



(12) 发明专利

(10) 授权公告号 CN 108055352 B

(45) 授权公告日 2021.03.16

(21) 申请号 201810003226.5

(22) 申请日 2013.12.24

(65) 同一申请的已公布的文献号
申请公布号 CN 108055352 A

(43) 申请公布日 2018.05.18

(30) 优先权数据

61/754,524 2013.01.18 US

13/839,050 2013.03.15 US

13/839,084 2013.03.15 US

13/839,126 2013.03.15 US

(62) 分案原申请数据

201380070711.X 2013.12.24

(73) 专利权人 苹果公司

地址 美国加利福尼亚

(72) 发明人 M·布劳沃 D·B·德阿特勒
M·D·安德勒尔

(74) 专利代理机构 中国贸促会专利商标事务所
有限公司 11038

代理人 李晓芳

(51) Int.Cl.

H04L 29/08 (2006.01)

H04L 9/12 (2006.01)

H04L 9/32 (2006.01)

H04L 29/06 (2006.01)

(56) 对比文件

CN 102546176 A, 2012.07.04

CN 1818920 A, 2006.08.16

CN 1363160 A, 2002.08.07

CN 1526217 A, 2004.09.01

US 2005027755 A1, 2005.02.03

US 2008165807 A1, 2008.07.10

US 2011179270 A1, 2011.07.21

审查员 王绮宇

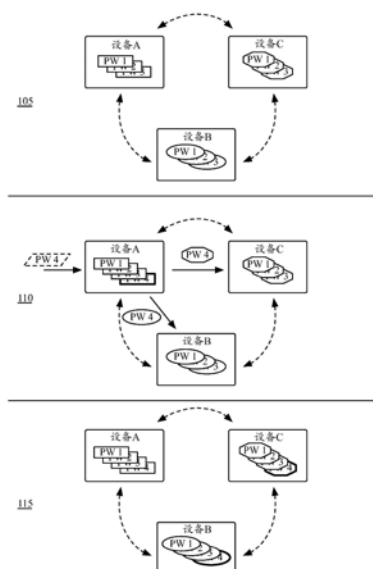
权利要求书3页 说明书32页 附图28页

(54) 发明名称

用于密钥链同步的系统和方法

(57) 摘要

本发明涉及用于密钥链同步的系统和方法。本发明公开了一些实施例,这些实施例提供了存储程序的非暂态机器可读介质,该程序在由设备的至少一个处理单元执行时将存储在设备上的一组密钥链与一组其他设备进行同步。所述设备与所述一组其他设备通过对等(P2P)网络来通信地耦接到彼此。所述程序接收对存储在所述设备上的所述一组密钥链中密钥链的修改。所述程序为所述一组其他设备中的每个设备生成更新请求,以便将存储在设备上的所述一组密钥链与所述一组其他设备进行同步。所述程序通过所述P2P网络经由一组独立的安全通信信道将所述一组更新请求发送到所述一组其他设备。



1. 一种用于将存储在对等设备集合中的第一设备上的密钥链与存储在所述对等设备集合中的其他设备上的密钥链集合进行同步的方法, 每个密钥链包括密钥链项集合, 所述方法包括:

由第一设备接收当第一设备离线时所述对等设备集合中的第二设备已经将第一密钥链项添加到特定密钥链的通知;

由第一设备检索由所述对等设备集合中的第二设备添加到所述特定密钥链的第一密钥链项;

由第一设备确定与第一密钥链项相关联的第一主密钥与存储在所述第一设备上的所述特定密钥链中的第二密钥链项所关联的第二主密钥匹配, 其中与密钥链项相关联的主密钥至少是与密钥链项相关联的一个或多个属性的子组;

由第一设备基于确定第一主密钥与存储在所述第一设备上的所述特定密钥链中的第二密钥链项所关联的第二主密钥匹配, 解决第一密钥链项和第二密钥链项之间的冲突; 以及

由第一设备基于冲突的解决来更新第一设备上的所述特定密钥链。

2. 根据权利要求1所述的方法, 其中如果第一主密钥与第一设备上的所述特定密钥链中的任何项所关联的任何主密钥都不匹配, 则将第一密钥链项添加到第一设备上的所述特定密钥链。

3. 根据权利要求1所述的方法, 其中解决所述冲突包括:

确定第一密钥链项和第二密钥链项中的哪个较新; 以及

如果第一密钥链项较新, 则将第一设备上的所述特定密钥链中的第二密钥链项的值设置为第一密钥链项的值。

4. 根据权利要求3所述的方法, 其中如果第二密钥链项较新, 则通过不修改第二密钥链项来解决所述冲突。

5. 根据权利要求3所述的方法, 其中对于第一密钥链项和第二密钥链项中的哪个较新的确定基于与第一密钥链项和第二密钥链项相关联的时间戳。

6. 根据权利要求1所述的方法, 其中第一密钥链项是从云存储装置中检索的。

7. 根据权利要求1所述的方法, 其中检索第一密钥链项包括:

接收加密的第一密钥链项; 以及

对加密的第一密钥链项进行解密。

8. 一种用于将存储在设备集合中的第一设备上的密钥链与存储在所述设备集合中的其他设备上的密钥链集合进行同步的方法, 每个密钥链包括密钥链项集合, 所述方法包括:

由第一设备接收用于更新存储在所述第一设备上的密钥链的第一密钥链项;

由第一设备, 确定与第一密钥链项相关联的第一主密钥是否与存储在所述第一设备上的密钥链中的第二密钥链项所关联的第二主密钥匹配, 其中与密钥链项相关联的主密钥至少是与密钥链项相关联的一个或多个属性的子组; 以及

由第一设备, 解决第一密钥链项与第二密钥链项之间的冲突, 并且当确定第二主密钥匹配第一主密钥时基于所述解决来更新第二密钥链项, 其中第一密钥链项与第一冲突解决程序相关联并且第二密钥链项与第二冲突解决程序相关联,

其中解决所述冲突包括: 响应于第二冲突解决程序是与第一冲突解决程序相同的冲突解决程序或者第二冲突解决程序是比第一冲突解决程序较新近更新的冲突解决程序, 使用

第二冲突解决程序解决所述第一密钥链项与第二密钥链项之间的冲突。

9. 根据权利要求8所述的方法,还包括:

当确定第一主密钥与存储在第一设备上的密钥链中的任何密钥链项的主密钥都不匹配时,将第一密钥链项添加到存储在第一设备上的密钥链。

10. 根据权利要求8所述的方法,其中解决所述冲突还包括:

识别与第一密钥链项相关联的冲突解决元数据和与第二密钥链项相关联的冲突解决元数据;

基于冲突解决元数据,确定与第一密钥链项相关联的第一冲突解决程序和与第二密钥链项相关联的第二冲突解决程序是否冲突;以及

当确定第一冲突解决程序和第二冲突解决程序不冲突时,使用第二冲突解决程序来解决第一密钥链项和第二密钥链项之间的所述冲突。

11. 根据权利要求8所述的方法,其中解决所述冲突还包括:

确定第一密钥链项是否比第二密钥链项更新;

当确定第一密钥链项更新时,作为所述冲突的解决而将第二密钥链项的值设置为第一密钥链项的值。

12. 根据权利要求11所述的方法,其中确定第一密钥链项是否比第二密钥链项更新包括基于与第一密钥链项和第二密钥链项相关联的时间戳来确定第一密钥链项是否比第二密钥链项更新。

13. 根据权利要求8所述的方法,其中所述密钥链项集合包括访问网站的密码和访问应用的密码中的至少一个。

14. 根据权利要求8所述的方法,其中所述设备集合中的设备是在对等网络中通过网络存储设备集合可通信地耦接到彼此的对等设备,所述方法还包括从所述网络存储设备集合接收所述对等设备集合中的第二设备已经将第一密钥链项存储在所述网络存储设备集合中以供第一设备检索的通知,其中接收第一密钥链项包括从所述网络存储设备集合中检索第一密钥链项。

15. 根据权利要求8所述的方法,其中所述设备集合中的设备是在对等网络中通过网络存储设备集合可通信地耦接到彼此的对等设备,所述方法还包括:

从所述网络存储设备集合接收当第一设备离线时所述对等设备集合中的第二设备已经将第一密钥链项存储在所述网络存储设备集合中以供第一设备检索的通知;以及

从所述网络存储设备集合中检索第一密钥链项。

16. 根据权利要求15所述的方法,其中所述对等网络被实现为根据星型拓扑配置的覆盖网络,其中所述网络存储设备集合是所述星型拓扑的中心。

17. 根据权利要求16所述的方法,其中所述网络存储设备集合为所述对等设备集合提供云服务。

18. 一种存储程序的机器可读介质,所述程序用于由至少一个处理单元执行,所述程序包括用于实现根据权利要求1-17中任一项所述的方法的指令集合。

19. 一种电子设备,包括:

一组处理单元;以及

机器可读介质,所述机器可读介质存储用于由处理单元中的至少一个处理单元执行的

导航应用,所述导航应用包括用于实现根据权利要求1-17中任一项所述的方法的指令集合。

20.一种用于密钥链同步的装置,所述装置包括用于实现根据权利要求1-17中任一项所述的方法的部件。

用于密钥链同步的系统和方法

[0001] 本申请是申请日为2013年12月24日、申请号为201380070711.X、名称为“密钥链同步”的发明专利申请的分案申请。

技术领域

[0002] 本公开涉及一种用于在多个设备之间共享数据的系统和方法。

背景技术

[0003] 在多个设备之间共享数据对于多个设备的用户而言是越来越受欢迎的特征。数据共享特征通过更新整个文件以及在某些情况下更新被指定用于在所述多个设备之间进行同步的整组文件来实现。提供数据共享特征的很多应用程序以未受保护的方式在所述多个设备之间发送和接收数据。

发明内容

[0004] 本发明的一些实施例提供了一种新颖的方法用于促进在被指定为同步组(也被称为同步分组或同步圈)的成员的多个设备之间密钥链的同步(也被称为“同步处理”)。在一些实施例中,密钥链是限定的数据集合,其可包括密码、私钥、证书、安全笔记等。在一些实施例中,该方法通过对等(P2P)网络在设备之间同步密钥链。一些实施例的方法使用通信安全特征,用于阻止对设备之间的通信的未授权访问。

[0005] 不同实施例使用不同的技术来实现设备相互通信所通过的P2P网络。例如,一些实施例使用具有全连接网状拓扑的覆盖网络,而其他实施例使用具有星型拓扑的覆盖网络。此外,一些实施例使用任意数量的附加和/或不同的覆盖网络来实现P2P网络。

[0006] 在一些实施例中,该方法提供安全传输层,用于保护设备相互通信的数据。一些实施例的方法通过在每个所述设备之间利用基于消息的通信协议(例如无记录(OTR)消息传送)提供安全通信信道来实现安全传输层,而其他实施例的方法通过在每对设备之间利用基于流的通信协议(例如安全套接字层(SSL))提供安全通信信道来实现安全传输层。

[0007] 一些实施例的方法通过同步密钥链的单独项(也被称为密钥链项)(而不是同步整个密钥链)来在设备之间同步密钥链。在一些情况下,在同步密钥链项时,一些实施例的方法检测到相同密钥链项的多个版本之间的冲突。不同实施例的方法以不同方式解决这样的冲突。例如,在一些实施例中,该方法使用密钥链项的最新版本作为要在设备之间同步的密钥链项。在一些实施例中可使用附加的和/或不同的方法。

[0008] 在一些实施例中,该方法提供数据保护特征,用于根据所定义的一组条件和/或要求来限制对设备上的密钥链数据(例如密钥链项)的访问。例如,设备上的每个密钥链项在一些实施例中被指定为属于特定保护域。一些实施例的方法只有在为特定密钥链项所属于的特定保护域定义的一组条件和/或要求被满足时才允许设备访问所述特定密钥链项。条件和/或要求的示例包括设备处于解锁状态、设备处于锁定状态、设备的用户输入特定密码等等。在这种方法下,可以粒度的方式来控制对设备上密钥链项的访问。

[0009] 上述发明内容旨在用作对本发明的一些实施例的简单介绍。其并非意味着对在本文档中所公开的所有发明主题进行介绍或概述。随后的具体实施方式以及在具体实施方式中所参照的附图将进一步描述发明内容中所述的实施例以及其他实施例。因此,为了理解该文档所描述的所有实施例,需要全面审阅发明内容、具体实施方式和附图。此外,要求保护的主体不限于发明内容、具体实施方式以及附图中的示例性的细节,而是由所附权利要求限定,这是因为要求保护的主体能够以其他特定形式实施而不脱离本主题的实质。

附图说明

[0010] 在所附的权利要求中阐述了本发明的新颖特征。然而,出于说明目的,在以下附图中阐释本发明的若干实施例。

[0011] 图1根据本发明的一些实施例概念性地示出了在多个设备之间同步密码。

[0012] 图2根据本发明的一些实施例概念性地示出了用于直接P2P网络的网络架构。

[0013] 图3根据本发明的一些实施例概念性地示出了用于间接P2P网络的网络架构。

[0014] 图4根据本发明的一些实施例概念性地示出了发起同步圈并添加设备到同步圈的示例。

[0015] 图5概念性地示出了一些实施例的用于请求加入同步圈的过程。

[0016] 图6概念性地示出了一些实施例的用于处理加入同步圈的请求的过程。

[0017] 图7概念性地示出了用于对密码进行同步的通过图2中所示网络架构的示例性数据流。

[0018] 图8和图9概念性地示出了用于对密码进行同步的通过图3中所示网络架构的示例性数据流。

[0019] 图10根据本发明的一些实施例概念性地示出了用于密钥链的数据结构。

[0020] 图11概念性地示出了描述一些实施例的密钥链管理器的不同状态及这些状态之间的转换的状态图。

[0021] 图12概念性地示出了一些实施例的用于将更新推送到对等设备的过程。

[0022] 图13概念性地示出了一些实施例的用于处理来自对等设备的更新的过程。

[0023] 图14概念性地示出了一些实施例的用于解决发生冲突的冲突解决方案的过程。

[0024] 图15概念性地示出了一些实施例的用于解决密钥链项冲突的过程。

[0025] 图16概念性地示出了不同设备中的不同密钥链项。

[0026] 图17概念性地示出了一些实施例为了处理密钥链项而执行的过程。

[0027] 图18概念性地示出了用于存放传入的密钥链项的处理队列。

[0028] 图19概念性地示出了一些实施例为了处理从源设备接收的密钥链项而执行的过程。

[0029] 图20示出了受到保护域保护的密钥链项,该保护域要求该设备被解锁,以便属于该保护域的密钥链项在设备处可用。

[0030] 图21示出了受到保护域保护的密钥链项,该保护域要求该设备在被启动之后至少被解锁一次,以便属于该保护域的密钥链项在设备处可用。

[0031] 图22示出了受到保护域保护的密钥链项,该保护域要求该设备被开启,以便属于该保护域的密钥链项在设备处可用。

[0032] 图23示出了受到保护域保护的密钥链项,该保护域要求该设备被解锁并且还要求附加的认证,以便属于该保护域的密钥链项在设备处可用。

[0033] 图24示出了受到两个保护域保护的数据,这两个保护域具有对于设备的不同条件组。

[0034] 图25概念性地示出了由多个设备形成的多个同步圈。

[0035] 图26概念性地示出了多个设备形成的用于多个不同保护域的同步圈。

[0036] 图27概念性地示出了一些实施例的密钥链管理器的软件架构。

[0037] 图28概念性地示出了用以实施本发明一些实施例的电子系统。

具体实施方式

[0038] 在本发明的以下具体实施方式中,提出并描述了本发明的许多细节、示例和实施例。然而,对于本领域的技术人员来说将清楚和显而易见的是,本发明并不限于所陈述的实施例,并且本发明可在没有使用所讨论的一些具体细节和示例的情况下被实施。例如,为了简化和/或解释的目的,本申请中的很多附图都是针对特定数量的设备进行描述的。本领域的普通技术人员将认识到,本发明不限于这些附图中所示的设备数量,并且本发明可以任意数量的不同设备来实施。

[0039] 本发明的一些实施例提供了一种新颖的方法用于促进被指定为同步组(也被称为同步分组或同步圈)的成员的多个设备之间密钥链的同步。在一些实施例中,密钥链是限定的数据集合,其可包括密码、私钥、证书、安全笔记等。在一些实施例中,该方法通过P2P网络在设备之间同步密钥链。一些实施例的方法使用通信安全特征,用于阻止对设备之间的通信的未授权访问。

[0040] 不同实施例使用不同的技术来实现设备相互通信所通过的P2P网络。例如,一些实施例使用具有全连接网状拓扑的覆盖网络,而其他实施例使用具有星型拓扑的覆盖网络。此外,一些实施例使用任意数量的附加和/或不同覆盖网络来实现P2P网络。

[0041] 在一些实施例中,该方法提供安全传输层,用于保护设备相互通信的数据。一些实施例的方法通过利用基于消息的通信协议(例如OTR消息传送)在每对设备之间提供安全通信信道来实施安全传输层,而其他实施例的方法通过利用基于流的通信协议(例如SSL)在每对设备之间提供安全通信信道来实施安全传输层。

[0042] 一些实施例的方法通过同步密钥链的单独项(也被称为密钥链项)(而不是同步整个密钥链)来在设备之间同步密钥链。在一些情况下,在同步密钥链项时,一些实施例的方法检测到相同密钥链项的多个版本之间的冲突。不同实施例的方法以不同方式解决这样的冲突。例如,在一些实施例中,该方法使用密钥链项的最新版本作为在设备之间进行同步的密钥链项。在一些实施例中可使用附加的和/或不同的方法。

[0043] 在一些实施例中,该方法提供数据保护特征,用于根据所定义的一组条件和/或要求来限制对设备上密钥链数据(例如密钥链项)的访问。例如,在一些实施例中,设备上的每个密钥链项被指定为属于特定保护域。一些实施例的方法只有在为特定密钥链项所属于的特定保护域定义的一组条件和/或要求被满足时才允许设备访问所述特定密钥链项。条件和/或要求的示例包括设备处于解锁状态、设备处于锁定状态、设备的用户输入特定密码等。在这种方法下,可以粒度的方式控制对设备上密钥链项的访问。

[0044] 图1概念性地示出了根据本发明的一些实施例在多个设备A-C之间同步密码。具体地,图1示出了处于设备A-C之间示例性密码同步的三个不同阶段105-115的设备A-C。在这个示例中,设备A-C被指定为同步圈的彼此对密码进行同步的成员。设备A-C中每一者可以是台式计算机、膝上型计算机、智能电话、平板电脑、或任何其他类型的计算设备。

[0045] 第一阶段105示出了密码1-3在设备A-C之间同步,这是通过设备A-C中每一者都具有相同密码1-3的副本来指示的。对于这个示例,设备A-C中每一者上的密码1-3以只有该设备能够解密和访问的加密格式存储在该设备上。安全特征在图1中是通过将该组密码1-3在设备A-C中每一者中描绘为特定形状来表现的。具体地,存储在设备A上的密码1-3被显示为矩形,存储在设备B上的密码1-3被显示为椭圆形,而存储在设备C上的密码1-3被显示为不规则的凸八边形。这样,在该示例中,设备A只能解密和访问矩形密码,设备B只能解密和访问椭圆形密码,而设备C只能解密和访问不规则凸八边形密码。

[0046] 图1的第二阶段110显示了将密码4添加到设备A(例如,设备A的用户使用设备A创建密码4)。如图所示,密码4被加密并以矩形形状存储在设备A上。在第二阶段110中,设备A正向设备B和C发送密码4的副本,以便将密码4与设备B和C同步。在一些实施例中,当设备A接收到密码4时,设备A向设备B发送密码4的以只有设备B能解密的格式加密的副本,并且向设备C发送密码4的另一个以只有设备C能解密的格式加密的副本。这是通过设备A将密码4作为椭圆形形状发送给设备B并将密码4作为不规则凸八边形形状发送给设备C来指示的。

[0047] 如上所述,一些实施例提供通信安全特征,用于阻止对设备之间通信的未授权访问。为了保护与设备B的通信,设备A在这个示例中对密码4的副本加密并利用安全通信协议(例如SSL、OTR等)通过安全信道将其发送给设备B。一些实施例的安全通信信道是被认证和加密的通信信道。在一些实施例中,设备B以先前被用来通过安全信道传输密码4的加密格式来存储密码4。类似地,设备C在一些实施例中以先前被用来通过安全信道传输密码的加密格式来存储密码4。

[0048] 第三阶段115示出了在设备A-C之间被同步的密码1-4。如图所示,设备B正在存储设备B从设备A接收的密码4的加密副本,并因此与设备A同步。同样,设备C正在存储设备C从设备A接收的密码4的加密副本,并因此与设备A进行同步。如上面所讨论的那样,在这个示例中,存储在设备B上的密码4以只有设备B能解密的格式被加密,而存储在设备C上的密码4以只有设备C能解密的格式被加密。

[0049] 在本专利申请中描述了涉及设备存储密码以在作为同步圈成员的设备之间进行同步的多个细节、示例、和实施例。但是,本领域的普通技术人员应当理解,在一些实施例中,同步圈中的一个或多个设备还存储不与同步圈中的一些或全部其他设备共享(即同步)的密码。

[0050] 此外,虽然本专利申请中所解释的大多数细节、示例、和实施例涉及对被存储作为密钥链一部分的密码进行同步,但本领域的普通技术人员将认识到,本发明并不限于对密码进行同步,并且本发明可被实施用于在同步圈中的设备之间同步密钥链中的其他类型的数据(例如私钥、证书、安全笔记等)。此外,本领域的普通技术人员将认识到,本发明可被实施用于在同步圈中的设备之间同步多于一个密钥链。

