



(12) 发明专利申请

(10) 申请公布号 CN 103748827 A

(43) 申请公布日 2014.04.23

(21) 申请号 201280038007.1

(74) 专利代理机构 中国国际贸易促进委员会专

(22) 申请日 2012.07.31

利商标事务所 11038

(30) 优先权数据

13/204, 171 2011.08.05 US

代理人 宋海宁

(85) PCT国际申请进入国家阶段日

(51) Int. Cl.

2014.01.29

H04L 9/08 (2006.01)

G06F 11/14 (2006.01)

(86) PCT国际申请的申请数据

PCT/US2012/048944 2012.07.31

(87) PCT国际申请的公布数据

W02013/022647 EN 2013.02.14

(71) 申请人 苹果公司

地址 美国加利福尼亚

(72) 发明人 C·索尔沃德 V·R·巴阿萨

K·B·麦克尼尔 T·B·达菲

M·L·H·布罗维尔 M·J·拜姆

M·D·阿德勒 E·B·汤姆拉

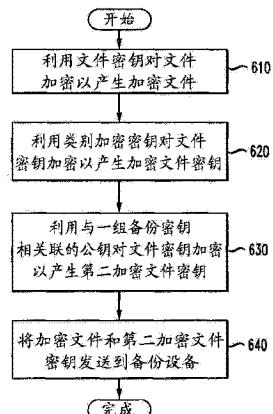
权利要求书2页 说明书10页 附图12页

(54) 发明名称

用于无线数据保护的系统和方法

(57) 摘要

本文公开了利用主设备和备份设备上的密码密钥管理来进行无线数据保护的系统、方法和非暂态计算机可读存储介质。系统利用文件密钥对文件加密并且对文件密钥加密两次，从而得到两个加密文件密钥。系统对每个文件密钥不同地加密并且将第一文件密钥存储在主设备上，并将加密文件密钥之一与加密文件一起发送到备份设备以存储。在备份设备上，系统将加密文件密钥与由用户口令保护的一组备份密钥相关联。一个实施例中，系统基于文件密钥生成用在密码操作中的初始化向量。另一实施例中，系统在用户口令改变期间管理备份设备上的密码密钥。



1. 一种方法,包括:

利用文件密钥对文件加密以产生加密文件;

利用类别加密密钥对所述文件密钥加密以产生加密文件密钥;

利用与一组备份密钥相关联的公钥对所述文件密钥加密以产生第二加密文件密钥;以及

将所述加密文件和所述第二加密文件密钥发送到备份设备。

2. 如权利要求1所述的方法,其中,所述类别加密密钥与一组文件相关联,其中所述一组文件具有至少一个相似的属性。

3. 如权利要求1所述的方法,其中,所述文件密钥是随机生成的。

4. 一种方法,包括:

在备份设备处接收加密文件和加密文件密钥;

将所述加密文件密钥与一组备份密钥相关联;

利用备份密钥组密钥对所述一组备份密钥加密以产生一组加密备份密钥;以及

在所述备份设备上存储所述加密文件、所述加密文件密钥和所述一组加密备份密钥。

5. 如权利要求4所述的方法,其中,所述备份密钥组密钥是由主设备随机生成的。

6. 如权利要求5所述的方法,其中,备份设备托管所述备份密钥组密钥。

7. 如权利要求6所述的方法,其中,所述备份设备利用用户口令保护所述备份密钥组密钥。

8. 如权利要求7所述的方法,其中,所述用户口令与用户账户口令相同。

9. 如权利要求4所述的方法,其中,所述备份密钥组密钥可由服务提供者恢复。

10. 如权利要求4所述的方法,其中,所述备份密钥组密钥不可由服务提供者恢复。

11. 如权利要求4所述的方法,其中,所述备份密钥组密钥是从用户口令得出的。

12. 如权利要求11所述的方法,其中,所述用户口令是单独的备份口令。

13. 一种方法,包括:

将加密文件数据、加密文件密钥和一组加密备份密钥从备份设备发送到主设备,其中所述一组加密备份密钥是根据包括以下步骤在内的步骤生成的:

在备份设备处接收加密文件和加密文件密钥;

将所述加密文件密钥与一组备份密钥相关联;以及

利用备份密钥组密钥对所述一组备份密钥加密以产生一组加密备份密钥。

14. 一种系统,包括:

处理器;

存储器,存储指令,用于控制所述处理器执行步骤,包括:

执行第一加密密钥的散列以产生第一中间结果;

截短所述第一中间结果以产生第二中间结果;

利用块偏移的函数生成第三中间结果;以及

利用所述第二中间结果对所述第三中间结果加密以产生初始化向量,来用在密码操作中。

15. 如权利要求14所述的系统,其中,所述第一加密密钥是文件加密密钥。

16. 如权利要求14所述的系统,其中,SHA-1 加密算法用于执行所述第一加密密钥的散

列。

17. 如权利要求 14 所述的系统,其中,所述第一中间结果被截短到加密密钥大小。

18. 如权利要求 14 所述的系统,其中,所述块偏移的函数是线性反馈移位寄存器。

19. 如权利要求 18 所述的系统,其中,所述块偏移是所述线性反馈移位寄存器的种子。

20. 如权利要求 14 所述的系统,其中,生成用于加密的初始化向量是对每个数据块执行的。

21. 如权利要求 14 所述的系统,其中,所述初始化向量用于对每个数据块加密。

22. 一种存储指令的非暂态计算机可读存储介质,所述指令当被计算设备执行时使得该计算设备执行步骤,包括:

创建第二组备份密钥;

将新的文件加密密钥与所述第二组备份密钥相关联;以及

利用新口令对所述第二组备份密钥加密。

23. 如权利要求 22 所述的非暂态计算机可读存储介质,其中,在从用户接收新口令之前,存在第一组备份密钥。

24. 如权利要求 22 所述的非暂态计算机可读存储介质,其中,所述新的文件加密密钥是在创建新文件时生成的。

25. 一种生成加密密钥的方法,该方法包括:

创建文件和文件加密密钥,其中所述文件属于一组保护类别之一;

利用设备加密密钥对所述文件加密密钥加密;

生成非对称密钥对;

基于所述非对称密钥对生成包装加密密钥;以及

利用所述包装加密密钥对所述文件加密密钥加密。

用于无线数据保护的系统和方法

技术领域

[0001] 本公开涉及无线数据保护,更具体而言涉及保护与设备之间的备份有关的密码密钥。

背景技术

[0002] 诸如电话、PDA、膝上型电脑等等之类的移动通信设备是许多用户的日常操作的关键方面。移动设备提供电子邮件、文本消息、即时聊天、语音和视频形式的通信。这些设备经常存储有价值的信息,例如个人数据和机密的公司数据。这种设备可存储的信息量越来越多,存储信息的重要性也越来越高。当移动设备丢失或损坏时,设备内存储的所有信息也丢失。

[0003] 一些计算系统采用备份机制,使得在计算系统丢失或毁坏的情况下,至少一些数据是可恢复的。备份机制通常涉及将文件的全部或一部分拷贝到备份系统以存储。可选地,备份系统存储先前备份的文件的增量备份,使得只有变化了的数据被发送到备份系统。

[0004] 存在定期自动备份移动设备上存储的数据的移动设备备份机制。这些机制可将数据备份到诸如电脑、膝上型计算机、桌面型计算机和服务器之类的其他设备或计算系统,当移动设备上的数据可访问时这是足够的。然而,当数据不可访问时,例如当移动设备被锁定时,备份机制不能备份数据,因为其不能访问用户口令来解锁设备。克服此弱点的一种方法是备份机制只在设备被解锁时执行备份。此方法提供了一种备份手段,但不能备份自上次解锁事件以后设备上存储的更新近数据。另一个解决方案是用户解锁移动设备来执行备份。然而,此方法要求来自用户的输入。

发明内容

[0005] 本公开的额外特征和优点将在接下来的描述中记载,并且一部分从描述中显现出来,或者可通过实现本文公开的原理来获知。本公开的特征和优点可凭借所附权利要求中具体指出的手段和组合来实现和获得。本公开的这些和其他特征将通过接下来的描述和所附权利要求而变得更充分清楚,或者可通过实现本文记载的原理来获知。

[0006] 本申请公开了用于在主设备与备份设备之间的备份期间保护密码密钥的系统、方法和非暂态计算机可读存储介质。主设备可以是任何计算设备,例如个人计算机、膝上型电脑、网络上的工作站、服务器、蜂窝电话、个人数字助理或者其他能够存储数据的固定或移动设备。类似地,备份设备可以是任何计算设备,例如个人计算机、膝上型电脑、网络上的工作站、服务器、蜂窝电话、个人数字助理或者其他能够存储数据的固定或移动设备。示范性系统通过利用文件密钥对文件加密以得到加密文件来在主设备上管理密码密钥。系统利用类别加密密钥 (class encryption key) 对文件密钥 (file key) 加密,从而得到加密文件密钥。类别加密密钥根据文件作为其成员的类别来保护文件密钥。在系统利用类别加密密钥对文件密钥加密之后,系统利用与一组备份密钥 (backup key) 相关联的公钥 (public key) 来第二次对文件密钥加密,从而得到第二加密文件密钥。系统随后将加密文件和第二

加密文件密钥发送到备份设备。第一加密文件密钥被存储在主设备上。

[0007] 示范性备份设备通过在备份设备处从主设备接收加密文件和加密文件密钥来管理密码密钥。系统将加密文件密钥与一组备份密钥相关联并且利用备份密钥组密钥对该组备份密钥加密,从而得到一组加密备份密钥。备份设备在备份设备上存储加密文件、加密文件密钥和该组加密备份密钥以便用于恢复。

