密钥被泄露的机会。解密到来的加密传输所需要的密钥可以从密钥基中导出。该方法将在下面使用图 4 进行更详细描述。

[0053] 如图 4 所示，处理从主机优选地在非易失性存储单元上存储一个密钥基开始(140)。该密钥基最好是一个用来产生另一个比特序列的随机比特序列。在本发明中，该密钥基用来产生一个密钥，它也是一个比特串。该密钥可以是在对称密码系统中使用的对称会话密钥或在公共密钥密码系统中使用的私有密钥。

[0054] 在密钥基已经被主机存储在非易失性存储单元之后，该主机然后在需要密钥来执行电子交易时运行一个产生密钥的单向函数 (141)。优选地该密钥不存储在该主机的任何非易失性存储单元中，因此该用户在任何时候都不能存取该密钥。但是，该密钥例如也可以暂时存储在随机访问存储器 (RAM) 中，这使得客户或任何其他人很难或甚至不可能通过访问该客户主机复制该密钥。

[0055] 单向函数是一种二输入的函数，这两个输入是密钥基和主机标识 (主机 ID)。主机 ID 优选地是驻留该主机的永久和唯一的标识符并且在无需不利地影响主机操作的情况下很难或不可能改变。大多电子主机装置当前包含一个由它的制造商产生并保存在该主机装置中的唯一电子主机 ID。该主机 ID 被保存在哪里以及如何访问它根据主机装置的制造和型号而异。但是，对于给定的任何特定主机装置，受益于本发明的本领域技术人员，将能够识别主机 ID 存储在哪里以及如何能够访问它以便供本发明的实施例使用。作为替换，主机 ID 可以由一个专用算法产生，该算法使主机 ID 基于从主机中收集的信息，其中所述信息定义和描述该主机的硬件和配置。

[0056] 在一些实施例中，得到主机 ID 和密钥基从而产生相应密钥的单向函数可以使用下面的常用命令来调用 :Key = KeyGen(Host ID,KeySeed)。该命令语法可以修改以适应期望的密钥管理协议的语言。

[0057] 如果函数 (F) 是不可逆的，那么它就可以说是单向的。换句话说，如果 F 的结果是 f，那么找到一个输入 x 使得 F(x) = f 在计算上是不可行的，这里 F(x) 意思是 F 是 x 的函数。在本发明的该实施例中，产生该密钥的函数是单向的事实意味着很难 (虽然不是不可能) 从该密钥中导出密钥基。例如，如果给定该密钥基和一个新的主机 ID 值，一个黑客可以得到该密钥基的相应新值，那么他或她可能导出用于许多未经授权主机的新密钥基。这些新的密钥基可以与它们的相应主机 ID 组合从而产生能够在电子交易中使用的有效密钥。但是，单向函数使得在给定一个密钥值和一个主机 ID 的情况下确定一个密钥基在计算上不可行。

[0058] 返回图 4，如果该主机具有一个正确的密钥基 (142) 和一个正确的主机 ID(143)，该函数可以产生能在电子通信中使用的一个有效密钥 (144)。但是，如果该密钥基或该主机 ID 是错的，那么该函数产生一个无效密钥 (145)。

[0059] 图 4 所示的密钥产生处理的示范应用是客户与网站在互联网上的交互。例如，如果一个客户从网站上预订按月付费内容，那么该网站操作员可以发送一个密钥基和一个密钥产生函数给该客户以安装在他或她的主机上。该函数把客户主机 ID 和密钥基看作输入。当需要时该函数询问主机它的 ID。如果正确的主机 ID 和密钥基没有准确地输入到该函数，那么该函数将不产生有效密钥。优选地该客户必须在他或她期望得到按月付费内容时运行该函数并且使用产生的密钥。因为该函数只对该客户主机 ID 和密钥基起作用，因此很难或不可能把该函数传送给一个具有不同主机 ID 的不同主机并在执行该函数时得到有效密钥。这是因为即使客户复制该密钥基和函数并且把他们分发给其他人，他们也不能产生有效密钥，因为他们的主机 ID 与被设计为对该主机 ID 起作用并提供有效密钥的函数的该主机 ID 不同。