[0051] 在下面的章节中描述了本发明的若干更详细的实施例。章节I概念性地描述了根据本发明的一些实施例的示例性P2P网络架构的细节。然后,章节II概念性地描述了根据本

发明的一些实施例创建同步圈以及将设备注册到同步圈中。章节III描述了根据本发明的一些实施例在同步圈的设备之间同步密钥链。然后,章节IV描述了根据本发明的一些实施例用于密钥链的数据保护特征。章节V描述了一些实施例的密钥链管理器的软件架构。最后,章节VI描述了实现本发明的一些实施例的电子系统。

[0052] I. 对等网络架构

[0053] 如上所述,一些实施例通过P2P网络在作为同步圈成员的设备之间同步密钥链。不同实施例的P2P网络利用不同的网络架构来实施,以便有利于同步圈中的设备之间的通信。后面的附图示出了P2P网络架构的不同具体实施的几个示例。

[0054] 图2概念性地示出了根据本发明的一些实施例用于直接P2P网络的网络架构。在这个示例中,设备A-C是同步圈的成员。如图所示,设备A-C中每一者都具有用于存储密码的存储装置210和密钥链管理器205。一些实施例的密钥链管理器205负责执行用于促进设备A-C之间密码同步的功能。例如,在一些实施例中,密钥链管理器205处理将设备注册到同步圈中、在设备A-C之间同步密码、解决发生冲突的密码之间的冲突、生成不同类型的密钥链清单、提供用于在设备A-C之间传送数据的安全通信信道、等等。

[0055] 如图2中所示,设备A-C通过具有全连接网状拓扑的覆盖网络来彼此通信。这样,设备A-C中每一者都能与其他设备中的每一者直接通信。即,设备A能与设备B和C直接通信,设备B能与设备A和C直接通信,设备C能与设备A和B直接通信。

[0056] 如上所述,一些实施例提供安全传输层来保护设备彼此通信的数据。对于这个示例,设备A-C通过在设备A-C中每一对之间建立的安全通信信道来彼此通信。安全通信信道可利用任意数量的不同协议来实现,诸如基于消息的通信协议(例如OTR消息传送)、基于流的通信协议(例如SSL)等。

[0057] 图3概念性地示出了根据本发明的一些实施例用于间接P2P网络的网络架构。与图2类似,对于这个示例,设备A-C是同步圈的成员,并且设备A-C中每一者都具有存储装置210和密钥链管理器205。

[0058] 如图3中所示,设备A-C通过具有星型拓扑的覆盖网络来彼此通信。特别地,设备A-C通过云服务305来彼此通信,云服务充当星型拓扑的中心节点并提供用于存储数据的云存储服务和其他云服务(例如云计算服务)。例如,当设备A想要向设备B传送数据时,设备A将该数据存储在云服务305中,云服务305(例如经由推送通知服务)向设备B通知该数据,并且设备B从云服务305检索该数据。

[0059] 如图所示,云服务305将同步圈的名称和指定为该同步圈的成员的设备同步圈设备列表存储在存储装置310中。在一些实施例中,这些设备通过唯一地识别所述设备的数据来指定。这样的数据的示例包括用于认证设备身份的设备签名公钥/私钥对中的公钥、设备的设备类型(例如台式计算机、平板电脑、智能电话等)、设备的名称等、或任意数量的此类数据的组合。

[0060] 云服务305还将用户签名存储在存储装置315中。在一些实施例中,用户签名是用于认证用户作为消息、文档、或任何其他类型的数据的签名者的身份的数字签名。在一些实施例中,同步圈链接到云服务帐户,并且与云服务帐户相关联的设备(例如具有用于访问与该帐户相关联的云服务的应用程序或程序的设备)是用于注册到该同步圈中的候选设备。在一些这样的实施例中,存储装置315包括以基于云服务帐户的密码生成的用户签名公钥/

私钥对中的私钥签名的签名,以指示云服务305帐户的用户是签名者。存储在存储装置315中的用户签名的示例包括以用户签名公钥/私钥对中的私钥签名的同步圈设备列表的签名、以用户签名密钥对中的私钥签名的注册请求的签名、和/或用于认证云服务帐户的用户的身份的任何其他签名。

[0061] 图3还示出了云服务305将设备签名存储在存储装置320中。在一些实施例中,设备签名是用于认证设备圈中的设备作为消息、文档、或任何其他类型的数据的签名者的身份的数字签名。例如,在一些实施例中,存储装置320包括同步圈设备列表的签名,同步圈设备列表的签名以属于作为同步圈成员的设备的设备签名公钥/私钥对中的私钥来签名。这样的签名表明签名设备确认同步圈设备的列表中的设备列表是同步圈的成员。在一些实施例中,当同步圈处于稳定状态时(例如没有注册请求待处理或未被批准),存储装置320中的设备签名对于作为同步圈成员的每个设备包括以该设备的设备签名公钥/私钥对中的私钥签名的同步圈设备列表的签名。即,在这样的实例中,签名共同地指示同步圈设备列表中所列出的每个设备同意同步圈设备列表中所列出的设备是同步圈的成员。

[0062] 此外,云服务305在存储装置325中存储用于在同步圈中的设备之间同步密钥链的密钥链数据,并且在存储装置330中存储其他数据,所述其他数据可包括用户签名公钥/私钥对中的公钥、用于生成用户签名密钥对中的在同步圈中设备之间共享的随机串(例如256位串)、以及待处理注册请求的列表。在一些实施例中,云服务305将存储装置310-330实现为键值存储。

[0063] 虽然存储装置310-330在图3中被显示为是分开的存储装置,但在一些实施例中,存储装置310-330被实现为单个存储装置,而在其他实施例中,存储装置310-330在多个存储装置上实现。

[0064] 在一些实施例中,上文中参考图2所述的安全传输层被用来保护设备通过云服务305彼此通信的数据。即,虽然设备A-C通过设备A-C中每一对之间建立的安全通信信道来彼此通信,但设备A-C使用云服务305作为用于传输所述通信的机制。一些实施例的安全通信信道在一些实施例中可利用任意数量的不同协议(例如基于消息的通信协议(例如OTR消息传送)、基于流的通信协议(例如SSL)等等)来实现。

[0065] II. 同步圈

[0066] 如上所述,作为同步圈成员的设备在这些设备之间同步密钥链。在本专利申请中,这样的设备也被称为对等设备,或者被简称为对等节点。下面的章节描述创建同步圈以在同步圈的设备之间同步密钥链以及将设备添加到同步圈的示例。

[0067] 图4概念性地示出了根据本发明的一些实施例发起同步圈420以及将设备添加到同步圈420的示例。具体地,图4示出了将设备A和B注册到同步圈420中的三个阶段405-415。阶段405-410中每一者显示了同步圈420以及存储用于同步圈420的数据的存储装置425的概念性图示。在一些实施例中,存储装置425实现在云存储服务305中,并且包括存储装置310-330中的数据,其在上文中参考图3进行了描述。在一些实施例中,结合将存储装置425实现在云存储服务中,作为同步圈420的成员的每个设备将存储装置425中数据的副本在本地存储在设备上。

[0068] 第一阶段405示出了在没有设备注册到同步圈420的情况下的同步圈420。如图所示,同步圈420是空的,并且存储装置425不包含关于同步圈420的成員的数据。一些实施

例的同步圈420链接到云存储服务账户,并且与该云存储服务帐户相关联的设备(例如具有用于访问与该帐户相关联的云存储装置的应用或程序的设备)是用于注册到该同步圈420中的候选设备。在一些此类实施例中,存储装置425存储用于描述与账户相关联的设备的元数据。

[0069] 第二阶段410示出了在有设备注册到同步圈420中的情况下的同步圈420。如第二阶段410中所示,设备A注册到同步圈420中,并且存储装置425正在存储将设备A识别为同步圈420的成員的数据。在一些实施例中,当同步圈420为空的时,同步圈420实际上并不存在。在一些这样的实施例中,同步圈420是在第一设备注册到同步圈420中时创建的。当与云存储服务帐户相关联的设备中的一个设备的用户在该设备上启用密钥链同步特征时,该设备创建同步圈420并将其自身注册到同步圈420中。

[0070] 为了注册到同步圈420中,设备A在存储装置425中存储唯一地将设备A识别为同步圈420的成員的数据。这样的数据的示例包括用于认证设备A的设备签名公钥/私钥对的公钥、设备A的设备类型(例如台式计算机、平板电脑、智能电话等)、设备A的名称等等、或者任意数量的此类数据的组合。

[0071] 在一些实施例中,在同步圈420中的或者潜在地可能加入同步圈420的每个设备使用相同的公钥密码学算法(例如RSA算法、椭圆曲线密码学(ECC)算法等等)来生成设备签名密钥对,从而设备可加密和解密彼此的消息。另外,在一些实施例中,每个设备随机地生成设备签名公钥/私钥对。这样,每个设备生成与任何其他设备所生成的设备签名公钥/私钥对不同的独特的设备签名公钥/私钥对。

[0072] 在一些实施例中,设备A(1)通过以用于认证云存储服务账户的用户的用户签名公钥/私钥对的私钥加密识别同步圈420的成員的数据(在这个示例中是唯一地识别设备A的数据)来生成该数据的签名,并且(2)将签名后的数据存储在存储装置425中。一些实施例的用户签名公钥/私钥对是基于(1)与云存储服务账户相关联的密码和(2)在同步圈420中的设备之间共享的随机串(例如256位串)来生成的。

[0073] 在一些实施例中,在同步圈420中的或者潜在地可能加入同步圈420的每个设备使用相同的公钥密码学算法(例如RSA算法、ECC算法等)来生成用户签名密钥对。在一些实施例中,这样的设备将用于生成设备签名密钥对的公钥密码学算法也用于生成用户签名密钥对。所有这些设备都生成相同的公钥/私钥对,因为这些设备各自使用与云存储服务账户相关联的密码和作为相同公钥密码学算法的输入的所述随机串。这样,在这个示例中,对同步圈420的成員进行识别的数据的签名用于认证云存储服务账户的用户正将设备A注册到同步圈420中。由于设备A是注册到同步圈420中的第一个设备,所以设备A将用户签名密钥对中的公钥和所述随机串存储在存储装置425中。

[0074] 第三阶段415示出了另一设备注册到同步圈420中。如图所示,设备B注册到同步圈420中,并且存储装置425正在存储将设备B也识别为同步圈420的成員的数据。此外,由于设备A和设备B是同步圈420的成員,所以设备A和设备B上的密码被同步。

[0075] 为了设备B注册到同步圈420中,一些实施例要求(1)设备B通过将加入同步圈420的请求存储在存储装置425中来提交该请求,并且(2)设备A批准该请求。不同实施例限定用于批准加入同步圈的请求的不同要求。例如,一些实施例只要求一个作为同步圈成員的设备批准该请求,而其他实施例要求每个作为同步圈成員的设备批准该请求。

[0076] 图5概念性地示出了一些实施例的用于请求加入同步圈的过程500。在一些实施例中,请求加入同步圈的设备(例如在该设备的用户在该设备上启用密钥链同步特征时)执行过程500。过程500将参考图4的设备B执行过程500来进行描述。

[0077] 过程500开始于(在510处)向设备B的用户提示输入密码。在一些实施例中,过程500通过在设备B的显示屏上显示请求用户输入对云存储服务账户的密码的弹出式窗口来向用户提示输入密码。

[0078] 然后,过程500(在520处)基于用户提供的密码来生成用户签名公钥/私钥对。在一些实施例中,过程500基于该密码和用于在同步圈420的成员之间共享的随机串来生成用户签名密钥对。一些此类实施例的过程500从存储装置425检索该随机串,以便生成用户签名密钥对。在不同实施例中,过程500使用不同的技术来生成用户签名密钥对。例如,在一些实施例中,过程500可使用RSA算法、ECC算法、或任何其他类型的公钥加密法来生成设备签名密钥对。

[0079] 过程500然后(在530处)生成用于认证设备B的设备签名公钥/私钥对。不同实施例的过程500使用不同的技术来生成设备签名密钥对。在一些实施例中,过程500利用与在520处用于生成用户签名密钥对相同类型的公钥加密法来生成设备签名密钥对。在其他实施例中,过程500使用另一类型的公钥加密法来生成设备签名密钥对。

[0080] 一旦生成了设备签名密钥对,过程500就(在540处)生成加入同步圈420的请求。在一些实施例中,该请求包括设备B的用于唯一地识别设备B的设备签名密钥对的公钥和过程500从存储装置425检索取得的同步圈420中设备的列表。

[0081] 然后,过程500(在550处)基于所生成的密钥对生成该请求的签名。具体地,过程500(1)利用用户签名密钥对中的私钥生成该请求的签名,并且(2)利用设备B的设备签名密钥对中的私钥生成该请求的签名。

[0082] 最后,过程500(在560处)提交该请求和所生成的签名。在一些实施例中,过程500通过将该请求添加到存储于存储装置425中的注册请求列表来提交该请求。一些实施例的过程500通过将利用用户签名密钥对中的私钥签名的该请求的签名和利用设备B的设备签名密钥对中的私钥签名的该请求的签名存储在存储装置425中来提交这些签名。

[0083] 图6概念性地示出了一些实施例的用于处理加入同步圈的请求的过程。在一些实施例中,作为同步圈成员的设备在设备(例如经由推送通知服务)接收到关于加入该同步圈的请求已经被提交并且待处理的通知时执行过程600。过程600将参考图4的设备A执行过程600来进行描述。

[0084] 过程600开始于(在610)检索将设备B添加到同步圈420的请求。在一些实施例中,过程600通过如下方式来检索该请求:访问存储装置425并从注册请求列表、用设备B的设备签名密钥对中的私钥签名的该请求的签名、和用用户签名密钥对中的私钥签名的该请求的签名中检索该请求。

[0085] 然后,过程600(在620处)确定该请求是否被认证。在一些实施例中,过程600在过程600验证:(1)云存储服务账户的用户提交了将设备B注册到同步圈420中的请求,以及(2)将设备注册到同步圈420的请求确实是用于注册设备B的时候认证该请求。为了验证云存储服务账户的用户提交了注册设备B的请求,一些实施例的过程600(1)用用户签名密钥对中的公钥解密用用户签名密钥对中的私钥签名的该请求的签名,并且(2)核查从注册请求列

表检索得到的请求数据匹配所解密的签名。换言之,过程600核查:所解密的用用户签名密钥对中的私钥签名的该请求的签名包括设备B的设备签名密钥对中的公钥和同步圈420中设备的列表。

[0086] 在一些实施例中,过程600通过(1)用设备B的设备签名密钥对中的公钥解密用设备B的设备签名密钥对中的私钥签名的该请求的签名以及(2)核查从注册请求列表检索得到的请求数据匹配所解密的签名,来验证将设备注册到同步圈420的请求是用于注册设备B。作为解密用设备B的设备签名密钥对中的私钥签名的该请求的签名的替代或附加,一些实施例的过程600使用其他技术来验证将设备注册到同步圈420的请求是用于注册设备B。例如,过程600可提示用户输入在设备B请求注册到同步圈中时在设备B上随机生成并显示的密码、口令、个人识别号(PIN)代码等、选择设备A上显示的与在设备B请求注册到同步圈420中时在设备B上显示的图像匹配的图像、等等。

[0087] 在630处,过程600确定该请求是否已经被同步圈中的设备批准。在一些实施例中,在存储装置425包括用属于该同步圈中设备的设备签名公钥/私钥对中的私钥签名的(1)同步圈420中设备的列表和(2)进行请求的设备的签名时,过程600确定请求已经被该同步圈中的设备批准。

[0088] 当过程600确定请求已经被批准时,过程600(在640处)确认请求的批准,然后过程600结束。一些实施例的过程600通过(1)用过程600正运行于其上的设备的设备签名密钥对中的私钥生成同步圈设备列表(其现在包括新批准的设备)的签名以及(2)将所生成的签名与设备签名一起存储在存储装置425中,来确认请求的批准。

[0089] 在过程600确定请求还没有被批准时,过程600(在650处)提示用户批准请求。不同实施例以不同方式批准请求。例如,一些实施例的过程600在用户提供对云存储服务账户的密码时批准请求。由于一些实施例的设备在用户将对云存储服务账户的密码输入到设备中时不对其进行存储,所以一些实施例的过程600通过在设备A的显示屏上显示(1)指示设备B的设备名称(例如“John Doe的智能电话”)已经请求加入同步圈420并(2)请求用户输入与云存储服务账户相关联的密码的弹出式窗口来提示用户输入密码。

[0090] 然后,过程600(在660处)确定是否接收到来自用户的批准请求的输入。在过程600确定用于批准请求的输入没有被接收到时,过程返回到660,以继续核查来自用户的输入。在过程600确定用于批准请求的输入被接收到时,过程600前进到670。

[0091] 在670处,该过程确定用户批准是否被认证。在对云存储服务账户的密码被用于验证云存储服务账户的用户批准了请求的实例中,一些实施例的过程600通过基于由用户在650处所提供的密码和存储在存储装置425中的随机串来生成用户签名公钥/私钥对来认证用户批准,以及验证由过程600生成的公钥与存储在存储装置425中的用户签名密钥对中的公钥匹配。如上所述,在一些实施例中,在同步圈420中的或潜在地可能加入同步圈420的每个设备使用相同的算法来生成用户签名密钥对。因此,过程600所生成的公钥与存储在存储装置425中的用户签名密钥对中的公钥匹配就验证了云存储服务账户的用户批准了请求。

[0092] 当过程600确定用户批准没有被认证时,过程600结束。当过程600确定用户批准被认证时,过程600(在680处)将进行请求的设备添加到同步圈。在一些实施例中,过程600通过将用于唯一地识别设备B的数据添加到同步圈420的同步圈设备列表、用设备A的设备签名密钥对中的私钥生成同步圈设备列表的签名、并将所生成的签名与设备签名一起存储在

存储装置425中,来将设备B添加到同步圈420。

[0093] 最后,过程600与设备B同步(在690处)被指定为在同步圈420中的设备之间进行同步的密钥链。在一些实施例中,过程600利用下文中参考图7-15所述的技术来同步密钥链。

[0094] 虽然图6示出了在同步圈中的一个设备批准请求后将进行请求的设备添加到该同步圈,但本领域的普通技术人员应当理解,在不同实施例中可使用任意数量的不同批准要求。例如,一些实施例可要求同步圈中的所有设备、限定数量的设备、限定百分比的设备等等在进行请求的设备可被添加到该同步圈之前批准该设备。

[0095] 一些实施例允许设备从同步圈中被移除。例如,如果同步圈中的设备的用户怀疑同步圈中的另一设备没有被授权加入该同步圈、用户丢失了同步圈中的设备、同步圈中的设备被盗等等,则用户可将不需要的设备从同步圈中移除。不同实施例不同地处理设备从同步圈中的移除。例如,在一些实施例中,当设备被从同步圈中移除时,同步圈中的其余设备继续在这些其余设备之间同步密码。被移除的设备在一些这样的实施例中被要求重新进行注册过程(例如上文中参考图4-6所述的那些)以便该设备被添加回该同步圈中。在另一方法下,当设备从同步圈中移除时,同步圈被解散(例如同步圈设备列表被删除)。在这样的情况下,同步圈必须被重新建立,并且设备被添加到新建立的同步圈(例如利用上文中参考图4-6所述的示例和过程)。

[0096] III. 同步密码

[0097] 一旦同步圈被建立并且至少两个设备被注册到该同步圈中,一些实施例的方法就被用于促进密钥链在被指定为该同步圈的成员的设备之间的同步。如上所述,在一些实施例中,该方法利用P2P网络来在设备之间传送数据,以便在设备之间同步密钥链。

[0098] 图7概念性地示出了用于同步密码的通过图2中所示的网络架构的示例性数据流。具体地,图7概念性地示出了当新密码在同步圈中的设备中的一个设备上被创建时用于在作为该同步圈的成员的设备之间同步密码的数据流操作1-9。在这个示例中,同步圈的建立和设备A-C注册到该同步圈中是利用与上文中参考图4-6所述的那些类似的技术来实现的。

[0099] 如所提及的,图7中所示的网络架构与上文中参考图2所述的那个类似。即,设备A-C中每一者都包括用于促进密码同步的密钥链管理器205和用于存储密码的存储装置210。此外,设备A-C通过允许设备A-C中每一者直接与其他设备中每一者进行通信的具有全连接网状拓扑的覆盖网络来彼此通信。在一些实施例中,对于设备A-C中的每一对(即设备A和B、设备A和C、以及设备B和C),设备上的密钥链管理器205促进在这对设备之间提供安全通信信道(例如利用OTR消息传送、SSL等等),用于在这些设备之间传送数据。

[0100] 在图7中的数据流操作1-9开始之前,设备A-C上的密码被同步。换言之,设备A-C每一者都具有存储在存储装置210中的相同密码。数据流开始于(在带圆圈的1处)添加密码705到设备A。例如,设备A的用户可能已经安装了要求用户输入与用户的社交网络账户相关联的用户名和密码的社交网络应用程序(例如Facebook®应用程序、Twitter®应用程序、Google+®应用程序、LinkedIn®应用程序等)。

[0101] 当设备A接收到新密码705时,设备A(在带圆圈的2处)加密密码705并将密码705存储在设备A的存储装置210中。在一些实施例中,存储在设备A-C的存储装置210中的密码利用对称密钥算法(数据加密标准(DES)算法、三重数据加密算法(TDEA)、利用256位块大小和伽罗瓦/计数器模式(GCM)的高级加密标准(AES)等)以及密钥(例如用于登录设备的密码或