[0008] 在备份恢复实施例中,示范性系统可将加密文件数据从备份设备恢复到主设备。当诸如电话或膝上型电脑之类的主设备损坏或丢失时,系统可以将与设备一起丢失的数据从备份设备恢复到主设备或恢复到新设备。本文记载的方案可假定,当设备损坏或丢失时,与该设备相关联的口令、密钥或其他证书遭到了危害。系统将加密文件数据、加密文件密钥和一组加密备份密钥从备份设备发送到主设备。系统通过在备份设备处接收加密文件和加密文件密钥并将加密文件密钥与一组备份密钥相关联来创建该组加密备份密钥。然后,系统利用备份密钥组密钥来对该组备份密钥加密,从而得到一组加密的备份密钥。

[0009] 在数据恢复期间,在主设备处,系统从备份设备接收加密文件数据、加密文件密钥和一组加密备份密钥。系统利用备份密钥组密钥对该组加密备份密钥解密,从而得到一组解密的备份密钥。然后,系统利用备份密钥对加密文件密钥解密,从而得到解密的文件密钥。利用解密的文件密钥对加密文件数据解密,从而得到解密的文件数据。然后,系统将文件数据存储在主设备上。

[0010] 在另一实施例中,管理密码密钥的系统可生成用在密码操作中的初始化向量。系统对第一加密密钥执行密码散列并将所得到的散列截短到加密密钥大小。系统随后利用以块偏移作为种子的线性反馈移位寄存器生成中间结果。利用第一加密密钥的截短的散列对中间结果加密,从而得到初始化向量。在利用以密码块链接模式 (cipher block chaining mode) 运行的分块加密器算法进行的加密和解密期间利用该初始化向量。初始化向量初始化分块加密器算法。

[0011] 此外,系统可在用户执行的口令改变期间备份加密密钥。系统假定旧的口令已遭到危害并且生成额外的一组密钥来保护文件密钥。系统将在创建新文件时生成的新文件加密密钥与该额外的一组备份密钥相关联。然后,系统利用从用户接收的新口令来对第二组备份密钥加密。这样,系统在口令改变期间备份加密密钥。

附图说明

[0012] 为了描述能够获得本公开的上述和其他优点和特征的方式,对上文简要描述的原理的更具体描述将通过参考在附图中图示的其具体实施例来给出。在理解到这些附图只是描绘了本公开的示范性实施例并因此不应被认为在限定其范围的同时,通过使用附图来更加具体且详细地描述和说明这里的原理,附图中:

- [0013] 图 1 图示了示例系统实施例;
- [0014] 图 2 图示了非对称密钥密码术;
- [0015] 图 3 图示了对称密钥密码术;
- [0016] 图 4 图示了密码块链接(cipher-block chaining, CBC) 模式加密;
- [0017] 图 5 图示了电子码书(electronic codebook, ECB) 模式加密;
- [0018] 图 6 图示了用于主设备上的密码密钥管理的示范性方法实施例;

- [0019] 图 7 图示了利用类别的示例文件密钥保护；
- [0020] 图 8 图示了用于备份设备上的密码密钥管理的示范性方法实施例；
- [0021] 图 9 图示了主设备上的示范性密码密钥管理；
- [0022] 图 10 图示了备份设备上的示范性密码密钥管理；
- [0023] 图 11 图示了备份密钥组密钥保护的框图；
- [0024] 图 12 图示了用于恢复备份设备上的备份数据的示范性方法实施例；
- [0025] 图 13 图示了用于在主设备上恢复备份数据的示范性方法实施例；
- [0026] 图 14 图示了用于生成初始化向量的示范性方法实施例；
- [0027] 图 15 图示了用于生成初始化向量的示范性逻辑流；
- [0028] 图 16 图示了用于口令变化期间的备份密钥管理的示范性方法实施例；
- [0029] 图 17 图示了用于口令变化期间的备份密钥管理的示例体系结构；并且
- [0030] 图 18 图示了示范性备份密钥生成过程。

具体实施方式

[0031] 下面详细论述本公开的各种实施例。虽然论述了具体实现方式，但应当理解这样做只是为了说明。相关领域的技术人员将认识到，在不脱离本公开的精神和范围的情况下，可以使用其他组件和配置。

[0032] 本公开解决了现有技术中对无线数据保护的需求。公开了系统、方法和非暂态计算机可读介质，该系统、方法和非暂态计算机可读介质通过在主设备和备份设备上管理密码密钥、将文件数据从备份设备恢复到主设备并且生成初始化向量来用在密码操作中并在口令变化期间保护文件密钥，从而来保护无线数据。本文公开了对图 1 中的可用来实现这些概念的基本通用系统或计算设备的简要介绍。然后将是对无线数据保护的更详细描述。本公开现在转向图 1。

[0033] 参考图 1，示范性系统 100 包括通用计算设备 100，其包括处理单元（CPU 或处理器）120 和系统总线 110，系统总线 110 将各种系统组件耦合到处理器 120，所述各种系统组件包括系统存储器 130，例如只读存储器（ROM）140 和随机访问存储器（RAM）150。系统 100 可包括与处理器 120 直接连接、紧邻处理器 120 或者集成为处理器 120 的一部分的高速存储器的缓存 122。系统 100 将数据从存储器 130 和 / 或存储设备 160 拷贝到缓存 122 以供处理器 120 迅速访问。这样，缓存提供了避免处理器 120 在等待数据的同时延迟的性能提升。这些和其他模块可控制或被配置为控制处理器 120 执行各种动作。也可以有其他系统存储器 130 供使用。存储器 130 可包括具有不同性能特性的多种不同类型的存储器。可以明白，本公开可在具有多于一个处理器 120 的计算设备 100 上操作或者在联网在一起以提供更大处理能力的计算设备的群组或群集上操作。处理器 120 可包括任何通用处理器和硬件模块或软件模块，例如存储在存储设备 160 中的模块 1162、模块 2164 和模块 3166，它们被配置为控制处理器 120 以及专用处理器，在专用处理器中软件指令被包含到实际处理器设计中。处理器 120 实质上可以是完全独立自给的计算系统，包含多个核或处理器、总线、存储器控制器、缓存，等等。多核处理器可以是对称的或非对称的。

[0034] 系统总线 110 可以是若干种类型的总线结构中的任何一种，包括存储器总线或存储器控制器、外围总线和本地总线，使用多种总线体系结构中的任何一种。存储在 ROM140

等中的基本输入 / 输出(BIOS)可提供帮助——例如在启动期间——在计算设备 100 内的元件之间传送信息的基本例程。计算设备 100 还包括存储设备 160, 例如硬盘驱动器、磁盘驱动器、光盘驱动器、磁带驱动器, 等等。存储设备 160 可包括用于控制处理器 120 的软件模块 162、164、166。设想到了其他硬件或软件模块。存储设备 160 通过驱动接口连接到系统总线 110。驱动器和关联的计算机可读存储介质为计算设备 100 提供计算机可读指令、数据结构、程序模块和其他数据的非易失性存储。在一个方面中, 执行特定功能的硬件模块包括存储在非暂态计算机可读介质中的软件组件, 该软件组件结合诸如处理器 120、总线 110、显示器 170 等等之类的必要硬件组件执行该功能。基本组件是本领域技术人员已知的, 并且取决于设备的类型, 例如设备 100 是小型手持计算设备、桌面型计算机还是计算机服务器, 设想到了适当的变化。

[0035] 虽然本文描述的示范性实施例采用了硬盘 160, 但本领域技术人员应当明白, 在示范性操作环境中也可使用其他类型的可被计算机访问的能够存储数据的计算机可读介质, 例如盒式磁带、闪存卡、数字多功能盘、盒式录音带、随机访问存储器(RAM)150、只读存储器(ROM)140、包含比特流的线缆或无线信号, 等等。非暂态计算机可读存储介质明确排除了诸如能量、载波信号、电磁波和信号本身之类的介质。

[0036] 为了使得用户能够与计算设备 100 交互, 输入设备 190 表示任意数量的输入机制, 例如用于话音的麦克风、用于手势或图形输入的触敏屏、键盘、鼠标、运动输入、话音, 等等。输出设备 170 也可以是本领域技术人员已知的多种输出机制中的一个或多个。在一些情况下, 多模式系统使得用户能够提供多种类型的输入来与计算设备 100 通信。通信接口 180 一般控制并管理用户输入系统输出。对于在任何特定硬件布置上操作没有限制, 因此这里的基本特征可容易地在改进的硬件或固件布置被开发出来时被其所替代。

[0037] 为了说明清晰起见, 说明性系统实施例被呈现为包括个体功能块, 其中包括被标记为“处理器”或处理器 120 的功能块。这些块表示的功能可通过使用共享或专用硬件来提供, 包括但不限于: 能够执行软件的硬件, 和被特制来作为在通用处理器上执行的软件的等同物操作的硬件, 例如处理器 120。例如, 图 1 中呈现的一个或多个处理器的功能可由单个共享处理器或多个处理器提供。(对术语“处理器”的使用不应当被解释为专门指能够执行软件的硬件。) 说明性实施例可包括微处理器和 / 或数字信号处理器(DSP)硬件、用于存储执行下文论述的操作的软件的只读存储器(ROM)140、以及用于存储结果的随机访问存储器(RAM)150。也可提供超大规模集成(VLSI)硬件实施例, 以及定制的 VLSI 电路结合通用 DSP 电路。

[0038] 各种实施例的逻辑操作被实现为:(1)在通用计算机内的可编程电路上运行的由计算机实现的步骤、操作或过程的序列,(2)在专用可编程电路上运行的由计算机实现的步骤、操作或过程的序列, 和 / 或(3)可编程电路内的互连机器模块或程序引擎。图 1 中所示的系统 100 可实现所描述的方法的全部或一部分, 可以是所描述的系统的一部分, 和 / 或可以根据所描述的非暂态计算机可读存储介质中的指令来操作。这种逻辑操作可实现为被配置为控制处理器 120 根据模块的编程执行特定功能的模块。例如, 图 1 图示了三个模块 Mod1162、Mod2164 和 Mod3166, 它们是被配置为控制处理器 120 的模块。这些模块可被存储在存储设备 160 上并在运行时被加载到 RAM150 或存储器 130 中, 或者如本领域中已知的可被存储在其他计算机可读存储器位置中。