[0060] 图 5 是说明当应用于公共密钥密码使用术系统中时本发明的一种示范方法的流程图。更具体地，图 5 说明能够用私有密钥基 (PKS) 初始地产生私有和公共密钥并且然后把该 PKS 存储在客户的非易失性存储单元中的方法。在该实施例中客户产生他或她自己的密钥对。一个密钥对优选地由一个私有和公共密钥组成。

[0061] 如图 5 中所示，客户初始地在他或她的主机上产生一个 PKS(150)。该 PKS 优选地由主机随机地产生。该客户然后使用一个单向函数从该 PKS(151) 中导出一个私有密钥，其中把 PKS 和主机 ID 作为对该函数的输入。

[0062] 该函数可以使用在采用公共密钥密码使用术的所选密钥管理协议中找到的命令来调用。协议实例是允许支持公共密钥密码使用术的具有 PKINIT 扩展的 Kerberos、互联网密钥交换 (IKE) 以及传输层安全性 (TLS)。可以结合这些函数使用的公共密钥算法的实例包括椭圆曲线数字签名算法 (ECDSA)、椭圆曲线 Diffie-Hellman(ECDH) 和椭圆曲线鉴别加密方案 (ECAES)。在基于椭圆曲线的算法的情况中，从 PKS 产生私有密钥的命令如下：“Private Key = PKGen(HostID, PKS)modulo Point-Order”。Point-Order 参数专用于椭圆曲线密码学。每个椭圆曲线对于 Point-Order 参数具有它自己的值。

[0063] 但是，本发明并不依赖于该 PKGen() 函数的选择。下面的常用命令调用从 PSK 产生私有密钥的函数：“Private Key = F(PKGen(HostID, PKS))”，这里函数 F 依赖于一个特定的公共密钥密码系统。该函数优选地足够快，以便在每次电子交易要求使用私有密钥时重新产生该私有密钥。

[0064] 返回图 5，在从 PKS 导出私有密钥 (151) 后，客户优选地从该私有密钥导出一个公共密钥 (152)。这可以通过使用对于密码使用术公知的各种数学函数来完成。然后把该公共密钥向一个受托管理机构登记 (153)。该受托管理机构通常称为发证机构 (CA)。

[0065] CA 返回给客户一个证明产生的公共密钥的有效性的证书或把该公共密钥存储在一个受托数据库中 (154)。这些证书是证明公共密钥和客户或其他实体绑定的数字文档。这些证书允许对一个特定的公共密钥实际上属于一个特定客户的声明的核查。他们有助于防止有人使用假冒的密钥冒充其他人。

[0066] 在他们最简单的形式中，这些证书包含一个公共密钥和一个名称。证书还可以包

含有效期、发证的 CA 的名称、序列号、证书颁发人的数字签名以及可能的其他信息。

[0067] CA 可以是愿意担保被授予证书的那些客户的身份以及它们与一个给定密钥的关联的任何受托集中管理机构。一个密钥分发中心 (KDC) 例如可以扩展为包括 CA 的功能。KDC 专用于密钥产生、核查和分发。

[0068] 如图 5 所示，在客户接收该证书或公共密钥被保存在受托数据库 (154) 后，客户主机把随机产生的 PKS 保存在非易失性存储单元中 (155)。该 PKS 现在可以用于产生私有密钥，该私有密钥可以在将来的电子交易中使用。

[0069] 图 6 是说明当应用于公共密钥密码系统时本发明的第二示范方法的流程图。更具体地，图 6 说明了一种方法，通过该方法客户优选地使用一个存储在非易失性存储单元中的随机产生的 PKS 来产生他或她可以在电子交易中使用的私有密钥。

[0070] 如图 6 所示，该处理从客户主机从非易失性存储单元读取 PKS 开始 (160)。使用用于初始产生私有密钥的同一函数，该客户基于所存储的 PKS 导出同样的私有密钥 (151)，其中该私有密钥用来产生公共密钥 (结合图 5 解释)。