口令、设备生成的或分配的随机密钥等、或者任意数量的此类密钥的组合)来进行保护。当设备A将密码705存储在存储装置210中时,密钥链管理器205利用对称密钥算法和密钥对密码进行加密。

[0102] 在存储密码705之后,设备A(在带圆圈的3处)为设备B和C中每一者解密和加密密码705。为了解密存储在存储装置205中的密码705,密钥链管理器205使用在设备A将密码705存储在存储装置210时用来对密码705进行加密的上述对称密钥算法和密钥。

[0103] 如上所述,在设备A-C中每一对之间使用安全通信信道来保护在设备之间传输的数据。由于设备A和B这一对和设备A和C这一对各自使用独立的安全通信信道,所以设备A的密钥链管理器205基于设备A已经与设备B建立的安全通信信道,利用第一密钥或密钥组来加密密码705的用于发送到设备B的副本。设备A的密钥链管理器205还基于设备A已经与设备C建立的安全通信信道,利用另一第二密钥或密钥组来加密密码705的用于发送到设备C的另一副本。

[0104] 例如,在一些实施例中,设备A和B之间的安全通信信道和设备A和C之间的安全通信信道各自都是利用OTR消息传送来实现的。在一些这样的实施例中,基于设备A和B的公钥/私钥对在设备A和B之间建立OTR会话。此外,基于设备A和C的公钥/私钥对在设备A和C之间建立另一独立的OTR会话。在一些实施例中,设备签名密钥对与上文中参考图4-6所述的为了将设备A-C注册到同步圈中而生成的设备签名密钥对相同。

[0105] 一旦设备A的密钥链管理器205加密了密码705的用于设备B的副本,设备A就(在带圆圈的4处)通过在设备A和B之间建立的安全通信信道将密码705的加密副本和描述密码705的元数据发送到设备B。用于描述密码705的元数据的示例包括密码的类型(因特网密码、应用程序密码、网络密码等)、密码所关联的或密码所用于的应用程序或网站的名称、该应用程序或网站的路径等等。

[0106] 当设备B接收到密码705的加密副本时,设备B(在带圆圈的5处)通过使用针对与设备A建立的安全通信信道而生成的密钥或密钥组来解密密码705的该副本。在解密密码705的该副本之后,设备B(在带圆圈的6处)加密并将密码705的该副本存储在设备B的存储装置210中,设备B现在更新有密码705,因此,存储在设备B上的密码与存储在设备A上的密码同步。

[0107] 转向用于在设备A和C之间同步密码的数据流操作,在设备A的密钥链管理器205加密了密码705的用于设备C的副本之后,设备A(在带圆圈的7处)通过在设备A和C之间建立的安全通信信道将密码705的加密副本和描述密码705的元数据发送到设备C。在一些实施例中,与密码705的加密副本一起被设备A发送到设备B的元数据与设备A发送到设备C的元数据相同。

[0108] 在接收到密码705的加密副本之后,设备C(在带圆圈的8处)通过使用针对与设备A建立的安全通信信道而生成的密钥或密钥组来解密密码705的副本。当设备C已经解密了密码705的副本时,设备C于是(在带圆圈的9处)加密密码705的副本并将密码705的副本存储在设备C的存储装置210中。设备C现在更新有密码705,并且因此,存储在设备C上的密码与存储在设备A上的密码同步。

[0109] 图8和图9概念性地示出了用于同步密码的通过图3中所示网络架构的示例性数据流。具体地,图8和图9概念性地示出了当新密码在同步圈中的设备中的一者上被创建时用

于在作为该同步圈的成员的设备之间同步密码的数据流操作1-11。图8概念性地示出了响应于在设备C上创建的新密码而执行的用于在设备B未联机期间在设备C和A之间同步密码的数据流操作1-8。图9概念性地示出了设备B联机以及将设备B的密码与设备C和A同步。在这个示例中,同步圈的建立以及设备A-C注册到同步圈中是利用与上文中参考图4-6所述的那些类似的技术来实现的。

[0110] 如所提及的,图8和图9中所示的网络架构与上文中参考图3所述的网络架构类似。即,设备A-C中每一者都具有用于促进密码同步的密钥链管理器205和用于存储密码的存储装置210。另外,设备A-C通过允许设备A-C中每一者通过云服务305间接地与其他设备中每一者通信的具有星型拓扑的覆盖网络来彼此通信,云服务充当星型拓扑的中心节点并提供用于存储数据的云存储服务。一些实施例的云服务305将同步圈的名称以及同步圈设备列表存储在存储装置310中、将用于认证设备用户的用户签名存储在存储装置315中、将用于认证同步圈中设备的设备签名存储在存储装置320中、将用于在同步圈中的设备之间同步密钥链的密钥链数据存储在存储装置325中以及将其他数据存储在存储装置330中。另外,在一些实施例中,对于设备A-C中的每一对(即设备A和B、设备A和C、以及设备B和C),设备上的密钥链管理器205在这对设备之间建立安全通信信道(例如利用OTR消息传送、SSL等等),这对设备通过该安全通信信道通信。设备A-C在这个示例中将云服务305用作用于传输通信的方式。

[0111] 在图8和图9中的数据流操作1-11开始之前,设备A-C上的密码被同步。即,设备A-C各自具有存储在存储装置210中的相同密码。另外,数据流开始于(在带圆圈的1处)将密码805添加到设备C。例如,设备C的用户可能已经安装了要求用户输入与用户的社交网络账户相关联的用户名和密码的社交网络应用程序(例如Facebook[®]应用程序、Twitter[®]应用程序、Google+[®]应用程序、LinkedIn[®]应用程序等等)。

[0112] 当设备C接收到新密码805时,设备C(在带圆圈的2处)加密密码805并将密码805存储在设备C的存储装置210中。在一些实施例中,存储在设备A-C的存储装置210中的密码利用对称密钥算法(数据加密标准(DES)算法、三重数据加密算法(TDEA)等)和密钥(例如用于登录设备的密码或口令、设备生成的或分配的随机密钥等、或者任意数量的此类密钥的组合)来进行保护。当设备A将密码805存储在存储装置210中时,密钥链管理器205利用对称密钥算法和密钥加密密码805。

[0113] 在存储密码805之后,设备C(在带圆圈的3处)为设备A和C中的每一者解密和加密密码805。为了解密存储在存储装置205中的经加密的密码805,密钥链管理器205使用在设备C将密码805存储在存储装置210中时用来加密密码805的上述对称密钥算法和密钥。

[0114] 如上所述,在设备A-C中的每一对之间使用安全通信信道来保护在这些设备之间传输的数据。由于设备A和B这一对和设备A和C这一对各自使用独立的安全通信信道,所以设备A的密钥链管理器205基于设备A已经与设备B建立的安全通信信道,利用第一密钥或密钥组来加密密码805的用于发送到设备B的副本。设备A的密钥链管理器205还基于设备A已经与设备C建立的安全通信信道,利用另一第二密钥或密钥组来加密密码805的用于发送到设备C的另一副本。

[0115] 例如,在一些实施例中,设备C和A之间的安全通信信道以及设备C和B之间的安全通信信道各自都利用OTR消息传送来实现。OTR会话在一些这样的实施例中基于设备C和A的

设备签名公钥/私钥对而在设备C和A之间建立。另外,另一独立的OTR会话基于设备C和B的设备签名公钥/私钥对而在设备C和B之间建立。一些实施例的设备签名密钥对与上文中参考图4-6所述的为了将设备A-C注册到同步圈中而生成的那些是相同的。

[0116] 一旦设备C的密钥链管理器205加密了密码805的用于设备A的副本和密码805的用于设备B的另一幅本,设备C就(在带圆圈的4处)将密码805的这些加密后副本和描述密码805的元数据存储在云服务305的存储装置325中。用于描述密码805的元数据的示例包括密码的类型(因特网密码、应用程序密码、网络密码等)、密码所关联的或密码被用于的应用程序或网站的名称、该应用程序或网站的路径等等。

[0117] 如上所述,存储装置310-330在一些实施例中为实现为键值存储。一些实施例的用于被发送设备存储在云服务305(例如存储装置325)中的数据的数据的旨在用于接收设备的密钥是第一和第二设备所属于的同步圈的名称、发送设备的识别符和接收设备的识别符的串接。在一些实施例中,接收设备用这个键值对来进行注册,从而当键值对的数值被发送设备改变(例如数值被添加、修改、删除等等)时,云服务305通知接收设备(例如经由推送通知服务)。

[0118] 在这样的方式下,当云服务305从设备C接收到用于设备A的密码805的副本及其对应元数据时,云服务305(在带圆圈的5处)将数据作为按上述方式形成的密钥的值存储在存储装置325中。云服务305然后(例如经由推送通知服务)向设备A通知与密钥相关联的值改变了(例如,在这个示例中,数据被添加)。类似地,当云服务305从设备C接收到用于设备B的密码805的副本及其对应元数据时,云服务305(在带圆圈的5处)将数据作为按上述方式形成的密钥的值存储在存储装置325中。云服务305然后(例如经由推送通知服务)向设备B通知与密钥相关联的值改变了(例如,在这个示例中,数据被添加)。由于设备B在图8中被显示为未联机,所以设备B在这个示例中还没有接收到通知。

[0119] 继续图8,当设备A从云服务305接收到通知时,设备A(在带圆圈的6处)利用与设备C先前用于将经加密的密码805的副本和元数据存储在云服务305中的密钥相同的密钥来检索经加密的密码805的副本和相关联的元数据。一旦设备A检索到密码数据,设备A就(在带圆圈的7处)通过使用针对与设备C建立的安全通信信道而生成的密钥或密钥组来解密密码805的副本。在解密密码805的副本之后,设备A(在带圆圈的8处)加密密码805的副本并将密码805的副本存储在设备A的存储装置210中。此时,设备A被更新有密码805,因此,存储在设备A上的密码与存储在设备C上的密码同步。

[0120] 如图9中所示,设备B现在联机。当云服务305检测到设备B联机时,云服务305向设备B发送通知,该通知指示与用于从设备C接收数据的键值对相关联的值改变了(例如,在这个示例中,数据被添加)。

[0121] 当设备B从云服务305接收到通知时,设备B(在带圆圈的9处)利用与设备C先前用于将经加密的密码805的副本和元数据存储在云服务305中的密钥相同的密钥来检索经加密的密码805的副本和相关联的元数据。在设备B检索到密码数据之后,设备B(在带圆圈的10处)通过使用为与设备C建立的安全通信信道生成的密钥或密钥组来解密密码805的副本。

[0122] 在设备B解密密码805的副本之后,设备B(在带圆圈的11处)加密并密码805的副本将密码805的副本存储在设备B的存储装置210中。此时,设备B被更新有密码805,因此,存储

在设备B上的密码与存储在设备C上的密码同步。

[0123] 虽然图7-图9中所示的数据流操作是基于图7-图9中所示的带圆圈的数字的数值次序而以特定次序进行描述的,但本领域普通技术人员将认识到,带圆圈的数字并非必须代表数据流操作的次序,并且数据流操作可以多种不同次序进行。例如,图7中所示的顺序数据流操作4-6的组和顺序数据流操作7-9的组在一些实施例中彼此独立地发生。类似地,图8和图9中所示的顺序数据流操作6-8的组和顺序数据流操作9-11的组彼此独立地发生。

[0124] A. 密钥链数据结构

[0125] 如上所述,密钥链在一些实施例中是限定的数据集合,其可包括密码、私钥、证书、安全笔记等。在一些实施例中,密钥链管理器生成并存储代表密钥链的数据结构。图10概念性地示出了一些实施例的密钥链管理器所存储的密钥链的数据结构1005。如图所示,数据结构1005包括密钥链ID 1010、密钥链项1-N、和访问数据1015。密钥链ID 1010是用于识别密钥链1005的唯一识别符。访问数据1015用于控制对密钥链1005自身的访问(例如什么应用程序可访问密钥链1005和/或对密钥链1005可执行什么操作(例如读、写、删除等)、等等),并且在结构上与下文中所述的访问数据1035类似。

[0126] 一些实施例的密钥链项代表单独数据片(例如密码、密钥、证书等)。如图10中所示,密钥链项1020代表密钥链1005的密钥链项1。密钥链项1020包括密钥链项ID 1025、数据1030、属性1-M、访问数据1035(也被称为访问对象)。密钥链项ID 1025是用于识别密钥链项1020的唯一识别符。

[0127] 数据1030是密钥链项1020的实际数据值。例如,如果密钥链1020代表密码,则数据1030存储密码的数值(例如字母数字字符串)。在一些实施例中,密钥链管理器在存储某些类型的密钥链项(例如密码、私钥等)的数据时对该数据进行加密。对于其他类型的密钥链项(例如证书)的数据,密钥链管理器简单地存储该数据,而不对数据进行加密。

[0128] 密钥链项1020的属性I-M用于存储描述密钥链项1020的元数据。不同类型的密钥链项具有不同的属性组。例如,因特网密码具有包括诸如安全域、协议类型(例如超文本传输协议(HTTP)、安全超文本传输协议(HTTPS)、文件传输协议(FTP)等)、路径(例如因特网资源的统一资源定位符(URL))等等。

[0129] 在一些实施例中,每个密钥链项包括指示对密钥链项的最新修改的时间和日期(也被称为时间戳)的日期字段属性。在一些实施例中,每个密钥链项还包括用于指定密钥链项是已经被删除的密钥链项(也被称为墓碑(tombstone))的属性。当该属性指定密钥链项是墓碑时,密钥链管理器保持该密钥链项的日期字段,但密钥链管理器将该密钥链项的数据1030的值设置为零或空。在一些实施例中,通过解决发生冲突的密钥链项而得到的密钥链项包括一组属性,这组属性包括(1)用于指示该密钥链项是冲突解决的结果的标记、(2)用于解决该冲突的冲突解决程序的版本号、以及(3)该密钥链项被解决得自的发生冲突的密钥链项(也被称为父密钥链项)。这组属性在一些实施例中被称为密钥链项的冲突解决元数据。

[0130] 在一些实施例中,密钥链项的这些属性或者这些属性的一个子组被用作用于唯一地识别该密钥链项的主密钥。即,具有相同主密钥的两个密钥链项被认为是同一密钥链项(不管密钥链的数据的数值是否相同)。

[0131] 访问数据1035用于控制对密钥链项1020的访问。如图所示,访问数据1035包括用

于控制对密钥链项1020的访问的访问控制列表 (ACL) 条目I-K。图10示出了代表访问数据1035的ACL条目1的ACL条目1040。ACL条目1040包括指定能在密钥链项1020上执行的操作 (例如读、写、删除、解密、认证等) 的授权标签1045。在这个示例中, 授权标签1045包括授权标签1-H。

[0132] 另外, ACL条目1040包括可信应用程序列表1050。如图所示, 可信应用程序列表1050包括应用程序ID 1-J。每个应用程序ID是用于识别可在没有用户授权的情况下执行授权标签1045所指定的操作的特定应用程序的唯一识别符。

[0133] 本领域普通技术人员将认识到, 密钥链数据结构1050仅仅是密钥链管理器可能用于存储密钥链所需要的信息的一种可能的数据结构。例如, 不同实施例可能存储附加的或更少的信息, 以不同次序存储信息等。

[0134] B. 同步密钥链项

[0135] 如上所述, 一些实施例的同步圈中的设备通过同步密钥链的单独密钥链项来在设备之间同步密钥链。图11概念性地示出了状态图1100, 该状态图描述了一些实施例的密钥链管理器的不同状态以及这些状态之间的转换。本领域普通技术人员将认识到, 在一些实施例中, 密钥链管理器将具有与所有不同类型的输入事件相关的很多不同状态, 并且状态图1100具体地专注于这些事件的一个子组。具体地, 状态图1100描述了用于与作为同步圈成员的设备来同步密码的输入事件和相关状态。在描述图11时, 密钥链管理器正运行于其上的设备将被称为本地设备。

[0136] 当密钥链管理器不是正在处理用于同步密钥链的任何事件时, 密钥链管理器处于稳定状态1105。在状态1105中, 密钥链管理器可执行不与同步密钥链相关的其他操作。例如, 密钥链管理器可执行注册操作, 以接受、拒绝、和/或确认加入同步圈的请求。

[0137] 在从同步圈中的对等设备接收到清单摘要后, 密钥链管理器转换到状态1110, 以处理清单摘要请求。在一些实施例中, 清单摘要是对等设备的当前密钥链项的列表。一些实施例的密钥链管理器为同步圈中的每个对等设备存储清单历史。

[0138] 在状态1110, 密钥链管理器通过将本地设备的用于对等设备的历史中的最新清单与从该对等设备接收的清单摘要进行比较, 来生成对清单摘要的响应。如果清单匹配并且本地设备具有与对等设备的清单摘要中的密钥链项相同的密钥链项, 则密钥链管理器生成指示本地设备与对等设备同步的消息。

[0139] 如果本地设备的用于对等设备的历史中的最新清单与从对等设备清单所接收的清单摘要匹配, 但本地设备具有与对等设备的清单列表中的密钥链项不同的一组密钥链项, 则密钥链管理器生成包括差量 (delta) 清单的消息。在一些实施例中, 差量清单包括 (1) 本地设备的密钥链项与对等设备的清单中所列出的密钥链项之间的差别的列表、以及 (2) 用于列表中对等密钥链项的数据。差量清单可包括没有被包括在对等设备的清单摘要中的密钥链项和/或相同 (例如具有相同主密钥) 但具有不同数据值的密钥链项。

[0140] 当本地设备的用于对等设备的历史中最新的清单与从对等设备接收的清单摘要不匹配时, 密钥链管理器生成包括本地设备的完整清单的消息。完整清单在一些实施例中包括 (1) 本地设备的所有密钥链项的列表、(2) 列表中对等密钥链项的数据。在处理来自对等设备的清单摘要之后, 密钥链管理器将所生成的响应发送给对等设备, 并转换回到稳定状态1005。

[0141] 在处于稳定状态1105中时,如果密钥链管理器接收到对本地密钥链的改变,则密钥链管理器前进到状态1115,以处理对本地密钥链的改变。在状态1115,密钥链管理器用该改变对本地密钥链进行更新。在一些实施例中,密钥链可包括被指定用于与同步圈中的对等设备同步的密钥链项和不用于与同步圈中的对等设备同步的密钥链项。如果对本地密钥链的改变不影响被指定用于与同步圈中的对等设备同步的任何密钥链项,则密钥链管理器返回到稳定状态1105。否则,密钥链管理器转换到状态1120,以同步(1)被指定用于与同步圈中的对等设备同步、并且(2)受到对本地密钥链的改变影响的密钥链项。

[0142] 在状态1120,密钥链管理器将对本地设备的密钥链的更新发送到同步圈中的每个对等设备。在一些实施例中,密钥链管理器执行下文中参考图12所述的用于发送更新到对等设备的过程1200。在密钥链管理器将更新发送给对等设备之后,密钥链管理器返回到稳定状态1105。

[0143] 当密钥链管理器处于稳定状态1105中并且从同步圈中的对等设备接收到完整清单时,密钥链管理器转换到状态1125,以处理完整清单。在一些实施例中,密钥链管理器通过生成包括(1)本地设备的密钥链项与对等设备的完整清单中所列出的密钥链项之间的差别的列表、以及(2)列表中对应密钥链项的数据的差量清单来处理完整清单。如果差量清单为空(即本地设备具有与对等设备的完整清单中所列出的密钥链项相同的密钥链项),则密钥链管理器将表明如此的消息发送到对等设备,然后返回到稳定状态1105。如果差量清单不为空,则(在状态1130处)密钥链管理器将差量清单发送到对等设备,然后返回到稳定状态1105。

[0144] 在稳定状态1105,如果密钥链管理器从对等设备接收到用于更新本地设备的密钥链的差量清单,则密钥链管理器转换到状态1135,以将来自对等设备的更新应用到本地设备的密钥链。在一些实施例中,密钥链管理器执行下文中参考图13所述的过程1300,以将来自对等设备的更新应用到本地设备的密钥链。一旦密钥链管理器将对等设备的更新应用到本地密钥链,密钥链管理器就将对等设备的更新应用到本地设备的用于该对等设备的历史中的最新清单,将修改后的清单存储在本地设备的用于该对等设备的历史的清单中。密钥链管理器然后将本地设备的用于该对等设备的历史中的最新清单(其是密钥链管理器刚刚存储的清单)与本地设备的当前密钥链项清单进行比较。

[0145] 如果清单匹配,但本地设备具有与对等设备的清单摘要中的密钥链项不同的一组密钥链项,则密钥链管理器转换到状态1140并调度安排更新以发送到同步圈中的对等设备。否则,密钥链管理器返回到稳定状态1105。

[0146] 在状态1140中,密钥链管理器核查是否还有来自对等设备的任何更新要处理。如果有,则密钥链管理器转换到状态1135以继续处理来自对等设备的任何差量清单,用于更新本地密钥链。如果没有来自对等设备的任何更新要处理,则密钥链管理器从状态1140转换到状态1145,以将调度安排的更新发送到同步圈中的对等设备。在一些实施例中,密钥链管理器执行下文中参考图12所述的过程1200以发送更新给对等设备。一旦密钥链管理器将所有调度安排的更新发送给了对等设备,密钥链管理器就返回到稳定状态1105。

[0147] 图12概念性地示出了一些实施例的用于将更新推送给对等设备的过程1200。在一些实施例中,本专利申请中所述的密钥链管理器执行过程1200,以将被应用于本地设备的本地密钥链的更新发送给同步圈中的对等设备。例如,当密钥链管理器处于上文中参考图