[0039] 密码术论述

[0040] 在公开了计算系统的一些组件后,本公开现在转向对密码术的简要论述。密码术包含加密和解密两者并且用于隐藏信息以使得只有消息的预期接收者能够访问该信息。加密是以使得可理解的信息看起来不可理解的方式改变可理解的信息的过程,而解密是逆过程,将不可理解的信息变回可理解的信息。加密和解密利用被保持秘密的密钥来在各形态之间改变信息。存在两种不同类型的密码术,即传统的对称密钥密码术和非对称(或公钥)密码术。

[0041] 公钥密码术是除了传统的对称密钥算法还额外地利用非对称密钥算法、或者取代传统的对称密钥算法而利用非对称密钥算法的密码方法。图 2 图示了非对称密钥密码术,图 3 图示了对称密钥密码术。非对称密钥算法与对称密钥算法的不同之处在于:对于加密 210 和解密 220 使用不同的密钥。对称密钥算法对于加密 310 和解密 320 使用相同密钥并且基于消息的发送者和接收者之间的共享秘密密钥的概念。因为公钥密码术对于加密和解密利用不同的密钥,所以不需要在发送者和接收者之间对秘密密钥的安全交换。传统的对称密钥密码术的优点包括速度,因为更加现代的非对称密钥算法更慢。

[0042] 在公钥密码术中,生成数学上相关的密钥对,私钥和公钥。虽然密钥是相关的,但基于一个密钥得出另一个是不现实的。私钥被保持秘密,而公钥被公布。发送者利用接收者的公钥 210 和加密算法 230 对消息加密,消息的接收者利用私钥 220 和相应的加密(或解密)算法 240 对消息解密。只有接收者的私钥能够对利用接收者的公钥加密的消息解密。例如,Alice 想要向 Bob 发送包含个人信息的消息并且对消息加密以保护该信息。Alice 利用公钥密码术来发送她的消息,因为她不能与 Bob 安全地共享密码密钥。Alice 利用 Bob 的公钥对给 Bob 的消息加密并且将加密的消息发送给他。Bob 接收到加密的消息并且利用与非对称密钥对相关的相应私钥来对消息解密。这样,在没有交换密码密钥的情况下,Alice 经由公钥密码术向 Bob 发送了加密消息。

[0043] 已论述了非对称和对称密钥密码术后,本公开现在转向对分块加密器的论述。分块加密器是逐块地对数据加密的密码算法,与逐比特地对数据加密的流加密器不同。分块加密器算法将输入数据分割成块并且在每个数据块上操作。分块加密器可以以诸如电子码书(ECB)或密码块链接(CBC)之类的不同模式操作。

[0044] 在 CBC 模式中,来自加密的一个块的输出被用作下一加密操作的输入。图 4 图示了以 CBC 模式运行的加密器。初始化向量(IV)410 与第一块未加密比特 b1420 相组合并且结果被加密。初始化向量随机化未加密比特,使得如果同一块明文被用相同密钥加密多于一次,则其看起来不是相同的密文。利用相同密钥对同一块明文加密多于一次产生相同密文。利用 IV410 防止了这个不合需要的效果的发生。IV410 被用于第一块数据,因为不存在来自前一轮的输出与第一块未加密比特相组合。加密算法输出一块密码比特 cb1430 并且将这些密码比特与下一块 b₂440 相组合,其随后被加密。系统重复此过程,直到所有数据块都已被加密为止。对于解密,颠倒该过程。每一块密码比特被利用块加密器解密算法来解密,然后与前一块的密码比特相组合以产生明文(未加密)比特。对于第一块,密码比特被解密并与 IV 组合以产生未加密数据。

[0045] 图 5 图示了在 ECB 模式中运行的加密器。在 ECB 模式中,输入数据被分割成数据块,这些数据块随后被加密。与 CBC 模式不同,没有与来自前一轮加密的输出的组合。第一

块未加密比特 b_1510 被用作加密算法的输入，并且算法输出密码比特 cb_1520 。在 ECB 模式中运行的加密器的一个问题是：相同明文比特块加密成相同密码比特块，因为算法使用相同密钥来对每个块加密。

[0046] 在公开了一些系统组件和加密概念后，本公开现在转向图 6 所示的示范性方法实施例。为了清晰起见，本文的每个示范性方法是就如图 1 中所示的被配置为实现各方法的示范性系统 100 来论述的。本文概述的步骤是示范性，并且可按其任何组合实现，包括排除、添加或修改某些步骤的组合。

[0047] 图 6 图示了通过在主设备上管理密码密钥来进行的无线数据保护。主设备可以是任何计算设备，例如个人计算机、膝上型电脑、网络上的工作站、服务器、蜂窝电话、个人数字助理或者其他能够存储数据的固定或移动设备。主设备的备份是必要的，因为设备会遭受意外的数据删除、丢失、毁坏和偷窃。在数据丢失的情况下，系统可将数据恢复到同一设备、同一类型的新设备和 / 或另一类型的设备。在备份事件期间保护密码密钥可确保安全的系统。实现该方法的系统利用文件密钥对文件加密，从而得到加密文件(610)。文件可包含文本、图像、视频、话音、多媒体等等，并且可以是任何格式的，例如 PNG、JPG、AVI 和 HTML。文件密钥的概念可被扩展到涵盖没有存储在文件中的数据，例如存储器片段或指令集，然而本文的原理是就文件来论述的。文件密钥是加密密钥并且可随机生成。文件密钥可以是 256 比特 AES 密钥或任何其他长度的密码密钥，用在任何加密算法中，例如 AES、DES、Blowfish 等等。在系统利用文件密钥对文件加密之后，系统利用类别加密密钥对文件密钥加密，从而得到加密文件密钥(620)。

[0048] 在系统利用类别加密密钥对文件密钥加密之后，系统利用与一组备份密钥相关联的公钥对文件密钥加密，从而得到第二加密文件密钥(630)。公钥可属于非对称密钥对，并且相应的私钥被存储在备份设备上。然后，系统将加密文件和第二加密文件密钥发送到备份设备(640)。备份设备可以是任何计算设备，例如个人计算机、膝上型电脑、网络上的工作站、服务器、蜂窝电话、智能电话、个人数字助理或者其他能够存储数据的固定或移动设备。备份设备可以为任意数目的设备存储一组或多组备份密钥。例如，备份服务器可为蜂窝电话存储五组备份密钥，并且为 PDA 存储两组备份密钥。

[0049] 类别加密密钥是用于对特定保护类别的密钥加密的密码密钥。图 7 图示了根据保护类别来保护文件密钥的文件系统。系统将每个文件指派到一组保护类别 710 之一，并且向每个保护类别指派类别加密密钥。在一方面，每个类别加密密钥是唯一的。系统利用相应的类别加密密钥 720 对每个文件加密密钥加密。例如，文件 1 和文件 5 是保护类别 A 的一部分，具有唯一的文件加密密钥。文件 1 被用密钥 1 加密，而文件 5 被用密钥 5 加密。密钥 1 和 5 都被用密钥 A 加密。保护类别允许了某些文件行为和访问权利。例如，被标记为在锁定时可读的文件可由一类别加密密钥来保护，被标记为在首先解密之后可读的文件可由一不同类别加密密钥来保护，由特定用户创建的所有文件可由一不同类别加密密钥来加密。其他文件标记包括：在锁定时可写和在解锁时可读。可出于不同的安全目的以不同方式来分类或标记文件。例如，分类系统可用于标记要求不同安全性的文件。例如，类别 A 文件可以是要求最高安全级别的文件，并且保护用于类别 A 的文件密钥的类别加密密钥可以是特别强的加密密钥，而类别 B 文件可以是要求中等安全级别的文件。保护用于类别 B 的文件密钥的类别加密密钥可以是中等强的加密密钥。这种通过保护类别实现的文件或证书

访问的层次化方法允许系统根据所期望的安全级别而不同地保护文件。

[0050] 图 8 图示了用于备份设备上的无线数据保护的示范性方法实施例。系统通过在备份设备处从主设备接收加密文件和加密文件密钥来在备份设备上管理密码密钥(810)。系统将加密文件密钥与一组备份密钥相关联(820)，并且利用备份密钥组密钥对该组备份密钥加密，从而得到一组加密的备份密钥(830)。备份设备将加密文件、加密文件密钥和该组加密备份密钥存储在备份设备上(840)。备份设备存储与主设备相同的加密文件数据。然而，用于对文件数据加密的文件密钥被不同地加密。主设备上存储的文件密钥是用类别加密密钥来加密的，而备份设备上存储的文件密钥是用与非对称密钥对相关的公钥来加密的。

[0051] 图 9 图示了利用主设备上的密码密钥管理的无线数据保护。系统在主设备上存储文件 1、文件 2 和文件 3，主设备在此示例中是蜂窝电话 910。每个文件被用单独的相应文件加密密钥 k_1 、 k_2 和 k_3 来加密。每个文件加密密钥被用与备份密钥组相关联的相应公钥 pk_1 、 pk_2 和 pk_3 来加密。主设备 910 将文件 1、文件 2 和文件 3 各自的加密文件数据和各个相应的加密文件密钥 k_1 、 k_2 和 k_3 发送到备份设备，备份设备在此示例中是桌面型计算机。公钥可以是设备的系统密钥包中的类别密钥的镜像。