[0071] 该客户现在优选地可以在电子交易中使用该私有密钥 (161)。如图 6 所示，如果该私有密钥与所登记的公共密钥正确相关 (162)，该服务器和客户就可以使用该私有密钥和公共密钥对来完成该电子交易 (163)。另一方面，如果该私有密钥与所登记的公共密钥不能正确相关，那么该电子交易失败 (164)。

[0072] 图 7 是说明当应用于对称会话密码系统时本发明的一种示范方法。更具体地，图 7 说明了一种方法，通过该方法一个客户优选地接收、存储并使用对称会话密钥基 (SKS) 以产生可以用来进行电子交易的对称会话密钥。在该实施例中的客户优选地产生与客户期望与之进行交易的服务器使用的密钥相一致的密钥。

[0073] 如图 7 所示，处理由客户从 KDC 或其他源接收 SKS 开始 (170)。不像在结合图 5 所描述的公共密钥密码系统中使用的处理，该客户优选地不产生将用于产生密钥的密钥基。取而代之的是，该 KDC 发送 SKS 给该客户。

[0074] 在该客户主机从该 KDC 接收该 SKS 之后，该主机把该 SKS 存储在非易失性存储单元中 (171)。然后，为了进行电子交易，该客户从该非易失性存储单元读取该 SKS(172) 并且通过在该主机上运行单向函数从该 SKS 导出对称会话密钥 (173)，其中该 SKS 和主机 ID 作为对该函数的输入。该单向函数优选地是由 KDC、服务器或其他源发送给该客户并且安装在该用户主机上的一个程序。

[0075] 可以使用在所选的密钥管理协议中找到的命令调用该函数。从 SKS 产生对称会话密钥的通用命令如下“Symmetric SessionKey = SKGen(Host ID, SKS)”。但是，该函数调用命令的语法可以根据所选的密钥管理协议而异。该函数优选地足够快，以便在每次电子交易要求使用对称会话密钥时重新产生该对称会话密钥。

[0076] 该客户现在优选地可以在与一个服务器的电子交易中使用导出的对称会话密钥 (174)，该服务器也使用对称会话密钥。服务器如何得到与客户使用的密钥相同的对称会话密钥有各种可能的方法。一种方法是 KDC 执行与该主机所执行的函数相同的单向函数并且从 SKS 产生该会话密钥。该方法要求 KDC 能够访问或复制客户主机的 ID。该 KDC 然后可以发送所产生的对称会话密钥给该服务器。作为替换，如在 Kerberos 协议的情况，该 KDC 可以采用对称会话密钥并且使用服务器使用的对称会话密钥来加密它，服务器使用的对称会

话密钥对于任何客户都是未知的。该加密的对称会话密钥与客户和服务器身份以及其他相关的信息一起称为证明书(ticket)。该证明书然后被发送给该客户主机。主机不能修改该证明书,因为它不知道服务器的对称会话密钥。该客户然后可以发送该证明书给该服务器。该服务器然后使用它的密钥对该证明书解密并且提取该会话密钥的副本。

[0077] 返回图 7,如果该客户对称会话密钥与该客户期望与之完成电子交易的服务器使用的对称会话密钥匹配 (175),该服务器和客户可以使用该对称会话密钥完成该电子交易(163)。另一方面,如果所导出的对称会话密钥与该服务器的对称会话密钥不匹配,那么该电子交易失败 (164)。

[0078] 前面给出的说明只是为了说明和描述本发明。并不意味着穷举或把本发明限制到所公开的任何精确形式。根据上面的教导可以有许多修改和变形。

[0079] 选择并描述优选的实施例,是为了最好地解释本发明原理以及它的实际应用。前面的描述能促使本领域技术人员以各种实施例和用适于所能想象的特定使用的各种修改最好地利用本发明。这意味着本发明的范围只受下面的权利要求的限定。

