



[12] 发明专利申请公开说明书

[21] 申请号 200510076248.7

[43] 公开日 2005 年 11 月 16 日

[11] 公开号 CN 1697367A

[22] 申请日 2005.3.30

[21] 申请号 200510076248.7

[30] 优先权

[32] 2004.4.2 [33] US [31] 10/816,756

[71] 申请人 微软公司

地址 美国华盛顿州

[72] 发明人 A·百克 B·德哈马拉简

D·I·图恩切瓦 K·W·查恩

R·S·纽瓦斯卡

[74] 专利代理机构 上海专利商标事务所有限公司

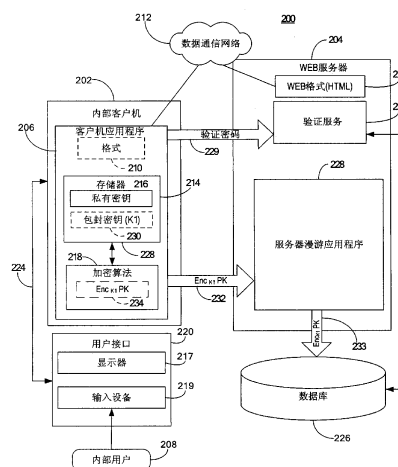
代理人 李 玲

权利要求书 6 页 说明书 16 页 附图 13 页

[54] 发明名称 一种用于通过通信网络不暴露专用数据对密码保护的专用数据进行恢复的方法和系统

[57] 摘要

一种用于将专用数据安全地从第一客户计算机漫游至通过通信网络相联的第二客户计算机的系统和方法。第一客户计算机的用户执行本地客户应用程序并且为了漫游对专用数据进行标识。本地客户机应用程序响应密码,生成第一密钥,并利用第一密钥对标识的专用数据进行加密。服务器接收并存储该加密专用数据。第二计算机的用户执行漫游客户机应用程序并请求从服务器传送加密专用数据。漫游客户机应用程序响应密码,生成第一密钥,并对服务器发送来的加密专用数据进行解密,进而得到专用数据。本发明进一步使得用户即使是在忘记了与第一密钥相关的密码的情况下,也能够重新获得来自于服务器的加密专用数据。并且,服务器并不知道专用数据,也不知道密钥。



1、一种在与数据通信网络相耦合的计算机之间，进行专用数据通信的方法，所述方法包括：

- 5 在网络服务器上，接收由第一客户机利用服务器未知的包封密钥进行加密的专用数据，所述服务器和所述第一客户机耦合到数据通信网络上；
 将接收到的加密专用数据存储在数据库中；
 在服务器上，接收来自第二客户机的用于加密专用数据的请求；
 响应接收到的请求，将加密专用数据从服务器发送至第二客户机，以利用包
10 封密钥对该数据进行解密。

2、如权利要求1所述的方法，其中接收加密专用数据包括接收加密私有密钥，所述加密私有密钥代表与第一客户机相关并且利用包封密钥进行加密的私有密钥，响应从第一客户机的用户接收的加密密码，在第一客户机中生成所述包封密钥。

- 15 3、如权利要求2所述的方法，进一步包括在第二客户机中利用包封密钥对加密专用数据进行解密，响应由第二客户机的用户接收的加密密码，在第二客户机中生成所述包封密钥。

4、如权利要求2所述的方法，进一步包括：

- 在服务器上，接收由第一客户机利用服务器未知的恢复密钥进行加密的包封
20 密钥，响应由用户选择的恢复选项，在第一客户机中生成所述恢复密钥；
 在服务器上，接收由第一客户机利用包封密钥进行加密的恢复密钥。

5、如权利要求4所述，进一步包括：

- 响应接收到的来自于第一客户机的加密专用数据，在服务器上生成备份密
 钥；
25 将生成的备份密钥存储在与服务器相连的数据库中；
 响应接收到的来自第一客户机的用户的恢复请求，重新得到存储的备份密
 钥；和

- 响应收到的恢复请求，通过数据通信网络，将备份密钥从服务器发送至第一
 客户机，所述第一客户机生成的备份加密恢复密钥代表利用发送的备份密钥进行
30 加密的恢复密钥存储在所述第一客户机中，所述备份密钥是服务器知道的。

6、如权利要求5所述的方法，进一步包括响应接收到的恢复请求，将加密私有密钥和加密包封密钥从服务器发送至第一客户机，在第一客户机中，利用发送的备份密钥对存储在所述第一客户机中的所述备份加密恢复密钥进行解密，从而获得恢复密钥，在第一客户机中，利用获得的恢复密钥对所述加密包封密钥进行解密，以得到包封密钥，以及在第一客户机中，利用获得的包封密钥对所述加密私有密钥进行解密，以得到私有密钥。

7、如权利要求5所述的方法，进一步包括响应接收到的来自第二客户机的用户的备份请求，向第二客户机发送加密恢复密钥和备份密钥，在第二客户机中，利用由第二客户机生成的包封密钥对所述发送来的加密恢复密钥进行解密，以得到恢复密钥，所述第二客户机利用发送来的备份密钥对得到的恢复密钥进行加密，以生成备份加密恢复密钥并存储在与第二客户机相连的存储器中。

8、如权利要求5所述的方法，进一步包括：

响应接收到的来自第二客户机的用户的恢复请求，重新获得已存储在与服务器相连的数据库中的备份密钥；和

响应接收到的恢复请求，将备份密钥从服务器发送至第二客户机。

9、如权利要求5所述的方法，进一步包括响应接收到的来自第二客户机的恢复请求，通过数据通信网络将加密私有密钥和加密包封密钥从服务器发送至第二客户机，在第二客户机中，利用发送来的备份密钥对存储在第二客户机中的所述备份加密恢复密钥进行解密，以获得恢复密钥，在第二客户机中，利用获得的恢复密钥对所述加密包封密钥进行解密，以及在第二客户机中，利用获得的包封密钥对所述加密私有密钥进行解密，以获得私有密钥。

10、如权利要求1所述的方法，其中第二客户机是与数据通信网络耦合的漫游客户计算机。

11、具有用于执行权利要求1的方法的计算机执行指令的一个或多个计算机可读媒介。

12、一种用于在数据通信网络中进行专用数据通信的系统，包括：

接收由第一客户机利用服务器未知的包封密钥进行加密的专用数据的服务器，所述服务器和所述第一客户机耦合到数据通信网络上；

与服务器相连的数据库，所述服务器被设置为将接收到的加密专用数据存储在数据库中，以及将已存储的加密专用数据发送至也耦合到数据通信网络上的第

二客户机，从而利用包封密钥对其进行解密，以响应对从第二客户机接收的加密专用数据的请求。

13、如权利要求 12 所述的系统，其中加密专用数据包括与第一客户机相关并利用包封密钥进行加密的私有密钥，响应接收到的来自第一客户机的用户的加密密码，在第一客户机中生成所述包封密钥。

14、如权利要求 13 所述的系统，其中第一客户机被设置为在第一客户机中生成包封密钥，利用生成的包封密钥加密专用数据，以及生成恢复密钥并存储在所述第一客户机中。

15、如权利要求 13 所述的系统，其中第二客户机被设置为在第二客户计算机中生成包封密钥和利用第二客户机中生成的包封密钥对发送来的加密专用数据进行解密，其中所述以响应接收到的来自第二客户机的用户的加密密码，在第二客户计算机中生成所述包封密钥。

16、如权利要求 15 所述的系统，进一步包括执行服务器应用程序的计算机可读指令，其中服务器响应接收到的来自第一客户计算机的用户的存储请求，执行服务器应用程序以将接收到的加密数据存储在数据库中，生成备份密钥并将其存储在数据库中的计算机可读指令，以及将生成的备份密钥发送给第一客户计算机的计算机可读指令，第一客户计算机利用所述备份密钥来生成第二加密恢复密钥，并存储在所述第一客户计算机中。

17、如权利要求 16 所述的系统，其中备份密钥是由服务器随机生成的，以响应接收来自于第一客户机的加密专用数据。

18、如权利要求 17 所述的系统，其中接收到的加密专用数据包括加密私有密钥，它代表与第一客户机相关并利用包封密钥进行加密的私有密钥，加密包封密钥，它代表利用恢复密钥进行加密的包封密钥，以及第一加密恢复密钥，它代表利用包封密钥进行加密的恢复密钥。

19、如权利要求 18 所述的系统，其中服务器进一步设置成响应接收到的来自第二客户机的备份请求，将第一加密恢复密钥和备份密钥发送至第二客户机，所述备份密钥包括定义的备份密码，利用第二客户机中生成的包封密钥在第二客户机中对发送来的所述第一加密恢复密钥进行解密，以获得恢复密钥，利用发送来的备份密钥对已获得的所述恢复密钥进行加密，进而生成第二加密恢复密钥并将其存储在与第二客户计算机相连的存储器中。

20、如权利要求 19 所述的系统，其中服务器进一步被设置为响应接收到的来自第二客户计算机的恢复请求，将加密私有密钥，生成的备份密钥和加密包封密钥发送至第二客户机，其中在第二客户机中利用发送的备份密钥对存储在与第二客户计算机相连的存储器中的第二加密恢复密钥进行解密，进而得到恢复密
5 钥，在第二客户机中，利用获得的恢复密钥对发送来的所述加密包封密钥进行解密，进而得到包封密钥，在第二客户机中，利用获得的包封密钥对发送来的所述加密私有密钥进行解密，进而得到私有密钥。

21、一种计算机可读媒介，包括计算机执行指令，用于在与数据通信网络相耦合的计算机之间进行专用数据通信，所述计算机可读媒介包括：

10 第一接收指令，用于在网络服务器上，接收由第一客户机利用服务器未知的包封密钥进行加密的专用数据，所述服务器和所述第一客户机耦合到数据通信网络上；

存储指令，用于将接收到的加密专用数据存储在服务器中；

15 第二接收指令，用于在服务器上，接收来自第二客户机的用于加密的专用数据的请求；和

发送指令，用于响应接收到的请求，将加密专用数据从服务器发送至第二客户机，进而利用包封密钥进行解密。

22、如权利要求 21 所述的计算机可读媒介，其中第一接收指令包括用于接收加密私有密钥 ($E_{k1}PK$) 的指令，该密钥代表与第一客户机相关并利用包封密
20 钥进行加密的私有密钥，响应接收到的来自第一客户机的用户的加密密码，在第一客户机中生成所述包封密钥。

23、如权利要求 22 所述的计算机可读媒介，其中发送指令包括用于发送加密私有密钥的指令，在第二客户机中，利用包封密钥对所述加密私有密钥进行解密，响应接收到的来自第二客户机的用户的加密密码，在第二客户机中生成所述
25 包封密钥。

24、如权利要求 22 所述的计算机可读媒介，其中第一接收指令进一步包括在服务器上，用于接收由第一客户机利用服务器未知的恢复密钥进行加密的包封
30 密钥的指令，响应用户通过第一客户机作出的恢复选择，在第一客户机中生成所述恢复密钥，并且在服务器上，接收由第一客户机利用包封密钥进行加密的恢复密钥。

25、一种在与数据通信网络相耦合的计算机之间进行专用数据通信的方法，所述方法包括：

在服务器上，接收来自漫游客户机的针对加密的专用数据的请求，所述请求包括验证密码的纲要或散列值，所述服务器和所述漫游客户机都与数据通信网络
5 耦合；

确定接收到的来自于漫游客户机的验证密钥的格式是否有效；

当验证密码的格式是有效的，则重新获得加密专用数据，利用服务器未知的加密密码预先对所述专用数据进行加密；

将重新获得的加密专用数据从服务器发送至漫游客户机，进而利用包封密钥
10 进行解密。

26、如权利要求 25 所述的方法，其中重新获得加密专用数据的过程包括重新获得加密私有密钥，所述加密私有密钥代表与本地客户机相关并利用包封密钥进行加密的私有密钥，响应接收到的来自漫游客户机的用户的加密密码，在本地客户机中生成所述包封密钥。

15 27、如权利要求 26 所述的方法，进一步包括利用包封密钥在漫游客户机上对发送来的加密私有密钥进行解密，响应接收到的来自漫游客户机的用户的加密密码，在漫游客户机中生成所述包封密钥。

