(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 104040938 B
(45)授权公告日 2017.10.27

(21)申请号 201380005234.9
(22)申请日 2013.01.12
(65)同一申请的已公布的文献号
申请公布号 CN 104040938 A
(43)申请公布日 2014.09.10
(30)优先权数据
13/350,661 2012.01.13 US
(85)PCT国际申请进入国家阶段日
2014.07.11
(86)PCT国际申请的申请数据
PCT/US2013/021344 2013.01.12
(87)PCT国际申请的公布数据
WO2013/106798 EN 2013.07.18

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 伊万·休·麦克莱恩
劳伦斯·G·伦德布拉德
布赖恩·哈罗德·凯利
罗伯特·G·沃克
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 宋献涛

(51)Int.Cl.
H04L 9/08(2006.01)
审查员 鲁卉

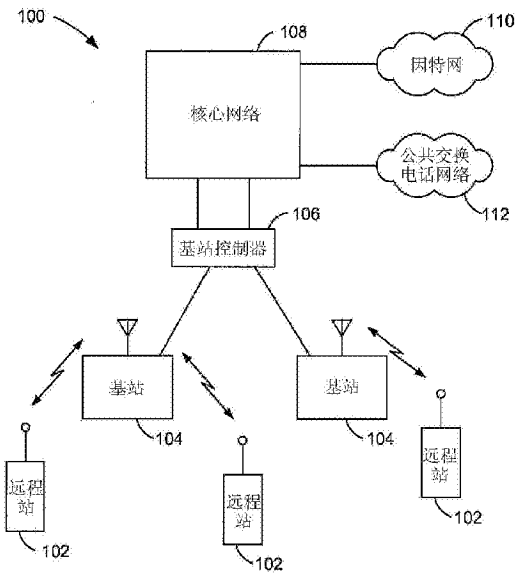
权利要求书3页 说明书6页 附图3页

(54)发明名称

用于产生基于权限的密钥的方法和设备

(57)摘要

本发明揭示了一种用于使用计算机来产生基于权限的密钥的方法。在所述方法中，权限从应用中被接收，并且验证为与所述应用相关联。所述计算机使用第一密钥以及所述权限以密码方式产生第二密钥。将所述第二密钥提供给所述应用。



CN 104040938 B

1.一种用于使用计算机来产生基于权限的密钥的方法,其包括:

由客户端环境从密钥请求应用中接收权限列表,其中数字签名是基于所述权限列表以及所述密钥请求应用的程序代码,且其中每一权限是对所述密钥请求应用访问和/或使用资源的权利的指示;

由所述客户端环境使用所述数字签名验证所述权限列表与所述密钥请求应用相关联;

在所述权限列表经所述客户端环境验证时:

由所述客户端环境将经验证权限列表传送到安全硬件;

由所述安全硬件使用第一密钥以及所述经验证权限列表以密码方式产生第二密钥;以及

由所述安全硬件将所述第二密钥提供给所述密钥请求应用。

2.根据权利要求1所述的用于产生基于权限的密钥的方法,其中所述第一密钥是共享秘密密钥。

3.根据权利要求1所述的用于产生基于权限的密钥的方法,其中所述第一密钥是对装置唯一的装置密钥。

4.根据权利要求1所述的用于产生基于权限的密钥的方法,其中所述第二密钥是加密密钥。

5.根据权利要求1所述的用于产生基于权限的密钥的方法,其中所述第二密钥是临时会话密钥。

6.根据权利要求1所述的用于产生基于权限的密钥的方法,其中所述权限列表包括文件系统许可。

7.根据权利要求1所述的用于产生基于权限的密钥的方法,其中所述权限列表包括资源访问权。

8.根据权利要求1所述的用于产生基于权限的密钥的方法,其中所述权限列表包括32位整数。

9.根据权利要求1所述的用于产生基于权限的密钥的方法,其中使用所述第一密钥以及所述权限列表以密码方式产生所述第二密钥包括将所述第一密钥以及所述权限列表用作输入来执行散列以产生所述第二密钥。

10.根据权利要求1所述的用于产生基于权限的密钥的方法,其中使用所述第一密钥以及所述权限列表以密码方式产生所述第二密钥包括将所述第一密钥以及所述权限列表用作输入来执行单向密码操作以产生所述第二密钥。

11.一种用于产生基于权限的密钥的设备,其包括:

用于从密钥请求应用中接收权限列表的装置,其中数字签名是基于所述权限列表以及用于所述密钥请求应用的代码,且其中每一权限是对所述密钥请求应用访问和/或使用资源的权利的指示;

用于使用所述数字签名验证所述权限列表与所述密钥请求应用相关联的装置;及用于在所述权限列表经验证时传送经验证权限列表的装置;

