



(12)发明专利申请

(10)申请公布号 CN 105849738 A

(43)申请公布日 2016.08.10

(21)申请号 201480071530.3

(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 11038

(22)申请日 2014.11.06

代理人 郑宗玉

(30)优先权数据

14/076,468 2013.11.11 US

(51)Int.Cl.

G06F 21/31(2006.01)

(85)PCT国际申请进入国家阶段日

G06F 21/46(2006.01)

2016.06.29

(86)PCT国际申请的申请数据

PCT/US2014/064379 2014.11.06

(87)PCT国际申请的公布数据

W02015/069921 EN 2015.05.14

(71)申请人 净睿存储股份有限公司

地址 美国加利福尼亚

(72)发明人 J·科尔格洛夫 E·米勒

J·海耶斯

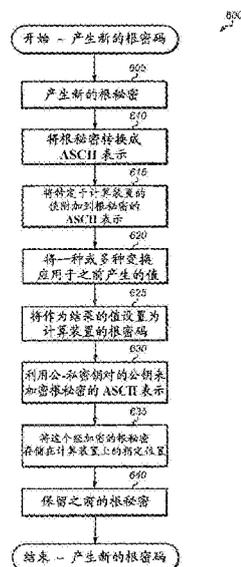
权利要求书2页 说明书8页 附图7页

(54)发明名称

存储阵列密码管理

(57)摘要

用于产生用于安全登入到存储阵列的密码的系统和方法。使用随机产生的根秘密以及区分ID产生用于在具有根特权的情况下登入到存储阵列中的根密码。根秘密被利用公-私密钥对的公钥加密并且存储在存储阵列上。经加密的根秘密随后被存储在存储阵列中。当需要进行根访问时,存储在存储阵列外部的私钥被用来对根秘密进行解密。然后使用经解密的根秘密以及区分ID重新产生根密码。



1. 一种系统,包括:
第一计算装置;和
第二计算装置,远程地连接到第一计算装置;
其中所述第一计算装置被配置为:
从随机产生的字符序列产生根秘密;
产生用于对第一计算装置进行根访问的根密码,其中基于根秘密产生根密码;
使用公-私密钥对的公钥来加密根秘密,其中公-私密钥对的私钥被存储在第二计算装置上;以及
将经加密的根秘密存储在所述第一计算装置上。
2. 如权利要求1所述的系统,其中基于根秘密和特定于第一计算装置的值的组合产生根密码。
3. 如权利要求2所述的系统,其中所述第一计算装置还被配置为在使用公-私密钥对的公钥来加密根秘密之前对根秘密执行一种或多种变换。
4. 如权利要求3所述的系统,其中所述一种或多种变换包括产生根秘密的美国信息交换标准码(ASCII)表示。
5. 如权利要求1所述的系统,其中所述第一计算装置还被配置为在产生新的根秘密和新的根密码之后保留之前存储的根秘密。
6. 如权利要求2所述的系统,其中所述第二计算装置被配置为:
使用公-私密钥对的私钥来解密经加密的根秘密;
从经解密的根秘密和特定于第一计算装置的值重新产生根密码。
7. 如权利要求1所述的系统,其中所述第一计算装置还被配置为在产生新的根秘密之前确定已有根秘密的寿命是否超过阈值。
8. 一种方法,包括:
在第一计算装置上从随机产生的字符序列产生根秘密;
产生用于对第一计算装置进行根访问的根密码,其中基于根秘密产生根密码;
使用公-私密钥对的公钥来加密根秘密,其中公-私密钥对的私钥被存储在第二计算装置上;以及
将经加密的根秘密存储在所述第一计算装置上。
9. 如权利要求8所述的方法,其中基于根秘密和特定于第一计算装置的值的组合产生根密码。
10. 如权利要求9所述的方法,还包括:在使用公-私密钥对的公钥来加密根秘密之前对根秘密执行一种或多种变换。
11. 如权利要求10所述的方法,其中所述一种或多种变换包括产生根秘密的美国信息交换标准码(ASCII)表示。
12. 如权利要求8所述的方法,还包括:在产生新的根秘密和新的根密码之后保留之前存储的根秘密。
13. 如权利要求9所述的方法,还包括:
在第二计算装置上使用公-私密钥对的私钥来解密经加密的根秘密;以及
从经解密的根秘密和特定于第一计算装置的值重新产生根密码。

14. 如权利要求8所述的方法,还包括:在产生新的根秘密之前确定已有根秘密的寿命是否超过阈值。

15. 一种存储程序指令的非暂态计算机可读存储介质,其中所述程序指令能由处理器执行以便:

在第一计算装置上从随机产生的字符序列产生根秘密;

产生用于对第一计算装置进行根访问的根密码,其中基于根秘密产生根密码;

使用公-私密钥对的公钥来加密根秘密,其中公-私密钥对的私钥被存储在第二计算装置上;以及

将经加密的根秘密存储在第一计算装置上。

16. 如权利要求15所述的计算机可读存储介质,其中基于根秘密和特定于第一计算装置的值的组合产生根密码。

17. 如权利要求16所述的计算机可读存储介质,其中所述程序指令还能由处理器执行以便在使用公-私密钥对的公钥来加密根秘密之前对根秘密执行一种或多种变换。

18. 如权利要求17所述的计算机可读存储介质,其中所述一种或多种变换包括产生根秘密的美国信息交换标准码(ASCII)表示。

19. 如权利要求15所述的计算机可读存储介质,其中所述程序指令还能由处理器执行以便在产生新的根秘密和新的根密码之后保留之前存储的根秘密。

20. 如权利要求15所述的计算机可读存储介质,其中所述程序指令还能由处理器执行以便:

在第二计算装置上使用公-私密钥对的私钥来解密经加密的根秘密;以及

从经解密的根秘密和特定于第一计算装置的值重新产生根密码。

存储阵列密码管理

技术领域

[0001] 本发明涉及管理用于存储阵列的密码。

背景技术

[0002] 企业日常管理的数据的数量和复杂性随着时间过去而持续增加。大规模存储阵列(诸如,数据中心)通常运行许多商业运营。数据中心(也可被称为服务器机房)是用于关于一个或多个企业的数据的存储、管理和传播的物理或虚拟的集中式存储库。如果存储阵列具有较差的性能,则公司运营可能受到损害。因此,存储阵列对数据可用性和高性能功能保持高标准。

[0003] 公司可能需要支持服务以确保其存储阵列的合适的操作。允许远程访问支持工程师是用于更新或解决影响存储阵列的问题的一种可能的解决方案。然而,允许远程访问存储阵列可能具有意外的结果。例如,未经授权的人可以能够通过获得远程地登入存储阵列所需的密码来远程地访问存储阵列上的敏感数据。根据存储阵列所需的支持的类型,可能需要不同级别的访问。

[0004] 传统计算机操作系统允许一些用户具有额外的特权和权限以修改计算机的操作系统。例如,操作系统可向用户提供不同级别的权限。给定的计算机操作系统可具有两个级别。可被称为根或管理员级别的第一级别允许用户具有修改计算机的无限能力。第二级别是分派给常规用户的级别。其他用户具有改变操作系统的有限权限或不具有改变操作系统的权限。这些用户在他们可以做什么方面以及在他们可以对计算机做什么改变方面受到限制。根据操作系统,一些计算机识别向一些用户授予另外的权利的其它中间级别。