11所述的状态1120和1145中时,密钥链管理器执行过程1200。

[0148] 过程1200开始于(在1210处)识别同步圈中的对等设备。在一些实施例中,过程1200通过访问同步设备列表的本地副本来识别对等设备,而在其他实施例中,过程1200通过访问存储在云服务305中(例如存储装置310中)的同步设备列表来识别对等设备。

[0149] 然后,过程1200(在1220处)确定本地设备的清单是否与对等设备的清单匹配。在一些实施例中,过程1200将本地设备的用于对等设备的历史中的最新清单用作对等设备的清单。当过程1200确定清单匹配时,过程1200前进到1260。否则,过程1200继续到1230。

[0150] 在1230处,过程1200基于本地设备和对等设备的清单来生成差量清单。如上所述,差量清单在一些实施例中包括:(1)本地设备的密钥链项与对等设备的清单中所列出的密钥链项之间的差别的列表、和(2)列表中对对应密钥链项的数据。在一些实施例中,过程1200通过(1)将本地设备的密钥链中的密钥链项与对等设备的清单中所列出的密钥链项进行比较并(2)识别差别来生成差量清单。

[0151] 过程1200然后(在1240处)利用用于对等设备的加密密钥或密钥组来加密在差量清单中指定的本地密钥链项的副本。如上所述,在一些实施例中,在同步圈中的每对设备之间使用安全通信信道。这样,过程1210识别针对用于与对等设备进行通信的安全通信信道而建立的密钥或密钥组,并将所识别的密钥或密钥组用于对本地密钥链项的副本进行加密。

[0152] 然后,过程1200(在1250处)通过安全通信信道将经加密的密钥链项和差量清单发送到对等设备。一旦过程1200将信息发送到对等设备,过程1200然后就(在1260处)确定是否还有同步圈中的任何对等设备要处理。当过程1200确定还有对等设备要处理时,过程1200返回到1210以继续将被应用到本地密钥链的更新发送到同步圈中的剩余对等设备。当过程1200确定没有对等设备还要处理时,过程1200然后结束。

[0153] 图13概念性地示出了一些实施例的用于处理来自对等设备的更新的过程1300。在一些实施例中,本专利申请中所述的密钥链管理器执行过程1300以将来自对等设备的更新应用到本地设备的本地密钥链。例如,当密钥链管理器处于上文中参考图11所述的状态1135中时(例如当密钥链管理器从对等设备接收到差量清单要处理时)执行过程1300。

[0154] 过程1300开始于(在1310处)识别在从对等设备接收的差量清单中指定的被更新密钥链项。然后,过程1300(在1320处)解密被更新密钥链项。如上所述,在一些实施例中,在同步圈中的每对设备之间使用安全通信信道。因此,过程1310识别针对用于与对等设备进行通信的安全通信信道而建立的密钥或密钥组,并使用所识别的密钥或密钥组来解密被更新密钥链项。

[0155] 过程1300然后(在1330处)识别被更新密钥链项的主密钥。如上所述,在一些实施例中,将密钥链项的属性或属性子组用作唯一地识别密钥链项的主密钥。

[0156] 然后,过程1320(在1340处)确定本地密钥链中的密钥链项是否具有与被更新密钥链项的主密钥相同的主密钥。当过程1300确定本地密钥链中没有任何密钥链项具有与被更新密钥链项的主密钥相同的主密钥时,过程1300(在1350处)将被更新密钥链项应用到本地密钥链。在一些实施例中,过程1300通过将被更新密钥链添加到本地密钥链来将被更新密钥链项应用到本地密钥链。

[0157] 当过程1300确定本地密钥链中的密钥链项具有与被更新密钥链项的主密钥相同

的主密钥时,过程1300(在1360处)解决被更新密钥链项与本地密钥链项之间的冲突,并将冲突解决的结果应用到本地密钥链。不同实施例的过程1300不同地解决发生冲突的密钥链项之间的冲突。下文中参考图15来介绍一种此类方法。过程1300(在1370处)确定是否还有经更新的密钥链项要处理,并且如果有任何这样的密钥链项要处理,则返回到1310。否则,过程结束。

[0158] C. 解决密钥链项冲突

[0159] 在同步密钥链项时,一些实施例的密钥链管理器可能检测到同一密钥链项的多个版本之间的冲突。在不同实施例中,密钥链管理器利用不同技术来解决密钥链项冲突。例如,在一些实施例中,该方法将密钥链项的最新版本用作在设备之间同步的密钥链项。在一些实施例中可使用附加的和/或不同的方法。

[0160] 在一些实施例中,设备可更新它们的冲突解决过程(也被称为“冲突解决程序”)。在一些实例中,经更新的过程和先前的未更新过程在确定应当使用哪些密钥链项数值时提供不同的结果。在一些实施例中,可能出现以下情况,即同步圈中的一个或多个设备正在使用经更新的冲突解决过程,而同一同步圈中的一个或多个其他设备正在使用先前版本的冲突解决过程。图14概念性地示出了一些实施例的用于解决发生冲突的冲突解决程序的过程1400。在一些实施例中,上文中参考图13所述的过程1300执行过程1400来实现操作1360。

[0161] 过程1400开始于(在1410处)识别发生冲突的密钥链项的冲突解决元数据。如上所述,一些实施例的冲突解决元数据包括(1)用于指示密钥链项是冲突解决结果的标记、(2)用于解决冲突的冲突解决程序的版本号、以及(3)密钥链项被解决得自的发生冲突的密钥链项(也被称为父密钥链项)。

[0162] 然后,过程1400(在1420处)确定被更新密钥链项的冲突解决程序是否与本地密钥链项的冲突解决程序冲突。在一些实施例中,被更新密钥链项与本地密钥链项的冲突解决程序在如下情况下发生冲突:(1)这两个密钥链项都具有用于指示密钥链项是冲突解决结果的标记、(2)被更新密钥链项与本地密钥链项被指定为被更新密钥链项的父密钥链项、以及(3)用于解决被更新密钥链项的冲突解决方案的版本号与本地设备的冲突解决程序的版本号不同时。

[0163] 当过程1400确定冲突解决程序不冲突时,过程1400(在1430处)用本地设备的冲突解决程序解决密钥链项冲突,然后过程1400结束。当过程1400确定冲突解决程序发生冲突时,过程1400(在1440和1450处)确定是否使用本地设备的冲突解决程序。当本地冲突解决程序的版本号比用于解决被更新密钥链项的冲突解决程序的版本号高时,过程1400(在1430处)用本地设备的冲突解决程序解决密钥链项冲突。否则,过程1400(在1430处)将被更新密钥链项用作对密钥链项冲突的解决方案。然后过程1400结束。

[0164] 图15概念性地示出了一些实施例的用于解决密钥链项冲突的过程1500。在一些实施例中,上文中参考图14所述的过程1400执行过程1500来实现操作1460。

[0165] 过程1500开始于(在1510处)识别发生冲突的被更新密钥链项和本地密钥链项的时间戳。如上所述,密钥链项的数据结构在一些实施例中包括日期字段,该日期字段指示对密钥链项的最新修改的时间和日期。在一些实施例中,过程1500通过访问每个密钥链项的日期字段属性来识别时间戳。

[0166] 然后,过程1500(在1520处)确定被更新密钥链项的时间戳是否较新。当过程1500

确定被更新密钥链项的时间戳较新时,过程1500(在1540处)用被更新密钥链项来更新本地密钥链项,然后过程1500结束。当过程1500确定被更新密钥链项的时间戳并非较新时,过程1500(在1530处)用本地密钥链项来更新本地密钥链项,然后过程1500结束。

[0167] IV. 为密钥链使用数据保护域

[0168] 本发明的一些实施例提供数据保护特征,用于根据所定义的条件和/或要求组来限制对设备上的密钥链数据(例如密钥链项)的访问。在一些实施例中,定义多个不同的保护域(也被称为数据保护类),并且设备上的每个密钥链项属于所定义的保护域之一。每个保护域与一组条件相关联。当对于特定数据保护域,一组条件被满足时,属于该特定保护域的设备中的密钥链项变得可供该设备使用。

[0169] A. 数据保护域

[0170] 图16概念性地示出了不同设备中的不同密钥链项。具体地,该图示出了属于不同保护域的密钥链项根据设备对于不同保护域满足的条件而变得可用。该图示出了源设备1605和1610、目标设备1615-1635、和密钥链项S1-S3和C4-C5。

[0171] 在一些实施例中,保护域被预先定义并作为设备的操作系统(例如iOS™、Windows™等等)的一部分而被提供给设备。被这些操作系统管理的设备可通过只有在与保护域相关联的条件被满足之后才使密钥链项在设备中可用,来使用保护域保护密钥链项。这些预先定义的保护域在本专利申请中被称为系统保护域。

[0172] 在一些实施例中,保护域可由在设备上运行的应用程序的开发者或者设备的用户来自定义限定。在这些实施例中,设备或操作系统的制造商为用户提供了工具,使得用户能通过为保护域定义不同的条件组来定义自定义限定的保护域。另外,设备或操作系统的制造商为开发者提供软件开发套件(SDK),使得开发者能通过为由开发者编写的用于运行在设备上的应用程序定义保护域的不同条件组来定义自定义限定的保护域。

[0173] 如上所述,不同保护域与不同的条件或要求组相关联。在一些实施例中,可定义多个保护域,以为某些密钥链项提供附加的安全等级。即,第一保护域的条件是第二保护域的条件的一个子组,从而属于第二保护域的密钥链项只有在设备在第一保护域的条件之外满足了第二保护域的附加条件的情况下才变得对于设备可用。例如,第一保护域的条件包括设备被启动并且正在运行,而第二保护域的条件包括设备被解锁以及被启动和正在运行。

[0174] 在一些实施例中,保护域可被定义为具有可能重叠、也可能不重叠的不同条件组。例如,第一保护域的条件可包括在设备被解锁之后的附加认证(例如附加密码)。第二保护域的条件可包括设备中的特定应用程序的存在。第一保护域和第二保护域的这些条件不重叠。

[0175] 在这个示例中,源设备1605是将被更新的密钥链项S1-S3推送给目标设备1615-1625的设备。如图所示,设备1605中的密钥链项S1-S3分别属于保护域1-保护域3。在这个示例中,保护域1-保护域3是系统保护域。保护域1-保护域3为密钥链项提供不同的安全等级。在这个示例中,保护域3的条件是保护域2的条件的子组,而保护域2的条件是保护域1的条件的子组。

[0176] 在这个示例中,设备1615-1625满足不同的条件组。具体地,设备1625满足保护域3的所有条件。设备1620满足保护域2的所有条件。设备1615满足保护域1的所有条件。因此,密钥链项S3可供设备1625使用,但密钥链项S1和S2不可供其使用。密钥链项被图示为虚线

平行四边形,以指示这些项的不可用性。密钥链项S2和S3可供设备1620使用,但密钥链项S1不可供其使用。所有三个密钥链项S1-S3可供设备1615使用。

[0177] 不同实施例采用不同的方式将密钥链项保留为不可供设备使用。例如,一些实施例的设备中的密钥链管理器在设备没有满足密钥链项所属于的保护域的所有条件时不对该密钥链项进行解密,并因此使该密钥链项不能使用。另选地或结合地,一些实施例的密钥链管理器使密钥链项在设备满足该密钥链项所属于的保护域的条件之前不能被运行于该设备中的应用程序访问。在一些实施例中,目标设备的密钥链管理器不接受从源设备推送的密钥链项,除非在密钥链被推送时,目标设备满足该密钥链项所属于的保护域的条件。

[0178] 源设备1610在这个示例中是将被更新密钥链项C4和C5推送给目标设备1630-1635的设备。如图所示,设备1610中的密钥链项C4和C5分别属于保护域4和保护域5。保护域4和保护域5是自定义限定的保护域,它们具有不同的条件组。在这个示例中,保护域4的条件与保护域5的条件不重叠。

[0179] 设备1630在这个示例中满足保护域4的所有条件,但不满足保护域5的所有条件,而设备1635满足保护域5的所有条件,但不满足保护域4的所有条件。因此,密钥链项C4可供设备1630使用,但密钥链项C5不可供其使用。密钥链项C5可供设备1635使用,但密钥链项C4不可供其使用。

[0180] 本领域普通技术人员将认识到,一些实施例对保护域的使用并不限于保护密钥链项。任何类型的数据都可被定义为属于不同保护域,以便接收不同的安全等级。例如,在一些实施例的第一设备中更新的文档可被推送到第二设备,但该文档在第二文档满足该文档所属于的保护域的所有条件之前仍然保持为不可供第二设备使用。

[0181] 图17概念性地示出了一些实施例为了处理密钥链项而执行的过程1700。在一些实施例中,过程1700由一个或多个源设备已经将密钥链项推送到的目标设备来执行。具体地,在这些实施例中,目标设备的密钥链管理器可执行过程1700。一些实施例的目标设备将来自源设备的密钥链项存放在处理队列中。下文中将参考图18进一步介绍示例性处理队列。过程1700在一些实施例中在目标设备被启动并且已经从源设备接收到一个或多个密钥链项时启动。

[0182] 过程1700开始于(在1710处)从处理队列检索密钥链项。在一些实施例中,处理队列是用于保持从源设备推送的密钥链项的存储结构(例如文件系统)。在一些实施例中,源设备利用目标设备先前发布的目标设备的公钥来加密密钥链项中的数据(例如密码)。在这些实施例中,密钥链项被加密地存储在处理队列中。

[0183] 目标设备使用对应的私钥(即,包括源设备用来加密密钥链项的公钥的公钥私钥对中的私钥)来解密密钥链项。在一些实施例中,目标设备为设备支持的每个保护域生成公钥私钥对。下文中将参考图25和图26进一步介绍关于不同保护域的密钥对的更多细节。

[0184] 过程1700然后(在1720处)识别所检索密钥链项的保护域。密钥链项在一些实施例中还包括或与用于识别该密钥链项所属于的保护域的识别符相关联。在一些实施例中,源设备用来加密密钥链项中的数据的公钥用作保护域识别符。过程1700读取密钥链项的保护域识别符,以识别所检索的密钥链项属于的保护域。

[0185] 然后,过程1700(在1730处)确定所识别的保护域是否可用。即,过程1700确定目标设备是否已经满足了所识别的保护域的所有条件。在一些实施例中,目标设备获得作为设

备的操作系统的一部分的这些条件的定义。另选地或结合地,一些实施例的目标设备可在目标设备与源设备建立包括目标和源设备的同步圈时获得这些条件的定义。

[0186] 当过程1700 (在1730处) 确定没有满足所识别的保护域的所有条件时,过程1700 (在1740处) 通过将密钥链项存放回处理队列中来将密钥链项返回到处理队列中,从而密钥链项能等待该密钥链项所属于的保护域的条件被满足。过程1700然后前进到下文中将进一步介绍的1760。

[0187] 当1700 (在1730处) 确定所识别的保护域的所有条件都被满足时,过程1700 (在1750处) 处理密钥链项。在1750处,一些实施例的过程1700通过发起对密钥链项的同步来处理密钥链项。在一些实施例中,过程1700对于所识别的保护域利用目标设备的私钥来解密密钥链项。

[0188] 然后,过程1700 (在1760处) 确定处理队列中是否还有其他密钥链项要处理。当过程1700确定处理队列中还有其他密钥链项时,过程1700返回到1710以检索另一密钥链项。否则,过程1700结束。

[0189] 图18概念性地示出了用于存放传入的密钥链项的处理队列。具体地,该图示出了一些实施例的处理队列是与不同保护域相关联的一组桶。该图示出了源设备1805、目标设备1810、和处理队列1815。

[0190] 源设备1805更新一个或多个密钥链项,并将密钥链项推送给目标设备1810。在一些实施例中,源设备1805发送的密钥链项1840与保护域识别符1835相关联,源设备1805将保护域识别符1835与密钥链项1840一起发送。在一些实施例中,源设备1805用目标设备1810的公钥(未示出)来加密密钥链项1840,目标设备1810先前已经为目标设备1810支持的每个保护域发布了目标设备1810的公钥。在这些实施例中的一些实施例中,用于加密密钥链项的公钥可用作保护域识别符。

[0191] 目标设备1810用来存放密钥链项的处理队列1815具有桶1820、1825和1830。每个桶与一保护域相关联,如图所示。目标设备1810基于保护域识别符所识别的保护域,将密钥链项存放在处理队列1815的桶1820-1830之一中。在一些实施例中,目标设备1810还存放与每个密钥链项相关联的保护域识别符。在其他实施例中,当目标设备1810将密钥链项存放在处理队列1815中时,目标设备1810将识别符与密钥链项分离。如图所示,桶1820具有三个密钥链项1845、1850和1855,桶1820具有一个密钥链项1860,桶1830具有两个密钥链项1865和1870,设备1810已经在没有保护域识别符的情况下存放了这些密钥链项。

[0192] 在一些实施例中,当密钥链项位于处理队列1815中时,密钥链项不可供设备1810使用。密钥链项被图示为虚线椭圆,以指示密钥链项对设备1810的不可用性。

[0193] 在一些实施例中,目标设备1810将密钥链项与公钥的对应私钥的私钥相关联,该公钥作为源设备1805用来对推送给目标设备1810的密钥链项进行签名。目标设备1810将私钥与密钥链项一起存放在处理队列中,因此使私钥不可供设备1810使用。

[0194] 在一些实施例中,目标设备1810通过利用与保护域相关联的其他密钥对私钥进行加密,来使存储在处理队列中的私钥不可用。在这些实施例中,存储在处理队列中的私钥只有在设备满足保护域的条件时才能被用那些其他密钥进行解密。密钥链项然后能被用所解密的私钥进行解密,并由此变得可供设备使用。用于加密私钥的那些其他密钥在本专利申请中被称为本地域保护密钥。

[0195] 当设备1810满足为与特定桶相关联的保护域定义的所有条件时,目标设备1810能通过用本地域保护密钥解密私钥,然后用所解密的私钥解密密钥链,来从该特定桶中取出密钥链项。目标设备1810然后处理所解密的密钥链项。在一些实施例中,设备1810发起同步过程,以将所接收到的密钥链项与设备1810已经具有的密钥链项(未示出)同步。

[0196] 应当指出的是,当目标设备1810在目标设备1810满足密钥链项所属的保护域的条件期间从源设备1805接收到该密钥链项时,目标设备1810不需要对用于保护域的私钥进行加密。目标设备1810因此能用私钥对密钥链项进行解密,而不将密钥链项存放在处理队列1815中。

[0197] 图19概念性地示出了一些实施例为了处理从源设备接收的密钥链项而执行的过程1900。在一些实施例中,源设备在单个事务(例如单个消息)中推送一组密钥链项,而不是每个事务推送一个密钥链项。在一些情况下,一组中的密钥链项以这些密钥链项要被目标设备一起处理的方式相关。在一些实施例中,过程1900由按组接收密钥链项并将一组中的密钥链项一起进行处理的目标设备来执行。具体地,在这些实施例中,目标设备的密钥链管理器可执行过程1900。一些实施例的目标设备将来自源设备的密钥链项组存放在处理队列中。过程1900在一些实施例中在目标设备被启动并已经从源设备接收了一个或多个组的密钥链项时启动。

[0198] 过程1900开始于(在1910处)从处理队列中检索一组密钥链项,处理队列是用于保持从源设备推送的密钥链项组的存储结构(例如文件系统)。在一些实施例中,源设备通过使用目标设备的用于密钥链项所属的保护域的公钥来对存储在处理队列中的组中的每个密钥链项中的数据进行加密。目标设备使用对应的私钥来解密组中的密钥链项。过程1900然后(在1920处)识别所检索的密钥链项组中每个密钥链项的保护域。

[0199] 然后,过程1900(在1930处)确定是否所检索的组的所有所识别的保护域都可用。即,过程1900确定目标设备是否已经满足了每个所识别的保护域的所有条件。一些实施例的过程1900迭代地对所述组的每个所识别的保护域进行确定。

[0200] 当过程1900(在1930处)确定对于任何所识别的保护域没有满足保护域的所有条件时,过程1900(在1940处)通过将这组密钥链项存放回处理队列中来将这组密钥链项返回到处理队列中。过程1900然后前进到下文中将进一步介绍的1960。

[0201] 当过程1900(在1930处)确定每个所识别的保护域的所有条件被满足时,过程1900(在1950处)处理这组密钥链项。在1950处,一些实施例的过程1900通过发起同步过程来处理密钥链项。在一些实施例中,过程1900利用目标设备的用于所识别的保护域的私钥来解密密钥链项。

[0202] 然后,过程1900(在1960处)确定处理队列中是否还有其他密钥链项组要处理。当过程1900确定处理队列中有其他密钥链项组时,过程1900返回到1910,以检索另一组密钥链项。否则,过程1900结束。

[0203] B. 使用案例

[0204] 图20示出了受到保护域保护的密钥链项,该保护域要求该设备要被解锁,以便属于该保护域的密钥链项在设备处可用。具体地,该图以六个不同阶段2001-2006示出了处理被源设备2010更新并被推送给目标设备2015的密钥链项2020。该图还示出了处理作为对应密钥链项要与密钥链项2020同步的密钥链项2025。

[0205] 为了使密钥链项2020和2025在目标设备2015处可用,密钥链项2020和2025所属于的保护域要求目标设备2015被解锁。在本专利申请中,设备被“解锁”可以不是指设备的屏幕被解锁以对屏幕进行任何输入。相反,设备被解锁是指用户已经被认证来使用该设备。不同实施例的设备提供不同的认证机制。例如,一些实施例的设备要求用户提供密码(例如四位数字密码)来解锁设备。另选地或结合地,其他实施例可允许用户用长密码、视网膜扫描、指纹扫描、语音识别等来解锁设备。