28、如权利要求 27 所述的方法，进一步包括：

重新获得由漫游客户机利用服务器未知的恢复密钥进行加密的包封密钥，响
20 应用户通过本地客户机作出的恢复选择，在本地客户机中生成所述恢复密钥；

重新获得由本地客户机利用包封密钥进行加密的恢复密钥；

在漫游客户机上，利用漫游客户机中生成的包封密钥，对加密恢复密钥进行解密，进而获得恢复密钥；

响应接收到的来自漫游客户机的用户的备份请求，重新获得已存的备份密
25 钥，响应接收来自于本地客户机的加密专用数据，在服务器中生成所述的备份密钥；

响应接收到的恢复请求，通过数据通信网络以安全的方式将备份密钥从服务器发送至漫游客户机，所述漫游客户机利用重新得到的备份密钥对得到的恢复密钥进行加密；和

30 在漫游客户机中，存储备份加密恢复密钥，该密钥代表利用发送来的备份密

钥进行加密的恢复密钥。

29、如权利要求 28 所述的方法，进一步包括：

响应接收到的来自漫游客户机的用户的恢复请求，重新获得已存储的备份密钥，响应接收到的来自于本地客户机的加密专用数据，在服务器中生成所述的备份密钥；

响应接收到的恢复请求，通过数据通信网络以安全的方式将备份密钥从服务器发送至漫游客户机，所述漫游客户机对备份加密的恢复密钥进行解密，进而获得恢复密钥。

30、如权利要求 29 所述的方法，进一步包括响应接收到的恢复请求，将加密私有密钥和加密包封密钥从服务器发送至漫游客户机，在漫游客户机上，利用得到的恢复密钥对所述加密包封密钥进行解密，以获得包封密钥，以及在漫游客户机上，利用得到的包封密钥对所述加密私有密钥进行解密，以获得私有密钥。

31、一种计算机可读媒介，具有存储在其中的数据结构，该媒介包括：

包含专用数据的第一数据字段；

包含密钥数据的第二数据字段，该密钥代表接收到的来自于用户的输入数据流；和

第三功能字段，用于利用密钥数据对专用数据进行加密以及将加密的专用数据发送至中央位置进行存储。

32、如权利要求 31 所述的计算机可读媒介，其中加密专用数据包括加密私有密钥，所述加密私有密钥代表与本地客户机相关并利用包封密钥进行加密的私有密钥，响应接收到的来自本地客户机的用户的加密密码，在本地客户机中生成所述的包封密钥。

一种用于通过通信网络不暴露
专用数据对密码保护的专用数据进行恢复的方法和系统

5

技术领域

本发明涉及计算机网络环境领域。特别是，本发明涉及一种对通过通信网络连接的一个或多个用户计算机之间的漫游专用数据进行备份和恢复的系统和方法。

10

发明背景

Web 服务例如因特网网站经常为它们的用户提供信息，产品，服务等。但是网络安全已成为用户和 Web 服务所共同关心的一个主要问题，特别是在发送敏感信息的情况下。通常通过加密处理来为用户和/或 Web 服务提供信息安全。例如，公开密钥基础结构（PKI）和公开密钥密码系统是用于通信安全的公知的
15 密钥管理服务。这些服务通常作为必须进行安全存储以确保私密性的私有密钥仅用于个人计算机上。因此希望能够漫游，备份和恢复私有密钥。

当用户忘记初始密码时，现有的私有密钥漫游协议不能够实现端对端的安全关联以及数据的恢复。因此，当想要实现用户数据和用户通信的机密性，私密性，完整性和可靠性的情况下，就希望存在一个用于漫游私有用户数据的系统。

20

发明概述

本发明涉及在通过通信网络连接的一个或多个客户机之间的私有信息的增强漫游。特别是，在服务器不知道或未接收到私有信息的情况下，本发明使得用户能够漫游在与服务器相连的客户机之间的私有信息。而且，即使是在用户忘记了与私有密钥的加密相关联的密码的情况下，本发明使得用户能够恢复来自于服
25 务器的私有密钥的加密版本用于在用户端解密。通过使用该用户能够漫游在用户之间的私有信息以及隐藏这种来自于服务器的信息，网络的安全性能得到了显著增强，并且从而明显地削弱了恶意用户干扰安全通信的能力。

根据本发明的另一方面，提供了一种在与数据通信网络相耦合的计算机之间进行专用数据通信的方法。该方法包括在网络服务器上，接收由第一客户机利用
30 对服务器来说是未知的包封密钥而加密的私有数据。服务器和第一客户机耦合到

数据通信网络上。该方法进一步包括在服务器上对接收到的加密专用数据进行存储。该方法还包括在服务器上,接收第二客户机用于加密专用数据所发出的请求。该方法进一步包括响应接收到的请求,由服务器向第二客户机发送该加密的专用数据用于解密,利用包封密钥对其进行解密。

- 5 依照本发明的另一方面,提供一个系统,用于在数据通信网络中进行专用数据通信。服务器接收由第一客户机利用对服务器来说是未知的包封密钥进行加密的专用数据。服务器和第一客户机耦合到数据通信网络上。数据库与服务器相连接。服务器被设置为在数据库中存储接收到的加密的专用数据。服务器还被设置为响应从第二客户机接收的加密专用数据的请求,向耦合到数据通信网络上的第二客户机发送存储的加密的专用数据,从而利用包封密钥对该数据进行解密。

- 依照本发明的另一方面,提供了一个具有计算机执行指令的计算机可读媒介,该指令用于在与数据通信网络相耦合的计算机之间进行专用数据通信。在网络服务器上,第一接收指令接收由第一客户机利用服务器未知的包封密钥加密的专用数据。服务器和第一客户机耦合到数据通信网络上。存储指令在服务器上对接收到的加密专用数据进行存储。在服务器上,第二接收指令接收来自第二客户机用于加密的专用数据的请求。传送指令响应接收到的请求,从服务器向第二客户机发送加密专用数据,从而利用包封密钥对该数据进行解密。

- 仍依照本发明的另一方面,提供了一种方法,用于在与数据通信网络耦合的计算机间进行专用数据通信。该方法包括在服务器上,接收来自漫游客户机的用于加密专用数据所请求。该请求包括验证密码的纲要或散列值。服务器和漫游客户机耦合到数据通信网络上。该方法进一步包括确定来自于漫游客户机的验证密码的格式是否有效。该方法进一步包括当验证密钥的格式是有效的,重新获得加密的专用数据,其中先前利用服务器未知的加密密码对专用数据进行加密。该方法进一步包括从服务器向漫游客户机发送重新获得的加密专用数据,从而利用包封密钥进行解密。

依照本发明的另一方面,提供了一种具有其中存有数据结构的计算机可读媒介。第一数据字段包括专用数据。第二数据字段包括表示来自于用户的输入数据流的密钥数据。第三数据字段利用密钥数据对专用数据进行加密,并且将加密的专用数据发送给中心位置进行存储。

- 30 选择的,本发明可以包含其它多个方法和装置。

在下文中，将部分的显现和部分的指出其它特征。

附图简要说明

图 1 示出了能够应用本发明的示范性网络环境模块图。

图 2 根据本发明的一个实施例，示出了一个用于在本地客户机和服务器之间
5 通信加密的专用数据的系统模块图。

图 3 根据本发明的一个实施例，示出了一个用于在漫游客户计算机和服务器之间通信加密的专用数据的系统模块图。

图 4 根据本发明的一个实施例，示出了一个用于在本地客户机和服务器之间进行加密的专用数据通信和数据恢复的系统模块图。

10 图 5 根据本发明的一个实施例，示出了一个用于从服务器到漫游客户机，进行恢复数据通信的系统模块图。

图 6 根据本发明的一个实施例，示出了一个无需加密密码就能够从服务器到漫游客户机，进行加密专用数据恢复的系统模块图。

图 7 根据本发明的一个实施例，示出了在本地客户机和服务器之间进行专用
15 数据通信的方法的示意性流程图。

图 8 根据本发明的一个实施例，示出了从服务器到漫游客户机，进行加密的专用数据通信的方法的示意性流程图。

图 9A 和 9B 根据本发明的一个实施例，示出了在服务器和本地客户机之间进行加密的专用数据通信和恢复的方法的示意性流程图。

20 图 10 根据本发明的一个实施例，示出了在服务器和漫游客户机之间进行恢复数据的通信的方法的示意性流程图。

图 11 根据本发明的一个实施例，示出了无需加密密码而恢复从服务器到漫游客户机的加密的专用数据的方法的示意性流程图。

图 12 示出了能够实现本发明的适合的计算机系统环境的模块图。

25 相应的参考标记指示了整个附图的相应部分。

具体实施例的描述

现在参见图 1，一台内部或本地计算机 102 耦合到数据通信网络 104 上。在这个例子中，网络 104 是因特网（或环球网）。然而，本发明的教导能够适用于任何数据通信网络。多台漫游或远程客户计算机 106 和 108 也耦合到网络 104 上。

30 反过来，本地客户计算机 102 能够通过网络 104 与漫游客户计算机 106 和 108 进

行通信。本地客户计算机 102 表示用户有理由相信的计算机，因为没有信誉的第三方无法自由地或轻易地对其进行物理访问。漫游客户计算机 106 和 108 表示用户不完全相信的计算机，因为其属于第三方或由第三方进行物理控制。一个验证服务器 110 耦合到网络 104 上以允许在其自身以及内部客户计算机 102 和漫游客户计算机 106 和 108 之间进行通信。尽管将其称为“验证服务器”，但是该实施例中的验证服务器仅是一个能够对用户进行验证以及能够与 web 浏览器和其它 web 服务器相连接的 web 服务器。

在这个例子中，通过应用安全套接层（SSL）和因特网中常用的实现信息安全交换的协议，在验证服务器 110，客户机计算系统 102 和漫游客户计算机 106 和 108 之间进行安全的数据通信。更特别地，SSL 能够用于实现公开密钥加密。如本领域技术人员所知，公开密钥加密包括以这种方式对信息进行编码，该方式为只有具有私有密钥的人（或计算机）能够对其进行解码。当今所使用的计算机加密系统包括：对称密钥加密和公开密钥加密。

在对称密钥加密中，每台计算机具有一个保密密钥（或密码），用于在发送数据包到另外一个计算机之前，对该数据包进行加密。对称密钥需要你将要通信的是哪台计算机，以便在每一台计算机上安装一个密钥。为了成功地执行这种加密类型，计算机必须知道其保密密码以便对信息进行解码。

在公开密钥加密中，将私有密钥和公开密钥进行组合用于编码和解码信息。例如，特定的发端计算机（如本地客户机）安全地向具有公开/私有密钥对的漫游客户机（如漫游客户机）发送信息。在对该信息进行数学运算的过程中，该发端计算机利用漫游客户机的公开密钥产生加密消息，并用其私有密钥对这个消息进行标识以确保消息的完整性。该发端计算机还向漫游客户机提供它自己的公开密钥，但是对该发端计算机来讲私有密钥仍是其私有的（如保密的）。为了解码加密消息，接收者必须利用它自己的私有密钥和由发送者提供的公开密钥来验证该消息的签名。因此，如果接收者，本地客户机的用户 102，想要通过漫游客户机 106 和 108 对加密消息进行解码，该用户不得不向这些漫游客户机传送其私有密钥。

验证数据库 112 耦合到验证服务器 110 上，并且包含对客户计算机系统（和因特网中的其它用户）的用户进行验证时所必需的信息，和确定是内部客户计算机的用户还是漫游客户计算机有权存储数据库中的加密数据和/或接收来自于数

数据库 112 的加密数据时所必需的信息。

现在参见图 2，根据发明的一个实施例，模块图示出了用于对在本本地客户机 202（如本地客户计算机 102）和 web 服务器 204（如验证服务器 110）之间的加密的专用数据进行通信的系统。

5 本地客户机应用程序 206 允许本地用户 208 加密专用数据以及通过通信网络 212（如网络 104）将加密的专用数据传送至 web 服务器 204。通过本地客户机 202 来执行该本地客户机应用程序 206 并且响应用户输入来启动专用数据的加密，以及将加密的专用数据发送至 web 服务器 204。在这个实施例中，本地客户机应用程序 206 包括存储如图 1 所述的公开密钥加密进程中所使用的私有密钥
10 216 的存储器 214。本地客户机应用程序 206 包括用于在专用数据上执行数学运算以将其转换为加密专用数据的加密算法。更加特别的是，该加密算法 218 用于和密钥数据一起对专用数据进行转换。如本领域技术人员所知，许多加密算法（如 3DES 和 HMAC-RC4）用于对数据进行加密，如此在不知道加密密钥的情况下对相关内容进行解密几乎是不可能的。

15 本地客户机 202 的用户 208 可能希望能够漫游私有密钥 216 从而通过一个或多个漫游客户机（如漫游客户机 106，108）与 web 服务器进行安全地通信。但是，这种私有密钥 216 的漫游能够导致该私有密钥 216 被恶意方截取。结果，实质上削弱了用户 208 用特定密钥 216 安全地解密和标识数据的能力。