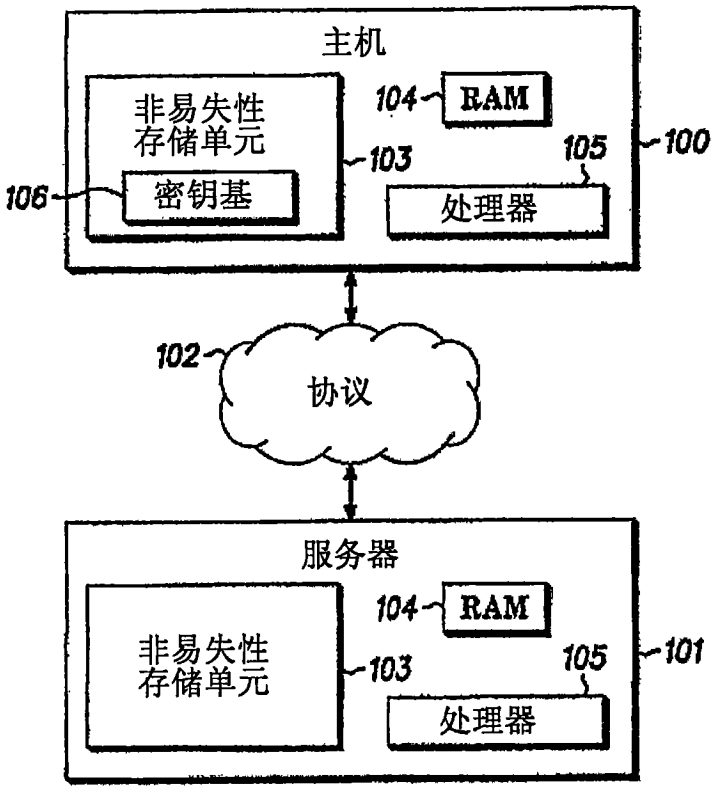

主机
非易失性
存储单元
104
RAM
103
105
100
106
密钥基
处理器
102
协议
服务器
非易失性
存储单元
104
RAM
103
105
101
处理器