[0005] 解决给定问题所需的支持级别可能需要支持工程师对存储阵列操作系统进行根访问。防止未经授权用户获得根访问同时仍然允许支持工程师进行根访问可能具有挑战性。

[0006] 考虑到以上情况,期望用于在存储阵列环境中管理密码的改进的技术。

发明内容

[0007] 设想用于在存储阵列中管理密码的系统和方法的各种实施例。

[0008] 在一个实施例中,存储阵列可在定期安排的基础上产生新的根密码,其中根密码允许对存储阵列的操作系统进行根访问。存储阵列可包括存储控制器和一个或多个存储装置。存储阵列可被耦合到一个或多个主机客户机系统。

[0009] 为了产生新的根密码,随机产生的字符序列(或根秘密)可与存储阵列的区分ID组合。在一个实施例中,根秘密可被转换成ASCII表示,然后区分ID可被附加到根秘密的ASCII表示。一种或多种变换也可被应用于这个值以创建新的根密码。然后,可针对存储阵列设置新的根密码。另外,可利用公-私密钥对的公钥来加密根秘密,然后经加密的根秘密可被存储在存储阵列上的指定文件中。仅存储阵列的经授权的本地用户可访问经加密的根秘密。公-私密钥对的私钥可被存储在存储阵列外部。

[0010] 当存储阵列的用户或管理员需要根访问时,用户可开始用于重新产生根密码的处理。为了重新产生根密码,经加密的根秘密可被传送给远程计算装置上的经授权的远程用户(诸如,支持工程师)。支持工程师可访问公-私密钥对的私钥。经授权的支持工程师可随后使用私钥来解密经加密的根秘密。支持工程师可随后使用根秘密和区分ID重新产生存储阵列的根密码。替代地,支持工程师可对经加密的根秘密进行解密,然后将根秘密传送给存储阵列的本地用户。用户可随后将根秘密与区分ID进行组合,然后执行一种或多种变换以创建根密码。用户可随后使用根密码在具有根特权的情况下登入到计算装置。

[0011] 在考虑到下面的描述和附图时,这些和其它实施例将会变得清楚。

附图说明

[0012] 图1是表示存储系统的一个实施例的一般性方框图。

[0013] 图2是表示用于远程地访问计算装置的系统的一个实施例的方框图。

[0014] 图3表示用于重新产生根密码的系统的一个实施例。

[0015] 图4表示密码产生单元的一个实施例的方框图。

[0016] 图5表示密码重新产生单元的一个实施例的方框图。

[0017] 图6是表示用于产生新的根密码的方法的一个实施例的一般性流程图。

[0018] 图7是表示用于重新产生根密码的方法的一个实施例的一般性流程图。

[0019] 尽管本发明容易具有各种变型和替代形式,但在附图中作为例子示出特定实施例并且在这里详细地描述特定实施例。然而,应该理解,附图及其详细说明并不旨在将本发明限制于所公开的特定形式,而是相反地,本发明应该覆盖落在如所附权利要求所定义的本发明的精神和范围内的所有变型、等同物和替代物。

具体实施方式

[0020] 在下面的说明中,阐述了许多特定细节以提供对本发明的透彻理解。然而,本领域普通技术人员应该意识到,可在没有这些特定细节的情况下实施本发明。在一些实例中,公知电路、结构、信号、计算机程序指令和技术未被详细示出以避免模糊本发明。

[0021] 现在参照图1,示出存储系统100的一个实施例的一般性方框图。存储系统100可包括存储控制器110以及存储装置组130和140,存储装置组130和140代表任何数量的存储装置组(或数据存储阵列)。如图中所示,存储装置组130包括存储装置135A-N,存储装置135A-N代表任何数量和类型的存储装置(例如,固态驱动器(SSD))。存储控制器110可直接耦合到工作站145,并且存储控制器110可远程地耦合到远程终端150。存储控制器110还可直接耦合到客户计算机系统125,并且存储控制器110可经由网络120远程地耦合到客户计算机系统115。客户机115和125代表可使用存储控制器110在系统100中存储和访问数据的任何数量的客户机。注意,一些系统可仅包括直接或远程地连接到存储控制器110的单个客户机。

[0022] 存储控制器110可包括被配置为提供对存储装置135A-N的访问的软件和/或硬件。虽然存储控制器110被示出为与存储装置组130和140分开,但在一些实施例中,存储控制器110可位于存储装置组130和140中的一个存储装置组内、或位于存储装置组130和140中的每个存储装置组内。存储控制器110可包括或耦合到基本操作系统(OS)、卷管理器和用于实现这里公开的各种技术的另外的控制逻辑。

[0023] 根据实施例,存储控制器110可包括任何数量的处理器和/或在任何数量的处理器上执行,并且可包括单个主机计算装置和/或在单个主机计算装置上执行或分散在多个主机计算装置上。在一些实施例中,存储控制器110可通常包括一个或多个文件服务器和/或块服务器或在一个或多个文件服务器和/或块服务器上执行。工作站145可被配置为允许用户或管理员登入到存储控制器110以管理和控制存储系统100。工作站145可为用户提供显示器和输入装置以与在存储控制器110上运行的OS和/或控制软件相接口连接。根据实施例,存储控制器110可运行任何类型的OS(例如,**Windows®**、**Unix®**、**Linux®**、**Solaris®**、**MacOS®**)。

[0024] 可存在用于从工作站145或远程终端150访问存储控制器110的不同级别的账号。第一级别可以是用于在存在于工作站145上的同时在本本地访问存储控制器110的用户账号。第二级别可以是用于从远程终端150远程地提供支持的支持工程师账号。支持工程师账号可能无法访问存储在存储装置组130和140中的客户数据。每个单独的用户可具有单独的密码,并且远程地登入的每个支持工程师也可具有唯一密码。第三级别可以是用于对存储控制器110进行根访问的根级别账号。根级别账号具有能够访问存储控制器110的所有命令和文件的根特权。根密码可通过加密方案来保护以防止未经授权的用户访问根密码并且故意损害系统100。

[0025] 注意,在替代实施例中,客户计算机、存储控制器、网络、存储装置组、工作站、远程终端和数据存储装置的数量和类型不限于图1中示出的数量和类型。另外,在各种实施例中,这里公开的方法和机制能够被实现在各种网络和系统(包括计算机系统、安全系统、无线网络、网络架构、数据中心、操作系统、通信装置和各种其它装置和系统)中。

[0026] 网络120可使用各种技术,包括无线连接、直接局域网(LAN)连接、广域网(WAN)连接(诸如因特网)、路由器、存储区域网络、以太网等。网络120可包括一个或多个LAN,所述一个或多个LAN也可以是无线的。网络120还可包括远程直接存储器存取(RDMA)硬件和/或软件、传输控制协议/因特网协议(TCP/IP)硬件和/或软件、路由器、中继器、交换机、网格等。诸如光纤信道、以太网光纤信道(FCoE)、iSCSI等的协议可被用在网络120中。网络120可与用于因特网的一组通信协议(诸如,传输控制协议(TCP)和因特网协议(IP)或TCP/IP)相接口连接。