[0052] 图 10 图示了备份设备上的无线数据保护。系统在备份设备上存储一组或多组备份密钥 1010 中的相应私钥。例如，系统在用于安全保护的桌面型计算机上存储该组备份密钥 1010。系统随后利用备份密钥组密钥 k_b 1020 对该组备份密钥 1010 加密。图 11 图示了备份密钥组密钥保护的示范框图。系统可从主设备接收随机生成的秘密 1120，备份密钥组密钥 k_b 1110，其被备份设备托管 1130。密钥托管 (key escrow) 是将密码密钥提供给第三方以便安全保护的过程。备份设备利用用户口令 1140 来保护备份密钥组密钥。用户口令可以与系统中已经使用的用户账户口令相同。在此情况下，如果用户忘记其口令，服务提供者可重置用户口令，而不更新加密密钥组。服务提供者可利用新的用户口令来保护备份密钥组密钥，使得用户可通过提供新的用户口令来访问备份密钥组。此外，备份设备可以以任何方式来对备份密钥组密钥加密，因为其在托管密钥。可选地，用户可选择保护备份密钥组以使得备份密钥组密钥不可由服务提供者恢复。用户可提供单独的备份口令 1150，其用于生成备份密钥组密钥 1160。在此情况下，如果用户忘记其口令，服务提供者不能恢复备份密钥组密钥。

[0053] 一些实现方式对于服务器上的备份密钥包提供了两级保护。例如，设备可生成随机备份密钥包秘密并且向服务器托管该备份密钥包秘密。服务器利用用户的常规账户口令来保护此秘密，但其不是用该口令来加密的。服务器可以以其作为托管秘密的一部分选择的任何方式来对该秘密加密。因为账户口令是可恢复的，所以备份密钥包秘密也是可恢复的。单独的随机备份密钥包秘密允许了账户口令变化，而无需更新加密密钥包。

[0054] 在另一示例中，用户可指定单独的备份口令。设备基于该口令生成备份密钥包秘密，但不将该秘密托管给服务器。用户在恢复时重输入此单独的备份口令，并且没有办法来恢复此口令，从而导致了不可恢复的口令。

[0055] 图 12 图示了将加密文件数据从备份设备恢复到主设备的示范性方法实施例。主设备可以就是从其执行备份的那个设备，或者是另一不同设备。例如，用户意外地从其电话中删除了数据，则用户可恢复直到电话的上次备份那刻为止的丢失数据。或者，如果用户的

电话遭窃，则用户可购买新的电话并且在新电话上恢复直到从用户的原始设备进行的上次备份那刻为止的丢失数据。实现该方法的系统将加密文件数据、加密文件密钥和一组加密备份密钥从备份设备发送到主设备(1200)。该组加密备份密钥是由系统或另一设备或设备集合生成的，其在备份设备处接收加密文件和加密文件密钥(1210)，将加密文件密钥与一组备份密钥相关联(1220)并且利用备份密钥组密钥对该组备份密钥加密，从而得到一组加密的备份密钥(1230)。

[0056] 图 13 图示了在主设备上恢复加密文件数据的示范性方法实施例。实现该方法的系统在主设备处接收加密文件数据、加密文件密钥和一组加密备份密钥(1310)。系统利用备份密钥组密钥对该组加密备份密钥解密，从而得到一组备份密钥(1320)。一旦解密了该组备份密钥，系统就利用来自该组备份密钥中的备份密钥对加密文件密钥解密，从而得到文件密钥(1330)。文件密钥被用于对加密文件数据解密以产生文件数据(1340)，并且系统在主设备上恢复解密的文件数据(1350)。

[0057] 初始化向量生成

[0058] 系统可生成初始化向量以用在密码操作中。初始化向量(IV)在 CBC 模式的加密期间用于向数据添加变化。图 14 图示了生成初始化向量的示范性方法实施例。系统执行第一加密密钥——文件密钥——的密码散列以产生第一中间结果(1410)。文件密钥是加密密钥并且可随机生成。文件密钥可以是 256 比特 AES 密钥或者任何其他长度的密码密钥，用在诸如 AES、DES、Blowfish 等等之类的任何加密算法中。接下来，系统截短第一中间结果以产生第二中间结果(1420)并且利用块偏移的函数生成第三中间结果(1430)。系统将第一中间结果——文件加密密钥的散列——截短成适用于特定密码算法的加密密钥大小，例如 16 字节，或任何其他大小。块偏移的函数可以是线性反馈移位寄存器(LFSR)或任何其他利用块偏移的函数。块偏移是对数据的索引，指示块号。最后，系统利用第二中间结果对第三中间结果加密以产生用在加密和解密中的 IV(1440)。利用第二中间结果对第三中间结果加密的加密算法可以是任何加密算法，例如 DES 或者其他适当的对称加密算法。

[0059] 图 15 图示了生成用在密码操作中的 IV 的迭代方法的示例逻辑流。当对文件数据加密时，系统为文件中的每个数据块生成 IV。例如，对于大小为 2MB 的文件，系统可将该文件分割成 500 个大小为 4KB 的块。对于 500 块的每一块，系统生成用于加密和解密中的 IV。首先，系统检查当前块是否是文件中的最后一块，1510。如果当前块是最后一块，则系统退出 IV 生成例程。如果其不是最后一块，则系统继续 IV 生成例程。系统通过利用 SHA-1 加密算法和每文件密钥 k_f 作为输入执行散列来生成 20 字节 k_{iv} ，1520。中间结果 k_{iv} 被截短到 16 字节以产生中间结果 k_t ，1530。截短大小是加密密钥大小并且可以是特定加密算法所要求的任何大小，例如 8、12 或 16 字节或任意数目的字节。此时，文件中的块偏移被用作 LFSR 的输入以产生伪随机值 rand，1540。

[0060] LFSR 是移位寄存器，其反馈比特是在先比特的线性组合。移位寄存器是逐比特地对数据操作、一次输出一比特的函数。在函数输出一比特之后，所有比特在寄存器中被移位一个位置并且新的比特基于在先比特来计算。过程重复，直到从该函数输出期望数目的比特为止。寄存器具有有限数目的状态，并且最终进入输出比特的重复循环。因为 LFSR 的重复性，它们不是真正随机的。软件和 / 或硬件 LFSR 可生成伪随机数。

[0061] 通过向块偏移应用 LFSR 生成变量 rand，1540。在系统生成 rand 之后，系统利用中

间结果 kt 对来自 LFSR 的输出 rand 加密, 1550, 并且输出用于当前块的 IV, 1560。系统返回检查当前块是否是文件中的最后一块, 1510。如果其是最后一块, 则系统在生成所有必要的 IV 之后退出。如果不是, 则系统继续为文件中的剩余数据块生成 IV。

[0062] 文件密钥用于以如下方式生成 IV: 如果攻击者获得对 IV 的访问权, 其不能获得对文件密钥的访问权。以所公开的方式计算 IV 的益处之一是 IV 没有被绑定到存储它的设备。存在生成 IV 的替换方法, 其将 IV 绑定到生成它的设备。这些方法在数据被恢复到原始设备时足够的, 然而当备份的数据被恢复到新设备时这些方法是不足够的——设备被偷窃或损坏时就是这种情况。所公开的方法支持数据恢复到不同的设备。

[0063] 允许备份过程中改变用户口令

[0064] 图 16 图示了改变用户口令的示范性方法实施例。当用户改变其口令时, 系统可假定旧的口令已遭到危害并且不再被信任来保护一组备份密钥。口令改变可以是强制事件, 例如当设备丢失或损坏时, 或者可以是自愿的由用户发起的事件。当用户改变其口令并且备份过程被允许时, 系统在备份设备上创建第二组备份密钥(1610)。系统将新的文件加密密钥与备份设备上的第二组备份密钥相关联(1620)。系统在新文件被创建时生成新的文件加密密钥。在用户口令改变之后, 为新创建的文件生成的任何新文件密钥都与第二组备份密钥相关联。系统最终利用新的用户口令对第二组备份密钥加密(1630)。系统可生成随机秘密并且利用新的用户口令来保护该随机秘密。备份系统可包含任意数目组的备份密钥。备份密钥包秘密可从口令得出, 而不是随机生成。文件密钥可被存储在密钥组中、由密钥组中的密钥加密、并且存储在文件元数据中。

[0065] 图 17 图示了改变用户口令的示范性体系结构。在口令改变之前, 备份密钥组 1710 由从用户口令得出的密钥 bk_1 保护。在第一组密钥中保护的那组备份密钥是 k_1, k_2 和 k_3 。这些密钥分别对用于存储在诸如蜂窝电话之类的主设备上的文件 1、文件 2、文件 3 的文件密钥加密。口令改变之后, 系统在备份设备上创建新的一组备份密钥并且存储新组中的新创建的备份密钥。例如, 系统创建文件 4 和文件 5, 并且存储新的一组备份密钥中的新生成的保护文件密钥的加密密钥 k_4 和 k_5 。用于文件 4 和文件 5 的文件密钥分别由加密密钥 k_4 和 k_5 加密并存储在相应的文件元数据中。系统从新的口令得出新的备份密钥组密钥 bk_2 1720 来保护新的那组备份密钥。系统可为任意数目的口令改变生成任意数目的备份密钥组。每次用户改变其口令时, 系统就在备份设备上创建额外的备份密钥组并且利用从新的用户口令得出的密钥来保护该新组。这样, 在口令改变期间, 系统保护在另一设备上存储的备份密钥组。

[0066] 在一个实施例中, 通过绕过缓冲器缓存来允许对加密数据的原始访问。与每次需要时则从盘取得数据相比, 缓存存储数据以使得对数据的请求能够更迅速地得以实现。缓冲器缓存被绕过, 使得系统能够从盘访问加密数据, 而不对数据解密。当以正常方式访问文件系统时, 文件系统访问层可自动对数据解密。