[0206] 第一阶段2001示出了分别在源设备2010和目标设备2015中的密钥链项2020和2025保持同步。在这个阶段,目标设备2015处于锁定状态。目标设备2015处于锁定状态,因为设备2015自设备被启动以来还没有被设备2015的用户解锁,或者因为设备2015在经过了一段空闲时间之后自动地从解锁状态进入锁定状态。如图所示,密钥链项2020和2025二者都包括数据1,但目标设备2015处的密钥链项2025被图示为虚线平行四边形,以表明密钥链项2025由于目标设备2015处于锁定状态而不可用。在这个示例中,目标设备2015通过使用用于密钥链项2025所属于的保护域的本地保护域密钥加密密钥链项2025,来使密钥链项2025不可用。

[0207] 第二阶段2002示出了源设备2010处的密钥链项2020已经从数据1更新为数据2。例如,密钥链项2020包括在源设备2010中运行的应用程序要求的用于访问远程服务器的密码,并且源设备2010的用户已经修改了密码。在这个阶段,密钥链项2025在目标设备2025处仍然保持为不可用,因为目标设备2015仍然处于锁定状态。

[0208] 下一阶段2003示出了源设备2010已经将密钥链项2020推送给目标设备2015,以便同步密钥链项2020和目标设备2015的对应密钥链项2025。在这个示例中,源设备2010在将密钥链项2020推送给目标设备2015之前用目标设备2015的用于该保护域的公钥对密钥链项2020进行加密。目标设备2015接收到密钥链项2020,但密钥链项2020在这个阶段不可用,因为目标设备处于锁定状态,并因此还没有用用于该保护域的对应私钥对密钥链项2020进行解密。私钥在这个示例中也已经是不可用的,因为目标设备2015已经用用于加密密钥链项2025的本地保护域密钥对私钥进行了加密。密钥链项2025在目标设备2015处仍然保持为不可用,因为目标设备2015处于锁定状态,并因此还没有用本地保护域密钥对密钥链项2025进行解密。

[0209] 在第四阶段2004,用户已经解锁目标设备2015。因此,密钥链项2020和2025二者都变得可供目标设备2015使用。即,设备2015在这个阶段用本地保护域密钥解密私钥,然后用所解密的私钥解密密钥链项2020。设备2015还用本地保护域密钥解密密钥链项2025。目标设备2015然后发起同步这两个密钥链项2020和2025,因为它们变得可用。

[0210] 第五阶段2005示出了密钥链项2020和2025被同步,并且因此密钥链项2025具有数据2。目标设备2015处于解锁状态,并且密钥链项2025可供目标设备2015使用。下一阶段2006示出了目标设备2015已经返回到锁定状态(例如由于空闲了一段时间或者由于用户已经锁定设备2015)。目标设备2015通过用本地保护域密钥加密密钥链项2025来使密钥链项2025不可用。

[0211] 图21示出了受到保护域保护的密钥链项,该保护域要求该设备在被启动之后被解锁至少一次,以便属于该保护域的密钥链项在设备处可用。具体地,该图以六个不同阶段2101-2106示出了目标设备2115处理密钥链项2120和2125。该图还示出了源设备2110,其更

新密钥链项2120并将其推送给目标设备2115以与密钥链项2125同步。

[0212] 为了使密钥链项2120和2125在目标设备2115处可用,密钥链项2120和2125所属的保护域要求目标设备2115在被启动(即从关闭状态被开启)之后被解锁至少一次。在一些实施例中,该保护域用于保护对于在后台运行的应用程序的密码。例如,运行于设备上的电子邮件应用程序需要密码来访问邮件服务器,以便在设备空闲期间(例如在设备不是正在接收任何用户输入时)获取电子邮件。

[0213] 第一阶段2101显示了分别在源设备2110和目标设备2115中的密钥链项2120和2125保持同步。如图所示,密钥链项2120和2125二者都包括数据1。在这个阶段,目标设备2115自目标设备2115被启动以来还没有被解锁。即,目标设备2115的用户在启动设备2115之后还没有解锁设备2115。目标设备2115处的密钥链项2125被图示为虚线平行四边形,以表明密钥链项2125不可用。在该示例中,目标设备2115已经用用于密钥链项2125所属的保护域的本地保护域密钥对密钥链项2125进行加密,以便使密钥链项2125不可用。

[0214] 第二阶段2102示出了源设备2110处的密钥链项2120已经从数据1更新为数据2。在这个阶段,目标设备2115处的密钥链项2125仍然保持为不可用,因为目标设备2115自被启动以来仍然还没有被解锁。

[0215] 下一阶段2103示出了源设备2110已经将密钥链项2120推送给目标设备2115,以便同步密钥链项2120和目标设备2115的对应密钥链项2125。在这个示例中,源设备2110在将密钥链项2120推送给目标设备2115之前用目标设备2115的用于该保护域的公钥来加密密钥链项2120。目标设备2115接收到密钥链项2120,但密钥链项2120在这个阶段不可用,因为目标设备2115自被启动以来还没有被解锁,并因此还没有用用于该保护域的对应私钥来解密密钥链项2120。所述私钥在这个示例中也已经是不可用的,因为目标设备2115已经用用于加密密钥链项2125的本地保护域密钥对私钥进行加密。密钥链项2125在目标设备2115处仍然保持为不可用,因为目标设备2115处于锁定状态,并因此还没有用本地保护域密钥解密密钥链项2125。

[0216] 在第四阶段2104,用户在设备2115已经被启动之后已经第一次解锁了目标设备2115。因此,密钥链项2120和2125二者可供目标设备2115使用。在这个示例中,目标设备2115通过用用于该保护域的私钥解密密钥链项2120来使密钥链项2120可用。目标设备2115已经用用于该保护域的本地保护域密钥解密了私钥以及密钥链项2125。目标设备2115发起同步这两个密钥链项2120和2125,因为它们变得可用。

[0217] 第五阶段2105示出了密钥链项2120和2125被同步,并且因此密钥链项2125具有数据2。目标设备2115处于解锁状态,并且密钥链项2125可供目标设备2115使用。在这个阶段,源设备2110的用户又将密钥链项2120从数据2更新为数据3。

[0218] 第六阶段2106示出了目标设备2115已经返回到锁定状态(例如因为空闲了一段时间或因为用户已经锁定了目标设备2115)。然而,密钥链项2125仍然可供设备2115使用,因为设备2115在设备2115被启动之后已经被解锁了一次,并且因此设备2115没有再次用本地保护域密钥加密密钥链项2125。

[0219] 在这个阶段2106,源设备2110还已经将密钥链项2120推送给目标设备2115,以便同步密钥链项2120和目标设备2115的对应密钥链项2125。源设备2110在将密钥链项2120推送给目标设备2115之前使用用于该保护域的公钥来加密密钥链项2120。目标设备2115接收

到密钥链项2120,并且即使目标设备2115处于锁定状态,密钥链项2120也变得可用。这是因为目标设备2115在设备2115被启动以后已经被解锁了至少一次,并且因此设备2115没有对私钥进行加密,私钥于是可用于解密密钥链项2120。即使目标设备2115保持在锁定状态中,密钥链项2120也将被同步。

[0220] 图22示出了受到保护域保护的密钥链项,该保护域要求该设备被开启,以便属于该保护域的密钥链项在设备处可用。具体地,该图以四个不同阶段2201-2204示出了目标设备2215处理密钥链项2220和2225。该图还示出了源设备2210,其更新密钥链项2220并将其推送给目标设备2215以与密钥链项2225同步。

[0221] 密钥链项2220和2225所属的保护域要求目标设备2215处于开启状态,以便使密钥链项2220和2225可供设备2215使用。即,只要目标设备2215已启动并在运行,密钥链项2220和2225就始终可供设备2215使用。因为这个保护域提供很小的保护,所以一些实施例的设备将该保护域用于需要始终运行的那些应用程序。此类应用程序的一个示例包括苹果公司(Apple, Inc.)的Find My iPhone™应用程序。

[0222] 第一阶段2201示出了分别在源设备2210和目标设备2215中的密钥链项2220和2225保持同步。如图所示,密钥链项2220和2225二者包括数据1。在这个阶段,目标设备2215被关闭。

[0223] 第二阶段2202示出了源设备2210处的密钥链项2220已经从数据1更新为数据2。在这个阶段,目标设备2215被启动,但还没有被解锁。然而,密钥链项2225可供目标设备2215使用,因为保护域的条件(即设备已启动并且正在运行)已经被满足,并因此设备2215没有用于该保护域的本地保护域密钥来加密密钥链项2225。在一些实施例中,密钥链项2225可仍然用与设备2215关联的密钥(例如由设备2215的UID导出的密钥)来加密,但密钥链项2225被认为是可用的,因为该密钥可用于在设备2215处解密密钥链项2225。

[0224] 下一阶段2203示出了源设备2210已经将密钥链项2220推送给目标设备2215,以便同步密钥链项2220和目标设备2215的对应密钥链项2225。源设备2210在将密钥链项2220推送给目标设备2215之前加密密钥链项2220。目标设备2215接收到密钥链项2220,并且密钥链项2220在该阶段变为在设备2215处是可用的,即使设备2215还没有被解锁。这是因为设备2215已启动并正在运行,并且因此对应的私钥可用于解密密钥链项2220。目标设备2215发起同步这两个密钥链项2220和2225,因为密钥链项2220和2225是可用的。

[0225] 在第四阶段2204,目标设备2215还没有被解锁。但是,第四阶段2204示出了密钥链项2220和2225被同步。因此,密钥链项2225现在具有数据2。

[0226] 图23示出了受到保护域保护的密钥链项,该保护域要求该设备被解锁并且还要求附加的认证,以便属于该保护域的密钥链项在设备处可用。具体地,该图以六个不同阶段2301-2306示出了处理被源设备2310更新并被推送给目标设备2315的密钥链项2320。该图还示出了处理密钥链项2325,该密钥链项2325是要与密钥链项2320同步的对应密钥链项。

[0227] 为了使密钥链项2320和2325在目标设备2315处可用,密钥链项2320和2325所属的保护域要求目标设备2315被解锁并且还要求附加的认证(例如密码、视网膜扫描、指纹扫描、语音识别、设备位于特定位置附近等)。在一些实施例中,该保护域用于保护对于需要附加安全措施的应用程序的密码。例如,一些实施例的密钥链管理器为应用程序生成安全随机密码,以访问远程服务器。在一些实施例中,该密码不被暴露给用户,并且密钥链管理器

用用户能记住和使用的更简单的或不同的密码来对用户进行认证。未暴露的密码在用户使用的设备之间同步。当未暴露的密码在源设备处被修改并且被推送给目标设备时,除非用户提供所述不同的密码来使用在目标设备处运行的同一应用程序,否则即使用户解锁了目标设备,未暴露的密码在目标设备处也不会变得可用。

[0228] 第一阶段2301示出了分别在源设备2310和目标设备2315中的密钥链项2320和2325保持同步。在这个阶段,目标设备2315处于锁定状态。如图所示,密钥链项2320和2325二者都包括数据1,但目标设备2315处的密钥链项2325是不可用的,因为目标设备2315处于锁定状态。在这个示例中,目标设备2315已经用用于密钥链项2325属于的保护域的本地保护域密钥对密钥链项2325进行了加密,以便使密钥链项2325不可用。

[0229] 第二阶段2302示出了源设备2310处的密钥链项2320已经被用户从数据1更新为数据2。例如,密钥链项2320包括实际上用于访问运行于源设备2310中的应用程序要求的远程服务器的未暴露密码,并且用户刚刚已经通过修改不同的密码而修改了未暴露密码,所述不同的密码由用户记住并使用来认证以使用应用程序。在这个阶段,密钥链项2325仍然保持为不可用,因为目标设备2315仍然处于锁定状态,并且因此还没有满足保护域的条件。

[0230] 第三阶段2303示出了源设备2310已经将密钥链项2320推送给目标设备2315,以便同步密钥链项2320和目标设备2315的对应密钥链项2325。在这个示例中,源设备2310在将密钥链项2320推送给目标设备2315之前用目标设备2315的用于该保护域的公钥来加密密钥链项2320。目标设备2315接收到密钥链项2320,但密钥链项2320在这个阶段不可用,因为目标设备处于锁定状态,并因此还没有用于该保护域的对应私钥解密密钥链项2320。密钥链项2325还保持为不可用,因为目标设备2315处于锁定状态。

[0231] 在第四阶段2304,用户已经解锁了目标设备2315。但是,密钥链项2320和2325二者都仍然不可供目标设备2315使用,因为还没有满足密钥链项2320和2325属于的保护域的条件-用户还没有提供这个保护域所要求的附加认证。

[0232] 第五阶段2305示出了用户已经提供了附加认证(例如键入用户记住的所述不同的密码)。密钥链项2320和2325二者现在已经变得可用了。这是因为已经满足了该保护域的所有条件,并且因此设备2315已经用本地保护域解密了私钥和密钥链项2325。设备2315已经用所解密的私钥解密了密钥链项2325。目标设备2315发起同步这两个密钥链项2320和2325。第六阶段2306示出了密钥链项2320和2325被同步,并且因此密钥链项2325具有数据2。

[0233] 图24示出了由具有用于设备的不同条件组的两个保护域保护的数据。具体地,该图以四个不同阶段2401-2404示出了目标设备2415处理元数据项2430和2435以及密钥链项2420和2425。该图还示出了源设备2410,其更新密钥链项2420并将其推送给目标设备2415以与密钥链项2425同步。

[0234] 如上所述,密钥链项与元数据项相关联,元数据项携带设备的信息,以用于解决在同步两个密钥链项时的任何冲突。在一些实施例中,密钥链项及其相关联的元数据项被定义为处于不同保护域中,从而元数据项在设备处变得可用,而密钥链项仍然保持为不可用。当在设备处,密钥链项不可用并且相关联的元数据项可用时,设备能利用相关联的元数据项携带的信息来解决密钥链项的任何冲突。

[0235] 元数据项2430和2435分别与密钥链项2420和2425相关联。在这个示例中,元数据

项2430和2435属于第一保护域,第一保护域要求目标设备2415被开启,以便元数据项2430和2435可供设备2415使用。密钥链项2420和2425属于第二保护域,第二保护域要求目标设备2415处于解锁状态,以便密钥链项在目标设备2415处可用。

[0236] 第一阶段2401示出了分别在源设备2410和目标设备2415中的密钥链项2420和2425不同步。如图所示,密钥链项2420和2425分别包括数据1和数据2。元数据项2430和2435具有不同信息。元数据项2430携带元数据1,而元数据项2435携带元数据2,如图所示。在这个阶段,目标设备2415处于锁定状态。目标设备2415处的密钥链项2425被图示为虚线平行四边形,以表明密钥链项2425在设备2415处不可用。在这个示例中,设备2425已经通过用于第二保护域的本地保护域密钥加密密钥链项2425而使密钥链项2425不可用。元数据项2435在设备2415处可用,因为当设备2425处于开启状态时,设备2425不加密元数据2435。

[0237] 第二阶段2402示出了源设备2410已经将密钥链项2420与相关联的元数据项2430一起推送给目标设备2415,以便同步密钥链项2420和目标设备2415的对应密钥链项2425。在这个示例中,源设备2410用目标设备2415的用于第一保护域的公钥来加密元数据项2430。源设备2410还在将元数据项2430和密钥链项2420发送给目标设备2415之前用目标设备2415的用于第二保护域的公钥来加密密钥链项2420。

[0238] 目标设备2415接收到密钥链项2420和元数据项2435,但密钥链项2420在这个阶段2402在目标设备2415处不可用。这是因为目标设备2415仍然处于锁定状态,并且因此设备2415没有用于第二保护域的私钥来解密密钥链项2425。密钥链项2425仍然保持为不可用,因为设备2415仍然处于锁定状态。元数据项2435在这个阶段2402在目标设备2415处是可用的,因为设备2415已启动并且正在运行。设备2415通过利用元数据项2430和2435解决密钥链项2420和2425之间的冲突,来发起同步这两个经加密的密钥链项2420和2425。

[0239] 在第三阶段2403,目标设备2415仍然处于锁定状态。然而,目标设备2415已经同步了密钥链项。因此,元数据项已经被更新有新的冲突解决信息(元数据3),并且密钥链项2425具有数据1。经更新的密钥链项2425通过仍然保持为被用于第二域的公钥加密而在目标设备2415处仍然不是可用的,这是因为设备2415仍然处于锁定状态。在第四阶段2404,目标设备2415处于解锁状态。在这个示例中,设备通过用于第二域的本地保护域密钥解密用于第二保护域的私钥,然后用所解密的私钥解密密钥链项2425,来使密钥链项2425可用。

[0240] C. 同步圈和保护域

[0241] 如上所述,设备可加入多个不同的同步圈,以同步不同的密钥链项(例如利用上文中参考图4-6所述的技术)。在一些实施例中,多个设备形成多个不同的同步圈,以便同步属于多个不同保护域的密钥链项。

[0242] 图25概念性地示出了由多个设备形成的多个同步圈。具体地,该图示出了三个设备A-C形成用于三个不同保护域1-3的三个不同的同步圈2505-2515。图的上部示出了三个同步圈2505-2515中的设备A-C。图的下部分开地示出了三个同步圈2505-2515。

[0243] 在一些实施例中,一组设备形成用于设备用来保护密钥链项的每个保护域的同步圈。在一些实施例中,这组中的每个设备使用相同的公钥/私钥对来加入同步圈,设备使用该公钥/私钥对来加密和解密密钥链项。另选地或结合地,其他实施例的设备使用分开的密钥对用于加入同步圈以及加密和解密密钥链项。

[0244] 如图所示,设备A-C形成用于保护域1的同步圈2505。设备A-C形成用于保护域2的

同步圈2510。设备A-C形成用于保护域3的同步圈2515。图25示出了三个同步圈由相同的三个设备A-C形成。但是,设备A-C中每一者可与除了设备A-C中另两个设备之外的设备形成其他同步圈(未示出),用于除了保护域1-3之外的保护域(未示出)。

[0245] 虽然同步圈2505-2515在该图中被图示为环形或圆形的形状,但每对设备建立安全传输层,以形成同步圈。即,同步圈中的设备在一些实施例中形成星型网络,而不是环形网络。

[0246] 图26概念性地示出了多个设备形成的用于多个不同保护域的同步圈。具体地,该图示出了三个设备A-C形成用于三个不同保护域1-3的同步圈2605。该图还示出了三组密钥链项2610-2620。

[0247] 在一些实施例中,一组设备形成单个同步圈用于多个不同保护域。在这些实施例的一些实施例中,该组的每个设备使用用于所述多个不同保护域的多个公钥/私钥对中的一对来加入所述单个同步圈。即,该组的每个设备选择用于加密和解密密钥链项的所述多个公钥/私钥对中的一对,并使用所选择的密钥对来加入所述单个同步圈。另选地或结合地,该组的每个设备在其他实施例中不是使用用于加密和解密密钥链项的密钥对中的任一对,而是使用单独的密钥对来加入所述单个同步圈。

[0248] 在一些实施例中,该组的每个设备使用所有用于所述多个不同保护域的所述多个公钥/私钥对来加入所述单个同步圈。即,在这些实施例中,该组的每个设备使用所有用于加密和解密密钥链项的密钥对来加入同步圈。因此,在这些实施例中,为了加入同步圈,设备需要满足所述多个不同保护域中每一者的所有条件,因为设备需要使所有这些密钥对可用。

[0249] 在该示例中,密钥链项2610属于保护域1。密钥链项2610正被设备C推送给设备A。设备C使用设备A的已经被发布给设备B和C的用于保护域1的公钥来加密密钥链项2610。但是,设备C在这个示例中已经使用用于保护域1-3的所有三个公钥/私钥对来加入同步圈2605。

[0250] 密钥链项2620属于保护域2。密钥链项2620正被设备B推送给设备C。设备B使用设备C的已经被发布给设备A和B的用于保护域2的公钥来加密密钥链项2620。在该示例中,设备B已经使用用于保护域1-3的所有三个公钥/私钥对来加入同步圈2605。

[0251] 密钥链项2615属于保护域3。密钥链项2615正被设备A推送给设备B。设备A使用设备B的已经被发布给设备A和C的用于保护域3的公钥来加密密钥链项2615。在该示例中,设备B已经使用用于保护域1-3的所有三个公钥/私钥对来加入同步圈2605。

[0252] V. 软件架构

[0253] 在一些实施例中,上文所述的过程被实现为运行于特定机器上或者存储在机器可读介质中的软件,特定机器诸如是计算机(例如台式计算机、膝上型计算机等)、手持设备(例如智能电话)、或平板计算设备。图27概念性地示出了一些实施例的密钥链管理器2700的软件架构。在一些实施例中,密钥链管理器是用于管理同步圈中设备之间密钥链同步的独立应用程序。一些实施例的密钥链管理器被集成到另一应用程序(例如密钥链管理应用程序、数据管理应用程序、安全应用程序等)中,而在其他实施例中,该应用程序可实现在操作系统内。此外,在一些实施例中,该应用程序被提供为基于服务器的解决方案的部分。在一些此类实施例中,经由瘦客户端来提供该应用程序。也就是说,该应用程序在服务器上运

行,而用户经由远离服务器的单独的机器来与该应用程序交互。在其他此类实施例中,该应用程序作为胖客户端来提供。也就是说,该应用程序从服务器分配到客户端机器并且在客户端机器上运行。