[0027] 客户计算机系统115和125、远程终端150和工作站145代表任何数量和类型的静止或移动计算机,诸如桌上型个人计算机(PC)、服务器、服务器群组(server farm)、工作站、膝上型计算机、手持式计算机、服务器、个人数字助手(PDA)、智能电话等。一般而言,客户计算机系统115和125、远程终端150和工作站145包括一个或多个处理器,所述一个或多个处理器包括一个或多个处理器核。每个处理器核包括用于根据预定义的通用指令集来执行指令的电路。例如,可选择x86指令集架构。替代地,可选择**ARM®**、**Alpha®**、**PowerPC®**、**SPARC®**或任何其它通用指令集架构。处理器核可访问高速缓存子系统以获取数据和计算机程序指令。高速缓存子系统可耦合到包括随机存取存储器(RAM)和存储装置的存储器分级体系。

[0028] 现在参照图2,示出用于向计算装置提供远程支持的系统的一个实施例的方框图。存储阵列220可被配置为允许支持工程师210(使用计算装置215)经由网络225远程地登入到存储阵列220上的用户账号。存储阵列220可被配置为允许本地用户(使用计算装置205)

登入到存储阵列220上的更优先的用户账号。在一个实施例中,计算装置205可以是耦合到存储阵列220的工作站。在其它实施例中,计算装置205可以是各种其它类型的计算装置中的任何计算装置。

[0029] 在一个实施例中,支持工程师210可使用公钥验证经由安全外壳(SSH)远程地登入到存储阵列220上的用户账号。给定的支持工程师210可具有其自己的公-私密钥对以登入到这个账号中,并且这个账号可默认地不具有根特权。这个用户账号可允许支持工程师210在存储阵列220上运行非根支持。另外,可防止这个用户账号访问存储在存储阵列220中的顾客数据以保护这种客户数据。

[0030] 在一个实施例中,对支持工程师的用户账号的访问可由.ssh文件夹中的标准authorized_keys(经授权的密钥)文件控制。被授权访问存储阵列的多个不同支持工程师可分别在authorized_keys文件中具有他们自己的公钥。在一个实施例中,可与存储阵列分开地保持可访问存储阵列的支持工程师的列表,并且可根据需要使用SSH内的安全复制推出对这个列表的更新。安全复制表示在主机之间安全地传送计算机文件的方式,并且安全复制是基于SSH协议的。为了撤销特定支持工程师的访问,工程师的公钥可被从authorized_keys文件去除。可访问支持工程师用户账号的任何人可实现这一点,或者可在中心实现这一点并且推出给多个存储阵列。

[0031] 单独的公-私密钥对可被用于存储阵列220以便加密用于登入到存储阵列220的根账号中的根密码。公钥可被安装并且存储在存储阵列220上,并且私钥可仅对于经授权的远程用户而言是已知的。在一个实施例中,存储阵列220可定期地更新根密码。在一个实施例中,用于存储阵列220的根密码可以是两个值的函数。第一个值可以是随机字符序列,并且第二个值可以是分派给存储阵列220的区分标识符(ID)。在一个实施例中,区分ID可以是存储阵列220的序列号。

[0032] 在一个实施例中,存储阵列220可通过首先产生随机字符序列(将会被称为“根秘密”)来产生新密码。可随后使用美国信息交换标准码(ASCII)字符编码方案将根秘密转换成十六进制(hex)表示。接下来,区分ID可被附加到根秘密的hex ASCII形式,然后可通过散列函数运行这个值,其后转换成更适合人类阅读的形式。这个值可随后被用作根密码。此外,根秘密的ASCII表示可被利用公钥加密并且存储在与根秘密关联的文件中。例如,在一个实施例中,根秘密的ASCII表示可被存储在命名为“root-secret-yyyy-mm-dd-hh”的文件中。这个文件名可包括当产生根秘密时的时间戳(年、月、日、小时)。计算装置205的经授权的本地用户可访问存储的经加密的根秘密,但是远程用户(例如,支持工程师210)可能无法访问存储的经加密的根秘密。

[0033] 根密码可被用于登入到存储阵列220的根级别用户账号。根级别用户账号是用于许多类型的计算机操作系统上的系统管理的特殊用户账号。例如,在**Linux®**和其它基于**Unix®**的操作系统中,“根”是可访问所有命令和文件的用户名或账号。Linux中的根账号包括与**Windows®**操作系统中的管理员或超级用户账号的相似性。其它操作系统可包括通过不同名称表示的管理员账号。应该理解,术语“根”、“根账号”、“根用户”和“根特权”也旨在表示用于其它类型的操作系统的具有最高特权的其它类型的管理或特殊用户账号。

[0034] 如果在存储阵列220上存在多个分区,则在一个实施例中,可在所有分区上设置根密码。在另一实施例中,替代于在多个分区上使用同一根密码,可仅在当前引导的分区上更

新根密码。当引导其它分区时,可更新所述其它分区。这将会在非引导的分区上导致更长久的密码。可使用基于时间的作业调度器(例如,cron)来运行这个处理。在一个实施例中,可运行检查以确保:如果存在小于24小时的已有密码,则不产生新密码。可随后每小时地运行这个处理以确保定期地产生新密码。注意,在以上说明中使用的示例性时间周期可根据实施例而不同。

[0035] 在一个实施例中,在最近的密码变化存在问题的情况下,可保存最近的较早的根秘密。这允许存储阵列220删除比一些周期更早的根秘密,并且提供有限的一组可能的根秘密。在一个实施例中,具有存储经加密的根秘密的这些文件的目录仅可由根写入,并且可由存储阵列的本地用户账号读取,但是不可由远程支持工程师账号读取。使用这种方案,经授权的支持工程师可以进行根访问的唯一方式是:经授权的本地用户向支持工程师提供经加密的根秘密。使用这种方案,如果用户向支持工程师提供经加密的根秘密,或者如果支持工程师以物理方式存在于存储阵列220处并且具有系统管理员密码或根秘密,则支持工程师可作为根登入。

[0036] 在一个实施例中,根秘密可以是具有至少 2^{70} (10^{21})位的随机性的文字(或音节)和数字的组合。在一个实施例中,可使用与4位数字交替的文字产生根秘密。例如,根秘密可以是“food-4981-cat-3340-certain-2096”。这可提供大约72位的随机性,并且与随机字符的序列相比更容易阅读和理解。

[0037] 现在参照图3,示出用于向计算装置提供远程支持的系统的另一实施例的方框图。工作站305的本地用户308可访问存储阵列320上的用户账号。远程用户310可使用计算装置315经由网络325(例如,因特网)连接到存储阵列320。在一个实施例中,远程用户310可以是存储阵列320的支持工程师。远程用户310可能无法访问本地地存储在存储阵列320上的经加密的根秘密。远程用户325可访问用于对根秘密进行加密的公-私密钥中的私钥。本地用户308可能无法访问对经加密的根秘密进行解密所需的私钥。

[0038] 当本地用户308确定他们需要存储阵列320进行根访问时,本地用户305可向远程用户310提供经加密的根秘密(以及区分ID)。本地用户305还可向远程用户310提供存储阵列320的区分ID。远程用户310可接收经加密的根秘密,然后远程用户310可在计算装置315上开始用于重新产生根密码的处理。私钥可被存储在计算装置315上,或者远程用户310可在计算装置315上手动地输入私钥。计算装置315可随后对经加密的根秘密进行解密,并且经解密的根秘密在计算装置315的放大的屏幕截图中被示出为“FOOD-4981-CAT-3340-FOUNTAIN-2096”。接下来,计算装置315可将区分ID与根秘密组合,并且执行重新产生根密码所需的任何变换。根密码在该屏幕截图中被示出为“ART-1724-GOAL-1558-TIGER-9920”。远程用户310可随后将该根密码传送给本地用户308,以便使本地用户308能够作为根用户登入到存储阵列320。替代地,远程用户310可使用该根密码作为根用户登入到存储阵列320。