图 1

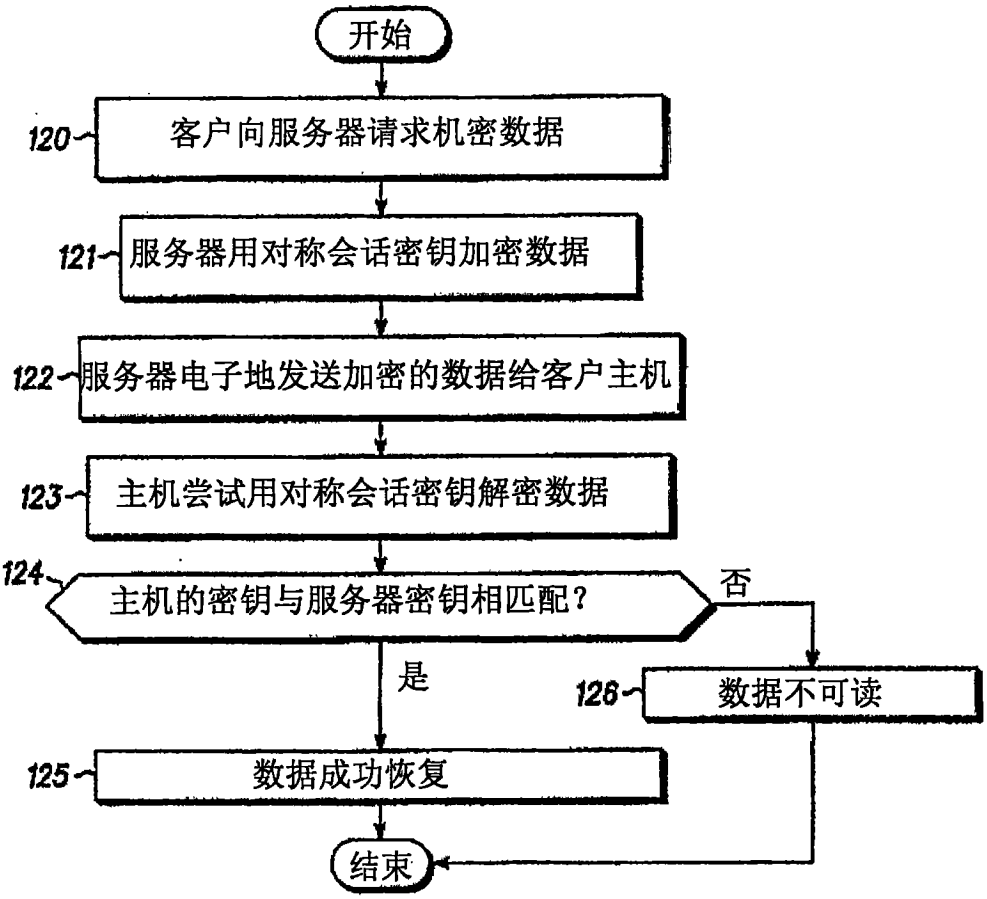

开始
120
客户向服务器请求机密数据
121
服务器用对称会话密钥加密数据
122
服务器电子地发送加密的数据给客户主机
123
主机尝试用对称会话密钥解密数据
124
主机的密钥与服务器密钥相匹配？
否
是
126
数据不可读
125
数据成功恢复
结束

图 2

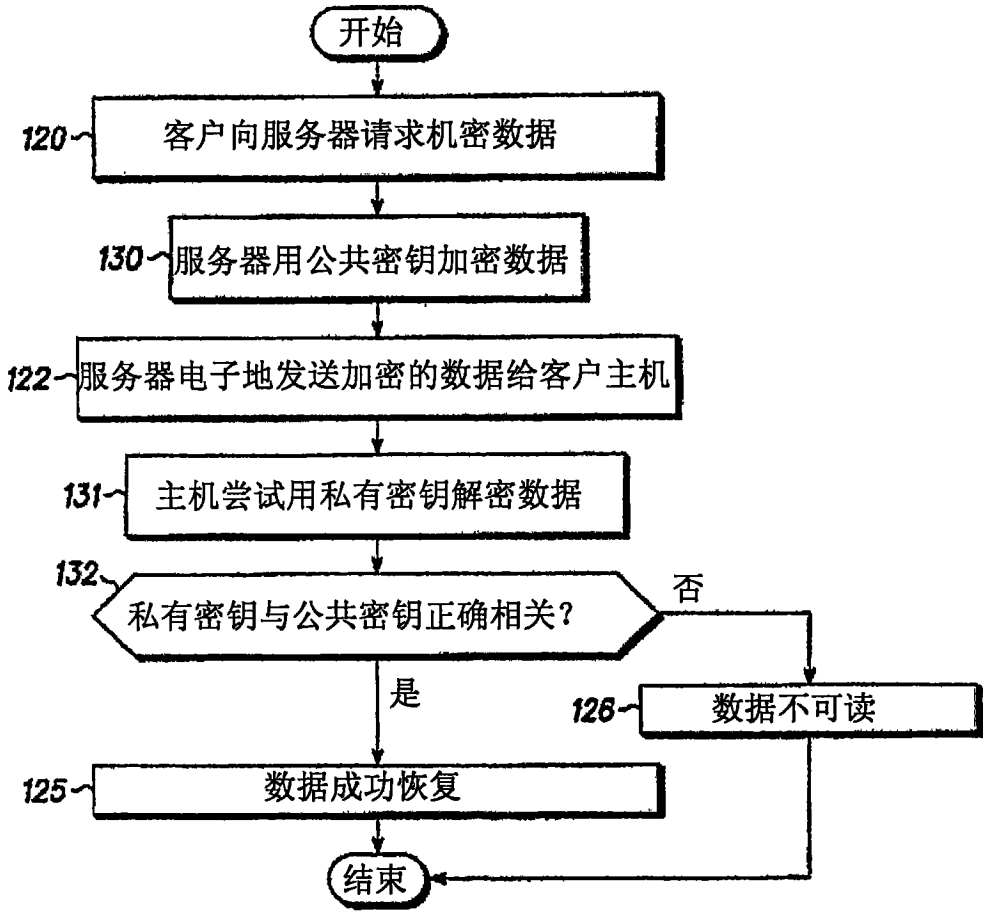

开始
120
客户向服务器请求机密数据
130
服务器用公共密钥加密数据
122
服务器电子地发送加密的数据给客户主机
131
主机尝试用私有密钥解密数据
132
私有密钥与公共密钥正确相关?
否
是
126
数据不可读
125
数据成功恢复
结束