用于使用第一密钥以及所述经验证权限列表以密码方式产生第二密钥的装置;以及

用于将所述第二密钥提供给所述密钥请求应用的装置。

12.根据权利要求11所述的用于产生基于权限的密钥的设备,其中所述第一密钥是共

享秘密密钥。

13.根据权利要求11所述的用于产生基于权限的密钥的设备，其中所述第一密钥是对装置唯一的装置密钥。

14.根据权利要求11所述的用于产生基于权限的密钥的设备，其中所述第二密钥是加密密钥。

15.根据权利要求11所述的用于产生基于权限的密钥的设备，其中所述第二密钥是临时会话密钥。

16.根据权利要求11所述的用于产生基于权限的密钥的设备，其中所述权限列表包括文件系统许可。

17.根据权利要求11所述的用于产生基于权限的密钥的设备，其中所述权限列表包括资源访问权。

18.根据权利要求11所述的用于产生基于权限的密钥的设备，其中所述权限列表包括32位整数。

19.根据权利要求11所述的用于产生基于权限的密钥的设备，其中用于使用所述第一密钥以及所述权限列表以密码方式产生所述第二密钥的装置包括用于将所述第一密钥以及所述权限列表用作输入来执行散列以产生所述第二密钥的装置。

20.根据权利要求11所述的用于产生基于权限的密钥的设备，其中用于使用所述第一密钥以及所述权限列表以密码方式产生所述第二密钥的装置包括用于将所述第一密钥以及所述权限列表用作输入来执行单向密码操作以产生所述第二密钥的装置。

21.一种用于产生基于权限的密钥的设备，其包括：

存储器，所述存储器经配置以存储数据；以及

处理器，所述处理器经配置以：

从密钥请求应用中接收权限列表，其中数字签名是基于所述权限列表以及所述密钥请求应用的代码，且其中每一权限是对所述密钥请求应用访问和/或使用资源的权利的指示；

使用所述数字签名验证所述权限列表与所述密钥请求应用相关联；及

在所述权限列表经验证时将经验证权限列表传送到安全硬件；及

所述安全硬件经配置以：

使用所述权限列表以及存储在所述存储器中的第一密钥以密码方式产生第二密钥；以及

将所述第二密钥提供给所述密钥请求应用。

22.根据权利要求21所述的用于产生基于权限的密钥的设备，其中所述第一密钥是共享秘密密钥。

23.根据权利要求21所述的用于产生基于权限的密钥的设备，其中所述第一密钥是对装置唯一的装置密钥。

24.根据权利要求21所述的用于产生基于权限的密钥的设备，其中所述第二密钥是加密密钥。

25.根据权利要求21所述的用于产生基于权限的密钥的设备，其中所述第二密钥是临时会话密钥。

26.根据权利要求21所述的用于产生基于权限的密钥的设备，其中所述权限列表包括

文件系统许可。

27.根据权利要求21所述的用于产生基于权限的密钥的设备，其中所述权限列表包括资源访问权。

28.根据权利要求21所述的用于产生基于权限的密钥的设备，其中所述权限列表包括32位整数。

29.根据权利要求21所述的用于产生基于权限的密钥的设备，其中使用所述第一密钥以及所述权限列表以密码方式产生所述第二密钥包括将所述第一密钥以及所述经验证权限列表用作输入来执行散列以产生所述第二密钥。

30.根据权利要求21所述的用于产生基于权限的密钥的设备，其中使用所述第一密钥以及所述权限列表以密码方式产生所述第二密钥包括将所述第一密钥以及所述经验证权限列表用作输入来执行单向密码操作以产生所述第二密钥。

用于产生基于权限的密钥的方法和设备

技术领域

[0001] 本发明大体上涉及将安全密码密钥提供给应用。

背景技术

[0002] 通信领域具有许多应用，所述应用包含(例如)寻呼、无线本地环路、因特网电话以及卫星通信系统。示例性应用是用于移动订户的蜂窝式电话系统。(如本文中所使用，术语“蜂窝式”系统涵盖蜂窝式以及个人通信服务(PCS)系统频率两者。)经设计以使多个用户访问常见通信媒体的现代通信系统(例如，无线通信系统)已经研发用于此类蜂窝式系统。这些现代通信系统可以基于多址技术或所属领域中已知的其它调制技术，所述多址技术例如码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)、空分多址(SDMA)、极分多址(PDMA)。这些调制技术对从通信系统的多个用户中接收的信号解调，由此实现通信系统的容量上的增加。在与其的连接中，已经建立各种无线通信系统，所述无线通信系统包含(例如)高级移动电话服务(AMPS)、全球移动通信系统(GSM)以及其它无线系统。