[0254] 一些实施例的密钥链管理器2700被实现为工作于不同操作系统上。在一些实施例中,不同操作系统(例如iOS[®]、Mac OS X[®]等)使用不同的架构来管理密钥链和密钥链项。一些实施例的密钥链管理器2700被实现为在使用不同密钥链管理架构的设备之间来同步密钥链和密钥链项。例如,在一些实施例中,密钥链管理器2700被实现用于特定密钥链管理架构(例如iOS[®]),并被移植以与另一密钥链管理架构(例如Mac OS X[®])工作。

[0255] 如图所示,密钥链管理器2700包括同步管理器2705、注册管理器2710、密钥链项管理器2715、加密模块2720、清单模块2725、和冲突解决器2730。密钥链管理器2700还包括同步圈数据存储装置2735、设备清单存储装置2740、冲突规则存储装置2745、密钥链存储装置2750和安全数据存储装置2755。在一些实施例中,同步圈数据2735存储上文中参考图3所述的存储装置310-330中所存储的数据的本地副本。即,同步圈数据存储装置2735存储同步圈名称、同步圈设备列表、用户签名、设备签名、和密钥链数据、以及其他数据。设备清单存储装置2740存储同步圈中每个设备的清单历史。冲突规则存储装置2745存储冲突解决程序的先前版本、用于解决密钥链项冲突的冲突解决程序的当前版本、以及与冲突解决程序的先前版本和当前版本相关联的各种规则。密钥链存储装置2750存储用于与同步圈中的设备同步的密钥链。在一些实施例中,密钥链存储装置2750还存储不与同步圈中的其他设备共享(即同步)的密钥链和/或密钥链项。安全数据存储装置2755存储与安全特征(例如安全通信信道(例如安全密钥)、数据加密(例如加密密钥)、数据解密(例如解密密钥)、数据认证(例如解密密钥)等)相关的数据,这些是密钥链管理器2700为了促进密钥链同步而提供的。在一些实施例中,存储装置2735-2755被存储在一个物理存储装置中,而在其他实施例中,存储装置2735-2755被存储在独立的物理存储装置中。此外,在一些实施例中,存储装置2735-2755中的一些或全部被实现在多个物理存储装置上。

[0256] 同步管理器2705负责管理同步圈中设备之间的密钥链同步。在一些实施例中,同步管理器2705在密钥链管理器2700工作的设备已经成功地注册到同步圈中之后由注册管理器2710启动。在一些实施例中,同步管理器2705处理上文中在章节IV中所述的数据保护特征。同步管理器与其他模块2710和2715-2730通信,以便实现同步圈中设备之间的密钥链同步。

[0257] 注册管理器2710处理与将设备注册到同步圈中相关的各种功能。例如,当密钥链管理器在其上运行的设备想要加入同步圈时,注册管理器2710在不存在同步圈时就创建一个同步圈。注册管理器2710还处理注册请求生成(例如通过执行上文中参考图5所述的过程500)、注册请求批准(例如通过执行上文中参考图6所述的过程600)、注册批准确认等。

[0258] 密钥链项管理器2715生成并管理密钥链的密钥链项。在一些实施例中,密钥链项管理器2715生成并保持代表密钥链中一些或全部密钥链项的数据结构(例如上文中参考图10所述的数据结构)。

[0259] 安全模块2720提供各种安全特征的功能性。例如,安全模块2720处理与同步圈中每个设备建立安全通信信道。安全模块2720执行不同的密码原语、算法、协议、和技术(例如OTR消息传送、迪菲-赫尔曼密钥交换、公钥/私钥对生成等),以便实现各种安全特征。

[0260] 清单模块2725负责基于本地密钥链项,并且在一些实施例中还基于对等设备的清单,生成不同类型的清单。例如,清单模块2725生成清单摘要、完整清单和增量清单。为了有利于清单生成,清单模块2725保持同步圈中每个设备的清单历史。清单模块2725在生成增量清单时还执行本地密钥链项(或本地清单)与对等设备的清单之间的比较。

[0261] 冲突解决器2730处理密钥链项之间冲突的解决。例如,冲突解决器2730对本地密钥链项和对等设备的密钥链项进行比较,以识别冲突。冲突解决器还执行冲突解决程序(例如存储在冲突规则存储装置2745中的),以便解决密钥链项冲突。另外,冲突解决器2730负责检测冲突解决程序之间的冲突并确定用于解决密钥链项冲突的冲突解决程序。

[0262] 虽然很多特征已经被描述为是由一个模块(例如注册模块2710、安全模块2720等)执行的,但本领域普通技术人员将认识到,这些功能可被分成多个模块。类似地,被描述为由多个不同模块执行的功能在一些实施例中可由单个模块来执行(例如密钥链项管理器2715和冲突解决器2730)。

[0263] VI. 电子系统

[0264] 上文所述的特征和应用程序中的许多可被实现为被指定为在计算机可读存储介质(还称为计算机可读介质)上记录的指令集的软件过程。在这些指令由一个或多个计算或处理单元(例如,一个或多个处理器、处理器的内核或者其他处理单元)执行时,这些指令使得一个或多个处理单元能够执行指令中所指示的动作。计算机可读介质的实例包括但不限于CD-ROM、闪存驱动器、随机存取存储器(RAM)芯片、硬盘驱动器、可擦可编程只读存储器(EPROM)、电可擦可编程只读存储器(EEPROM)等。计算机可读介质不包括无线地传送或通过有线连接的载波和电信号。

[0265] 在本说明书中,术语“软件”旨在包括能被处理器读取到存储器中进行处理的驻留在只读存储器中的固件或存储在磁存储装置中的应用程序。另外,在一些实施例中,可在保留不同的软件发明的同时,将多个软件发明实现为更大程序的子部分。在一些实施例中,还可将多个软件发明实现为单独程序。最后,共同实施这里所述的软件发明的单独程序的任何组合均在本发明的范围之内。在一些实施例中,当被安装以在一个或多个电子系统上运行时,软件程序定义执行和施行软件程序的操作的一个或多个特定机器具体实施。

[0266] 图28概念性地示出了电子系统2800,本发明的一些实施例借助该电子系统来实施。电子系统2800可为计算机(例如,台式计算机、个人计算机、平板电脑等)、电话、PDA或任何其他种类的电子或计算设备。此类电子系统包括各种类型的计算机可读介质以及用于各种其他类型的计算机可读介质的接口。电子系统2800包括总线2805、处理单元2810、图形处理单元(GPU) 2820、系统存储器2825、网络2815、只读存储器2830、永久性存储设备2835、输入设备2840和输出设备2845。

[0267] 总线2805总体表示可通信地连接电子系统2800的许多内部设备的所有系统、外围设备和芯片组总线。例如,总线2805可通信地将处理单元2810与只读存储器2830、GPU 2820、系统存储器2825和永久性存储设备2835连接。

[0268] 处理单元2810从这些各种存储器单元检索要执行的指令和要处理的数据,以便执行本发明的过程。在不同实施例中,一个或多个处理单元可以为单个处理器或者多核处理器。一些指令被传送至GPU 2815并且由GPU 2820执行。GPU 2820可卸载各种计算指令,或补充由处理单元2810提供的图像处理。在一些实施例中,可使用CoreImage的内核着色语言来

提供此类功能。

[0269] 只读存储器 (ROM) 2830 存储处理单元 2810 和电子系统的其他模块所需的静态数据和指令。另一方面,永久性存储设备 2835 是读写存储器设备。此设备是即使在电子系统 2800 关闭时也存储指令和数据的非易失性存储器单元。本发明的一些实施例将海量存储设备 (诸如磁盘或光盘及其对应盘驱动器) 用作永久性存储设备 2835。

[0270] 其他实施例将可移动的存储设备 (诸如软盘、闪存存储器设备等,及其对应的驱动器) 用作永久性存储设备。与永久性存储设备 2835 一样,系统存储器 2825 是读写存储器设备。但是,与存储设备 2835 不同的是,系统存储器 2825 是易失性读写存储器,诸如随机存取存储器。系统存储器 2825 存储处理器在运行时所需的指令和数据中的一些。在一些实施例中,本发明的过程存储在系统存储器 2825、永久性存储设备 2835 和/或只读存储器 2830 中。例如,各种存储器单元包括用于根据一些实施例处理多媒体片段的指令。处理单元 2810 从这些各种存储器单元检索要执行的指令和要处理的数据,以便执行一些实施例的过程。

[0271] 总线 2805 还连接至输入设备 2840 和输出设备 2845。输入设备 2840 使得用户能够将信息传达至电子系统以及选择对电子系统的命令。输入设备 2840 包括字母数字键盘和指向设备 (也被称作“光标控制设备”)、照相机 (例如,网络摄像机)、麦克风或用于接收语音命令的类似设备等。输出设备 2845 显示由电子系统生成的图像或以其他方式输出数据。输出设备 2845 包括打印机和显示设备 (诸如阴极射线管 (CRT) 或液晶显示器 (LCD))、以及扬声器或类似的音频输出设备。一些实施例包括充当输入设备和输出设备两者的设备,诸如触摸屏。

[0272] 最后,如图 28 中所示,总线 2805 还通过网络适配器 (未示出) 将电子系统 2800 耦接至网络 2815。这样,计算机可以是计算机的网络 (诸如局域网 (“LAN”)、广域网 (“WAN”) 或内联网) 的一部分,或者可以是网络的网络 (诸如互联网) 的一部分。电子系统 2800 的任何或所有部件均可与本发明结合使用。

[0273] 一些实施例包括将计算机程序指令存储在机器可读或计算机可读介质 (或者称为计算机可读存储介质、机器可读介质或机器可读存储介质) 中的电子部件,例如微处理器、存储装置以及存储器。此类计算机可读介质的一些示例包括 RAM、ROM、只读光盘 (CD-ROM)、可刻录光盘 (CD-R)、可重写光盘 (CD-RW)、只读数字通用光盘 (例如, DVD-ROM、双层 DVD-ROM)、各种可刻录/可重写 DVD (例如, DVD-RAM、DVD-RW、DVD+RW 等)、闪存存储器 (例如, SD 卡, mini-SD 卡、micro-SD 卡等)、磁性和/或固态硬盘驱动器、只读和可刻录 Blu-Ray[®] 盘、超密度光盘、任何其他光学或磁性介质以及软盘。计算机可读介质可存储计算机程序,该计算机程序可由至少一个处理单元来执行并且包括用于执行各种操作的指令集。计算机程序或者计算机代码的实例包括机器代码,例如由编译器所产生的机器代码,以及包括可由计算机、电子部件或微处理器使用解译器来执行的更高级别代码的文件。

[0274] 虽然上述讨论主要涉及执行软件的微处理器或多核处理器,但一些实施例由一个或多个集成电路来执行,该一个或多个集成电路例如专用集成电路 (ASIC) 或现场可编程门阵列 (FPGA)。在一些实施例中,此类集成电路执行存储在电路自身上的指令。此外,一些实施例执行存储在可编程逻辑设备 (PLD)、ROM 或 RAM 设备中的软件。

[0275] 如在本专利申请的本说明书以及任何权利要求中所使用的,术语“计算机”、“服务器”、“处理器”及“存储器”均是指电子或其他技术设备。这些术语不包括人或者人的群组。出于本说明书的目的,术语显示或正在显示意指在电子设备上显示。如在本专利申请的本

说明书以及任何权利要求中所使用的,术语“计算机可读介质”以及“机器可读介质”完全限于以可由计算机读取的形式存储信息的可触摸的物理对象。这些术语不包括任何无线信号、有线下载信号以及任何其他短暂信号。

[0276] 虽然已参考许多特定细节描述了本发明,但本领域的普通技术人员将认识到,可在不脱离本发明的实质的情况下以其他特定形式来体现本发明。此外,多个附图(包括图5、6、和12-15)概念性地示出了过程。这些过程的特定操作可不以所示出和描述的确切顺序被执行。可不在操作的一个连续系列中执行该特定操作,并且可在不同实施例中执行不同的特定操作。此外,该过程可使用若干子过程来实施,或者作为更大宏过程而实施。因此,本领域的普通技术人员将理解,本发明不受前述示例性细节限制,而是将由所附的权利要求所限定。

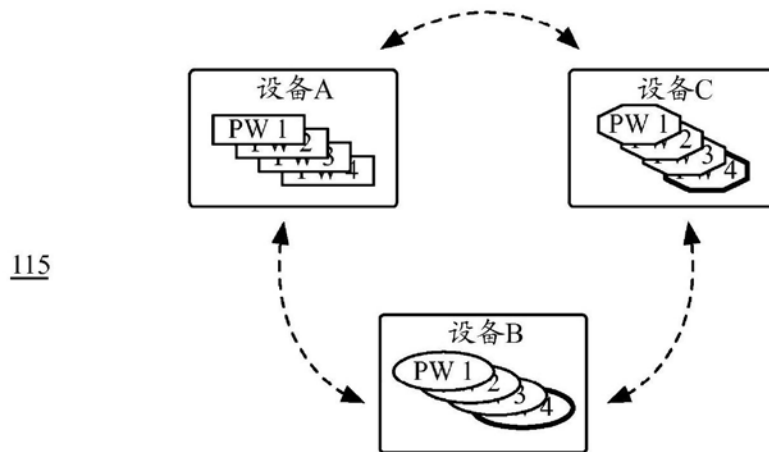
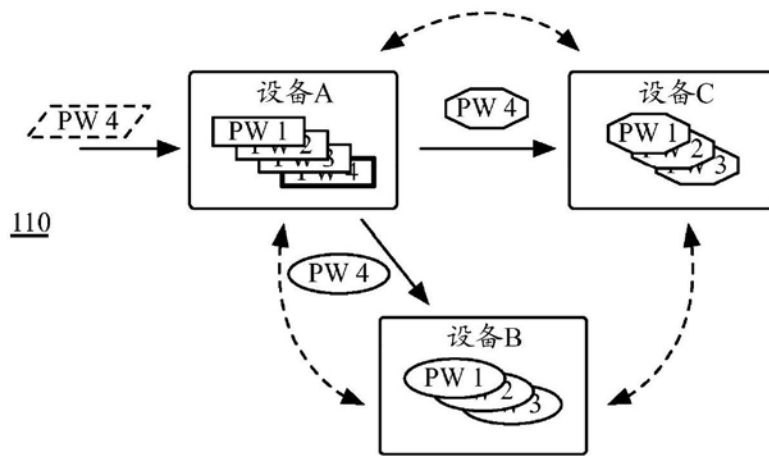
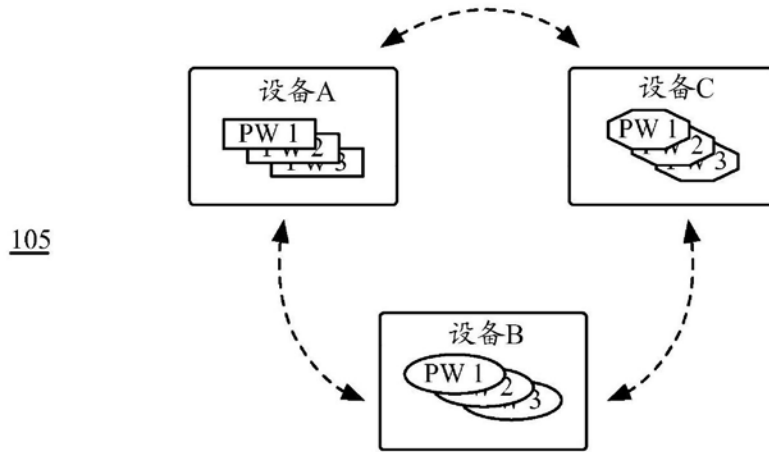