与本地客户机 202 相连的用户接口（UI）220 允许用户 208 访问 web 服务器
20 204。例如，UI 214 可以包括显示器 217，如用于观察数据和/或输入格式的计算机监视器，以及输入设备 219，如用于以该输入格式（未示出）输入数据的键盘或指示设备（如，鼠标，轨迹球，或触摸屏）。换句话说，UI 214 允许用户 208 选择本地客户机 210 中的数据进行加密，并且允许用户 208 提交请求以将来自于本地客户机 210 的加密数据发送至 web 服务器 204 中进行存储。

25 数据库 226（如，数据库 110）耦合到 web 服务器 204 上并且包含验证来自本地客户机 202（和网络中的其它用户）的请求以在数据库 226 中存储加密专用数据所必需的信息。尽管数据库 210 看起来是与验证服务器 204 分开的，但是应该理解，在本发明的其它实施例中，数据库 210 可以包含在 web 服务器 208 中。

在一个实施例中，web 服务器 204 是一个执行验证服务 227 的注册服务器，
30 以验证请求访问服务器 204 的用户 208。在这个实施例中，web 服务器 204 在允

许用户访问由该 web 服务器 204 提供的服务之前, 首先请求验证来自于用户 208 的信息, 如验证密码, 由参考字符 229 指示。

进一步参见图 2, 本地客户机 202 希望通过本地客户机应用程序 206 在服务器 204 中存储一个加密的私有密钥。在此之前, 本地客户机应用程序 206 需要对
5 服务器 204 验证/核准用户进行。在这个实施例中由用户 208 提供的验证密码就用来对访问服务器 204 验证用户 208。

为了安全地发送和存储专用数据, 本地客户机应用程序 206 请求输入数据, 如来自于用户 208 的加密密码。本地客户机应用程序 206 和 UI 220 允许用户 208 输入加密密码。本地客户机应用程序 206 响应用户输入的加密密码, 产生了一个
10 用于加密专用数据的包封密钥 K1 230。在这个实施例中, 包封密钥 K1 是一个用来加密私有密钥的对称密钥(如, 生成一个散列值)。本地客户机应用程序 206 向服务器漫游应用程序 228 发送加密专用数据, 如参考字符 232 所指示的。为了确保用户数据的私密性, 使得验证密码和加密密码成为两个独立的密码。但是, 应该明白, 它们也可以是一个密码。还应该明白, 服务器 204 可以用不同的验证
15 机制对用户 208 进行验证, 如智能卡, 一次性密码和生物测定学。

由服务器 204 执行的服务器漫游应用程序 228(如, web 服务)将接收到的加密专用数据存储在数据库 226 中, 如参考字符 233 所指示的。在这个实施例中, 专用数据是存储在存储器 214 中的私有密钥 216, 并且加密算法 218 利用生成的包封密钥 230 对私有密钥进行加密从而生成加密私有密钥 $E_{k1} PK$ 234。值得注意
20 的是, web 服务器 204 仍不知道生成的包封密钥和私有密钥 216。此外, 由于服务器不能支配用于生成包封密钥 230 的加密密码, 因此服务器漫游应用程序就无法对加密私有密钥 234 进行解密。

现在参见图 3, 根据本发明的一个实施例, 该模块图示出了在漫游客户机 302 和 web 服务器 204 之间对加密专用数据进行通信的系统 300。

在这个实施例中, 服务器漫游应用程序 228 通过漫游客户机应用程序 304
25 和通信网络 212 接收来自于漫游客户机 302 的请求从而获取数据库 226 中存储的加密专用数据。服务器漫游应用程序 228 响应接收到的请求信息, 由 web 服务器 204 执行对漫游用户 306 进行验证。在这个实施例中, 服务器 204 通过图 2A 所示的输入格式, 请求来自于漫游用户 306 的验证密码。

30 如图 2 所描述的实质上相同的方式中, 服务器漫游应用程序 228 验证从客户

机接收的验证密码的格式，从而确定是否核准漫游用户 306 以获取了来自于数据库的加密数据。如果验证密码没有通过验证，那么服务器漫游应用程序 228 会阻止漫游客户机 302 访问数据库 226 中存储的加密专用数据。选择的，如果验证密码通过了验证，那么服务器漫游应用程序 228 会获取来自于数据库 226 的加密数据，如参考字符 310 所指示的，并且将加密数据发送给漫游客户机 302，如参考字符 311 所指示的。漫游客户机应用程序 304 响应接收到的加密专用数据，请求来自于用户的加密密码并生成包封密钥 K1，并且执行解密算法 312。（308 在图 3 中未示出）这样的话，解密算法 312 利用漫游客户机 302 上生成的包封密钥 230 对接收到的加密专用数据进行解密从而获得与本地客户机 202 相关的私有密钥。

10 此后，漫游客户机应用程序 304 能够在与漫游客户机 302 相关的存储器 314 中存储已获得的私有密钥。

现在参见图 4，根据本发明的另外一个优选实施例，模块图示出了在本地客户计算机 202 和服务器 204 之间对加密专用数据进行通信和数据恢复的系统 400。

在这个实施例中，即使在用户忘记加密密码的情况下，本地用户 208 使用 UI 220 来选择恢复选项从而具有对存储在服务器 204 中的加密专用数据进行恢复的能力。在这个实施例中，如图 2 所描述的，除了利用加密密码生成包封密钥 K1 之外，漫游客户机应用程序 212 还响应恢复密钥请求，随机生成新的加密密钥（如恢复密钥 K2）。例如，用户将加密密码输入到表格（未示出）中之后，例如，用户 208 使用鼠标来点击“YES”键，随即向用户出现显示信息“ENABLE PRIVATE DATA RECOVERY WITHOUT ENCRYPTION PASSWORD”的对话框。

20 本地客户机应用程序 206 响应由用户作出的“YES”选择，随机生成恢复密钥 K2。值得注意的是，K2 不以任何方式与加密密码连接。服务器漫游应用程序 228 通过核准由客户机发送来的验证密码来验证用户 208。如果验证密码通过了验证，那么就允许用户 208 向服务器 204 发送包括用包封密钥 $E_{k1} PK$ 234 加密的私有密钥，用恢复密钥 $E_{k2} K1$ 414 加密的包封密钥和用包封密钥 $E_{k1} K2$ 416 加密的恢复密钥在内的加密专用数据，分别如 418，419 和 420 所指示的。服务器漫游应用程序 228 响应接收到的加密专用数据在数据库 226 中存储 $E_{k1} PK$ ， $E_{k2} K1$ 414 和 $E_{k1} K2$ ，分别如 421，422 和 423 所指示的。此外，服务器漫游应用程序 228 响应从本地客户机 202 接收的加密数据，随机生成备份密钥 K3 424 并存储在数据库 226 中，如 425 所指示的，并且将生成的备份密钥 424 发送给本

30

地客户机 202, 如 426 所指示的。注意 K3 的传输是通过安全信道(如, 通过 SSL)发生的。在没有安全信道的情况下, 值就会发生变化从而容易泄露恢复密钥。本地客户机应用程序 206 响应接收到的备份密钥 424, 生成第二加密恢复密钥 $E_{k3} K2$ 428 并存储在与本地客户机 202 相连的存储器 214 中和/或磁盘中。

5 在这个实施例中, 加密算法 216 用于生成加密私有密钥 234, 加密包封密钥 414, 第一加密恢复密钥 416 和第二加密恢复密钥 428。加密私有密钥 234 代表由包封密钥加密的私有密钥, 加密包封密钥 414 代表由恢复密钥 K2 加密的包封密钥, 第一加密恢复密钥 416 代表由包封密钥 K1 加密的恢复密钥 408, 以及第二加密恢复密钥 428 代表由备份密钥 424 加密的恢复密钥 408。尽管这样, 这里将
10 本发明描述为使用同一种加密算法, 但是可以预料不同的加密算法能够用于生成各自不同的加密密钥。

现在参见图 5, 根据本发明的一个实施例, 模块图 5 示出了从服务器 204 向漫游客户机 302 发送恢复数据的系统 500。

在这个实施例中, 服务器漫游应用程序 228 通过远程漫游客户机应用程序
15 304 接收来自于漫游客户机 302 的请求并且与网络 212 进行通信从而获取数据库中的备份数据。在这种情况下, 备份数据是第一个加密恢复密钥 416 和备份密钥 424。服务器漫游应用程序 228 通过核准客户机发送来的验证密码的格式来对用户 208 进行验证。如果验证密码通过验证, 那么服务器漫游应用程序 228 就能从数据库 226 中获取第一加密恢复密钥 416 和备份密钥 424, 例如分别由参考字符
20 506, 508 所指示的, 并且将 $E_{k1} K2$ 和 K3 发送给漫游客户机应用程序 304, 例如分别由参考字符 510, 512 所指示的。换句话说, 如果验证密码没有通过验证, 那么服务器漫游应用程序 228 会阻止访问数据库 226。

漫游客户机应用程序 304 响应接收到的第一加密恢复密钥 416, 请求接收用户发出的加密密码 504, 生成包封密钥 K1, 并且执行解密算法 312。在这种情况下,
25 解密算法 312 利用在漫游客户机 302 上生成的包封密钥 230 对接收到的第一加密恢复密钥 416 进行解密从而获得与内部客户计算机 202 相关联的恢复密钥 408。漫游客户机应用程序 304 响应接收到的备份密钥 424, 执行加密算法 218。在这种情况下, 加密算法 218 利用接收到的备份密钥 424 对已获得的恢复密钥 408 进行加密从而生成第二加密恢复密钥 428。此后, 漫游客户机应用程序 304 将第
30 二加密恢复密钥 428 存储在存储器 314 中或与漫游客户机 302 相连的磁盘上。由

于具有了存储在存储器 314 中的第二加密恢复密钥 428，以及来自于服务器的备份密钥 424 和加密包封密钥，漫游客户机 302 可以在不知道用于生成包封密钥 K1 的密码（如，加密密码）的情况下，对存储在数据库 226 中的加密私有密钥 234 进行恢复和解密。

5 现在参见图 6，根据本发明的一个实施例，模块图示出了在不知道加密密码的情况下，用于恢复从 web 服务器 204 到漫游客户机 302 的加密数据的系统 600。

在这个实施例中，在漫游客户机 302 上已经进行了上面所述的备份处理，因此漫游客户机 302 具有存储在存储器 314 中的第二加密恢复密钥 428。服务器漫游应用程序 228 通过漫游客户机应用程序 304 接收由漫游客户机 302 发出的请求，并且与网络 212 进行通信从而获得加密专用数据，如来自于数据库 226 的私有密
10 钥 216。服务器漫游应用程序 228 通过核准来自于客户机的验证密码来对用户 302 进行验证。当用户成功通过了验证时，服务器应用程序向漫游客户机应用程序 304 发送加密的专用数据 216。如图 3 和 5 所描述的，漫游客户机应用程序 304 响应接收到的加密专用数据，请求来自漫游用户 306 的加密密码以生成包封密钥 K1。

15 如果用户 306 忘记了加密密码，例如，用户会利用 UI 来选择“YES”选项，随即向用户出现另一个显示信息“RECOVERY PRIVATE DATA WITHOUT ENTERING ENCRYPTION PASSWORD”的对话框。服务器漫游应用程序 228 响应恢复请求，从数据库 226 中获得备份密钥 424，加密私有密钥 234 和加密包封密钥 414，分别如参考字符 604、606 和 608 所指示的，并且将获得的 K3、E_{k1} PK，
20 和 E_{k2} K1 发送至漫游客户机应用程序 304，分别如参考字符 610、612 和 614 所指示的。

漫游客户机应用程序 304 响应接收到的备份密钥 424，加密私有密钥 234 和加密包封密钥 414，执行解密算法 312。在这种情况下，解密算法 312 利用接收到的备份密钥 424 对以前存储在存储器（见图 5）中的第二加密恢复密钥 428 进
25 行解密，从而得到与本地客户机 202 相关的恢复密钥 408。接下来解密算法 312 利用得到的恢复密钥 408 对接收到的加密包封密钥 414 进行解密从而得到包封密钥 230。解密算法 312 利用得到的包封密钥继续对接收到的加密私有密钥 234 进行解密从而得到与本地客户机 202 相关的私有密钥 216。此后，漫游客户机应用程序 304 将获得的私有密钥 PK 存储在与漫游客户机 302 相连的存储器 214 中。

30 现在参见图 7，根据本发明的一个实施例，该示意性流程图示出了一种在内

部客户计算机和服务器之间进行专用数据通信，从而促使漫游客户计算机对专用数据进行恢复的方法。在 702 中，内部客户计算机的用户执行本地客户机应用程序，并且标识出存储在与内部客户计算机相连的存储器中的专用数据（如，私有密钥），从而将其加密并发送给服务器。在 704 中，本地客户机应用程序请求来自用户的加密密码。706 中，利用从用户接收到的加密密码生成包封密钥。708 中，利用生成的包封密钥对标识的专用数据进行加密。在 710 中，本地客户机应用程序将加密数据发送给执行服务器漫游应用程序的服务器。712 中，服务器应用程序响应已发送的加密专用数据，并且将加密专用数据存储在与服务器相连的数据库中。