[0039] 现在参照图4,示出密码产生单元的一个实施例。密码产生单元400可包括用于产生用于主机计算装置(未示出)的根密码的多个逻辑单元。单元400可包括根秘密产生单元405,并且单元405可被配置为产生随机字符序列作为根秘密410。例如,在一个实施例中,可从与4位数字交替的文字建立根秘密410。例如,在这个实施例中,随机产生的根秘密410可以是:food-4981-cat-3340-fountain-2096。这可提供大约72位的随机性,并且与12个随机

字符的序列相比更容易阅读和理解。在其它实施例中,可使用各种其它技术中的任何技术随机产生根秘密410。

[0040] 接下来,根秘密410可被ASCII转换单元415转换成美国信息交换标准码(ASCII)形式。单元415可产生根秘密的ASCII表示420,并且这种ASCII表示420可被传送给加密单元425和组合单元430。加密单元425可利用公-私密钥对中的公钥435对根秘密的ASCII表示420进行加密。这个经加密的根秘密值455可被本地地存储在主机计算装置上。在一个实施例中,主机计算装置可以是存储阵列。在其它实施例中,主机计算装置可以是各种其它类型的计算装置中的任何计算装置。在一个实施例中,经加密的根秘密值455可被存储在命名为“root-secret-yyyy-mm-dd-hh”的文件中,其中“yyyy-mm-dd-hh”代表当创建经加密的根秘密值455时的时间戳(年、月、日和小时)。

[0041] ASCII表示420也可被传送给组合单元430。单元430还可接收区分ID 440作为输入。在一个实施例中,区分ID 440可以是主机计算装置的序列号,而在其它实施例中,区分ID 440可以是特定于主机计算装置的一个或多个其它值。在一个实施例中,组合单元430可将区分ID 440附加到ASCII表示420的末尾。在其它实施例中,组合430可对ASCII表示420和区分ID 440执行其它组合和/或变换(例如,XOR、散列)。替代地,在另一个实施例中,组合单元430可被从密码产生单元400省略,并且ASCII表示420可在这个实施例中被直接传送给变换单元445。

[0042] 变换单元445可对输入值执行一种或多种变换以产生根密码450。由单元445执行的变换的类型和数量可根据实施例而不同。例如,在一个实施例中,单元445可通过散列函数运行输入值,然后转换成更加人类友好的形式。注意,在一些实施例中,单元445可被从密码产生单元400省略。在产生根密码450之后,根密码450可被设置为主机计算装置上的密码。

[0043] 应该理解,密码产生单元400的方框图仅是密码产生单元的逻辑表示。可使用硬件和/或软件的任何组合实现密码产生单元400中示出的各种单元。例如,在一个实施例中,在一个或多个计算装置上执行的一个或多个软件程序可执行由密码产生单元400的各种单元代表的功能。注意,密码产生单元400仅是可在一个实施例中使用的密码产生单元的一个例子。在其它实施例中,可按照与图4中示出的方式不同的方式来组织单元400。另外,在其它实施例中,单元400还可包括其它部件和/或省略单元400中示出的一个或多个部件。

[0044] 现在参照图5,示出密码重新产生单元500的一个实施例的方框图。单元500可接收经加密的根秘密505、区分ID 510和私钥515作为输入。在一个实施例中,单元500可位于实际使用正在重新产生的根密码的计算装置外部。私钥515可以是与最初被用来对与根密码对应的根秘密进行加密的公-私密钥对中的公钥(例如,图4的公钥435)对应的私钥。

[0045] 解密单元520可被配置为使用私钥515对经加密的根秘密505进行解密。单元520的输出可以是根秘密525。根秘密525可随后被ASCII转换单元530转换成它的ASCII表示535。然后,ASCII表示535可在组合单元540中与区分ID 510组合。然后,组合单元540的输出可被传送给变换单元545。单元540和545可被配置为使在对应的密码产生单元(例如,图4的单元400)的类似单元中执行的操作逆转。单元545的输出可以是根密码550,根密码550可被经授权的用户使用以作为具有根特权的根用户登入到对应的计算装置。

[0046] 应该理解,密码重新产生单元500的方框图仅是密码重新产生单元的逻辑表示。可

使用硬件和/或软件的任何组合实现密码重新产生单元500中示出的各种单元。例如,在一个实施例中,在一个或多个计算装置上执行的一个或多个软件程序可执行由密码重新产生单元500的各种单元代表的功能。

[0047] 注意,密码重新产生单元500仅是可在一个实施例中使用的密码重新产生单元的一个例子。在其它实施例中,可按照与图5中示出的方式不同的方式来组织单元500。另外,在其它实施例中,单元500还可包括其它部件和/或省略单元500中示出的一个或多个部件。还注意,在一些实施例中,单元500的各部分可分散在多个位置,在与根密码对应的计算装置处执行一些功能,而从不同的计算装置远程地执行一些功能。

[0048] 现在参照图6,示出用于产生新的根密码的方法600的一个实施例。在整个本说明书中描述的各种计算装置中的任何计算装置可通常根据方法600操作。另外,在这个实施例中,按照顺序次序示出步骤。然而,一些步骤可按照与示出的次序不同的次序发生,一些步骤可被同时执行,一些步骤可与其它步骤组合,并且一些步骤可不存在于另一个实施例中。

[0049] 计算装置可产生新的根秘密(块605)。可在定期安排的基础上(例如,每日、每周)产生新的根秘密。在一个实施例中,计算装置可以是存储阵列。在其它实施例中,计算装置可以是其它类型的计算装置(例如,膝上型计算机、桌上型计算机、网络服务器、智能电话)。根秘密可以是随机产生的一批字符。在一个实施例中,根秘密可以是文字(或音节)和数字的组合。可选择根秘密的长度,以使得根秘密具有至少预定水平的随机性。

[0050] 接下来,根秘密可被转换成ASCII表示(块610)。在其它实施例中,根秘密可使用除ASCII码之外的其它类型的转换而被转换成二进制表示。替代地,可按照二进制格式产生根秘密,从而有效地将块605和610组合成单个步骤。接下来,特定于计算装置的值可被附加到根秘密的ASCII表示(块615)。在一个实施例中,特定于计算装置的值可以是计算装置的序列号。在其它实施例中,其它类型的值可被附加到根秘密或与根秘密组合。在另一个实施例中,根秘密可不与另一值组合。相反地,根秘密可被单独用于方法600的其余步骤。

[0051] 接下来,一种或多种变换可被应用于在块615中产生的值(块620)。在一个实施例中,这些变换可包括通过散列函数运行该值,然后转换成人类可阅读的形式。然后,这个作为结果的值可被设置为计算装置的根密码(块625)。如果在计算装置上存在多个分区,则在块620中产生的值可在所有分区上被设置为根密码。替代地,这个值可仅在当前引导的分区上被设置为根密码,在其它分区上保持根密码不变。