图1

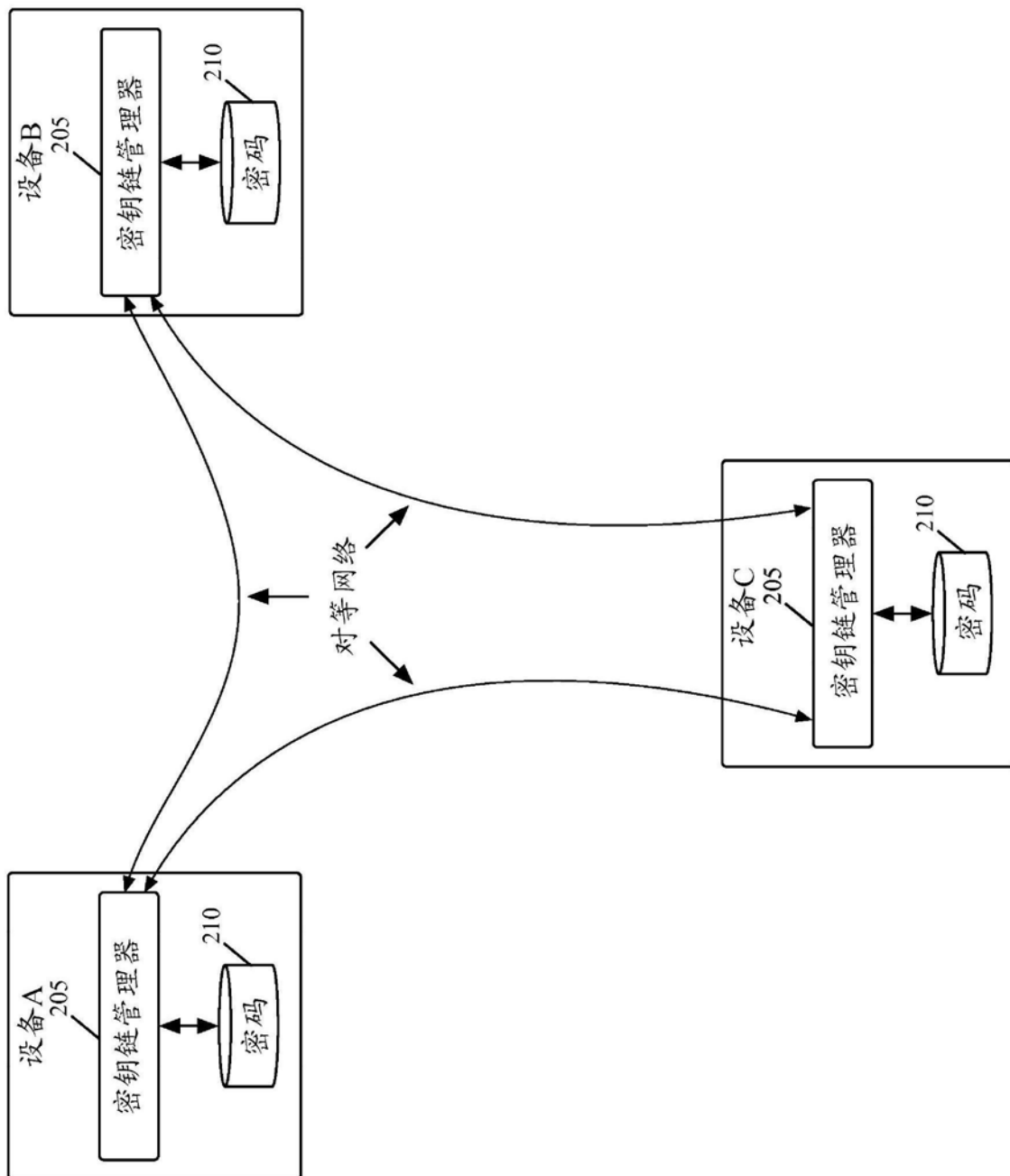


图2

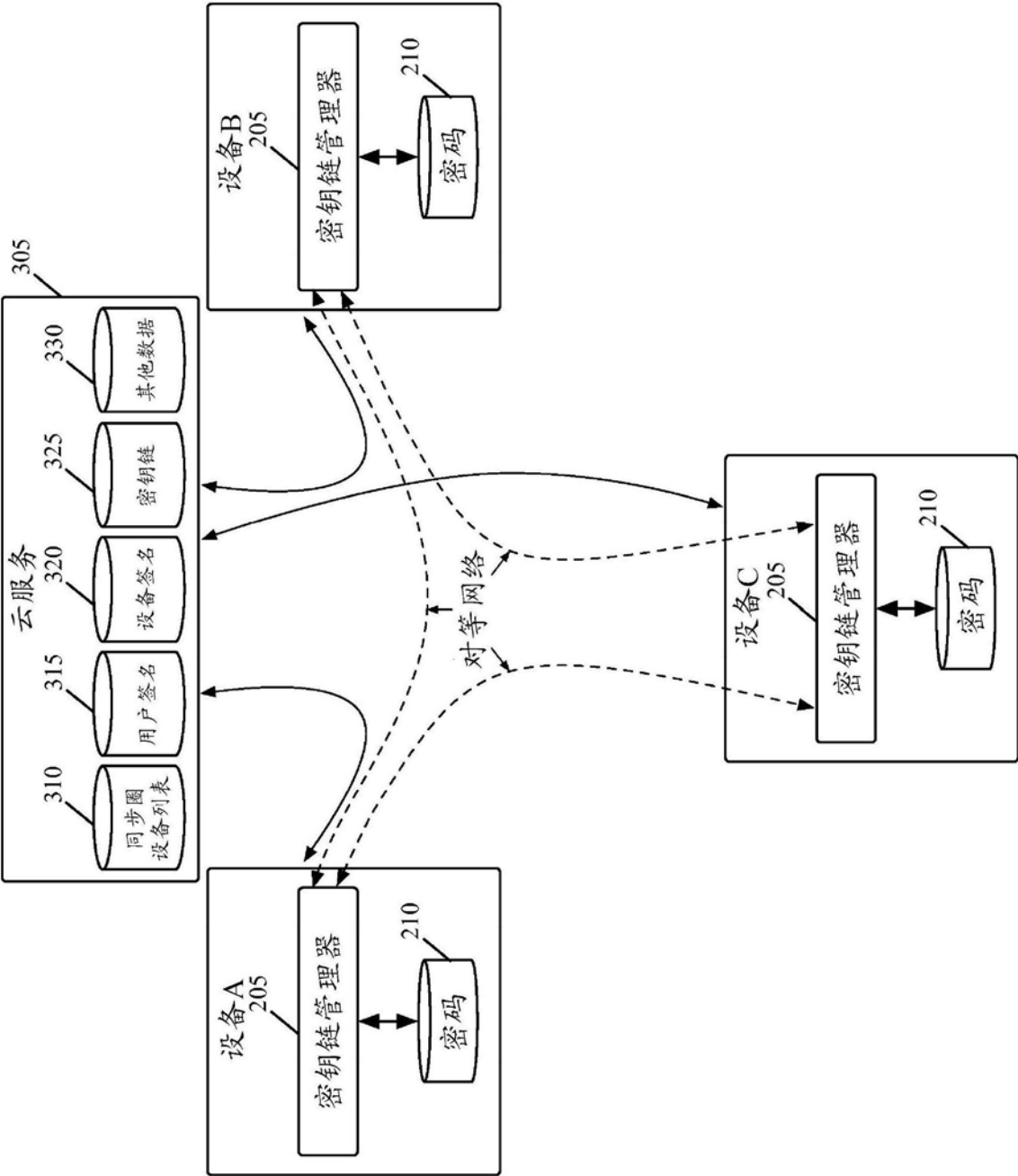


图3

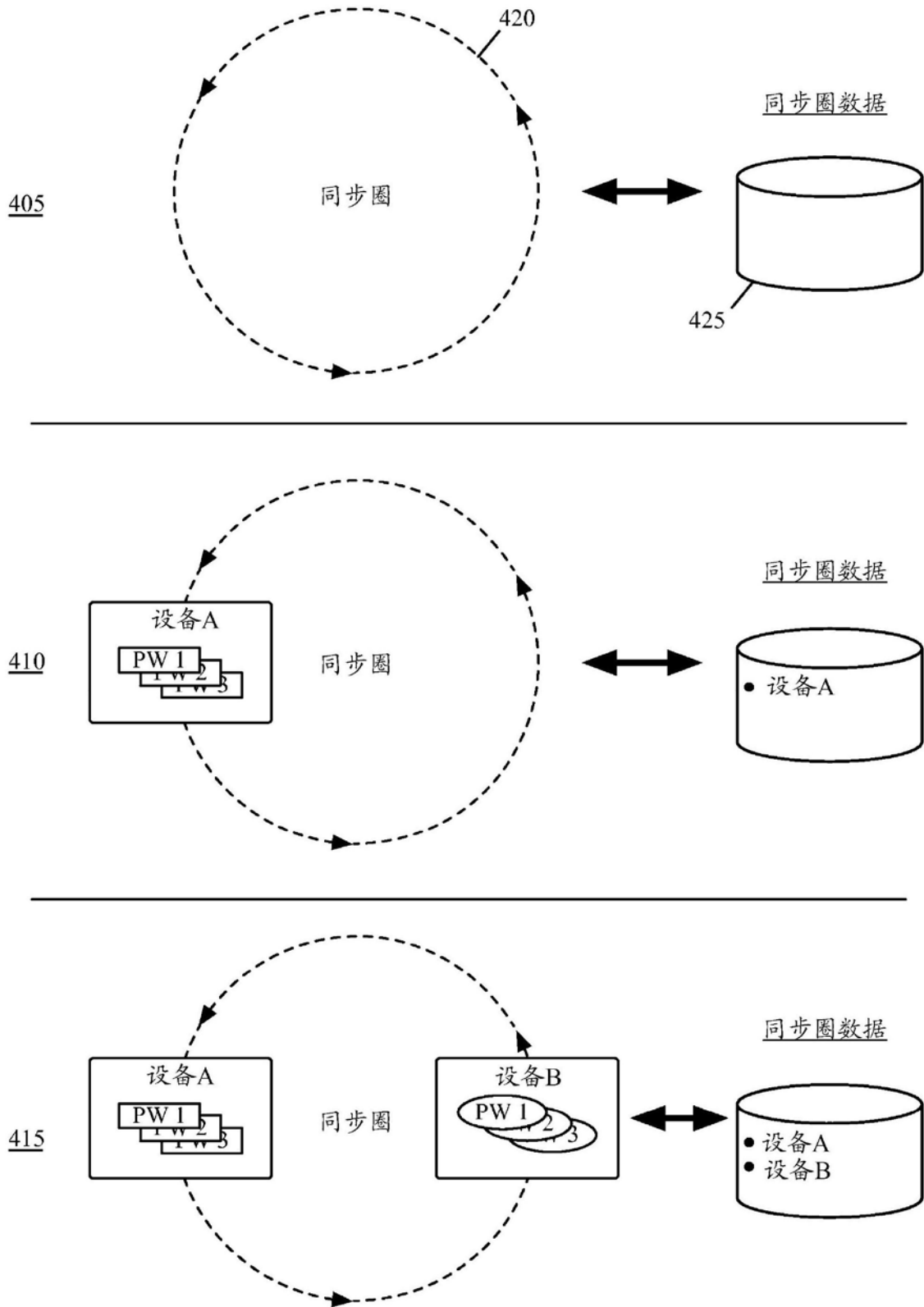


图4

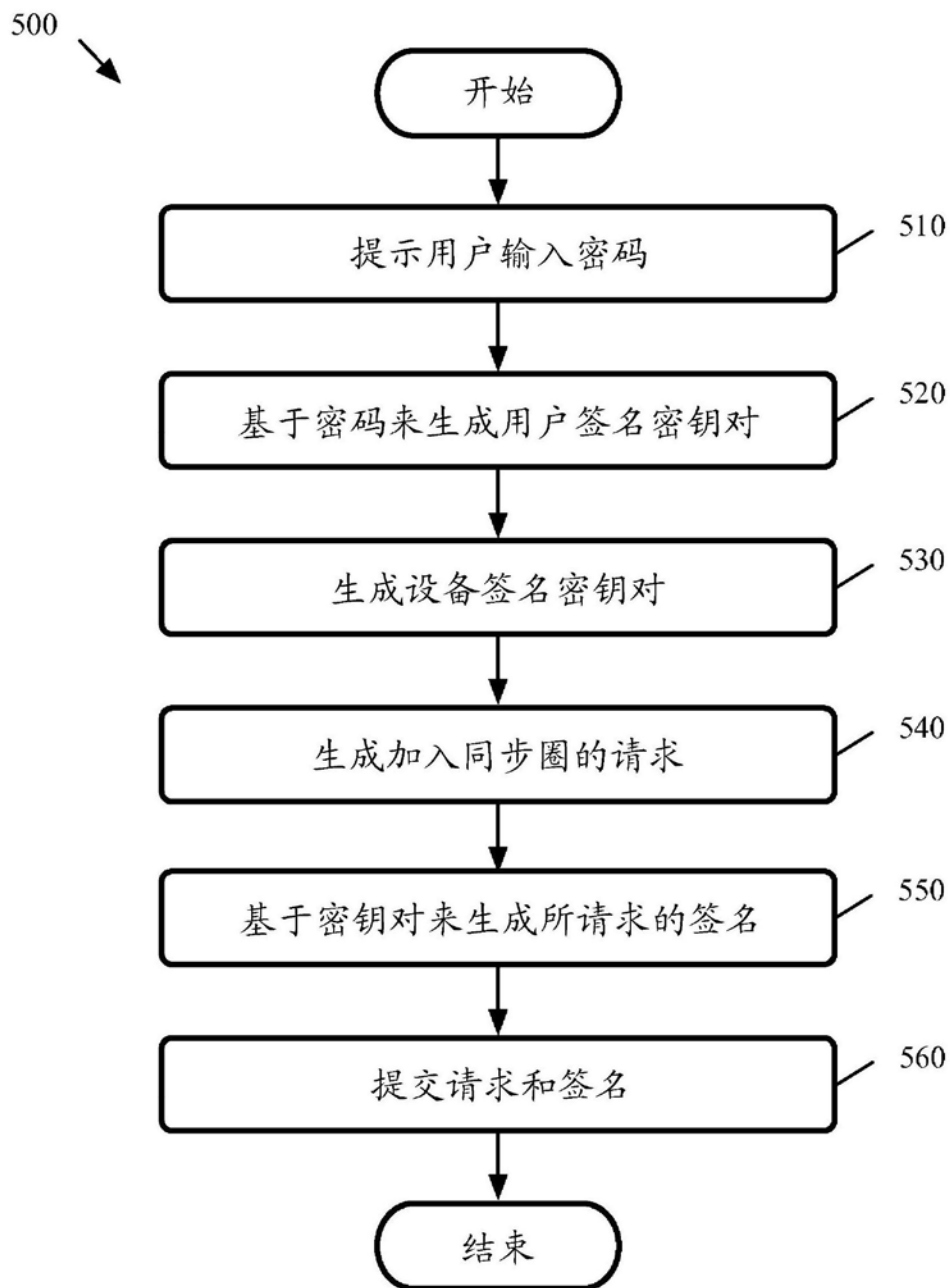


图5

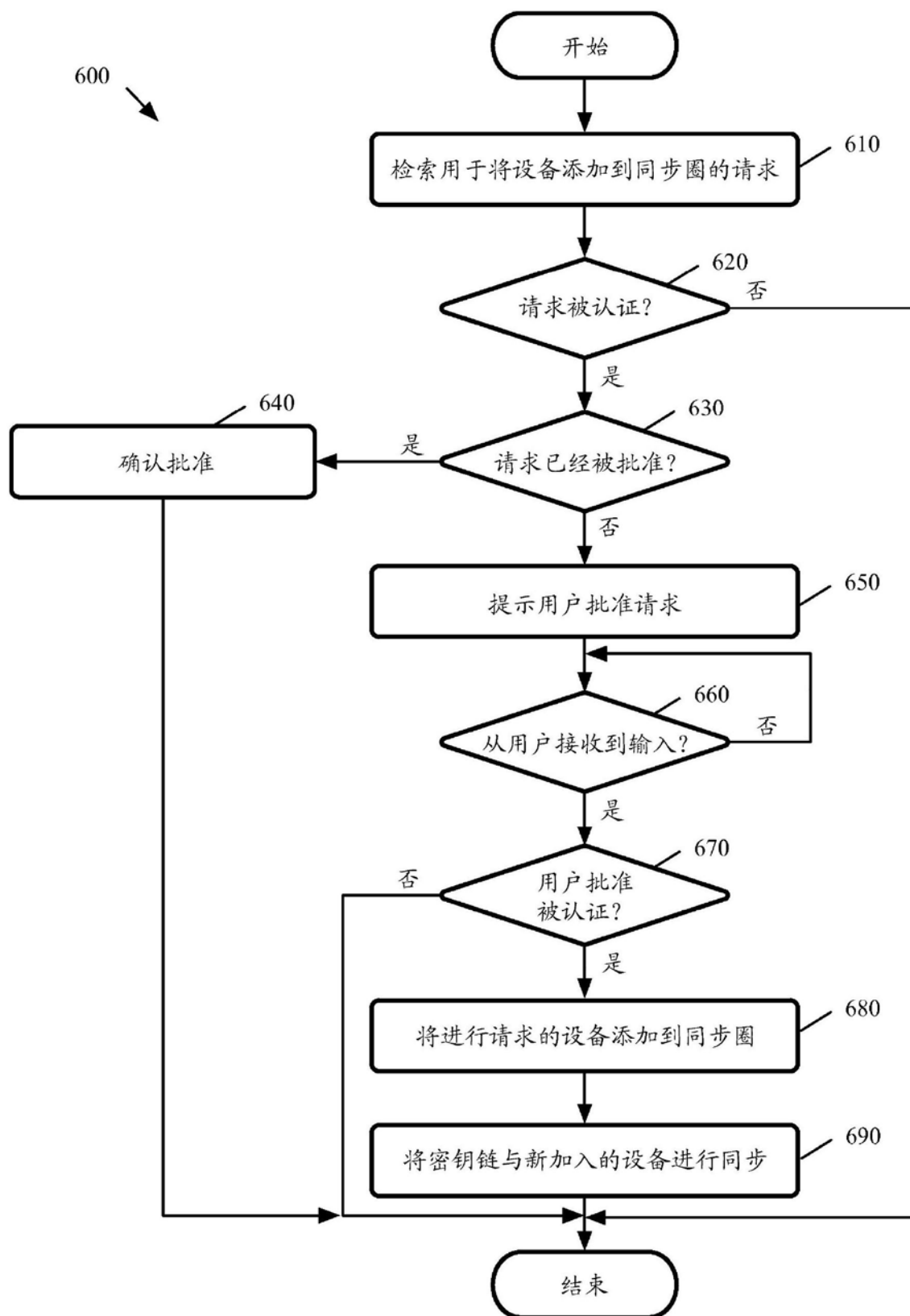


图6

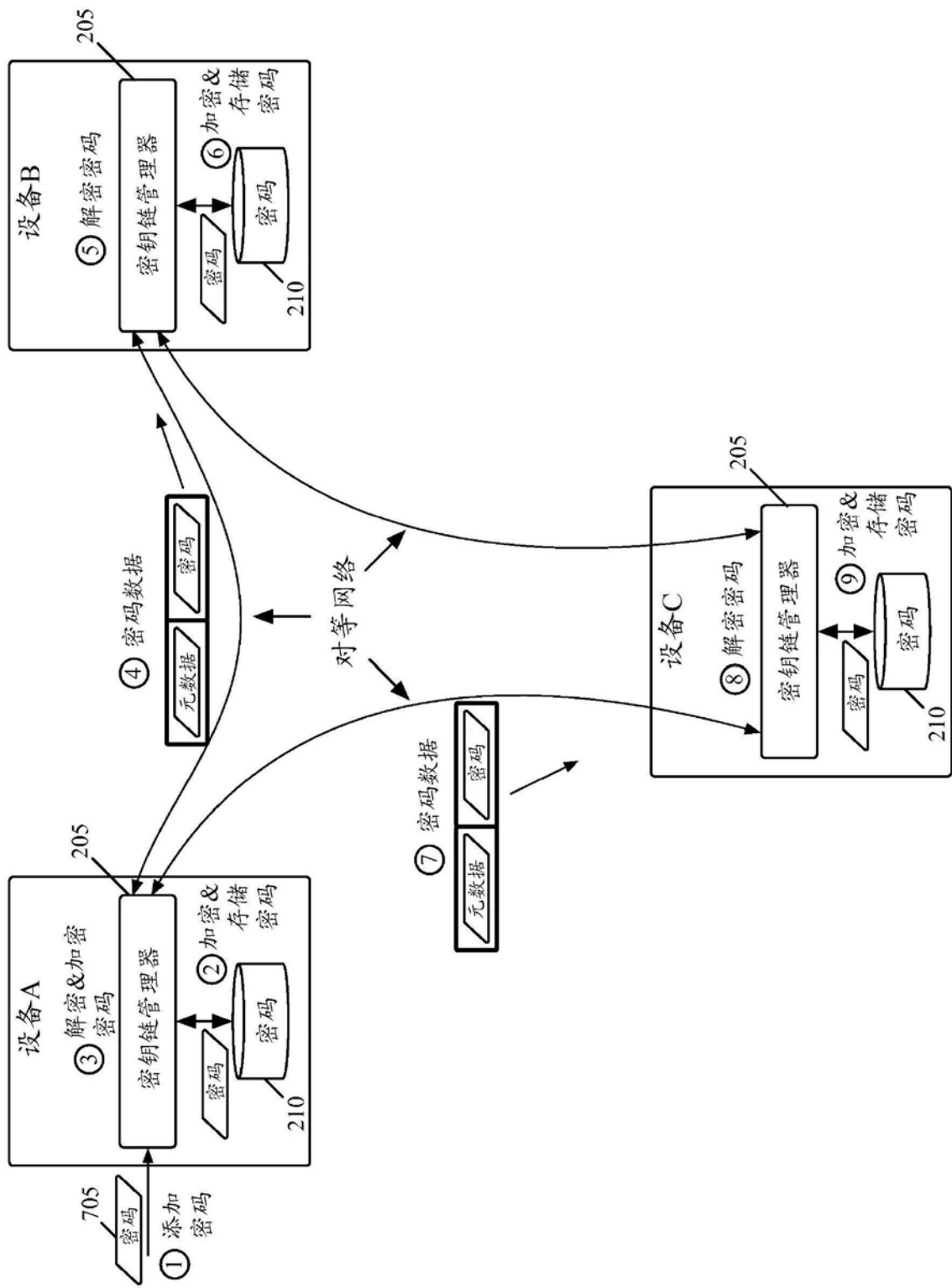


图7

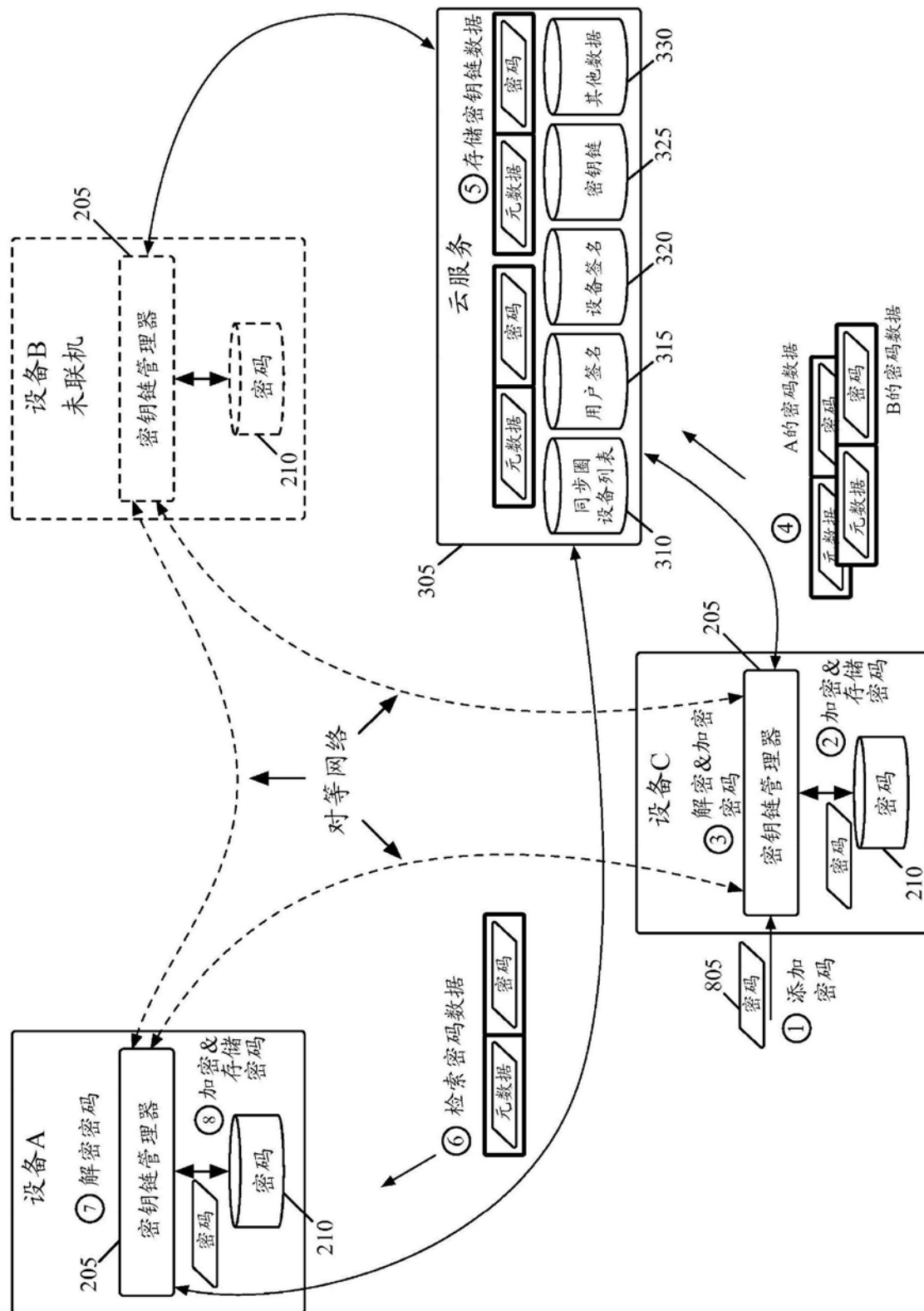