10 现在参见图 8，根据本发明的一个实施例，该示意性流程图示出了一种从服务器向漫游客户计算机发送加密专用数据的方法。

在 802 中，执行漫游客户机应用程序的漫游客户计算机的用户请求发送来自执行漫游应用程序的服务器的加密专用数据。在这个实施例中，用户通过上述参考图 7 所描述的方法，请求发送以前存储在与服务器相连的数据库中的加密私有密钥 $E_{k1}PK$ 。在 804 中漫游客户机应用程序请求来自用户的加密密码。在 806 中，通过漫游客户机应用程序利用从用户接收的加密密码生成包封密钥。验证服务器首先利用某一验证机制，如密码匹配，对用户进行验证。808 中如果验证失败，809 中服务器漫游应用程序会阻止用户访问请求的加密数据。806 中如果验证成功，在 810 中，服务器漫游应用程序重新获得数据库中的加密私有密钥 $E_{k1}PK$ 并将其发送给漫游客户计算机。在 802 中，漫游客户机应用程序通过已生成的包封密钥 230 解密接收到的加密私有密钥 $E_{k1}PK$ 以获得私有密钥 PK 。

现在参见图 9A 和 9B，根据本发明的一个实施例，上述示意性流程图示出了一种在内部客户计算机和服务器之间进行专用数据通信和数据恢复的方法。

在 902 中，内部客户计算机的用户执行漫游客户机应用程序并对存储在内部客户计算机的存储器中的专用数据进行标识从而对其进行加密，并且提交请求以将标识后的专用数据传送至服务器。如果该请求被批准，如上述参考图 8 所述，那么在 904 中，服务器执行漫游服务器应用程序。在 906 中，服务器漫游应用程序响应来自特定本地客户机的请求以决定是否这是首次执行 SRA。如果在 906 中服务器漫游应用程序确定这是首次执行或对于这个用户来讲无法在数据库中找到备份密钥 $K3$ ，那么在 908 中，服务器漫游应用程序生成随机备份密钥 $K3$ 。在

910 中, 服务器漫游应用程序在数据库中存储备份密钥 K3, 并且在 912 中, 向本地客户机应用程序提供用于对恢复数据进行加密的备份密钥 K3。如果在 907 中, 服务器漫游应用程序确定这不是首次执行, 并且在 912 中, 向本地客户机应用程序提供用于加密恢复数据的备份密钥 K3。

- 5 现在参见图 9B, 在 914 中本地客户机应用程序利用用户提供的加密密码生成包封密钥 K1。916 中本地客户机应用程序决定恢复密钥 K2 是否存储在内部客户计算机中。如果 916 中, 本地客户机应用程序决定恢复密钥 K2 没有存储在与本地客户机相连的存储器中, 并且第一加密恢复密钥 $E_{k1}K2$ 在服务器中不存在, 那么在 918 中本地客户机应用程序生成随机恢复密钥 K2。例如, 如果这是本地
- 10 客户机应用程序的首次执行, 那么恢复密钥就不会在内部客户计算机中存在。在 916 中, 如果本地客户机应用程序确定在与本地客户机相连的存储器中存储恢复密钥 K2, 那么 920 中, 本地客户机应用程序从存储器中重新获得恢复密钥 K2。在 922 中, 本地客户机应用程序生成加密私有密钥, 加密包封密钥 K1, 第一加密恢复密钥和第二加密恢复密钥。加密私有密钥代表经生成的包封密钥 K1 加密
- 15 的私有密钥 PK。加密包封密钥 $E_{k2}K1$ 代表经恢复密钥 K2 加密的包封密钥 K1。第一加密恢复密钥 $E_{k1}K2$ 代表经包封密钥 K1 加密的恢复密钥 K2。第二加密恢复密钥 $E_{k3}K2$ 代表经由服务器发送来的备份密钥 K3 加密的恢复密钥 K2。在 924 中, 本地客户机应用程序将第二加密恢复密钥 $E_{k3}K2$ 存储在与内部客户计算机相连的存储器中。926 中, 本地客户机应用程序将加密私有密钥, 加密包封密钥,
- 20 第一加密恢复密钥发送给服务器。再回到图 9A 中, 在 928 中, 服务器漫游应用程序接收发送来的加密私有密钥, 加密包封密钥和第一加密恢复密钥, 并将其存储在数据库中。

- 现在参见图 10, 示意性流程图示出了一种从服务器向漫游客户机发送恢复数据从而使得漫游客户机无需加密密码就能够获得专用数据的方法。在 1002 中,
- 25 执行漫游服务器应用程序的服务器接收来自执行漫游客户机应用程序的漫游用户的验证密码, 并请求对恢复数据进行转移或备份。在 1004 中漫游客户机应用程序响应由验证的用户所提供的加密密码, 生成包封密钥 K1。在 1006 中, 漫游服务器应用程序将备份密钥 K3, 第一加密恢复密钥 $E_{k1}K2$ 发送给漫游客户机应用程序。在 1008 中, 漫游客户机应用程序利用已生成的包封密钥 K1 对接收到的
- 30 第一加密恢复密钥 $E_{k1}K2$ 进行解密从而得到 K2。在 1010 中, 客户机应用程序

利用接收到的备份密钥 K_3 对得到的恢复密钥 K_2 进行加密从而生成第二加密恢复密钥 $E_{k3} K_2$ 。在 1012 中，漫游客户机应用程序将生成的第二加密恢复密钥存储在漫游客户机计算机相连的存储器中。

现在参见图 11，示意性流程图示出了一种无需加密密码，在漫游客户机中恢复来自服务器的专用数据的方法。在 1102 中，服务器接收来自执行漫游客户机应用程序的漫游客户机的验证密码，并且在无需加密密码的情况下请求传送加密私有密钥。在 1104 中，漫游客户机应用程序从数据库中重新获得备份密钥，加密包封密钥 $E_{k2} K_1$ 和加密私有密钥 $E_{k1} PK$ 。在 1106 中，漫游客户机应用程序将重新获得的备份密钥，加密包封密钥和加密私有密钥发送给漫游客户机。在 1108 中，漫游客户机应用程序利用重新获得的备份密钥 K_3 对先前存储在漫游客户机（见图 10）中的第二加密恢复密钥 $E_{k3} K_2$ 进行解密从而得到恢复密钥 K_2 。在 1110 中，漫游客户机应用程序利用已得到的恢复密钥 K_2 对加密包封密钥 $E_{k2} K_1$ 进行解密从而得到包封密钥 K_1 。在 1112 中，漫游客户机应用程序利用已得到的包封密钥对加密私有密钥进行解密。

值得注意的是，通过在客户机端生成 K_2 以及将其泄露给服务器，我们能够在服务器不知道其中任一个的情况下，在服务器上备份加密密码密钥 K_1 和恢复密钥 K_2 。同时，由于客户机至少知道两个密钥中的一个，也就是用户输入预先存储在客户机端的加密密码 K_1 或 K_2 ，客户机都能够利用 $E_{k1} K_2$ 和 $E_{k2} K_1$ 来恢复专用数据并且还能够对其进行备份。

图 12 示出了以计算机 130 形式的通用计算设备的例子。在本发明的一个实施例中，计算机，如计算机 130 适用于这里所示意和描述的其它附图。计算机 130 具有一个或多的处理器或处理单元 132 以及系统存储器 134。所示的实施例中，系统总线 136 耦合包括系统存储器 134 至处理器 132 在内的多个系统部件。总线 136 代表一种或多种总线结构的类型，其中包括记忆总线或记忆控制器，外部总线，加速图形端口以及处理器或采用任何一种总线结构的局部总线。作为例子，并且没有限制，这种结构包括工业标准结构（ISA）总线，微通道结构（MCA）总线，增强 ISA（EISA）总线，视频电子标准协会（VESA）内部总线，以及也公知的 Mezzanine 总线的外设部件互连（PCI）总线。

计算机 130 通常至少某些形式计算机可读介质。包括易失的和非易失的介质，可移动和不可移动介质在内的计算机可读介质可以是任何能够被计算机 130

访问的可用的媒质。作为例子，并且没有限制，计算机可读介质包括计算机存储介质和通信介质。计算机存储介质包括在任何方法和技术中用于信息存储的易失和非易失的，可移动和不可移动的介质，该信息如计算机可读指令，数据结构，程序模块或其它数据。例如，计算机存储介质包括 RAM, ROM, EEPROM, flash 5 存储或其它存储技术，CD-ROM，数字通用磁盘（DVD）或其它光学磁盘存储，磁盒，磁带，磁盘存储或其它磁存储设备，或其它任何能用来存储想要的信息并能够被计算机 130 访问的媒介。通信介质通常包含计算机可读指令，数据结构，程序模块，或调制数据信号中的其它数据，如载波或其它传输机制，以及包含任何信息的传递介质。本领域技术人员都熟知的调制数据信号具有一个或多个可以 10 被设定或改变的特征，从而对信号中的信息进行编码。有线介质，如有线网络或直接有线连接，和无线介质，如声学的，RF，红外线的以及其它无线介质，以上这些都通信介质的范例。以上这些的任意组合也都包含在计算机可读介质的范围内。

系统存储器 134 包括以可移动的和/和不可移动的，易失的和/或非易失的形式存储的计算机存储介质。在所示的实施例 15 中，系统存储器 134 包含只读存储器（ROM）138 和随机存取存储器（RAM）140。包含基础例程的基础输入/输出系统 142（BIOS）通常存储在 ROM138 中，该基础例程有助于在计算机 130 的元件间传送信息，例如在启动期间。RAM140 通常包含通过处理单元 132 就能够立即进行存取和/或运行的数据和/或程序模块。作为例子，并且不进行限定，图 12 20 示出了操作系统 144，应用程序 146，其它程序模块 148 和程序数据 150。

计算机 130 也可以包括其它可移动的/不可移动的，易失的/非易失的计算机存储介质。例如，图 12 示出了能够从不可移动的，非易失的磁介质中读取或写入的硬盘驱动器 154。图 12 还示出了能够在可移动的，易失的磁盘 158 中读取或写入的磁盘驱动器 156，以及能够在可移动的，非易失的光盘 162，如 CD-ROM 25 或其它光介质中读取或写入的光盘驱动器 160。其它可移动的/不可移动的，易失的/非易失的计算机存储介质也可以应用于包括磁带，flash 存储卡，数字通用盘，数字录像带，固态 ROM，固态 RAM 等在内的示意性操作环境中，但并不局限于此。硬盘驱动器 154，磁盘驱动器 156 和光盘驱动器 160 通常通过非易失存储接口，如接口 166 连接到系统总线 136 上。

30 图 12 所示的已讨论过的驱动器或其它大容量存储设备以及与它们相连的计

计算机存储介质存储了计算机可读指令，数据结构，程序模块和用于计算机 130 的其它数据。在图 12 中，例如，硬盘驱动器 154 示为用于存储操作系统 170，应用程序 172，其它程序模块 174 和程序数据 176。值得注意的是，这些部分可以与操作系统 144，应用程序 146，其它程序模块 148，和程序数据 150 相同，也可以不同。这里，针对操作系统 170，应用程序 172，其它程序模块 174，和程序数据 176 给出了不同的编号，最低的，它们是不同的副本。

用户可以通过输入设备或用户接口选择设备，如键盘 180 和指示设备 182（如，鼠标，轨迹球，笔或触摸屏），将命令和信息输入到计算机 130 中。其它输入设备（未示出）可以包括麦克风，操纵杆，游戏屏，圆盘式卫星电视天线，扫描仪等等。这些设备以及其它输入设备都可以通过耦合在系统总线 136 上的用户输入接口 184 与处理单元 132 相连接，但是也可以通过其它的接口和总线结构与处理单元相连，如并行端口，游戏端口，或通用串行总线（USB）。监视器 188 或其它类型的显示设备也可以通过接口与系统总线 136 相连，如视频接口 190。除监视器 188 之外，计算机通常包括其它外围输出设备（未示出），如打印机和扬声器，它们可以通过输出外围接口（未示出）相连接。

在网络环境中，计算机 130 可以利用逻辑接点与一个或多个漫游客户机相连，如漫游客户机 194。漫游客户机 194 可以是个人计算机，服务器，路由器，网络 PC，对等装置或其它通用网络节点，并且通常包括如上所述的与计算机相关的许多或所有单元。图 12 所述的逻辑接点包括局域网（LAN）196 和广域网（WAN）198，但是还可以包括其它网络。这些网络环境在办公室，企业宽带计算机网络，企业内部互联网和全球计算机网络（如，因特网）中是非常普遍的。