[0003] 在FDMA系统中，将总频谱划分成许多较小的子带并且给予每一个用户其自身的子带以访问通信媒体。替代地，在TDMA系统中，将总频谱划分成许多较小的子带，在许多用户之中共享每一个子带，并且使每一个用户使用所述子带在预定时隙传输。CDMA系统提供了与其它类型的系统相比可能的优点，所述优点包含增加的系统容量。在CDMA系统中，在所有时间上给予每一个用户整个频谱，但通过唯一码的使用区分其传输。

[0004] 安全通信通常包括使用安全密钥的数据加密。必须安全地维持所述密钥，从而产生密钥存储以及管理技术。

[0005] 因此需要用于有效提供安全密钥的技术。

发明内容

[0006] 本发明的一个方面可以在于一种用于使用计算机来产生基于权限的密钥的方法。在所述方法中，权限从应用中被接收，并且验证为与所述应用相关联。计算机使用第一密钥以及权限以密码方式产生第二密钥。将第二密钥提供给所述应用。

[0007] 在本发明的更加详细的方面中，第一密钥可以是共享秘密密钥，和/或对于装置唯一的装置密钥。第二密钥可以是加密密钥，例如临时会话密钥。权限可以包含文件系统许可或资源访问权，并且可以利用32位的整数来表示。使用第一密钥以及权限以密码方式产生第二密钥可以包含将第一密钥以及权限用作输入来执行散列、或类似的单向密码操作以产生第二密钥。

[0008] 本发明的另一方面可以在于一种用于产生基于权限的密钥的设备，所述设备包括：用于从应用中接收权限的装置；用于验证权限与所述应用相关联的装置；用于使用第一密钥以及权限以密码方式产生第二密钥的装置；以及用于将第二密钥提供给所述应用的装置。

[0009] 本发明的另一方面可以在于一种用于产生基于权限的密钥的设备，所述设备包

括：存储器，所述存储器经配置以存储数据；以及处理器，所述处理器经配置以：从应用中接收权限；验证权限与所述应用相关联；使用权限以及存储在存储器中的第一密钥以密码方式产生第二密钥；以及将第二密钥提供给所述应用。

[0010] 本发明的另一方面可以在于一种计算机程序产品，所述计算机程序产品包括：计算机可读媒体，所述计算机可读媒体包括：用于使计算机从应用中接收权限的代码；用于使计算机验证权限与所述应用相关联的代码；用于使计算机使用权限以及第一密钥以密码方式产生第二密钥的代码；以及将第二密钥提供给所述应用。

附图说明

[0011] 图1是示出无线通信系统的实例的框图。

[0012] 图2是根据本发明的一种用于产生基于权限的密钥的方法的流程图。

[0013] 图3是示出用于实施用于产生基于权限的密钥的方法的计算机实例框图。

[0014] 图4是根据本发明的一种用于产生基于权限的密钥的方法的另一流程图。

具体实施方式

[0015] 本文使用词“示例性”来意指“用作实例、例子或说明”。本文中被描述为“示例性的”任何实施例不必被理解为比其它实施例优选或有利。

[0016] 远程站，也被称为移动站(MS)、接入终端(AT)、用户设备或订户单元，可以是移动的或静止的，并且可以与一个或多个也被称为基站收发信台(BTS)或节点B的基站通信。远程站通过一个或多个基站将数据包传输到基站控制器并且从基站控制器接收数据包，所述基站控制器也被称为无线网络控制器(RNC)。基站以及基站控制器是被称为接入网络的网络的多个部分。接入网络在多个远程站之间输送数据包。接入网络可以进一步连接到接入网络外部的另外网络(例如，企业内部网络或因特网)上，并且可以在每一个远程站与此类外部网络之间输送数据包。已建立与一个或多个基站的有效业务信道连接的远程站被称为有效远程站，并且据称处于业务状态中。在建立与一个或多个基站的有效业务信道连接的过程中的远程站据称处于连接设置状态中。远程站可以是通过无线信道通信的任何数据装置。远程站此外可以是许多类型的装置中的任一者，所述装置包含但不限于PC卡、压缩闪存、外部或内部调制解调器或无线电话。远程站向基站发送信号所通过的通信链路被称为上行链路，也被称为反向链路。基站向远程站发送信号所通过的通信链路被称为下行链路，也被称为前向链路。