[0067] 在另一实施例中, 公开了一种基于备份设备上存储的每文件密钥 (per file key) 来生成备份密钥的高效方法。图 18 图示了备份密钥生成过程。例如, 系统可解锁主设备并且创建新的类别 A 文件和随机的每文件加密密钥(1810)。系统可利用设备密钥对每文件密钥加密(1820)。系统可生成暂时性的公钥 / 私钥对(1830), 该公钥 / 私钥对可在单个会话中被使用多于一次, 而非为每个文件生成新的公钥 / 私钥对。系统可生成包装密钥, 以利用

暂时性密钥和备份密钥组密钥之间的密钥交换来保护用于备份设备的每文件密钥(1840)。最后,系统利用包装密钥来对每文件加密密钥加密(1850)以便存储在备份设备上。在设备被解锁的时间期间,包装密钥和暂时性公钥 / 私钥对可被再使用。此过程避免为了为每个文件获得新的暂时性密钥对和包装密钥而进行昂贵的生成和密钥交换。所公开的方法在设备被解锁的时间期间应用于同一类别——在所提供的示例中是类别 A——中的文件密钥,而不损失安全性。

[0068] 本公开的范围内的实施例还可包括有形的和 / 或非暂态的计算机可读存储介质,用于携带或在其上存储计算机可执行指令或数据结构。这种非暂态计算机可读存储介质可以是可由包括如上所述的任何专用处理器的功能设计的通用或专用计算机访问的任何可用介质。作为示例而非限制,这种非暂态计算机可读介质可包括 RAM、ROM、EEPROM、CD-ROM 或者其他光盘存储装置、磁盘存储装置或其他磁存储设备、或者任何其他能够用于以计算机可执行指令、数据结构或处理器芯片设计的形式携带或存储期望的程序代码手段的介质。当信息通过网络或另外的通信连接(硬连线的、无线的或者其组合)被传送或提供到计算机时,计算机适当地将该连接视为计算机可读介质。从而,任何这种连接被适当地称为计算机可读介质。上述的组合也应当被包括在计算机可读介质的范围内。

[0069] 计算机可执行指令例如包括使得通用计算机、专用计算机或者专用处理设备执行特定的一个功能或一组功能的指令和数据。计算机可执行指令还包括由计算机在独立或网络环境中执行的程序模块。一般地,程序模块包括专用处理器等等的设计中固有的例程、程序、组件、数据结构、对象和函数,其执行特定任务或实现特定的抽象数据类型。计算机可执行指令、关联的数据结构和程序模块表示用于执行本文公开的方法的步骤的程序代码手段的示例。这种可执行指令或关联数据结构的特定顺序表示用于实现这种步骤中描述的功能的相应动作的示例。

[0070] 本领域技术人员将会明白,本公开的其他实施例可在具有许多类型的计算机系统配置的网络计算环境中实现,所述许多类型的计算机系统配置包括个人计算机、手持设备、多处理器系统、基于微处理器的或可编程的消费类电子产品、网络 PC、袖珍计算机、大型计算机,等等。实施例也可在分布式计算环境中实现,其中任务由通过通信网络(由硬链线链路、无线链路或者由其组合)链接的本地和远程处理设备执行。在分布式计算环境中,程序模块可位于本地和远程存储器存储设备中。

[0071] 上文描述的各种实施例只是作为说明提供的,而不应当被解释为限制本公开的范围。例如,本文的原理不仅适用于备份移动设备,而且适用于执行密码操作的其他设备或计算系统。本领域技术人员将容易认识到在不遵循本文图示和描述的示例实施例和应用并且不脱离本公开的精神和范围的情况下可对本文描述的原理进行的各种修改和改变。