当应用于局域网环境中，计算机 130 是通过网络接口或适配器 186 与 LAN 196 相连的。当应用于广域网环境中，计算机 130 通常包括调制器 178 或通过 WAN 198，如因特网，建立通信的其它装置。调制器 178 可以是内部的也可以是外部的，并且通过用户输入接口 184 或其它适当的机制与系统总线 136 相连。在网络环境中，所述的与计算机 130 或其中某部分相关的程序模块可以存储在远程记忆存储器设备中（未示出）。作为例子，并且没有限制，图 12 示出了将远程应用程序 192 驻留在存储器设备中。应该意识到所示的网络连接只是所举的一个例子，也可以采用其它装置来建立计算机间的通信链路。

通常，计算机的数据处理器借助于在不同时间，存储在计算机的各种计算机

可读存储介质中的指令来执行。例如，程序和操作系统通常是分存在软盘或 CD-ROM 中。接下来，将它们安装或下载到计算机的第二存储器中。在执行的过程中，至少将它们部分地下载到计算机的第一电子存储器中。当这种介质包含用于完成下面与微处理器或其它数据处理器相关的所述步骤的指令或程序时，这里
5 所述的本发明包括这些或其它类型的计算机可读存储介质。当根据这里所述的方法和技术编写程序时，本发明还包括计算机本身。

为了进行示意，这里用离散的模块示出了程序或其它的执行程序部件，如操作系统。然而，应该认识到，在不同时间，在计算机的各种存储元件中存储的这些程序和部件通过计算机的数据处理器执行。

10 尽管结合包括计算机 130 在内的示意性计算系统环境来描述，但是本发明也能够结合其它通用或专用计算系统环境或结构来实现。计算系统环境并对本发明的使用范围或功能范围进行任何的限定。而且，不应将计算系统环境视为对示意性操作环境所示出的任何一个元件或多个元件的组合具有任何的依赖性需求。举出的常见计算系统，环境，和/或结构的例子可适合本发明中的用户，但并不局
15 限于，个人计算机，服务器计算机，手持型或膝上型设备，多处理器系统，微处理器基础系统，机顶盒，可编程用户电子器件，网络 PC 机，微型计算机，大型计算机，适用于包括上述系统或装置在内的任何计算环境等。

本发明可以描述在计算机执行指令的通用环境中，如程序模块，并且可以用一个或多个计算机或其它设备来执行。通常，程序模块包含例程，程序，目标程
20 序，分量和执行特定的任务或实现特殊的抽象数据类型的数据结构，但又不局限于此程序模块。本发明还适用于分布式计算环境，该环境中的任务都由通过通信网络相连接的远程处理设备来执行。在分布式计算环境中，程序模块可位于具有记忆存储设备的本地和漫游客户机存储介质中。

在操作中，计算机 130 执行计算机执行指令，如图 7 至 11 所示出的，用以
25 加密和发送专用数据和/或接收和解密专用数据。

当介绍本发明或实施例的元件时，词“一个”，“一个”，“该”和“所述”实际上想要表示存在一个或多个元件。术语“包括”，“包含”和“具有”实际上是想要表示这里可能具有除了列出的元件之外的其它元件。