[0017] 参考图1，无线通信系统100包含一个或多个无线远程站(RS)102、一个或多个基站(BS)104、一个或多个基站控制器(BSC)106以及核心网络108。核心网络可以经由合适的回程连接到因特网110以及公共交换电话网络(PSTN)112上。典型的无线移动站可以包含手持式电话或膝上型计算机。无线通信系统100可以采用许多多址技术中的任一者或所属领域中已知的其它调制技术，所述多址技术例如码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)、空分多址(SDMA)、极分多址(PDMA)。

[0018] 参考图2到4，本发明的一个方面可以在于一种用于使用计算机300来产生基于权限的密钥的方法200。在所述方法中，权限420从应用430中被接收(步骤210)，并且验证为与所述应用相关联(步骤220)。计算机300使用第一密钥450以及权限以密码方式产生第二密

钥440(步骤230)。将第二密钥440提供给所述应用(步骤240)。

[0019] 在本发明的更加详细的方面中,第一密钥450可以是共享秘密密钥,和/或对于装置唯一的装置密钥。此外,第一密钥可以是可以充当密钥的标识符。第二密钥440可以是加密密钥,例如临时会话密钥。权限420可以包含文件系统许可或资源访问权,并且可以利用整数来表示,例如32位、64位、128位等的整数。使用第一密钥以及权限以密码方式产生第二密钥可以包含将第一密钥以及权限用作产生第二密钥的输入来执行散列或HMAC(基于散列的消息认证码)等任何合适的单向密码操作。

[0020] 远程站102可以是计算机300,所述计算机包含具有安全硬件320的处理器310、存储器(和/或磁盘驱动器)330、显示器340以及小键盘或键盘350。所述计算机还可以包含麦克风、扬声器、相机、网络浏览器软件及类似者。此外,远程站102还可以包含用于在网络(例如因特网110)上通信的USB、以太网以及类似接口360,并且可以是移动站。

[0021] 本发明的另一方面可以在于一种用于产生基于权限的密钥的设备300,所述设备包括:用于从应用430中接收权限420的装置310;用于验证权限与所述应用相关联的装置310;用于使用第一密钥450以及权限以密码方式产生第二密钥440的装置310;以及用于将第二密钥提供给所述应用的装置310。

[0022] 本发明的另一方面可以在于一种用于产生基于权限的密钥的设备300,所述设备包括:存储器330,所述存储器经配置以存储数据;以及处理器310,所述处理器经配置以:从应用430中接收权限420;验证权限与所述应用相关联;使用权限以及存储在存储器中的第一密钥450以密码方式产生第二密钥440;以及将第二密钥提供给所述应用。

[0023] 本发明的另一方面可以在于一种计算机程序产品,所述计算机程序产品包括:计算机可读媒体330,所述计算机可读媒体包括:用于使计算机300从应用430中接收权限420的代码;用于使计算机验证权限与所述应用相关联的代码;用于使计算机使用权限以及第一密钥450以密码方式产生第二密钥440的代码;以及将第二密钥提供给所述应用。

[0024] 在本发明的一个方面中,提供一个用于基于所提供的权限420产生密码密钥440的机构。应用430可以通过呈现给定的权限从客户端平台300请求密钥440。在发出密钥440之前,请求中的应用由平台证实以便确保它是所提供的权限的有效持有者。代码签名通常用于固定应用430以及它被赋予的权限420的安全性以及有效性。

[0025] 所产生的密码密钥440可以用于加密数据、文件或敏感通信。希望建立与彼此的安全通信、或想要共享文件或数据的应用可以通过建立并且约定唯一的权限420来执行此。在典型的情境中,应用开发者声明相关的权限并且随后授权方对应用430进行数字签名。

[0026] 验证权限420与密钥请求应用430相关联可以使用数字签名来实现,所述数字签名使用所述应用以及相关联权限(许可)来产生,如第7,743,407号美国专利案中所描述。第7,743,407号美国专利案以引用的方式并入本文中。

[0027] 所提供的机构与传统的密钥管理/密钥存储方案相比具有许多优点。它基本上去掉了传统的集中式“安全密钥存储”的需要。它为应用提供了简单机构以用于共享信息或建立安全通信,不管所述应用是在相同装置上还是在不同装置上执行。它利用了现有的代码签名的安全性以及由客户端操作环境和平台460(例如BREW)提供的最小权限安全性模型。

[0028] 客户端环境460可以从应用430中接收权限420(步骤210),并且验证权限与所述应用相关联(步骤220)。客户端环境460随后可以将经验证的权限传送到安全硬件410(步骤

225)以用于第二密钥440的产生(步骤230)。

[0029] 第二密钥440可以借助于对所提供的权限420执行单向密码操作来产生。例如,第二密钥可以通过在所提供的权限以及一些不变的/秘密装置密钥或标识符450上执行散列来产生。更具体地说:

[0030] 第二密钥=散列(权限+装置密钥)。

[0031] 在另一方面中,共享秘密密钥450可以用于促进安全地共享跨越装置的应用之间的数据的能力。在此方面中,第二密钥440可以通过在权限420以及多个装置之间共享的秘密密钥450上执行散列来产生。更具体地说:

[0032] 第二密钥=散列(权限+共享秘密密钥)。

[0033] 此方法的益处是不需要直接使用共享秘密密钥。此外,在不同装置上的应用的例子之间不需要专用密钥建立或密钥共享。

[0034] 用于产生第二密钥440的单向密码操作可以由安全硬件320/410(和/或在存储保护边界内)执行。第一密钥(例如,装置密钥或共享秘密450)从未暴露在调用应用430或非系统代码下。

[0035] 安全性可以在最小权限以及代码签名的概念上建立。如果应用430希望获得安全密钥440,那么应用开发者决定权限420,并且当提交应用以由授权方签名时包含所述权限。权限可以基于以下理解来产生或选择:权限可以是对本应用唯一的,并且从未被赋予到任何其它应用。

[0036] 替代地,如果应用开发者希望应用430与其它受信任的应用安全地共享信息,那么权限420必须基于经建立的信任关系来产生/选择/约定。其它应用将仅利用权限所有者/创建者的认可所考虑的权限来成功地签名。任何其它利用权限来签名的请求都将被拒绝。

[0037] 因为第二密钥440“在运行中”产生,所以应用不需要维持安全密钥存储。当使用装置密钥450时,所产生的密钥440是每权限、每装置唯一的。对于在相同装置上的具有给定的权限420的密钥的请求将始终返回相同的第二密钥440,不管哪一个应用发出请求,或何时发出请求,或随时间推移所述请求被重复多少次。密钥的不变性质将调用应用430从密钥管理或安全密钥存储的任何责任中释放。第二密钥440可以被应用使用,并且随后被破坏。

[0038] 此外,出于不同但相关的目的,应用还自由地使用任何数目的不同权限420或权限集。因此例如,应用430可以保留用于保护它不想与任何其它应用共享的数据或文件的一个或多个权限。它可以约定可以用于安全地与给定的信任环内一组受限的应用共享一些其它信息的另一权限(或权限集)。并且它可以使用又另一个权限来确保一些其它信息的安全并且与具有不同的安全需求或信任级别的一组不同的应用共享所述信息。

[0039] 作为一个实例,游戏应用430可以使用专用权限420来检索仅用于加密其许可证信息的密码密钥440。权限以及相关联的密钥对所述应用是唯一的,并且不与任何其它应用、或甚至在不同装置上运行的相同应用共享。

[0040] 相同的游戏应用430可以使用不同的权限420′来检索用于加密客户端凭证的加密密钥440′。这些凭证可以安全地与来自相同供应商的其它应用(或甚至来自不同供应商的受信任应用)共享。在此情况下,意图将是使共享限于在相同装置上运行的应用。

[0041] 此外,相同的游戏应用430可以使用又另一个不同的权限420″来检索用于加密高分以及游戏状态信息的密钥440″。在此情况下,密钥产生可以基于权限420″以及共享秘密

450。以此方式保护的信息可以安全地在相同装置上的应用之间，或在不同装置上运行的具有所需权限的应用之间共享。

[0042] 不同的权限420与相关联的密码密钥440一起可以用于控制对相同资源的不同类型的访问。例如，经加密文件系统可以实施权限，使得权限A/密钥X可以允许读访问，而权限B/密钥Y可以允许读/写访问。

[0043] 所属领域的技术人员将理解，可以使用多种不同技术和技艺中的任一者来表示信息和信号。例如，可以通过电压、电流、电磁波、磁场或磁粒子、光场或光粒子或其任何组合来表示在整个上文描述中可能参考的数据、指令、命令、信息、信号、位、符号和芯片。

[0044] 所属领域的技术人员将进一步了解，可以将结合本文中所揭示的实施例而描述的各种说明性逻辑块、模块、电路和算法步骤实施为电子硬件、计算机软件或两者的组合。为清楚说明硬件与软件的此互换性，上文已大体关于其功能性描述了各种说明性组件、块、模块、电路以及步骤。此功能性是实施为硬件还是软件取决于特定应用以及施加在整个系统上的设计约束。所属领域的技术人员可以针对每一个特定应用以不同方式来实施所描述的功能性，但此类实施方案决定不应被解释为导致脱离本发明的范围。