[0052] 此外,根秘密的ASCII表示可被利用公-私密钥对的公钥加密(块630)。然后,这个经加密的根秘密可被存储在计算装置上的指定位置(块635)。在一个实施例中,经加密的根秘密可被存储在具有基于当创建根秘密和对应根密码时的时间戳的文件名的文件中。注意,可在块620和625之前或者与块620和625同时执行块630和635。接下来,在新的根秘密存在问题的情况下,计算装置可保留之前的根秘密(块640)。计算装置可保留几个之前的根秘密,并且仅当旧的根秘密早于某个阈值数量的刷新周期时删除旧的根秘密。具有经加密的根秘密的这些文件的目录仅可由根写入,并且可由本地用户账号读取,但是不可被由远程用户(例如,非现场支持工程师)使用的账号读取。以这种方式,如果本地用户通过登入到本地用户账号来提供经加密的根秘密,则支持工程师仅可进行根访问。

[0053] 可在定期安排的基础上(例如,每日、每周)运行方法600。在一个实施例中,可在每日基础上产生新的根密码。在这个实施例中,可在计算装置上运行检查以确保:如果存在小

于24小时的已有根密码,则不产生新的根密码。可随后在每小时基础上运行方法600,首先执行检查以防止在存在小于24小时的已有根密码的情况下继续执行方法600。

[0054] 现在参照图7,示出用于重新产生根密码的方法700的一个实施例。在整个本说明书中描述的各种计算装置中的任何计算装置可通常根据方法700操作。另外,在这个实施例中,按照顺序次序示出步骤。然而,一些步骤可按照与示出的次序不同的次序发生,一些步骤可被同时执行,一些步骤可与其它步骤组合,并且一些步骤可不存在于另一个实施例中。

[0055] 经加密的根秘密可被从它的主机计算装置获取(块705)。在一个实施例中,可由主机计算装置的本地用户从合适的目录获取经加密的根秘密。接下来,经加密的根秘密可经由网络被传送给远程用户(块710)。在一个实施例中,远程用户可以是可访问对根秘密进行解密所需的公-私密钥对的私钥的支持工程师,并且远程用户可经由因特网连接到计算装置。接下来,可由远程用户使用公-私密钥对的私钥来解密根秘密(块715)。然后,根秘密可被从远程用户传送给计算装置的本地用户(块720)。接下来,可使用根秘密和特定于装置的值并且通过执行任何必要的变换来重建根密码(块725)。可执行各种变换以使当最初产生根密码时执行的任何变换逆转。替代地,在另一个实施例中,远程用户可重建根密码并且随后将根密码传送给本地用户。接下来,本地用户可使用根密码作为具有根特权的根用户在计算装置上登入(块730)。替代地,远程用户可使用根密码作为具有根特权的根用户在计算装置上登入。

[0056] 注意,上述实施例可包括软件。在这种实施例中,可在计算机可读介质上传送或存储实现所述方法和/或机制的程序指令。存在被配置为存储程序指令的许多类型的介质,并且所述许多类型的介质包括硬盘、软盘、CD-ROM、DVD、闪存、可编程ROM(PROM)、随机存取存储器(RAM)和各种其它形式的易失性或非易失性存储装置。

[0057] 在各种实施例中,这里描述的方法和机制的一个或多个部分可形成云计算环境的一部分。在这种实施例中,可根据一个或多个各种模型经由因特网提供资源作为服务。这种模型可包括基础设施即服务(IaaS)、平台即服务(PaaS)和软件即服务(SaaS)。在IaaS中,提供计算机基础设施作为服务。在这种情况下,计算装备通常由服务提供商拥有和操作。在PaaS模型中,由开发者用于开发软件解决方案的软件工具和底层装备可被提供作为服务并且由服务提供商拥有。SaaS通常包括服务提供商按照需要来许可软件作为服务。服务提供商可托管软件,或者可在给定时间段期间将软件部署给顾客。可实现并且可设想以上模型的许多组合。

[0058] 虽然已非常详细地描述了以上实施例,但一旦充分理解以上公开,许多变化和修改将会对于本领域技术人员而言变得清楚。下面的权利要求书旨在被解释为包括所有这种变化和修改。