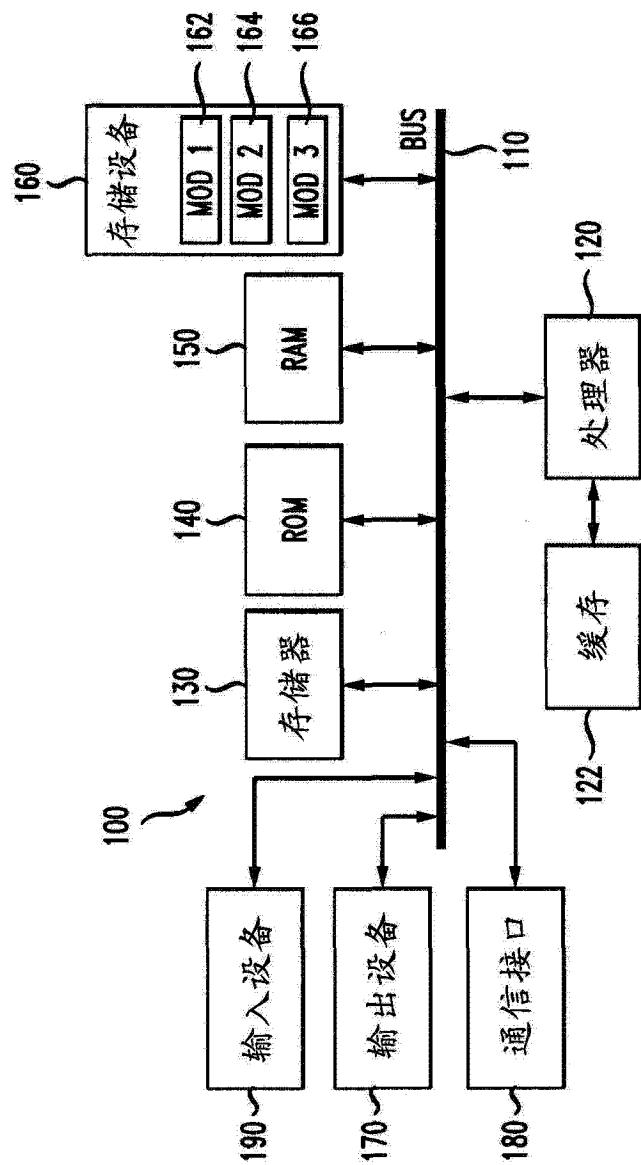


图 1

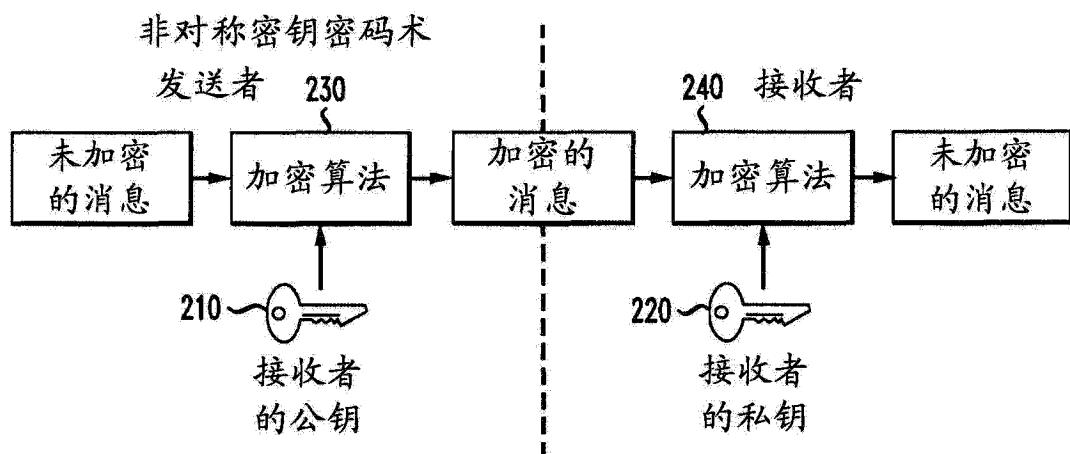


图 2

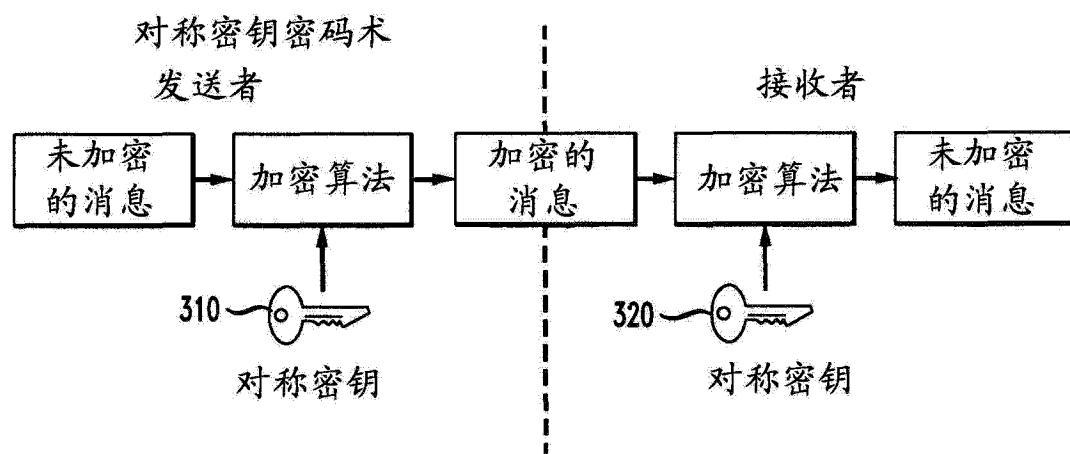


图 3

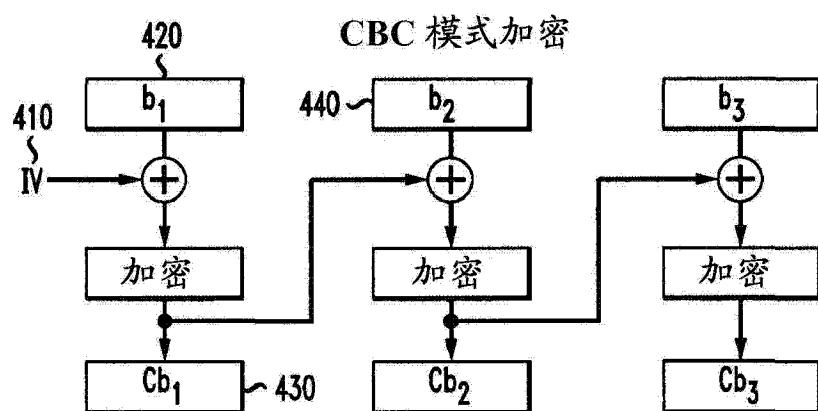


图 4

ECB 模式加密

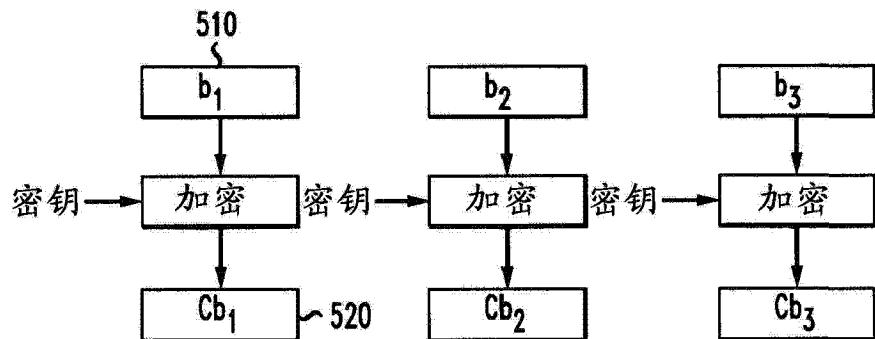


图 5

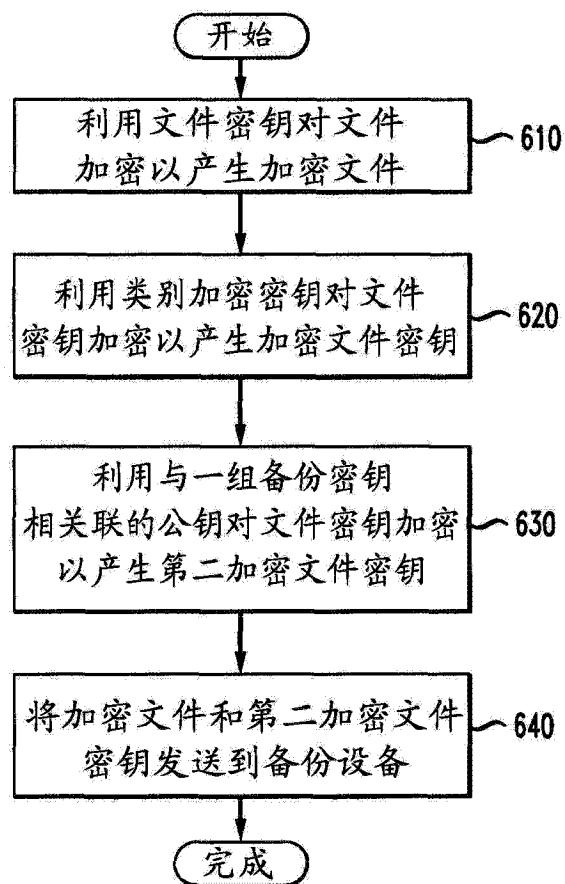


图 6

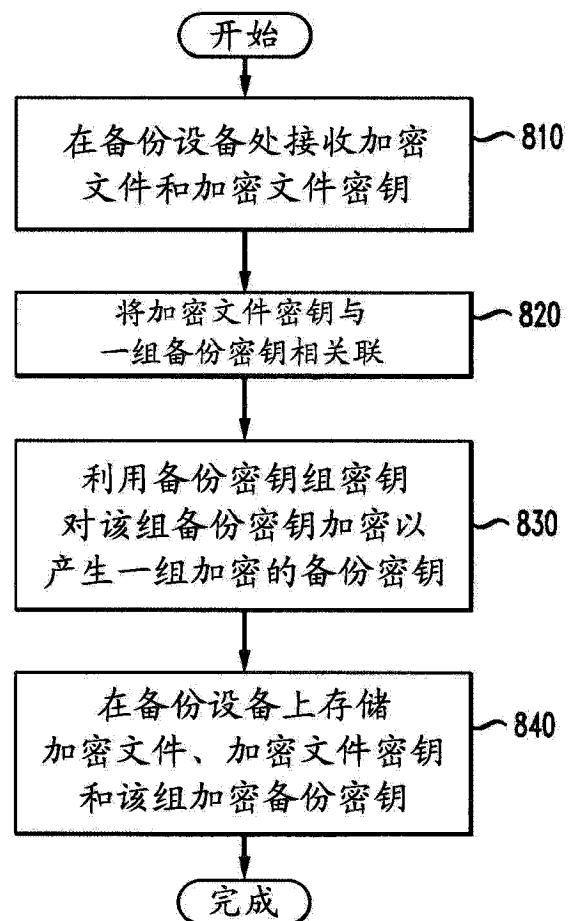
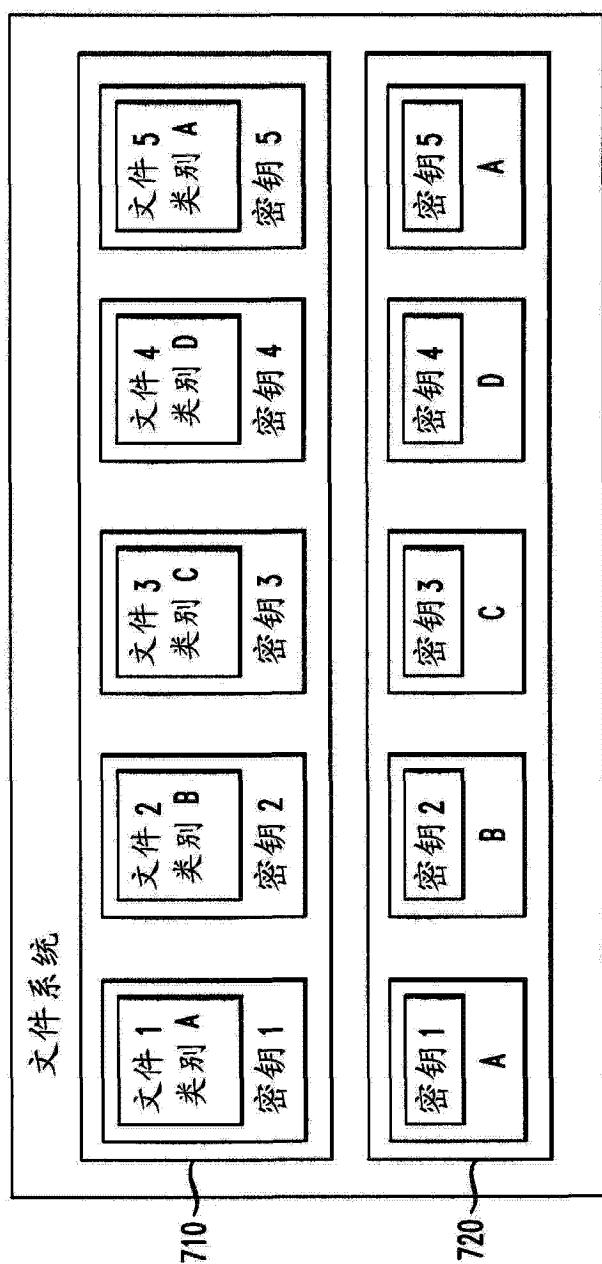