[0045] 可以用通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或其经设计以执行本文中所描述的功能的任何组合来实施或执行结合本文中所揭示的实施例而描述的各种说明性逻辑块、模块以及电路。通用处理器可以是微处理器，但在替代方案中，处理器可以是任何常规的处理器、控制器、微控制器或状态机。处理器还可以实施为计算装置的组合，例如，DSP与微处理器的组合、多个微处理器、结合DSP核心的一个或多个微处理器，或任何其它此配置。

[0046] 结合本文中所揭示的实施例而描述的方法或算法的步骤可以直接在硬件中、在由处理器执行的软件模块中或在所述两者的组合中实施。软件模块可以存在于RAM存储器、快闪存储器、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可装卸磁盘、CD-ROM，或所述领域中已知的任何其它形式的存储媒体中。示例性存储媒体耦合到处理器上，使得处理器可以从存储媒体中读取信息并且将信息写入到存储媒体中。在替代方案中，存储媒体可以与处理器整合。处理器以及存储媒体可以存在于ASIC中。ASIC可以存在于用户终端中。在替代方案中，处理器以及存储媒体可以作为离散组件存在于用户终端中。

[0047] 在一个或多个示例性实施例中，所描述的功能可以在硬件、软件、固件或其任何组合中实施。如果作为计算机程序产品在软件中实施，那么可以将功能作为一个或多个指令或代码存储在计算机可读媒体上。计算机可读媒体包含便于将计算机程序从一个位置传送到另一个位置的计算机存储媒体。存储媒体可以为可以由计算机存取的任何可用媒体。借助实例且并非限制，此类计算机可读媒体可以包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储装置、磁盘存储装置或其它磁性存储装置，或可以用于存储呈指令或数据结构的形式的所需程序代码并且可以由计算机存取的任何其它媒体。如本文中所使用，磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软性磁盘和蓝光光盘，其中磁盘通常以磁性方式再现数据，而光盘利用激光以光学方式再现数据。上文的组合也应包含在计算机可读媒体的范围内。计算机可读媒体可以是非暂时性的，使得它不包含暂时的传播信号。

[0048] 提供所揭示实施例的先前描述以使所属领域的技术人员能够制作或使用本发明。所属领域的技术人员将容易明白对这些实施例的各种修改，并且在不脱离本发明的精神或范围的情况下，本文中所界定的一般原理可以应用于其它实施例。因此，本发明并不意图限于本文中所示出的实施例，而应符合与本文中所揭示的原理以及新颖特征一致的最广范围。