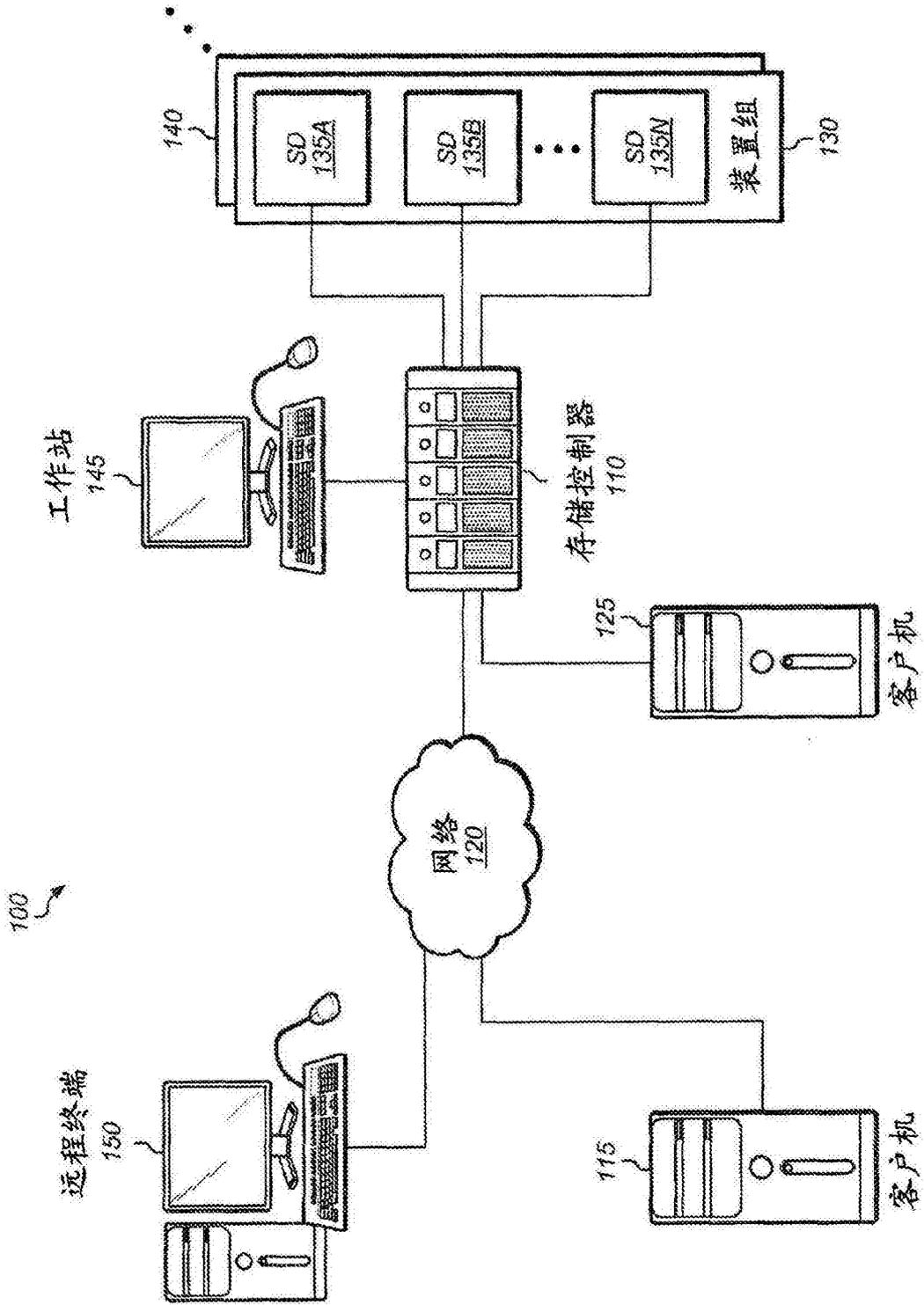


图1

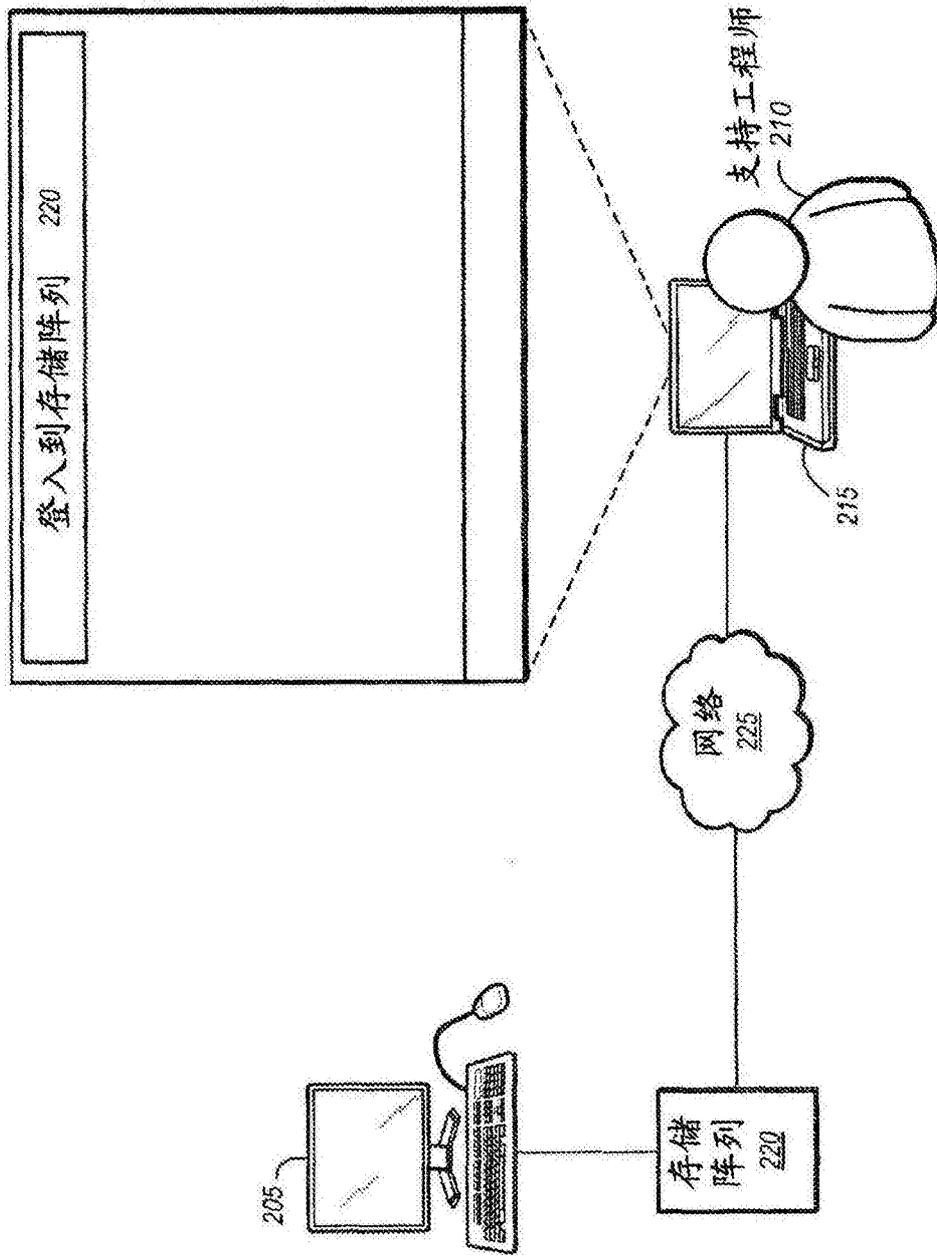


图2