图 8

图 7

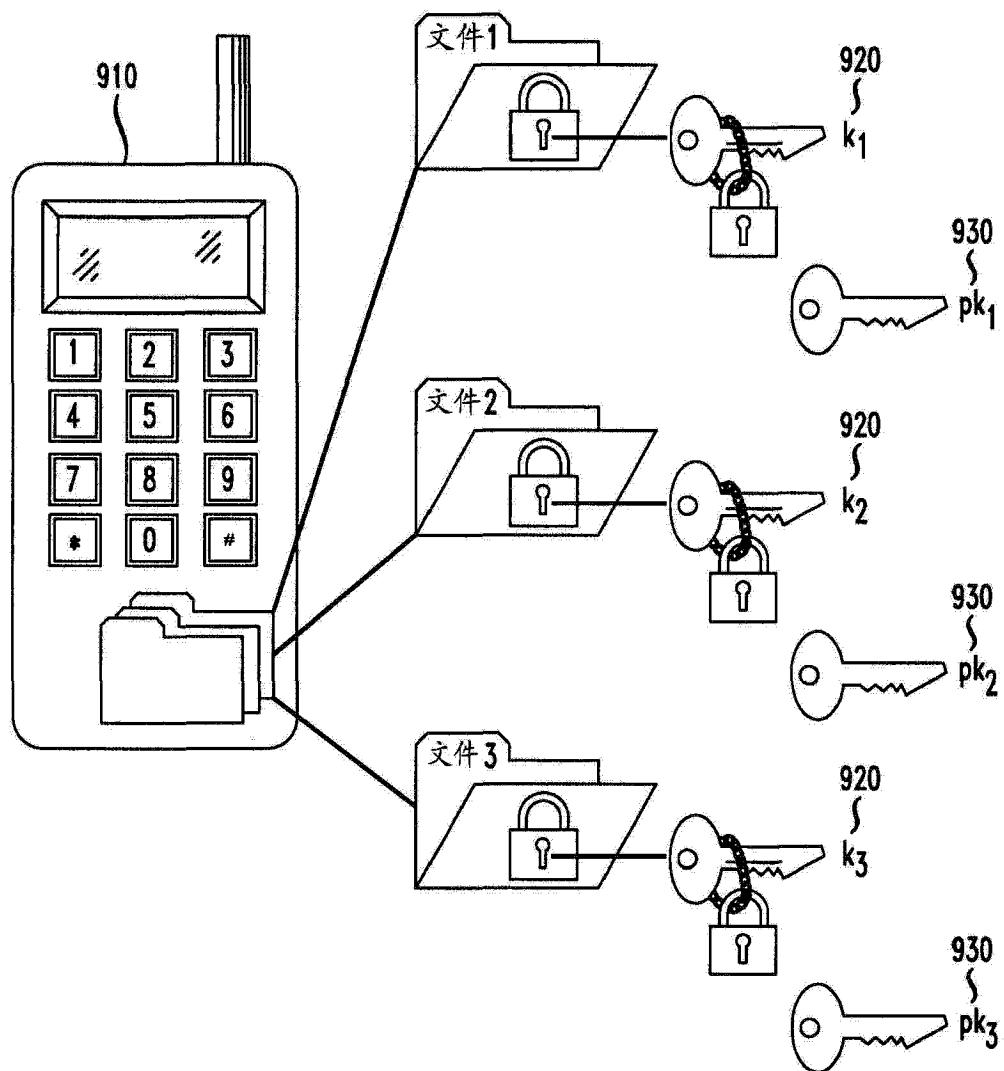


图 9

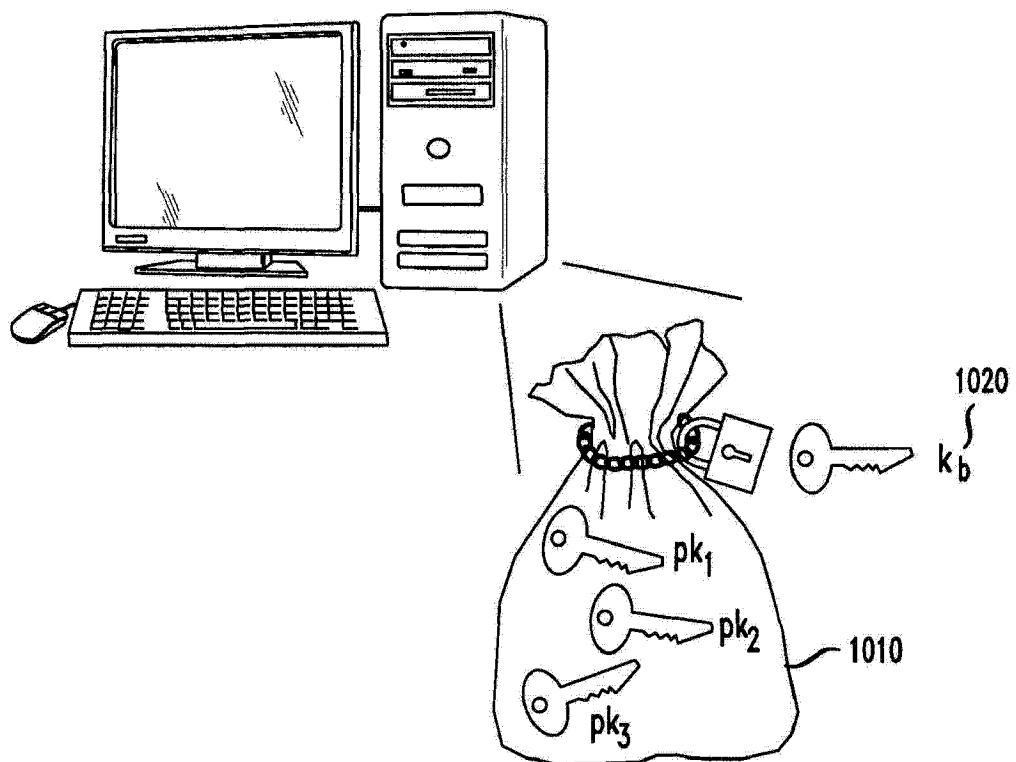


图 10

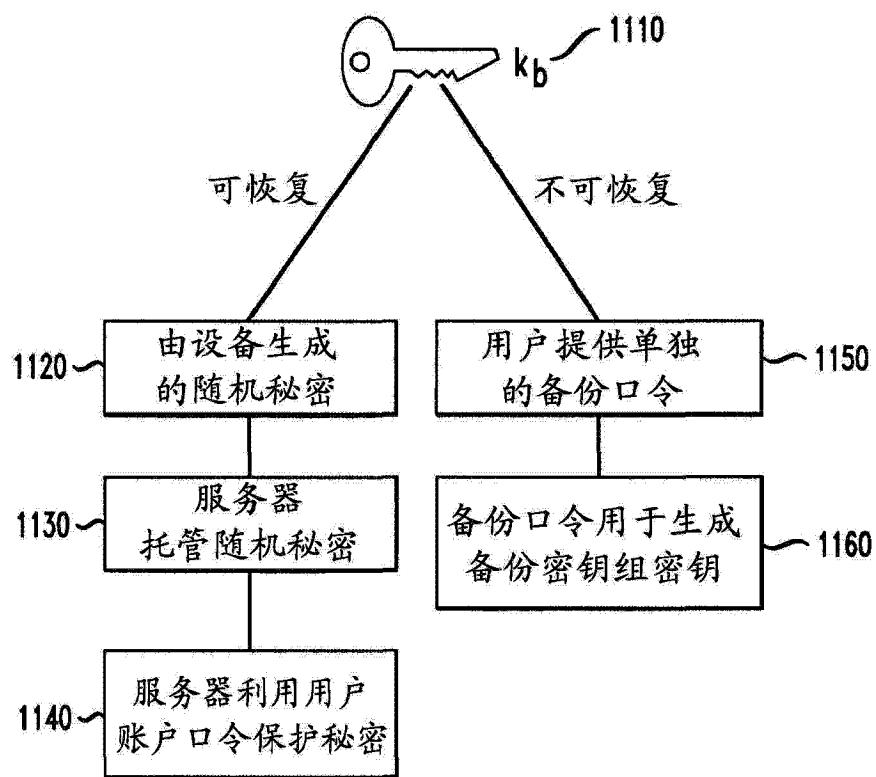
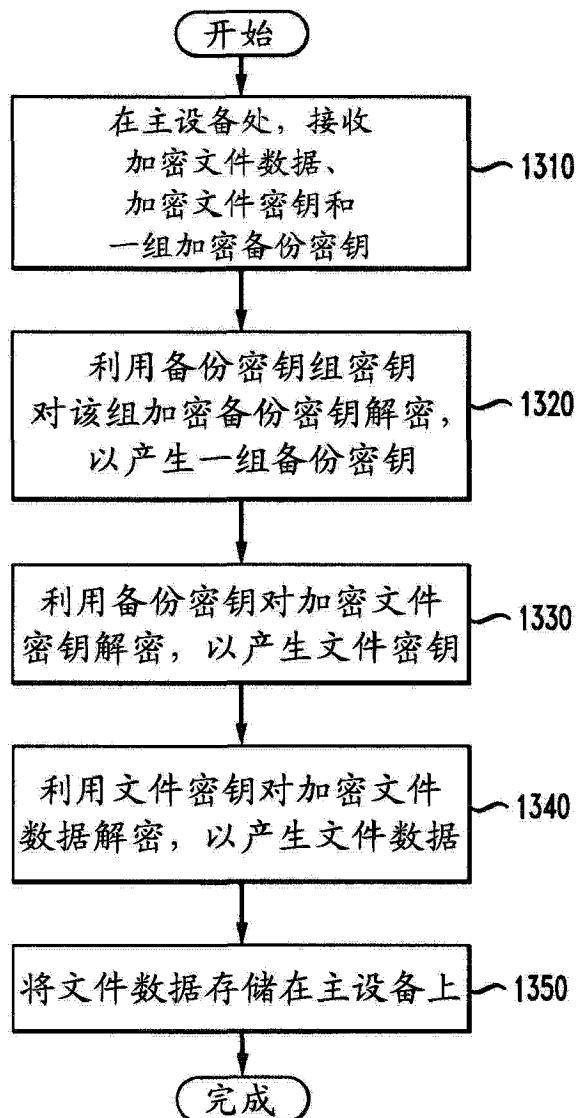
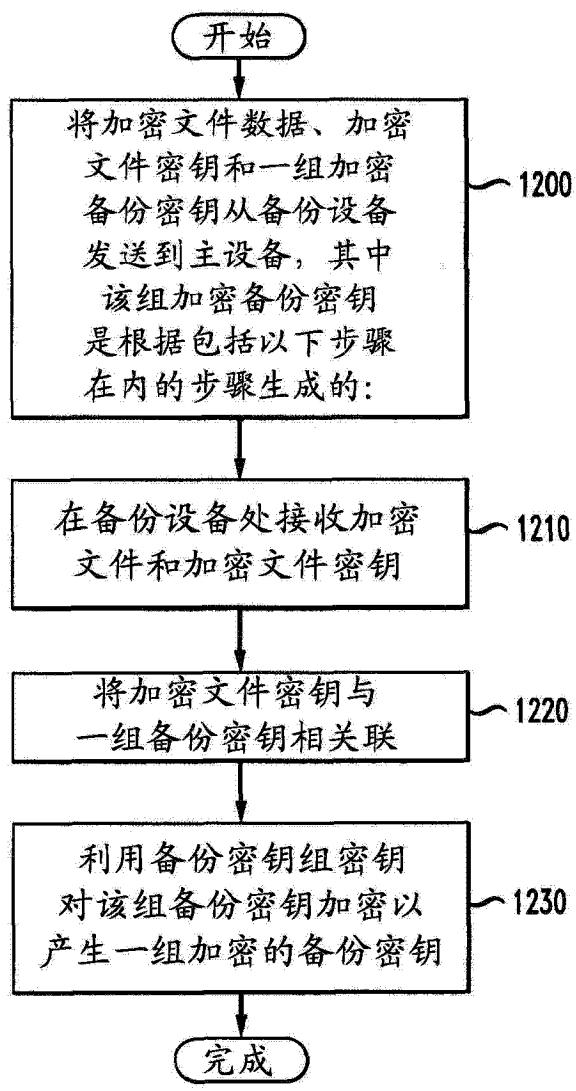