图 3

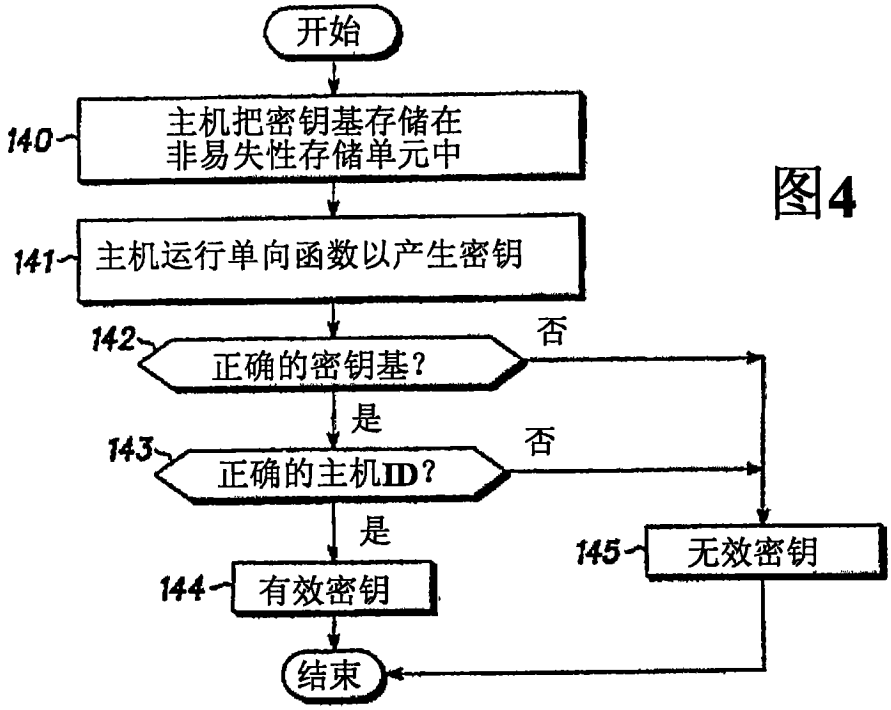

开始
140
主机把密钥基存储在非易失性存储单元中
141
主机运行单向函数以产生密钥
142
正确的密钥基?
否
是
143
正确的主机ID?
否
是
145
无效密钥
144
有效密钥
结束