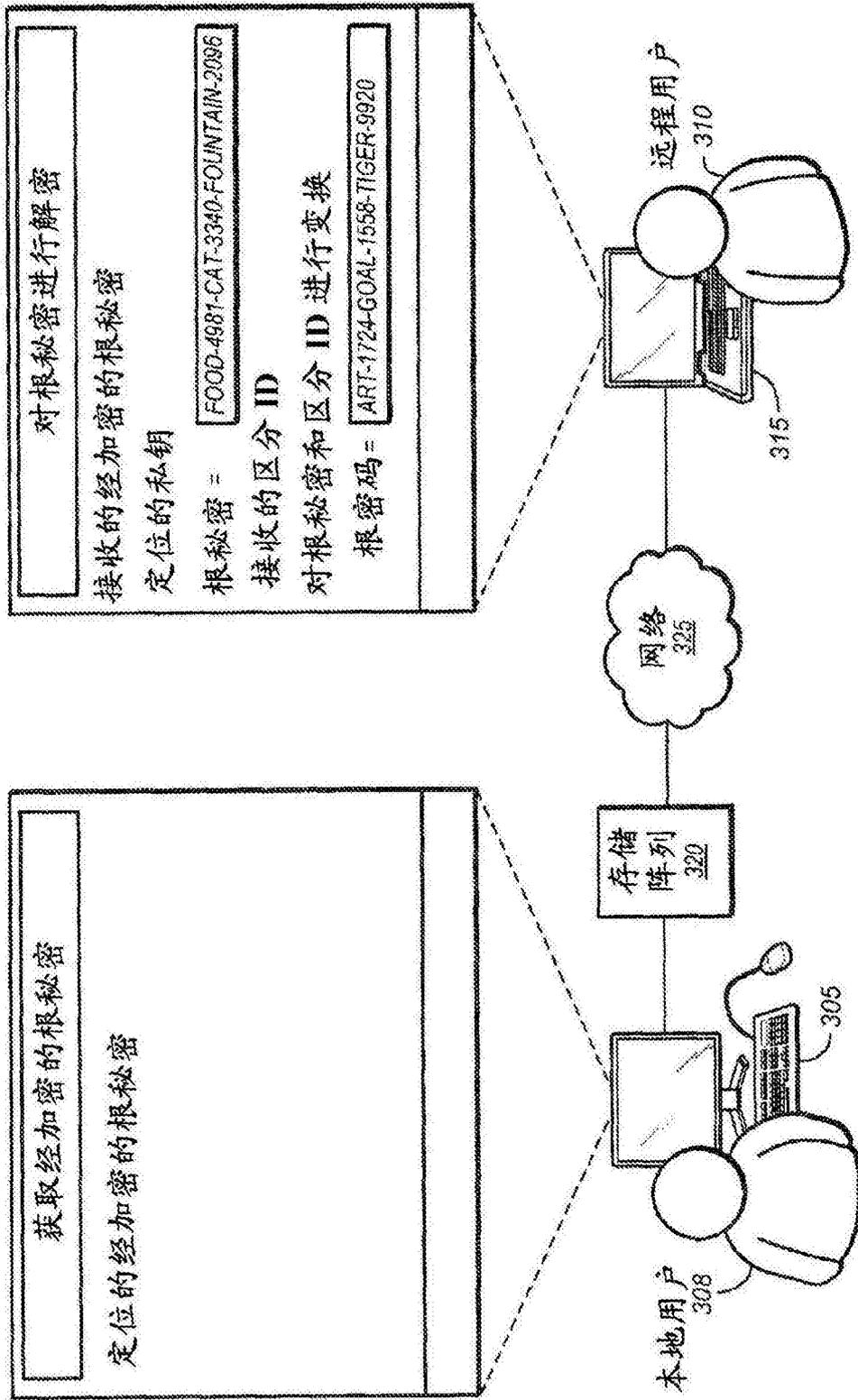


图3

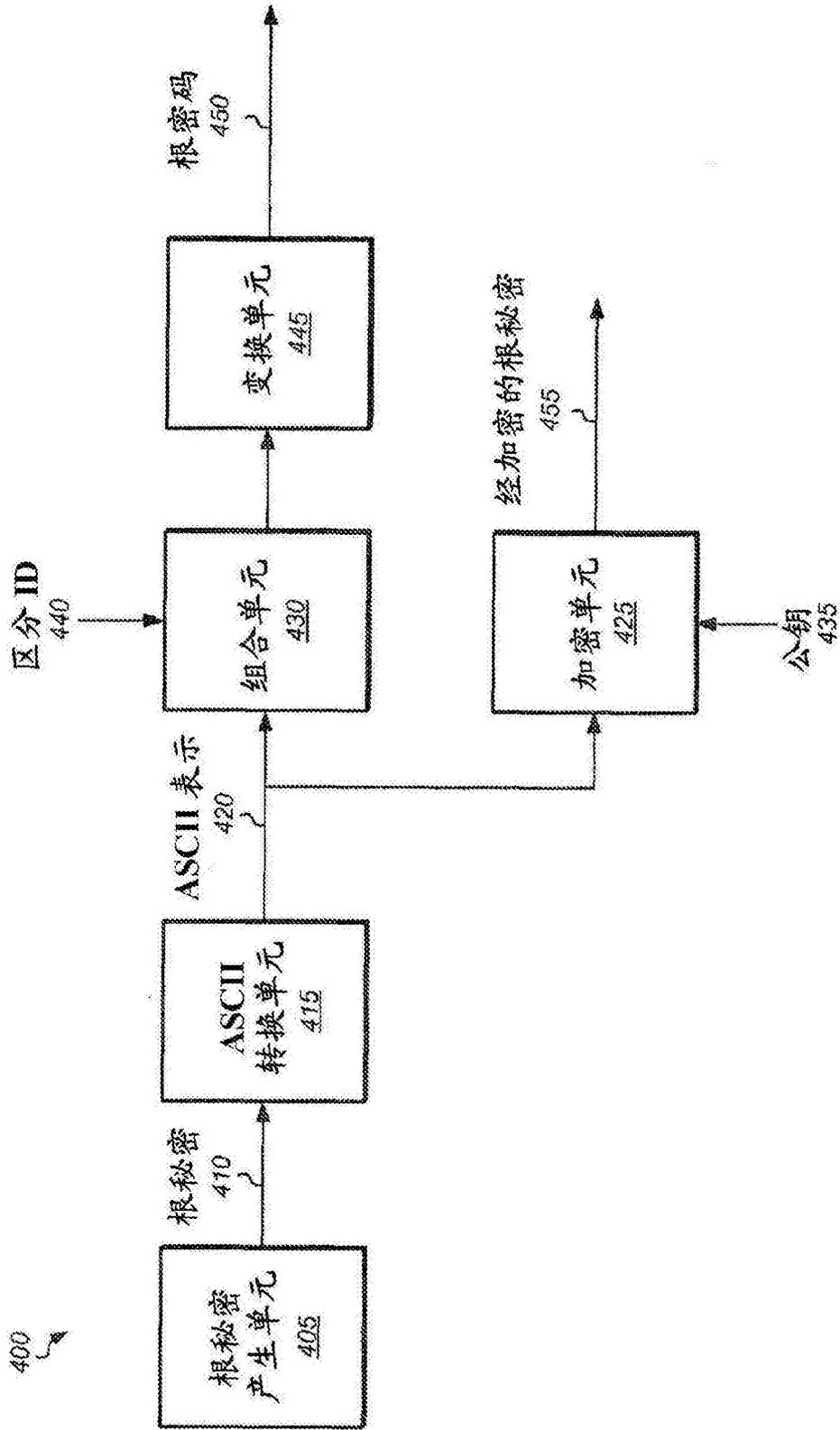


图4

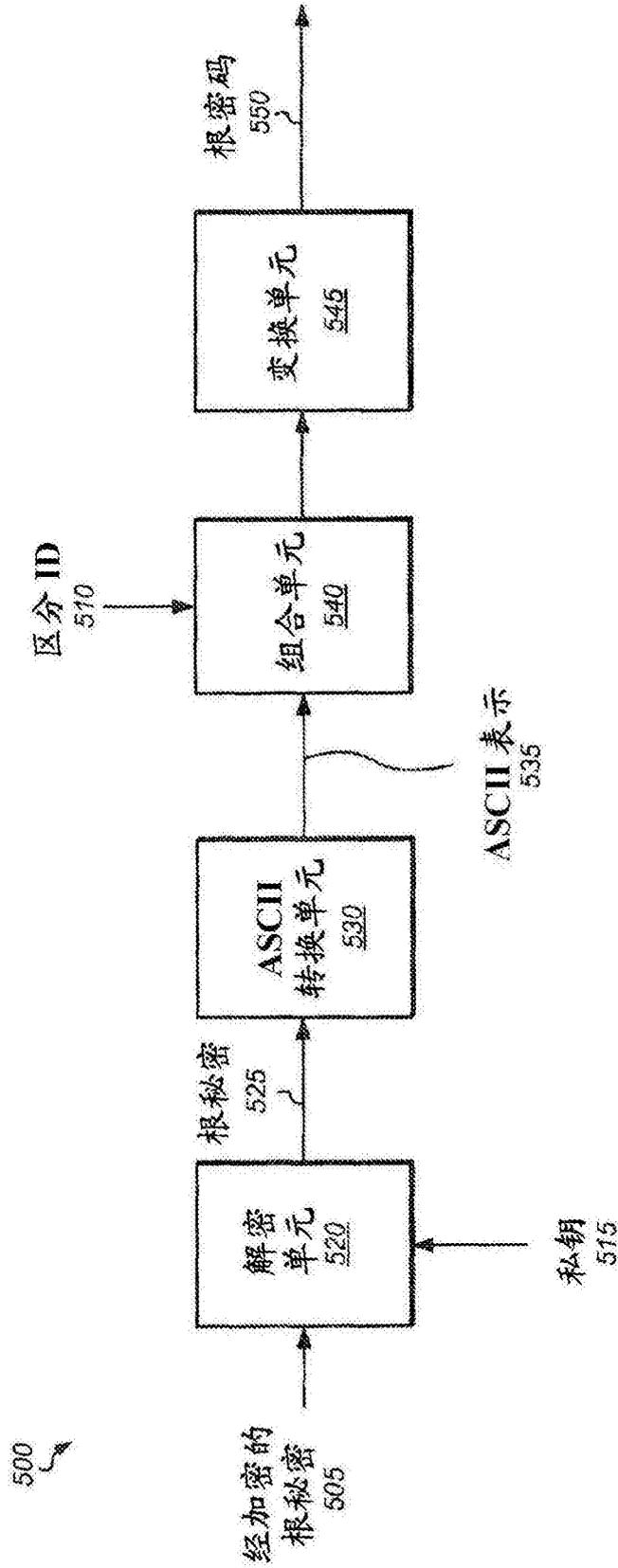