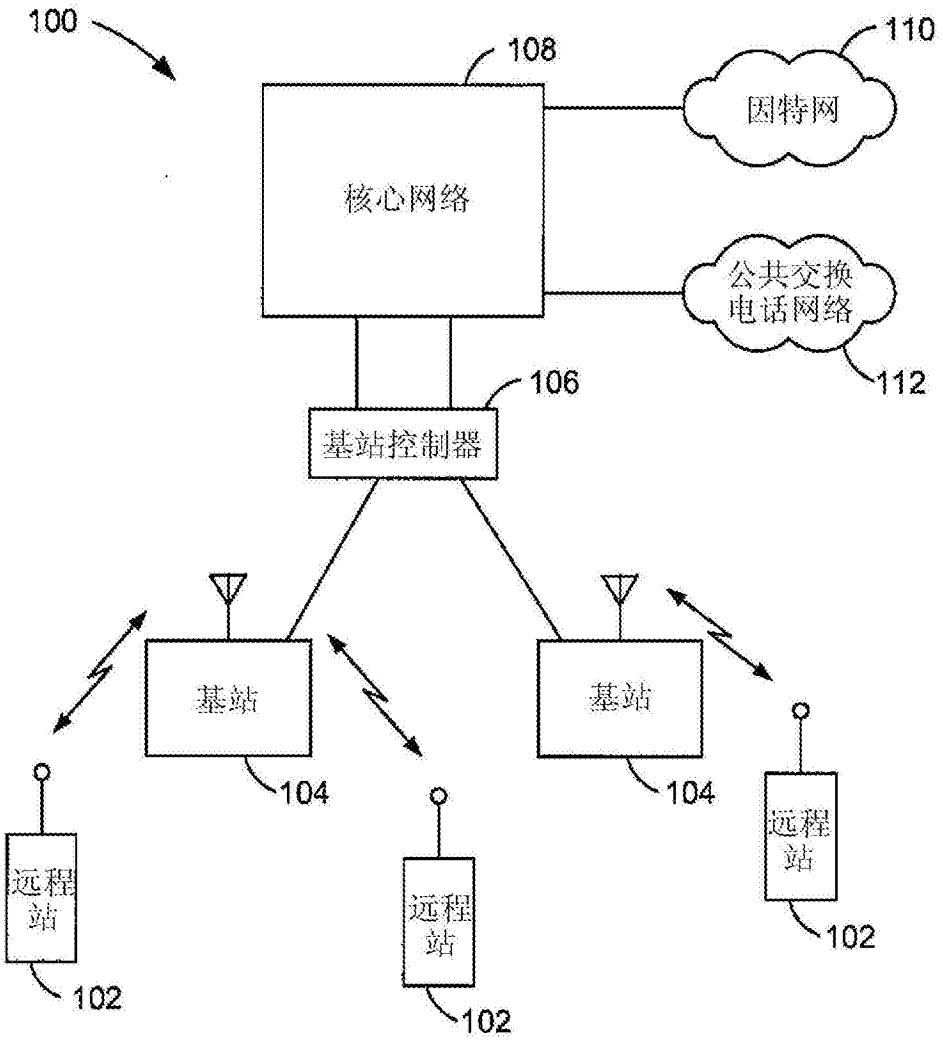

100
108
110
因特网
核心网络
公共交换
电话网络
112
106
基站控制器
基站
基站
104
104
远程
站
远程
站
远程
站
102
102
102