鉴于上面所述的，可以看出本发明的若干目的是可以实现的并且能够取得其
30 它有利的效果。

在不背离本发明范围的情况下，可以在结构和方法上进行多种变化，意味着上面所述的以及附图所示出的所有内容都应认为是说明性的并且不进行限制。

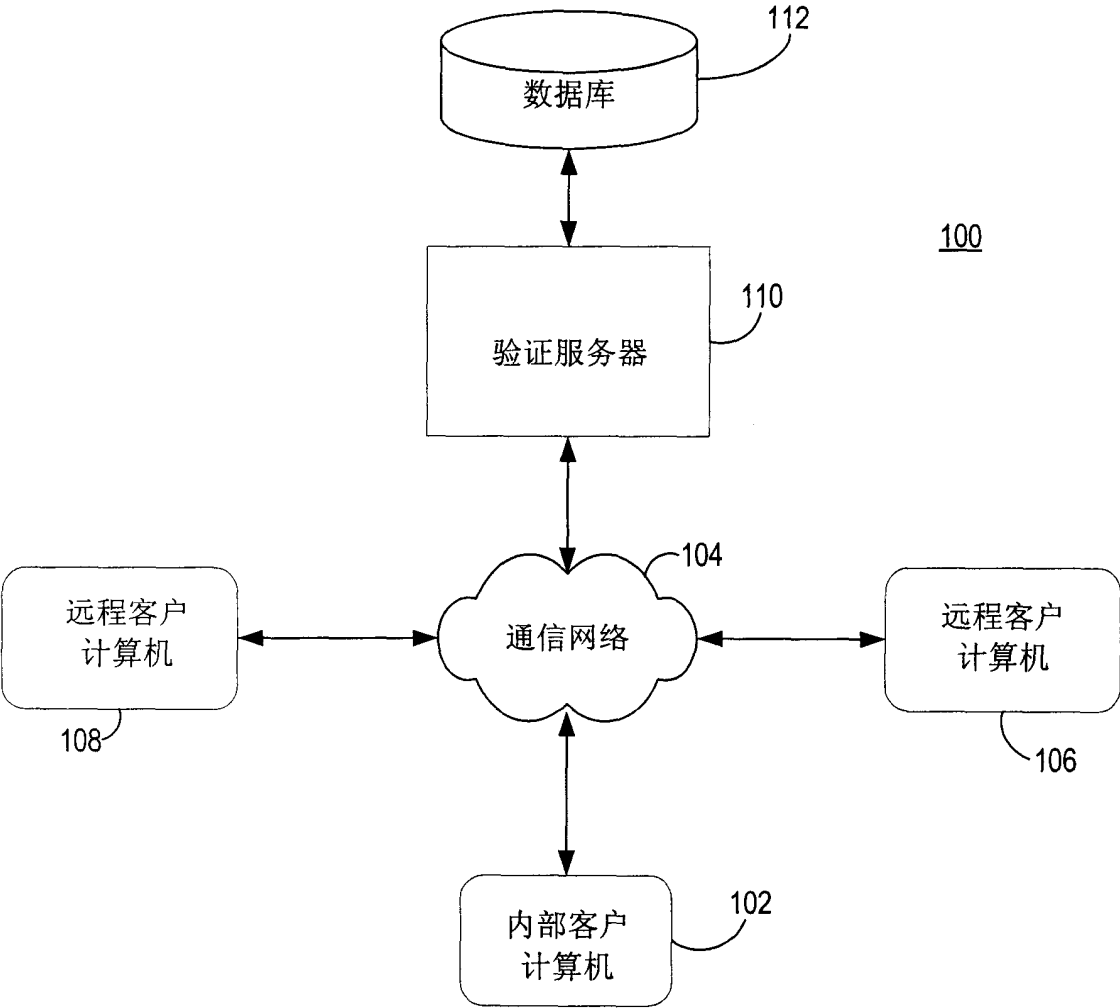


图 1

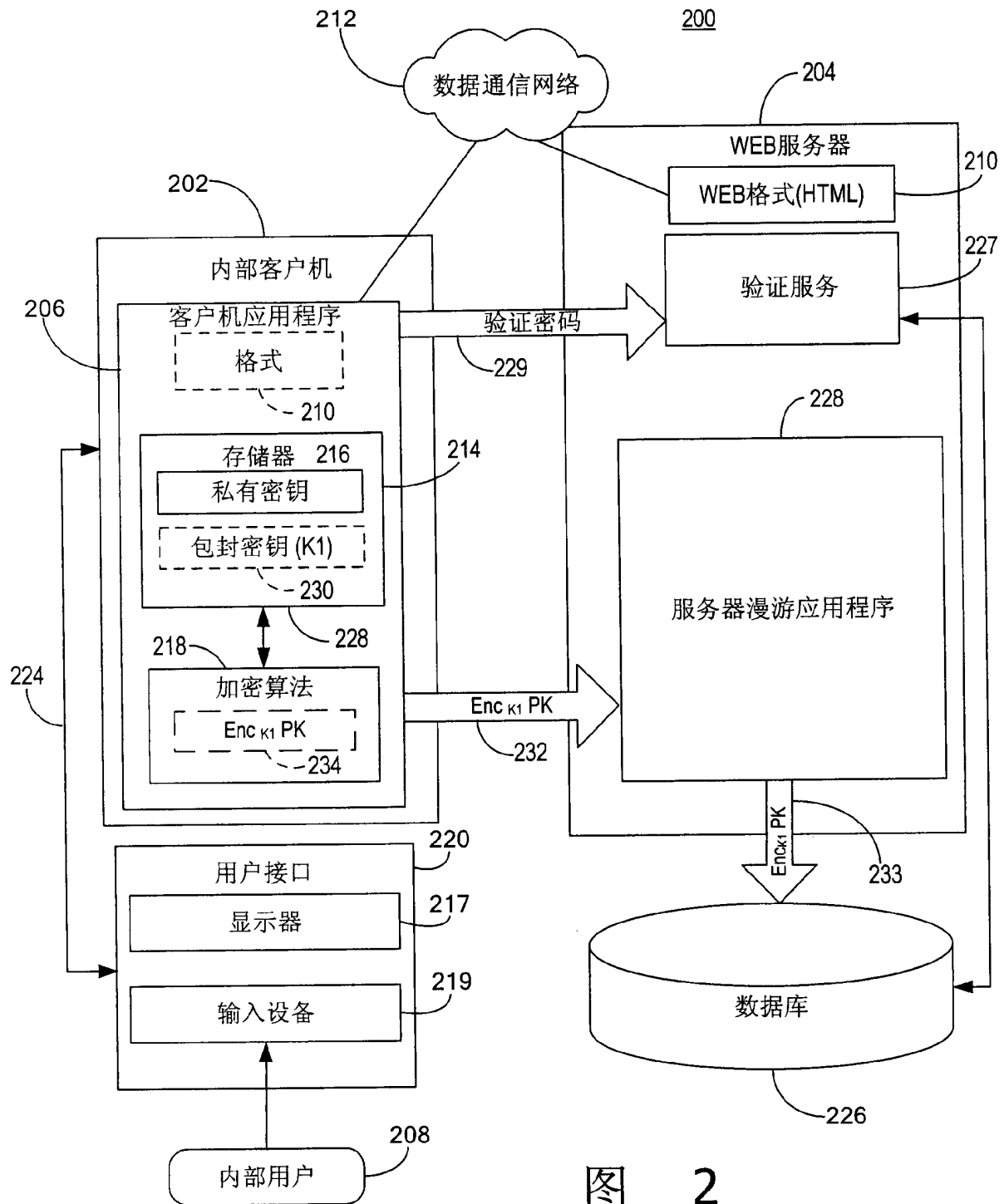


图 2

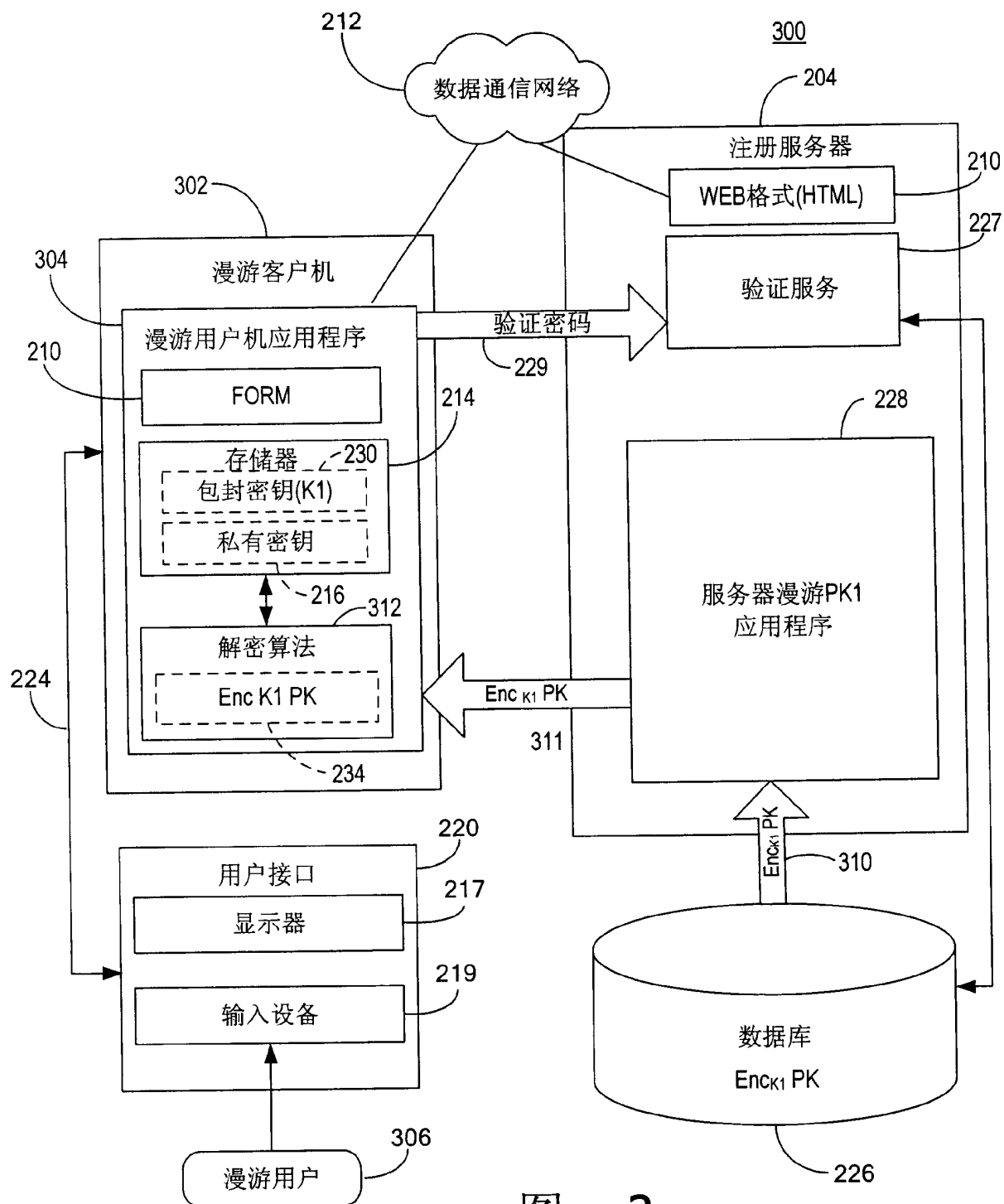


图 3