图4

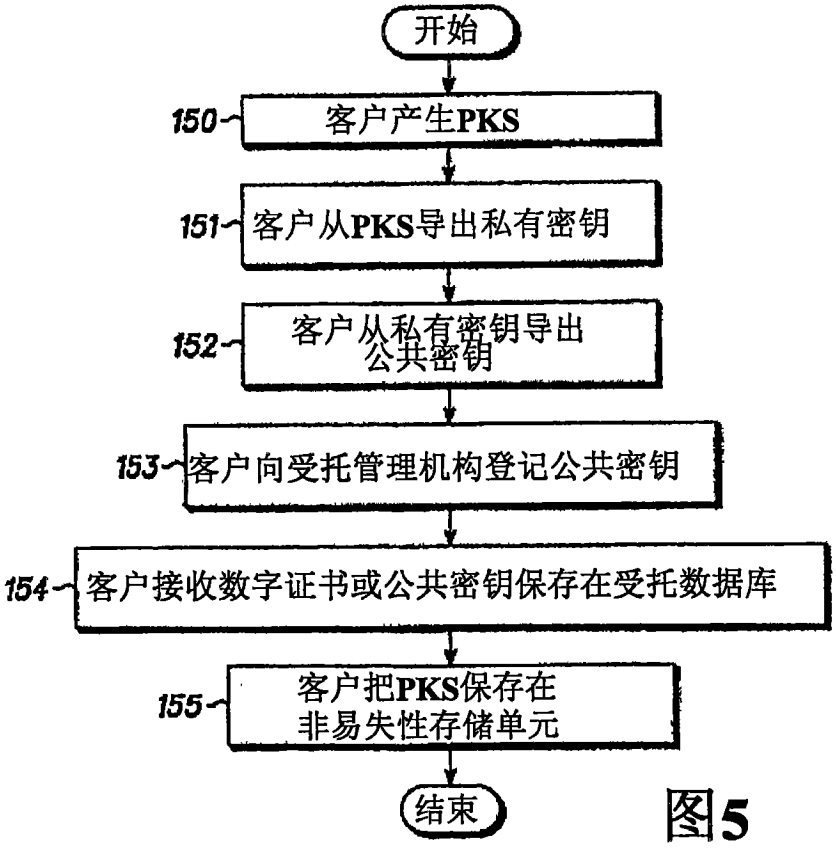

开始
150
客户产生PKS
151
客户从PKS导出私有密钥
152
客户从私有密钥导出公共密钥
153
客户向受托管理机构登记公共密钥
154
客户接收数字证书或公共密钥保存在受托数据库
155
客户把PKS保存在非易失性存储单元
结束

图5

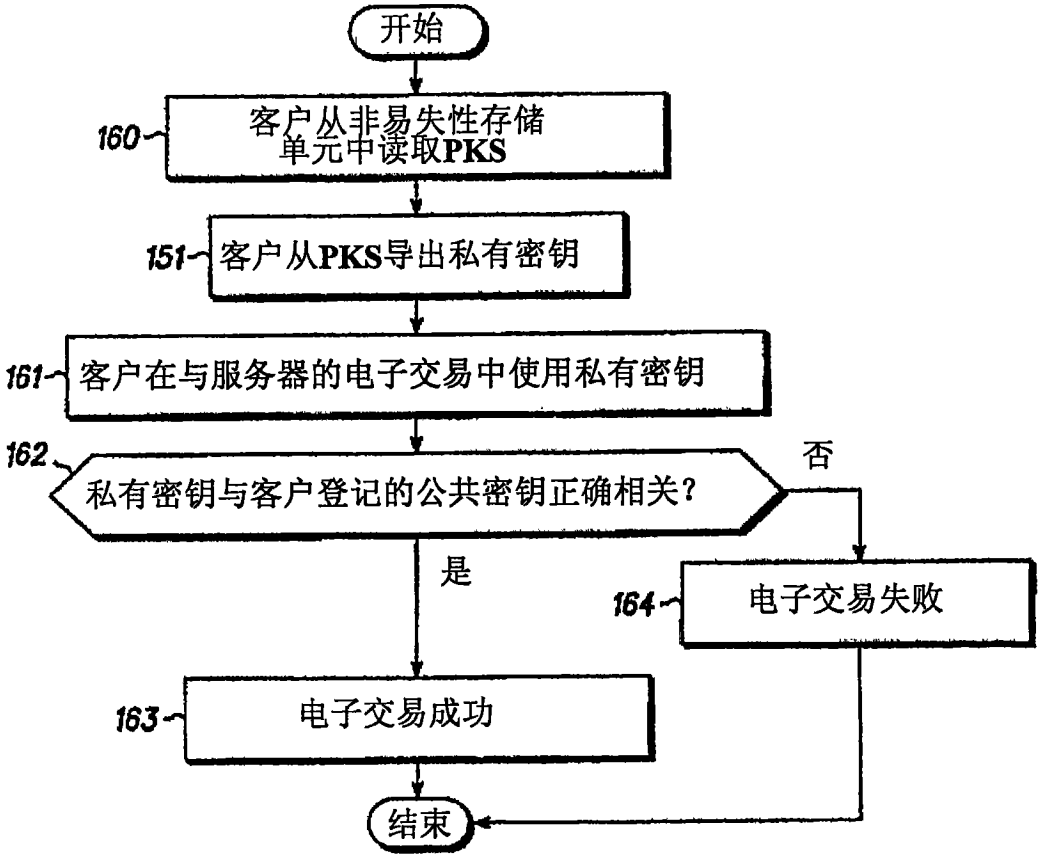

开始
160
客户从非易失性存储单元中读取PKS
151
客户从PKS导出私有密钥
161
客户在与服务器的电子交易中使用私有密钥
162
私有密钥与客户登记的公共密钥正确相关?
否
是
164
电子交易失败
163
电子交易成功
结束