图1

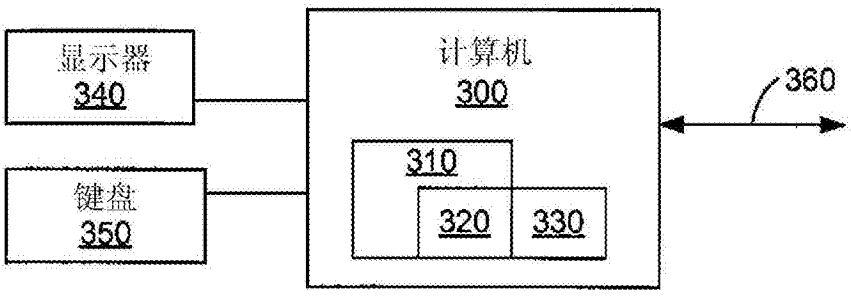

显示器
340
计算机
300
360
310
键盘
350
320
330

图3

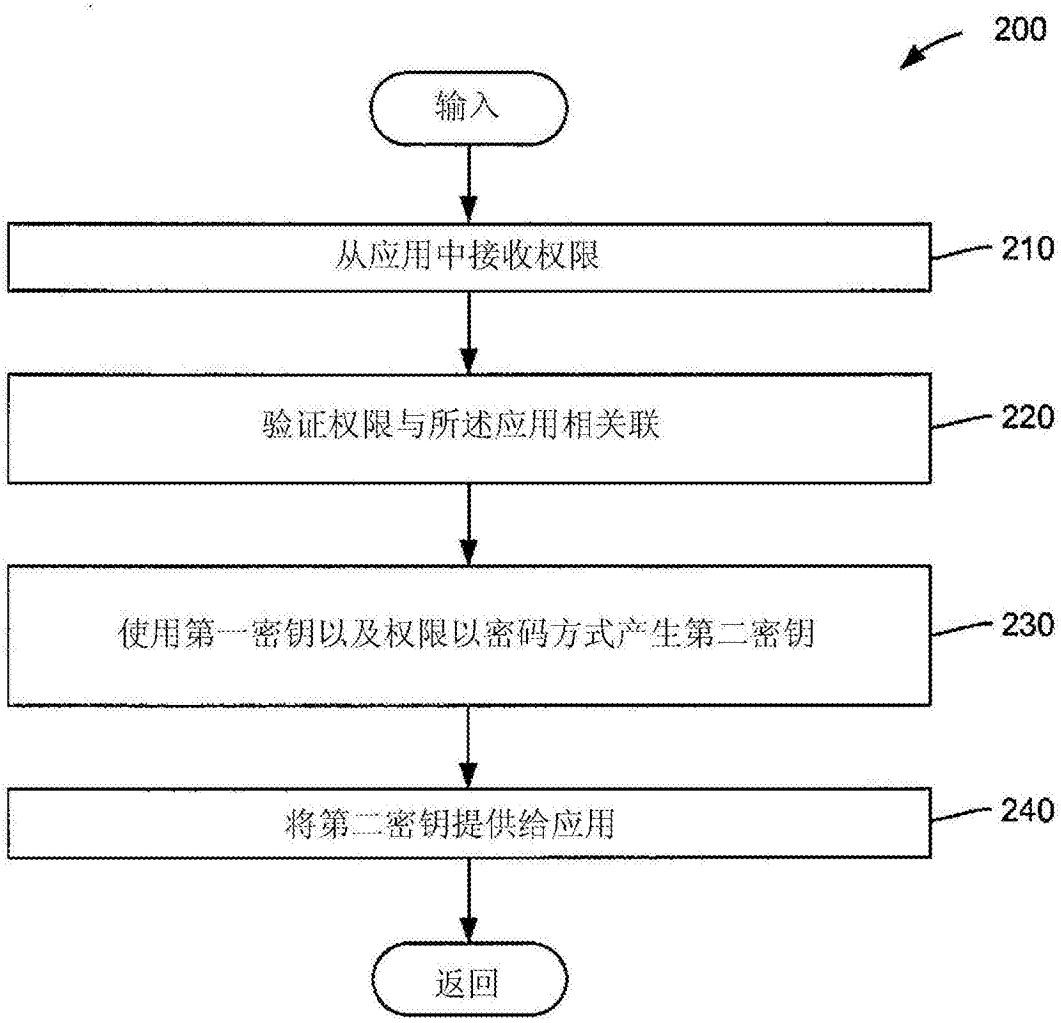

200
输入
从应用中接收权限
210
验证权限与所述应用相关联
220
使用第一密钥以及权限以密码方式产生第二密钥
230
将第二密钥提供给应用
240
返回

图2

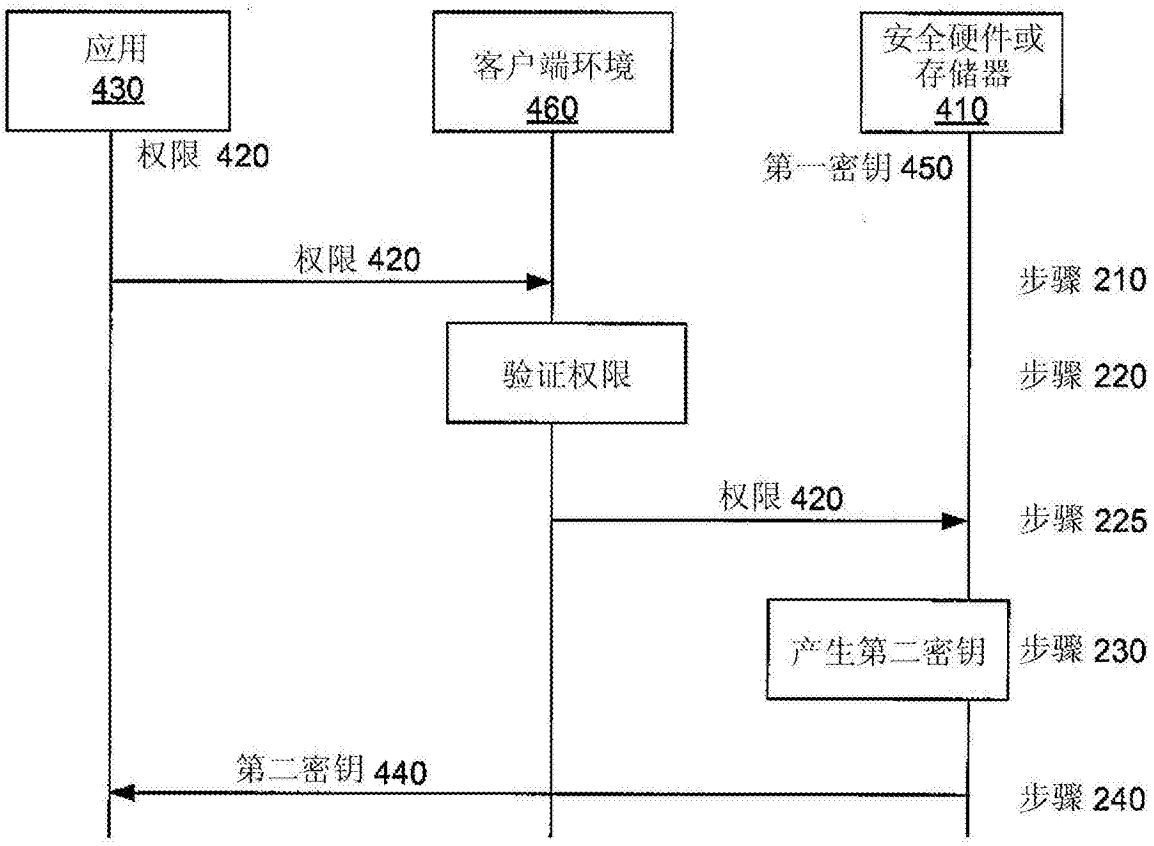

应用
430
客户端环境
460
安全硬件或
存储器
410
权限 420
第一密钥 450
权限 420
步骤 210
验证权限
步骤 220
权限 420
步骤 225
产生第二密钥
步骤 230
第二密钥 440
步骤 240

图4