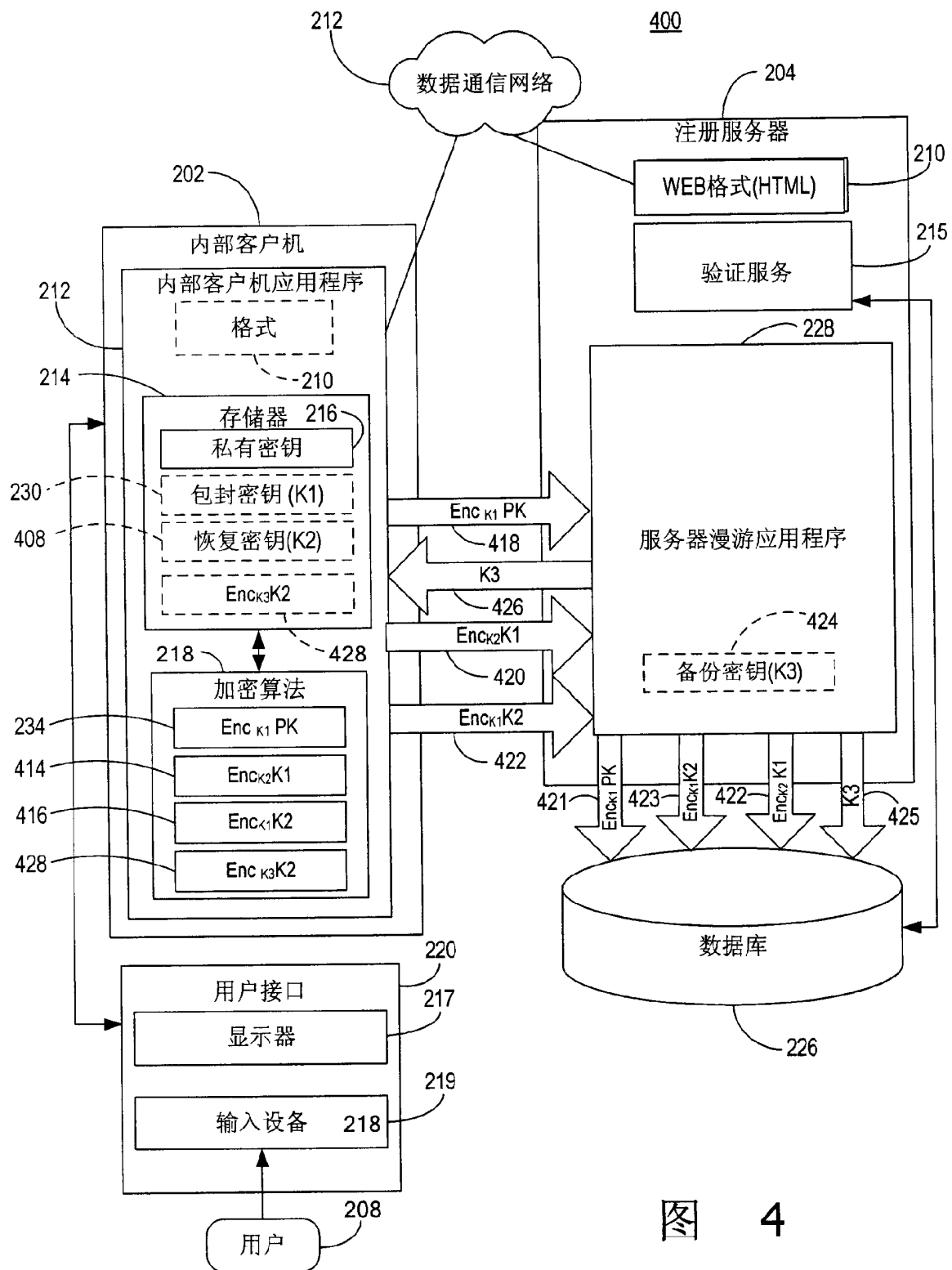


图 4

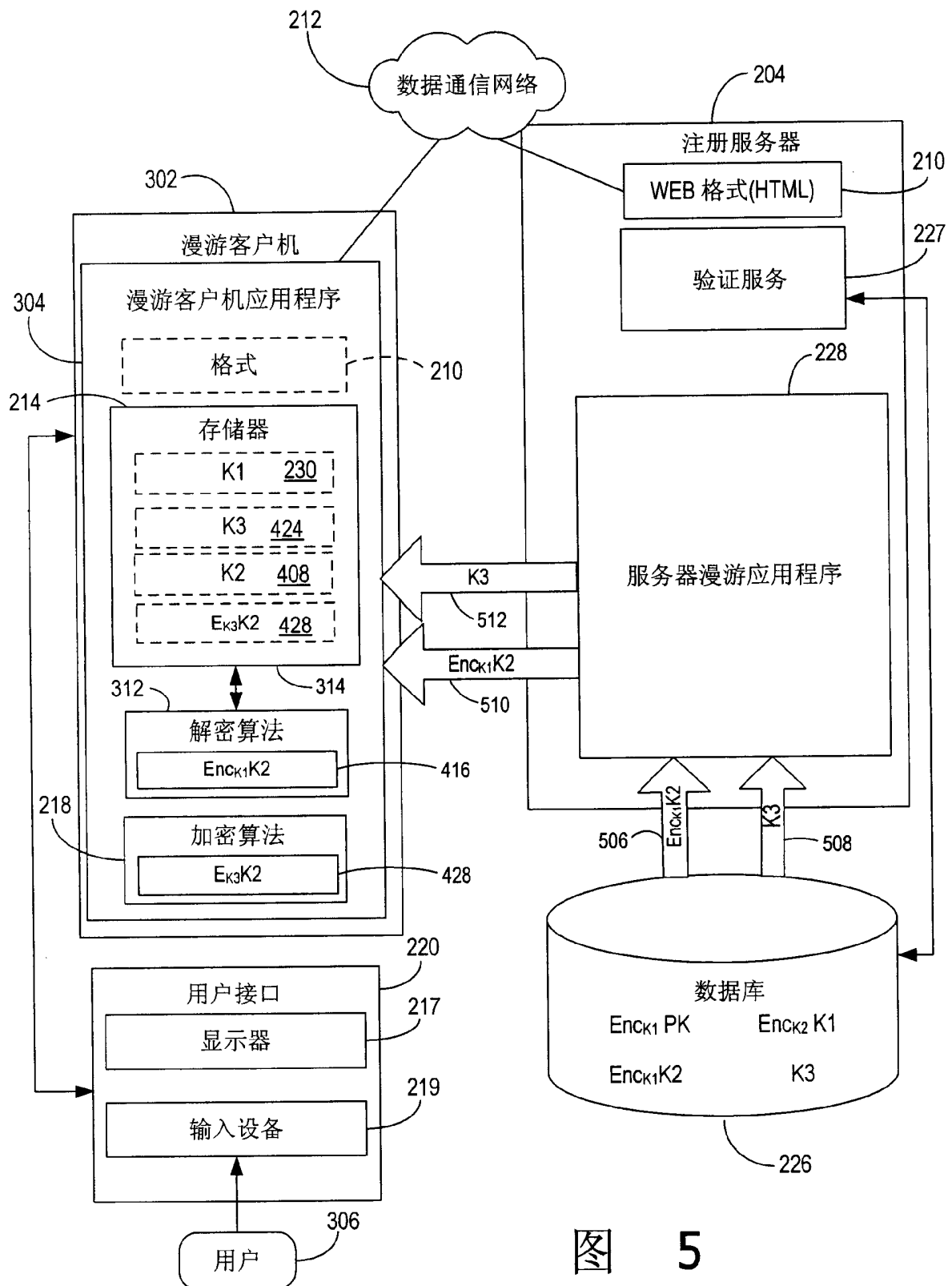


图 5

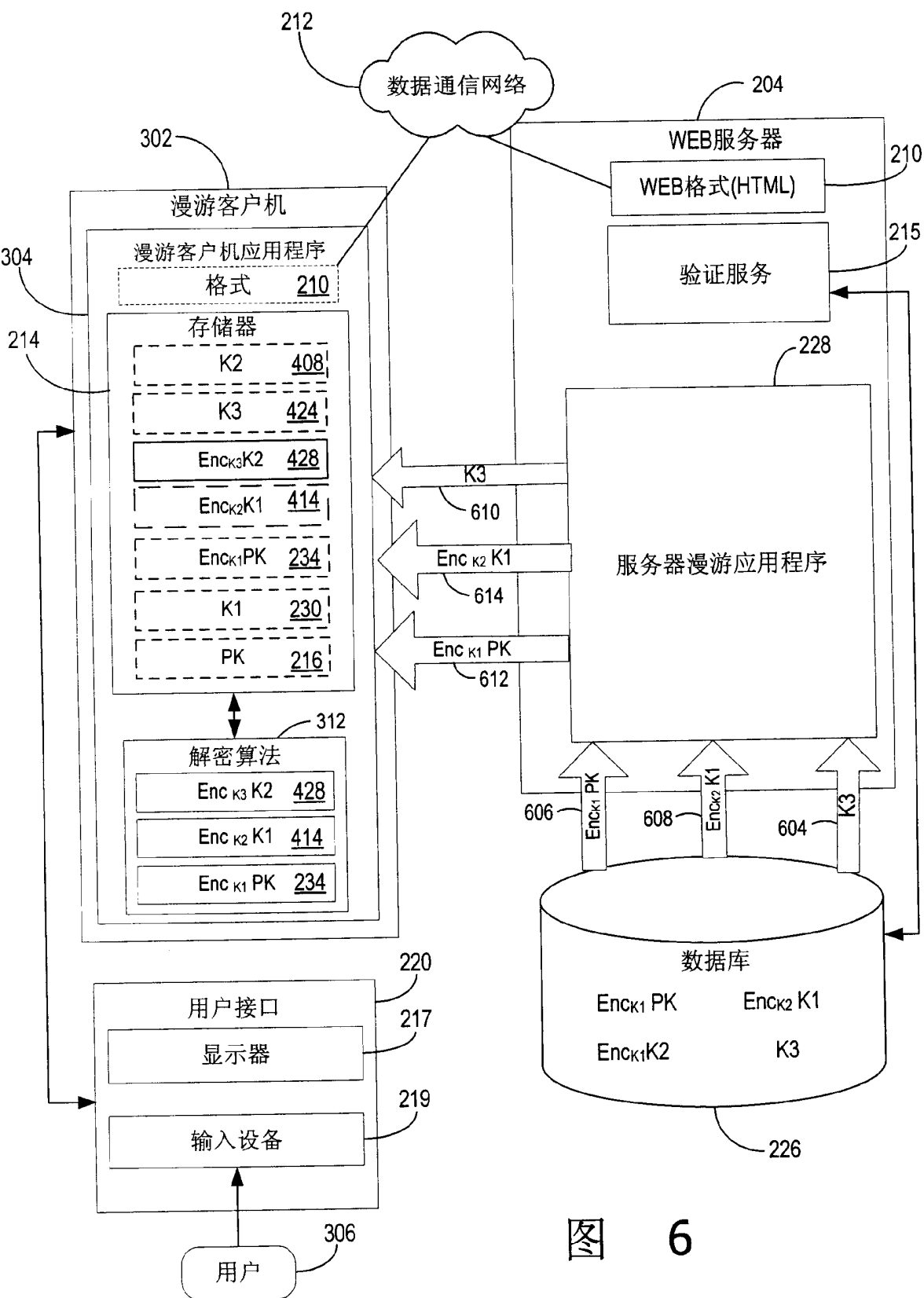


图 6

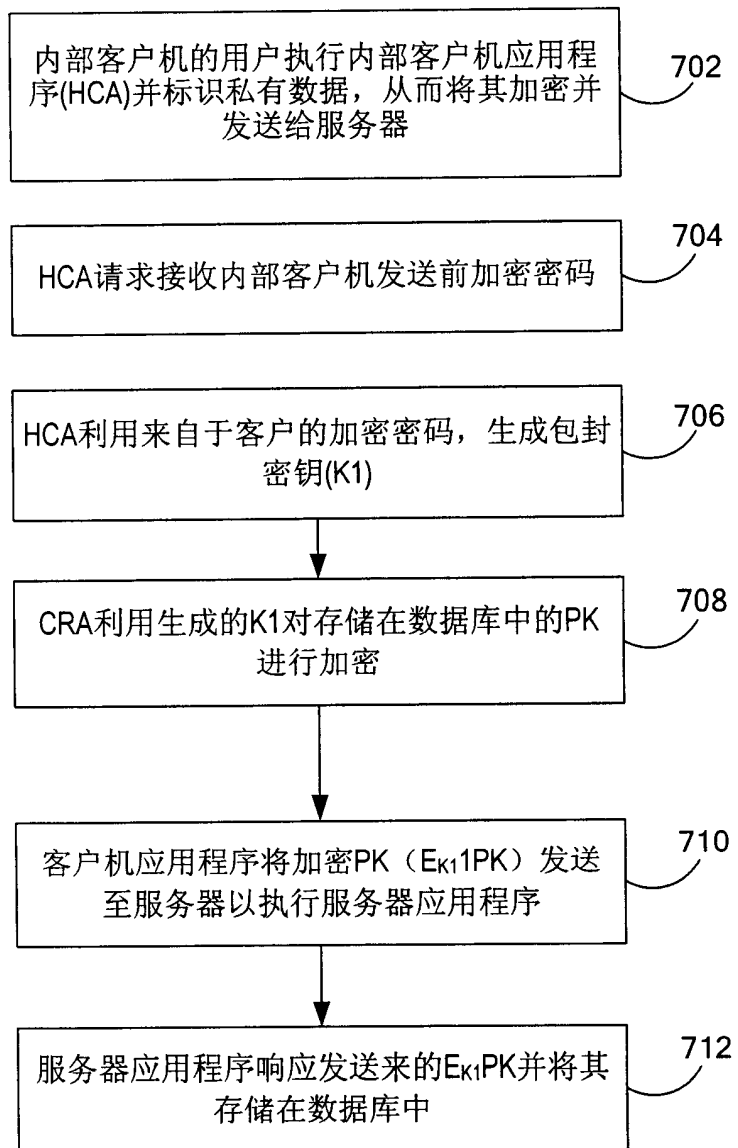


图 7

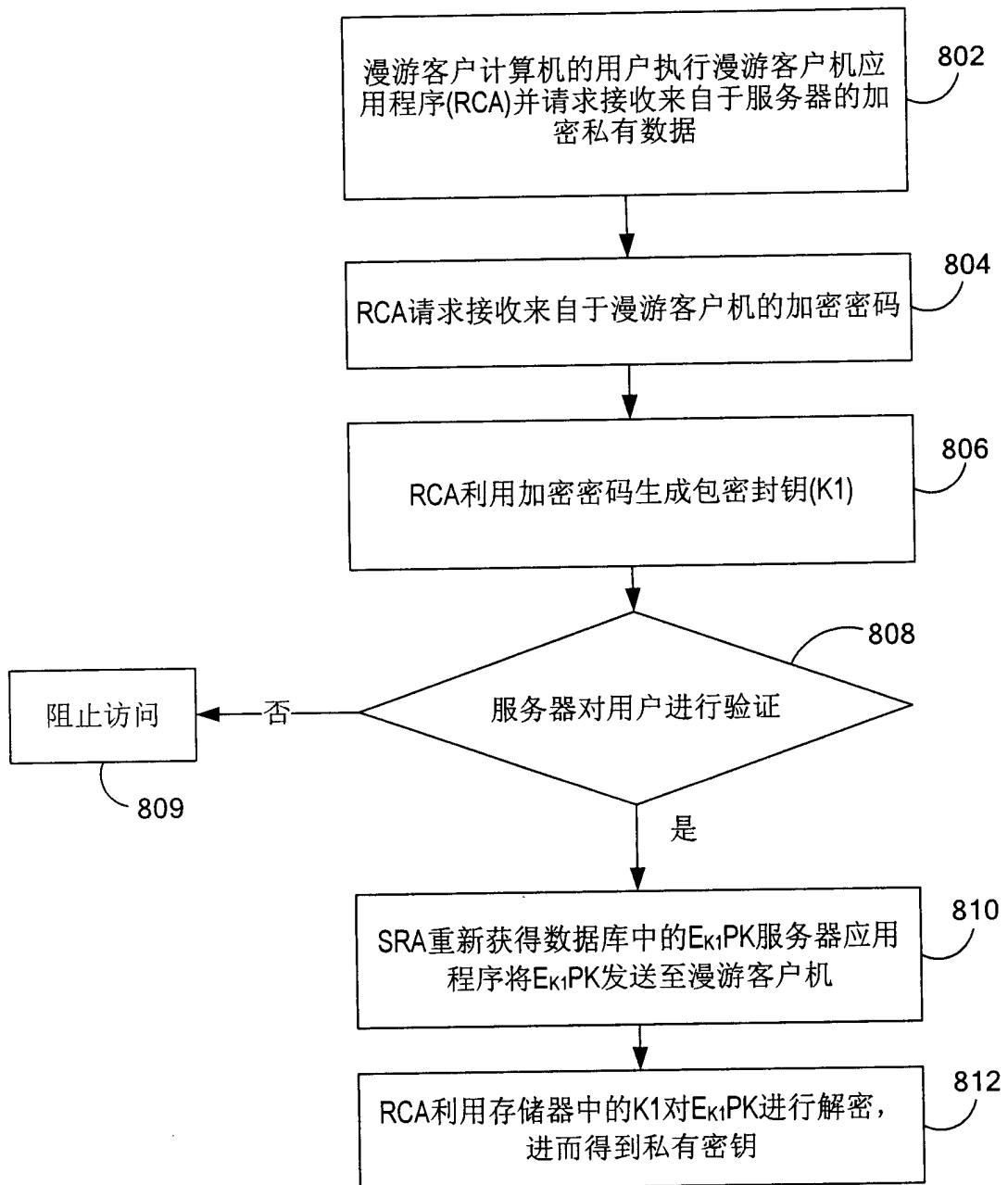
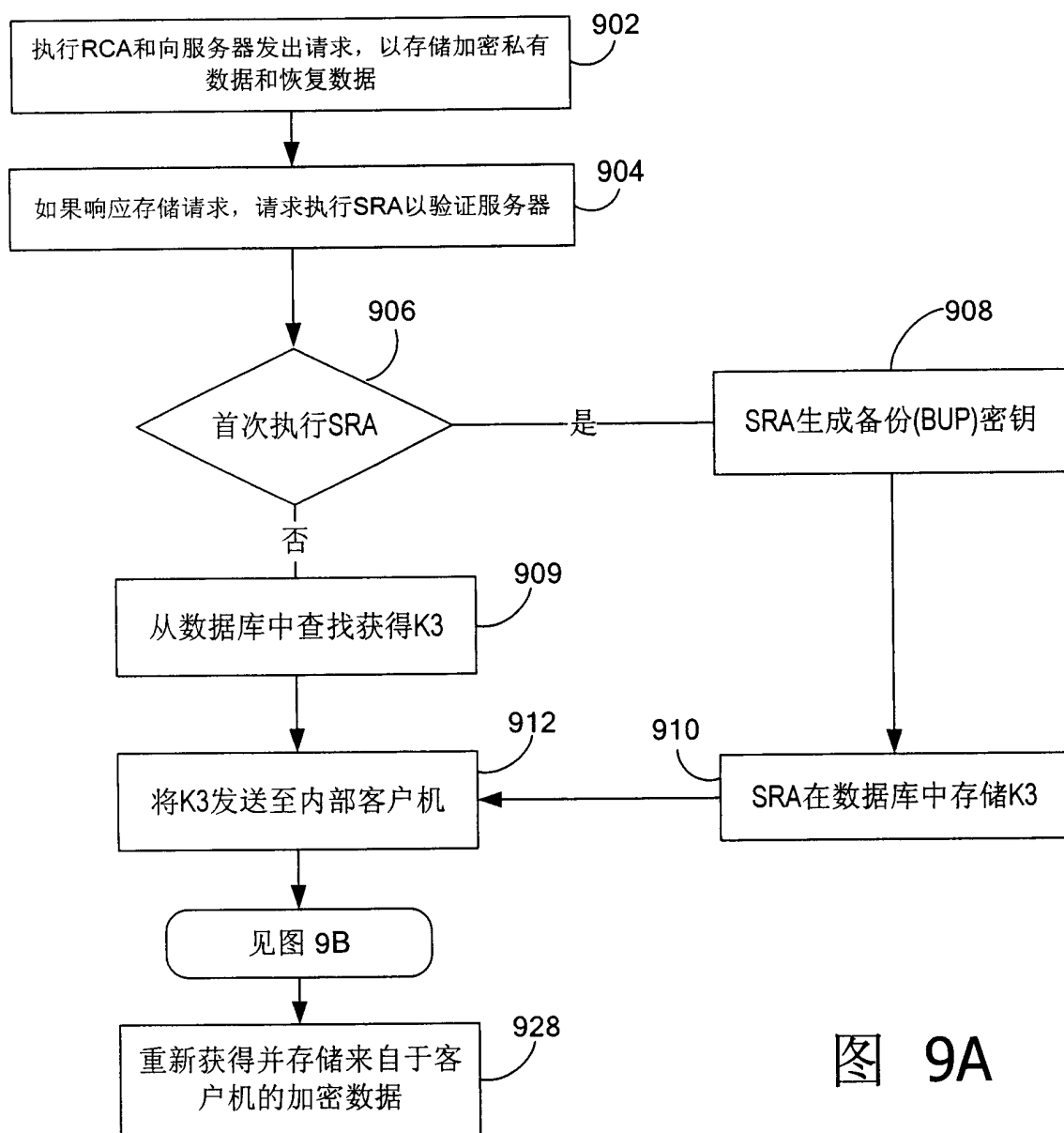