图5

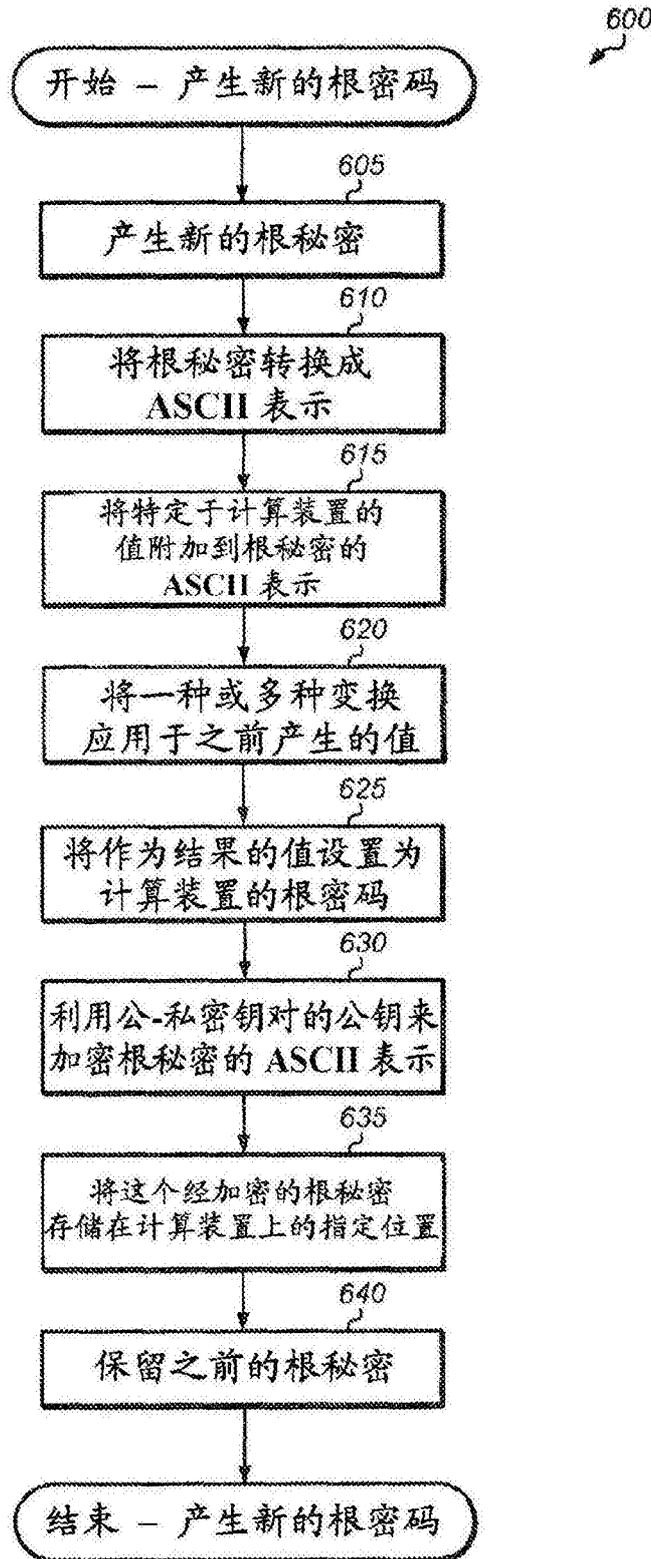


图6

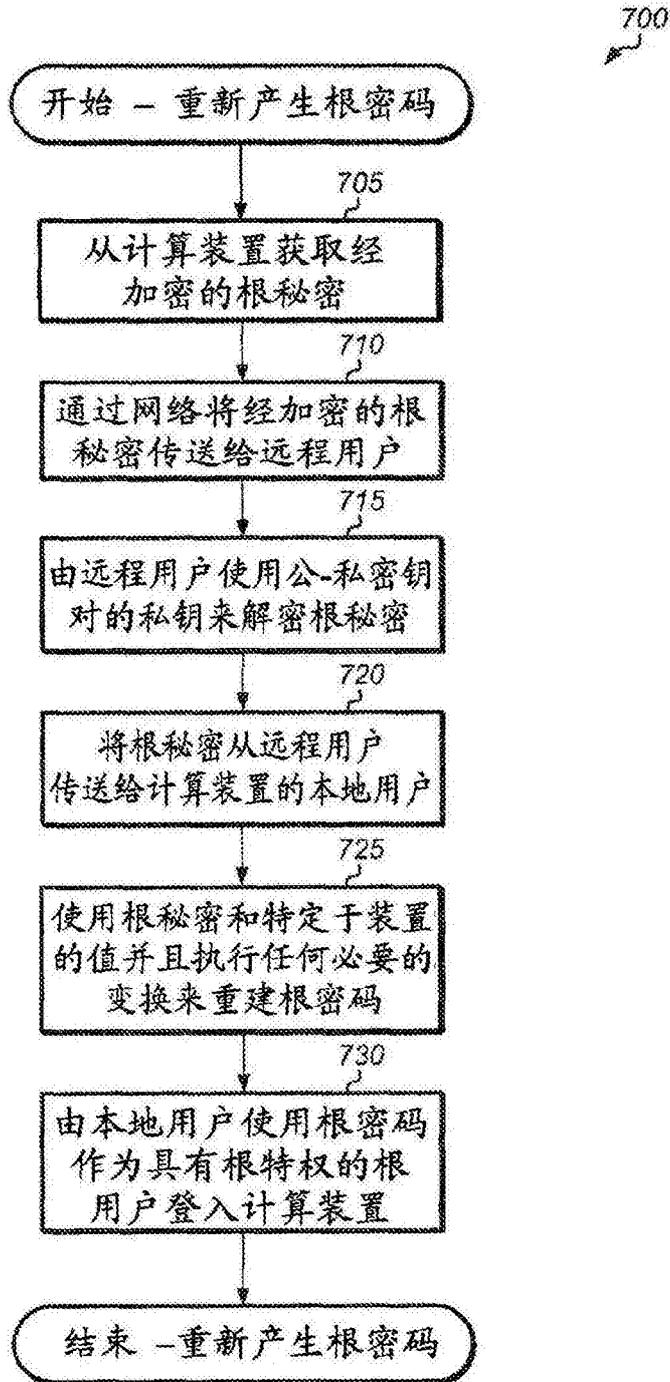


图7