图 6

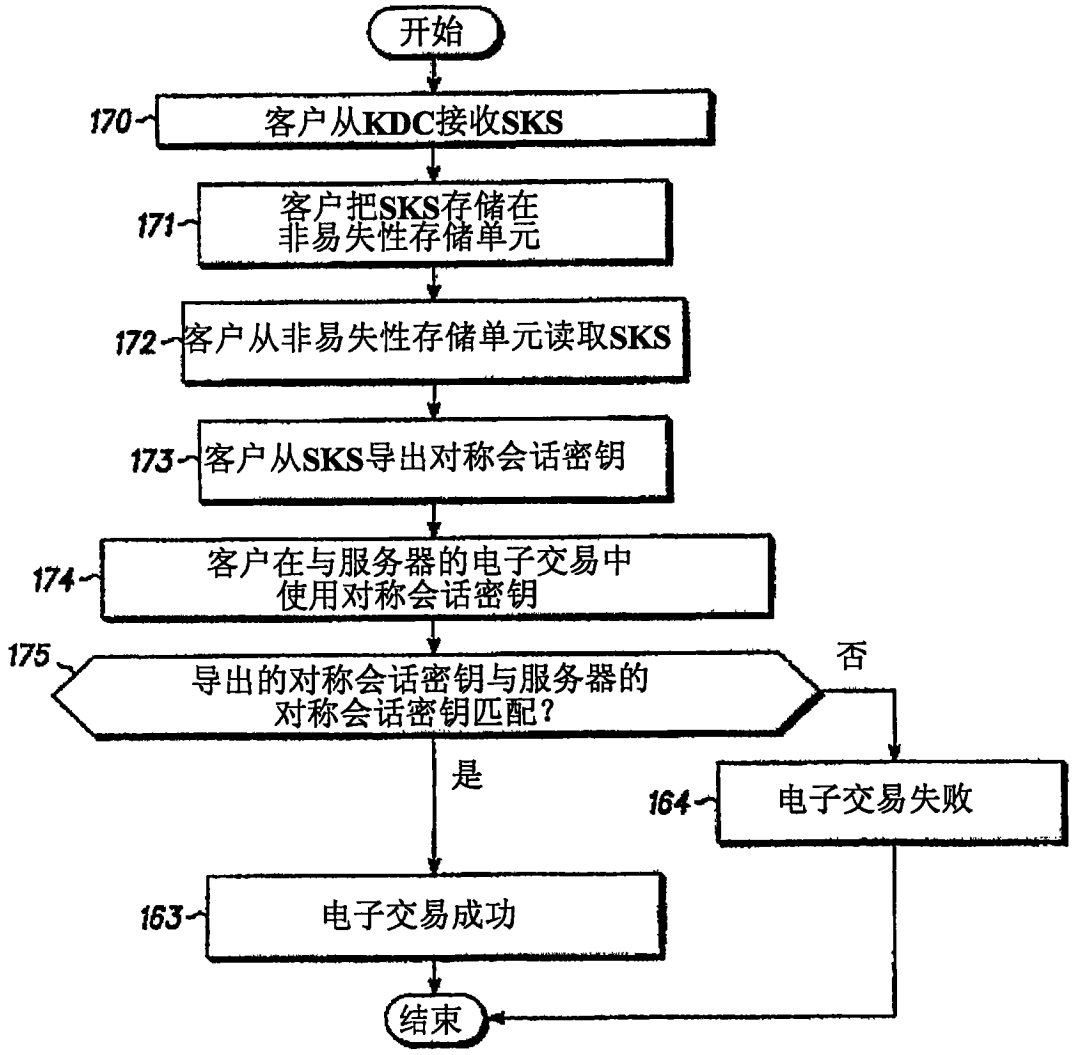

开始
170
客户从KDC接收SKS
171
客户把SKS存储在非易失性存储单元
172
客户从非易失性存储单元读取SKS
173
客户从SKS导出对称会话密钥
174
客户在与服务器的电子交易中使用对称会话密钥
175
导出的对称会话密钥与服务器的对称会话密钥匹配?
否
是
164
电子交易失败
163
电子交易成功
结束

图 7