图 8



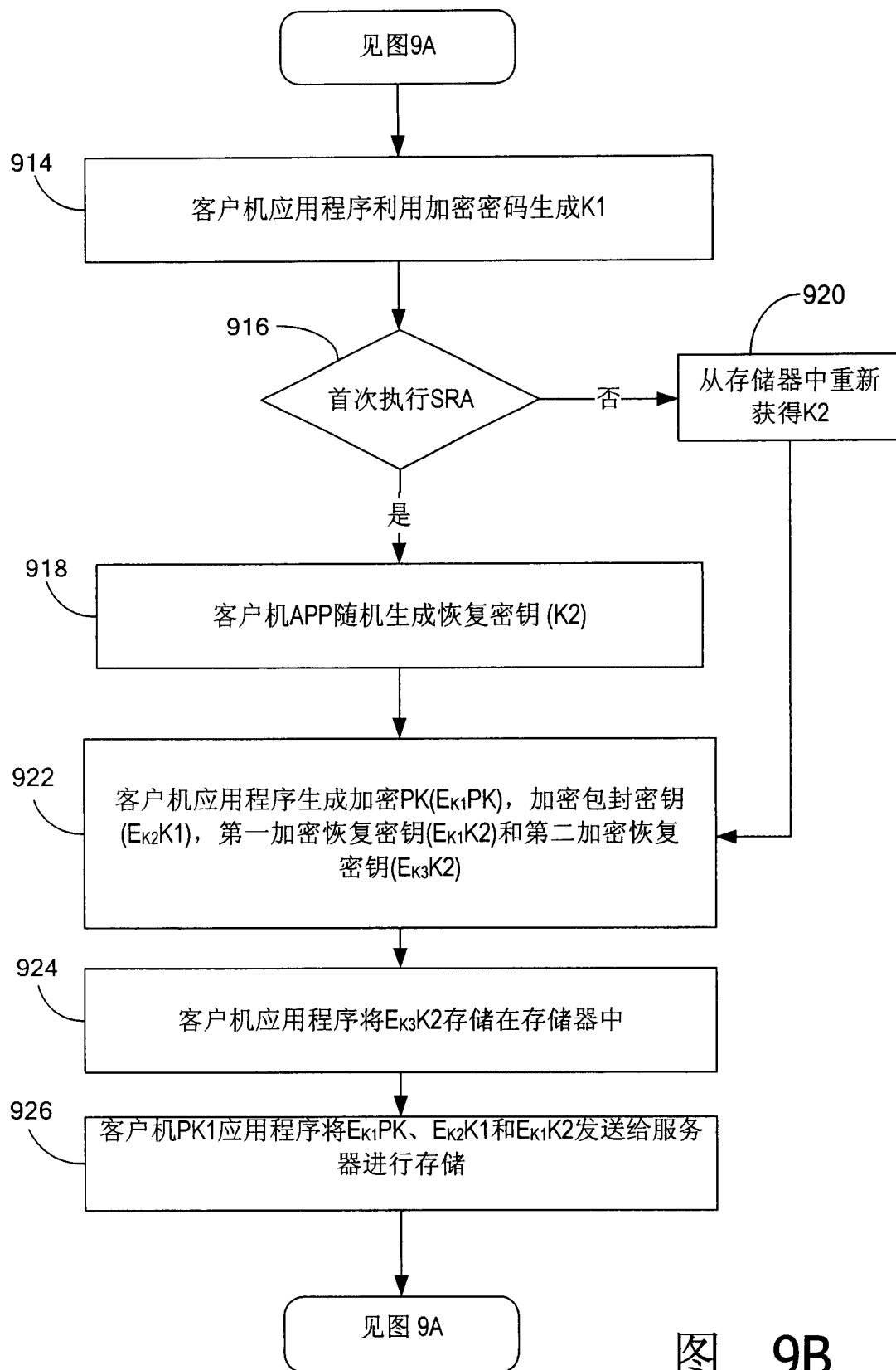


图 9B

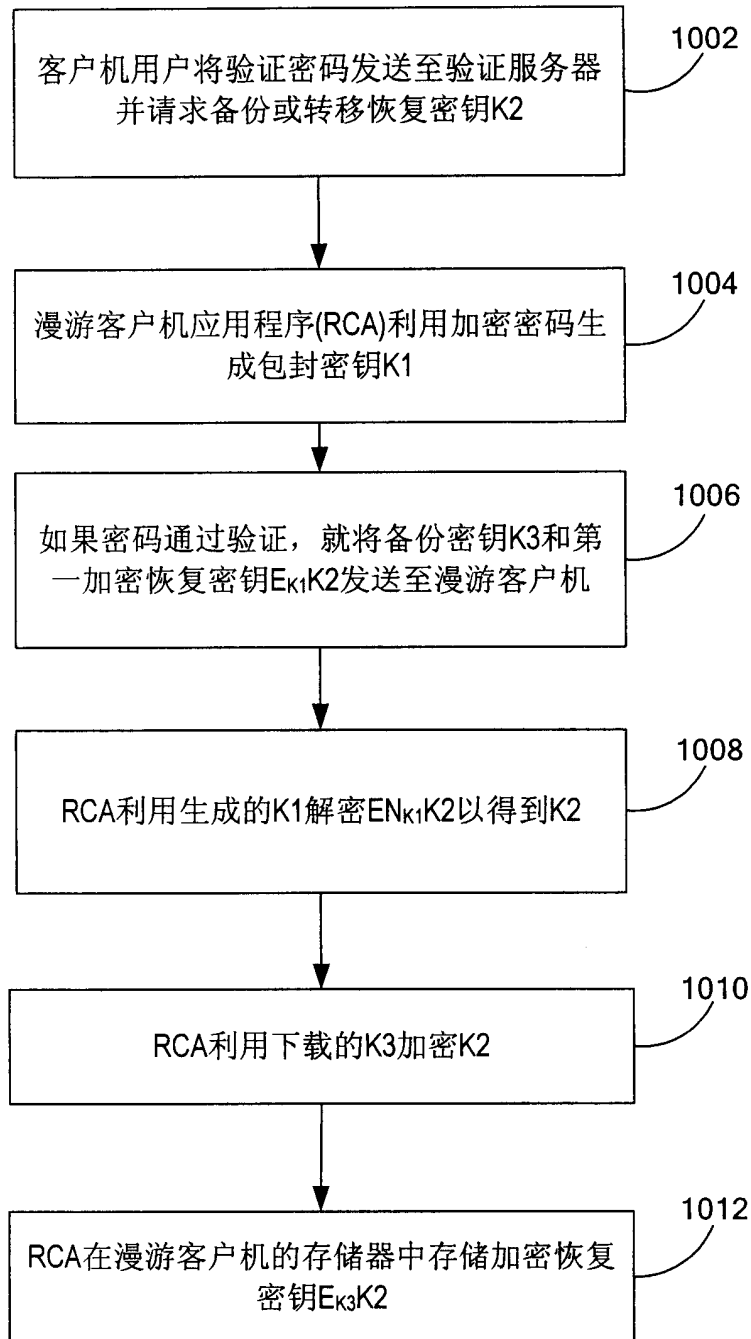


图 10

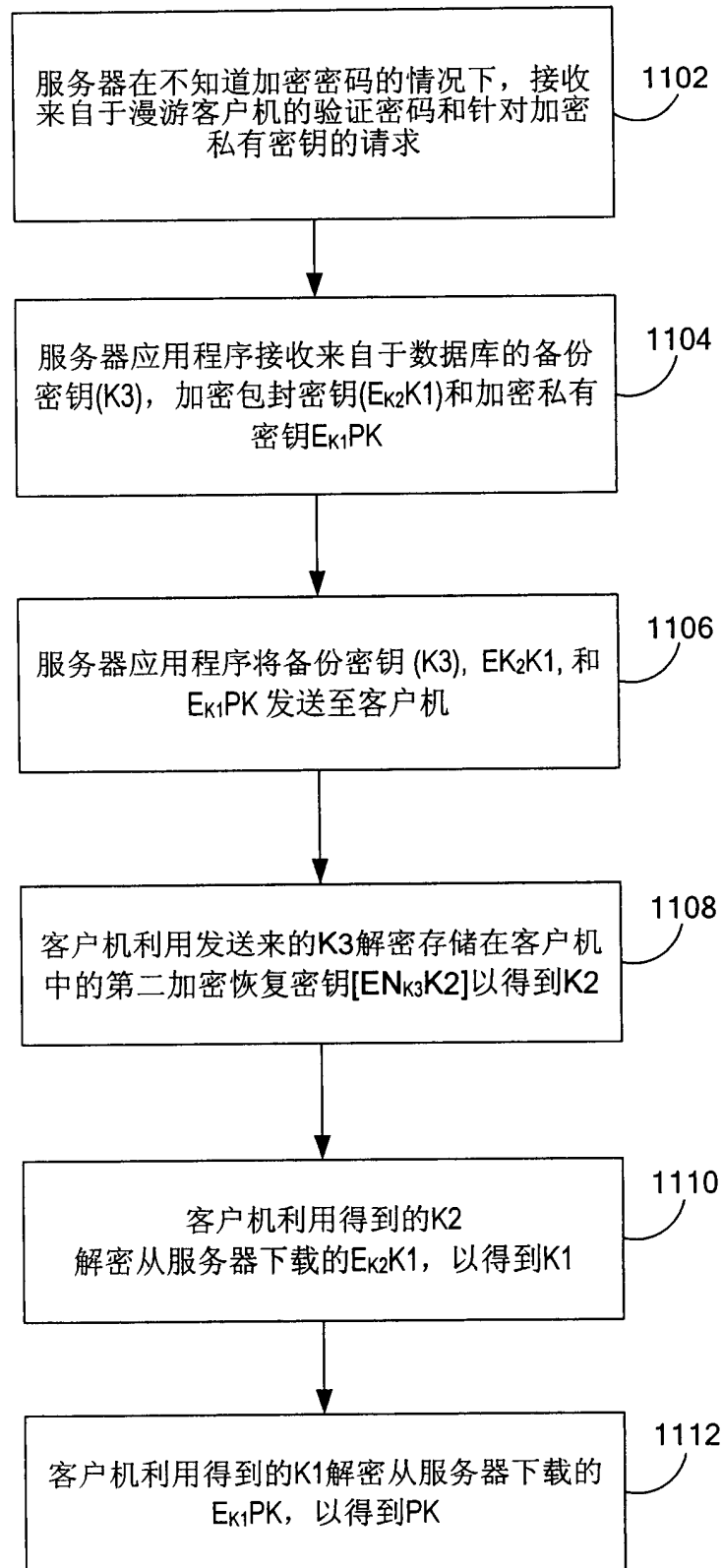


图 11

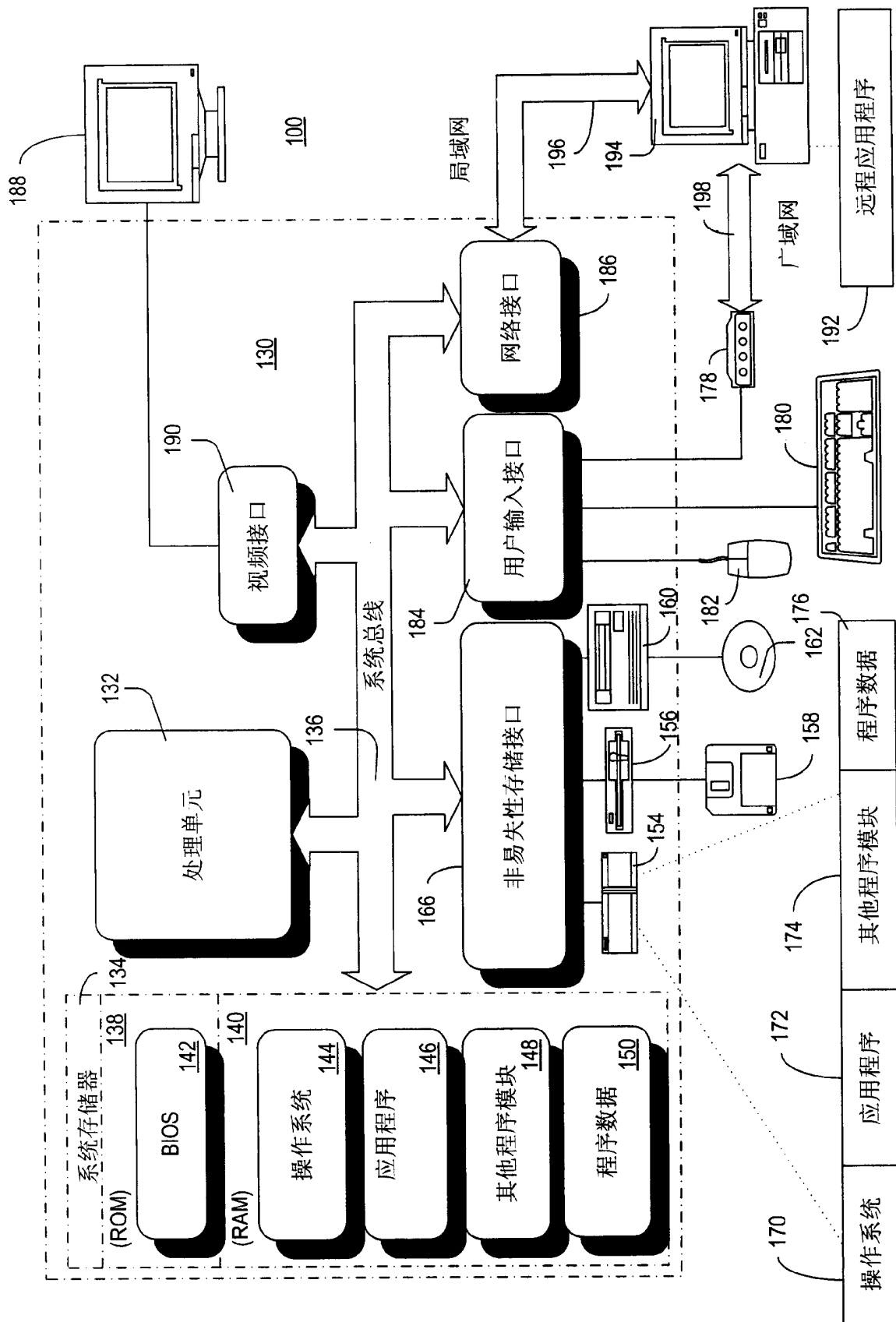


图 12