图 11



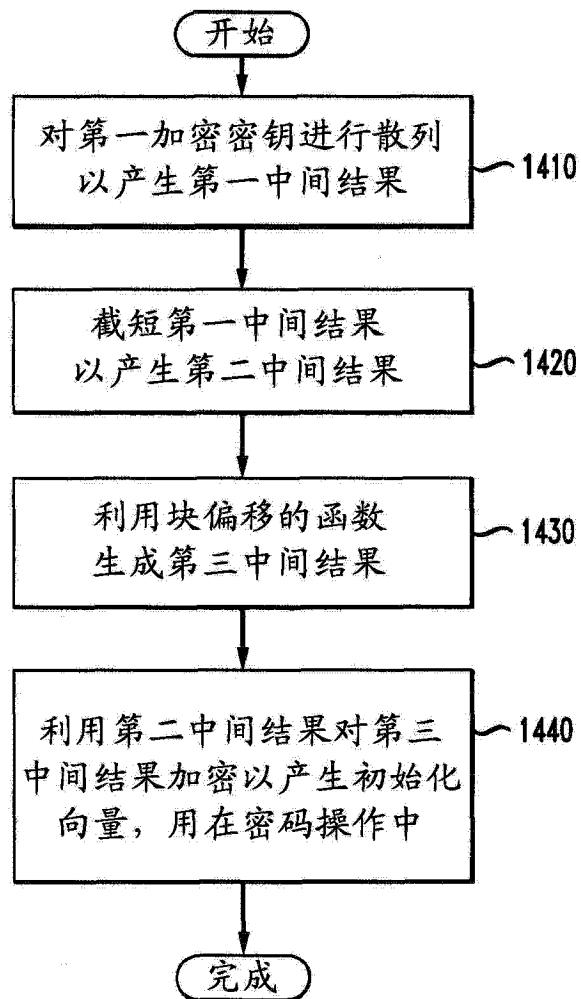


图 14

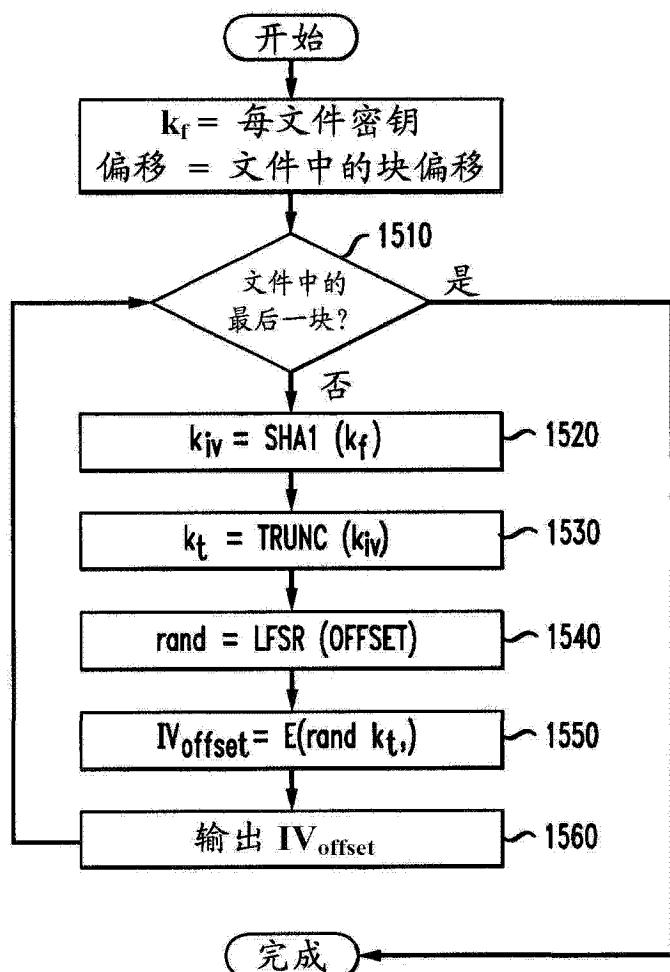


图 15

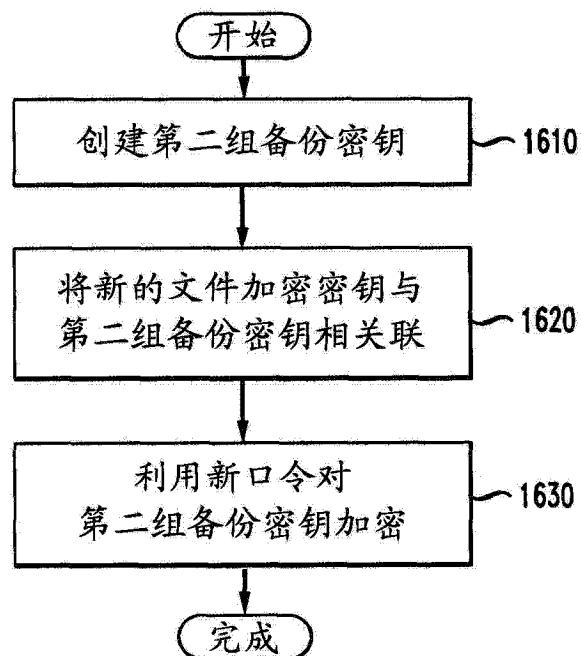


图 16

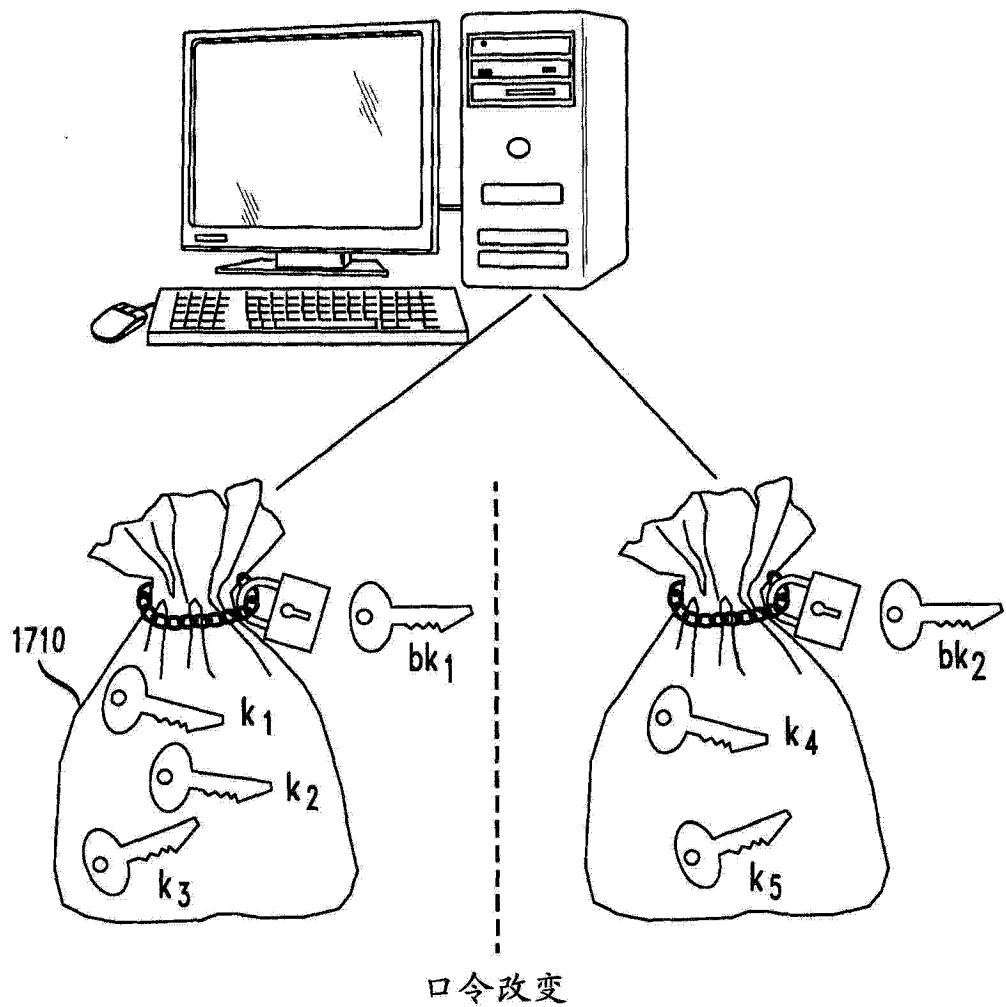


图 17

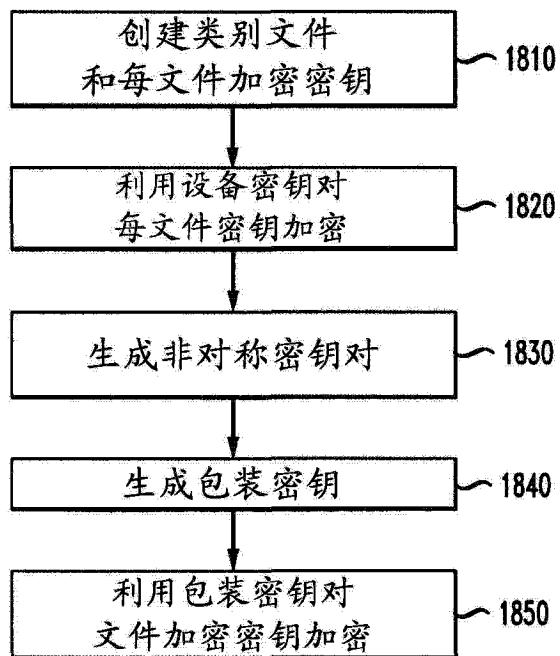


图 18