图8

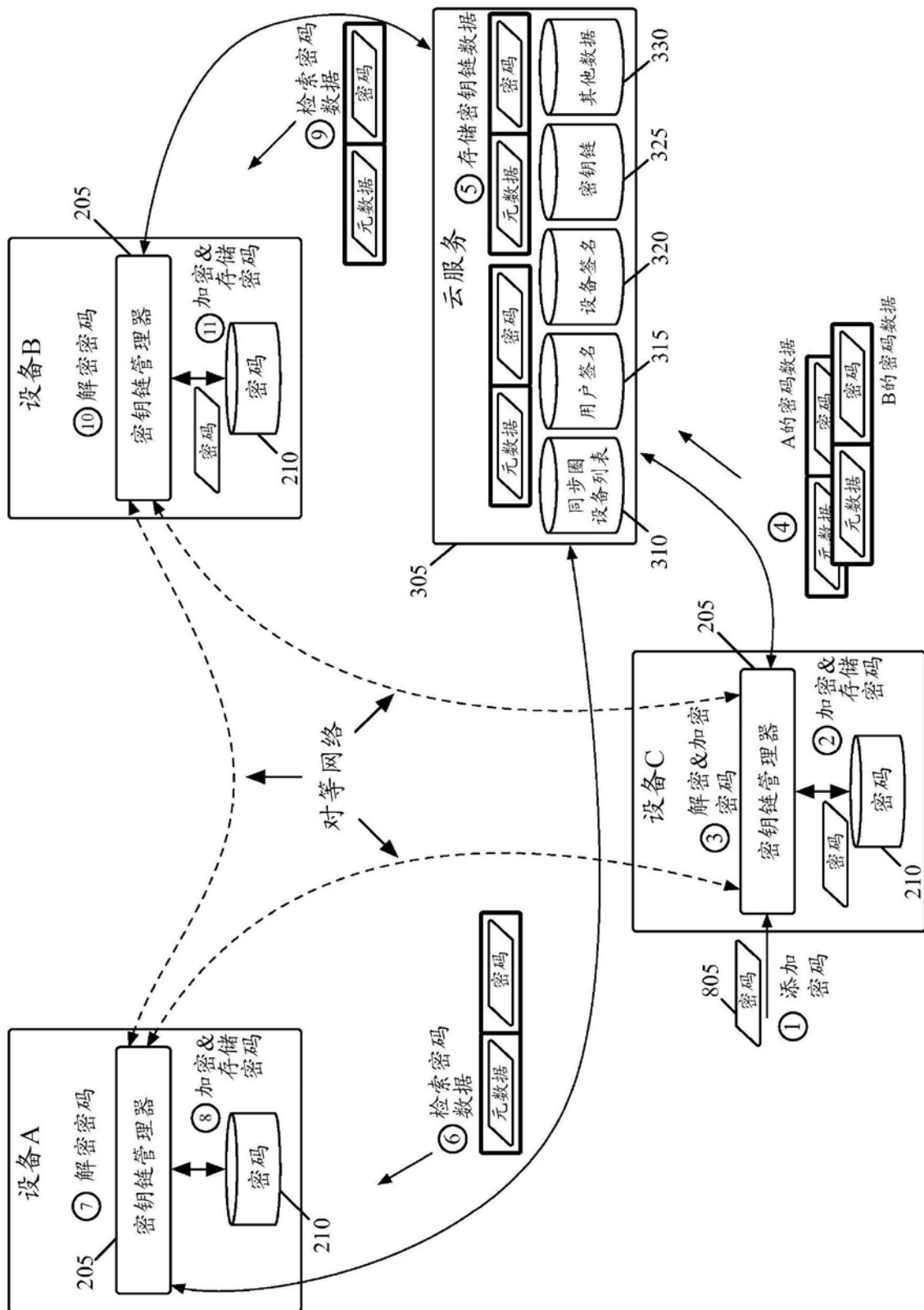


图9

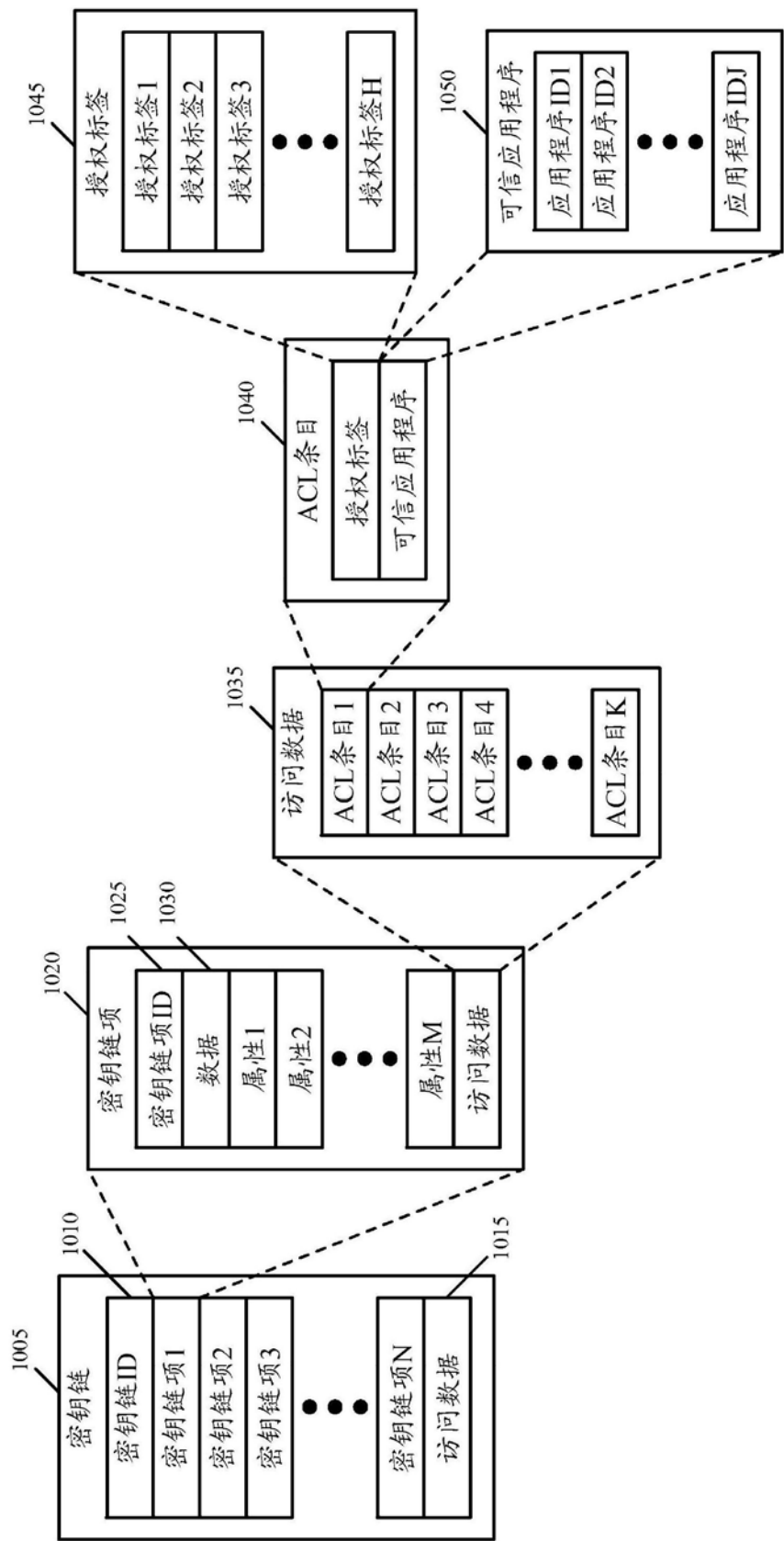


图10

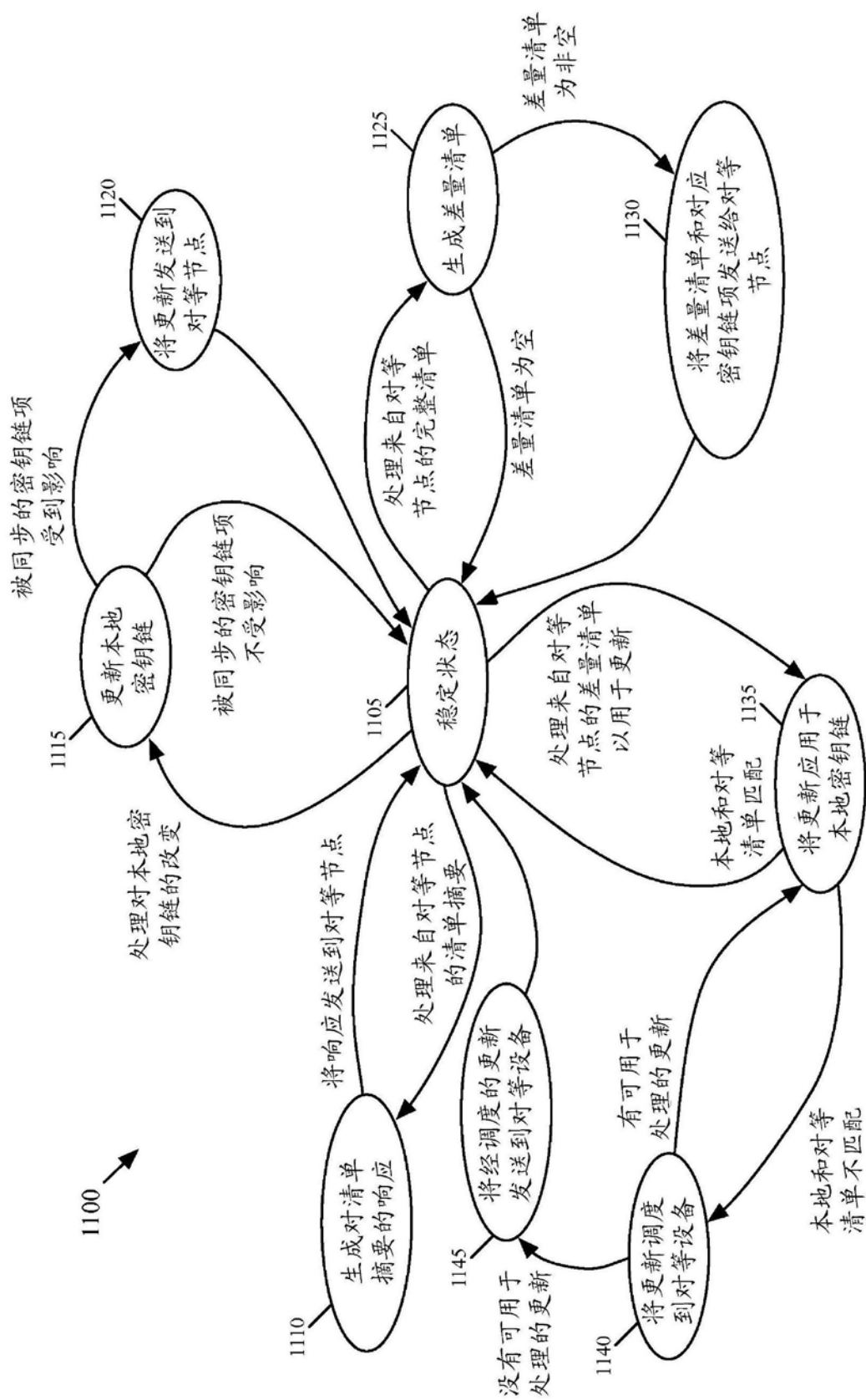


图11

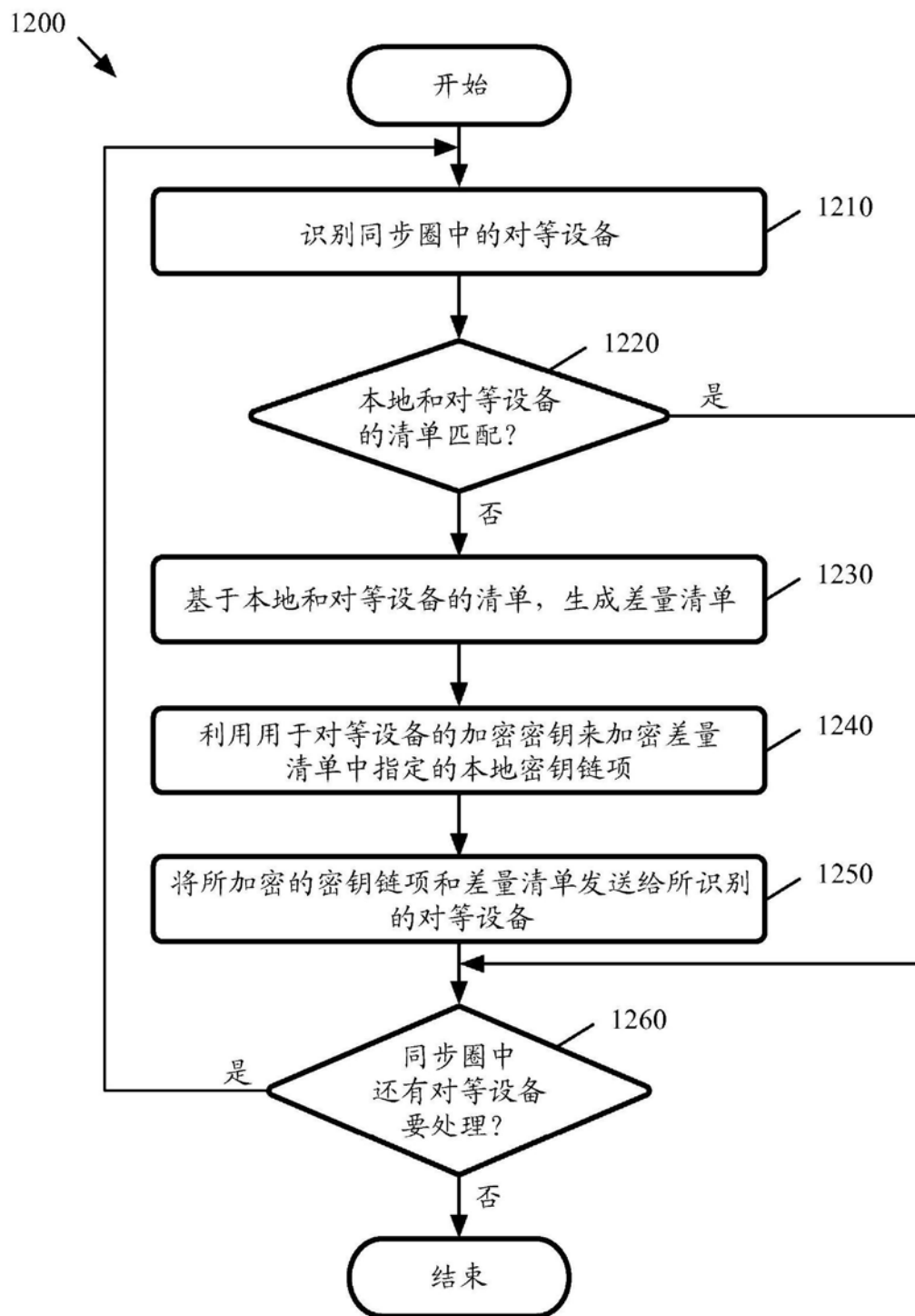


图12

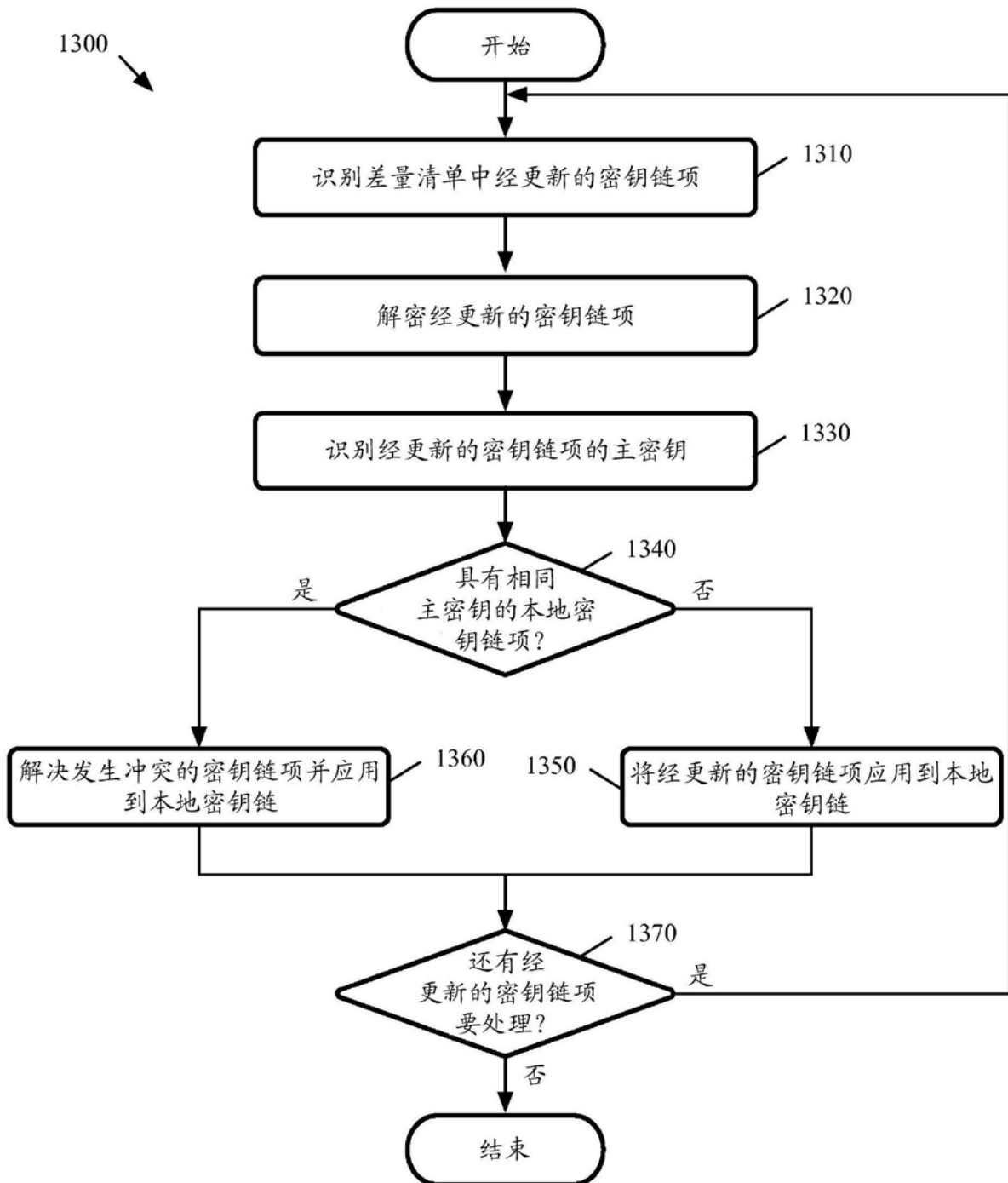


图13

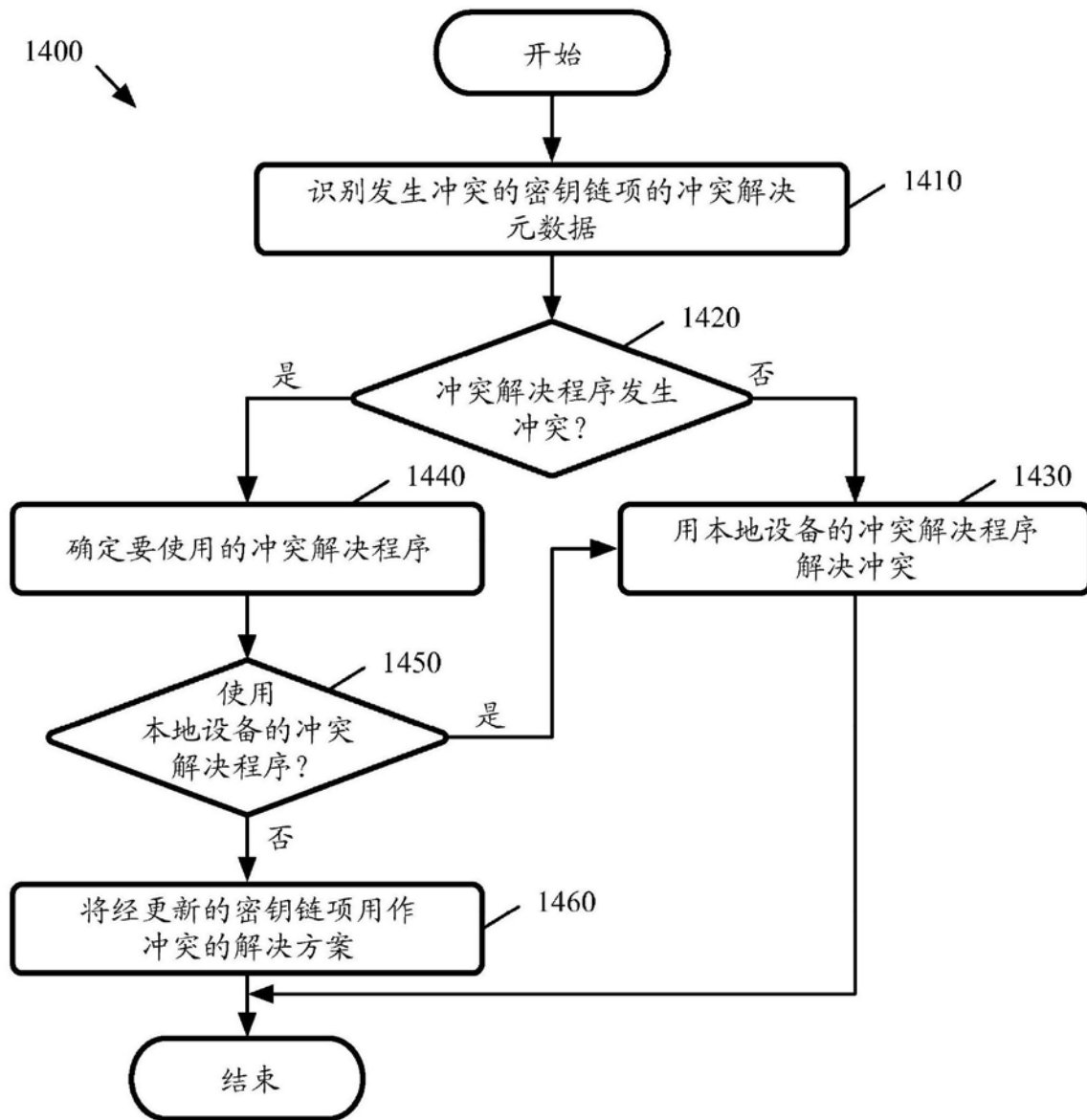


图14

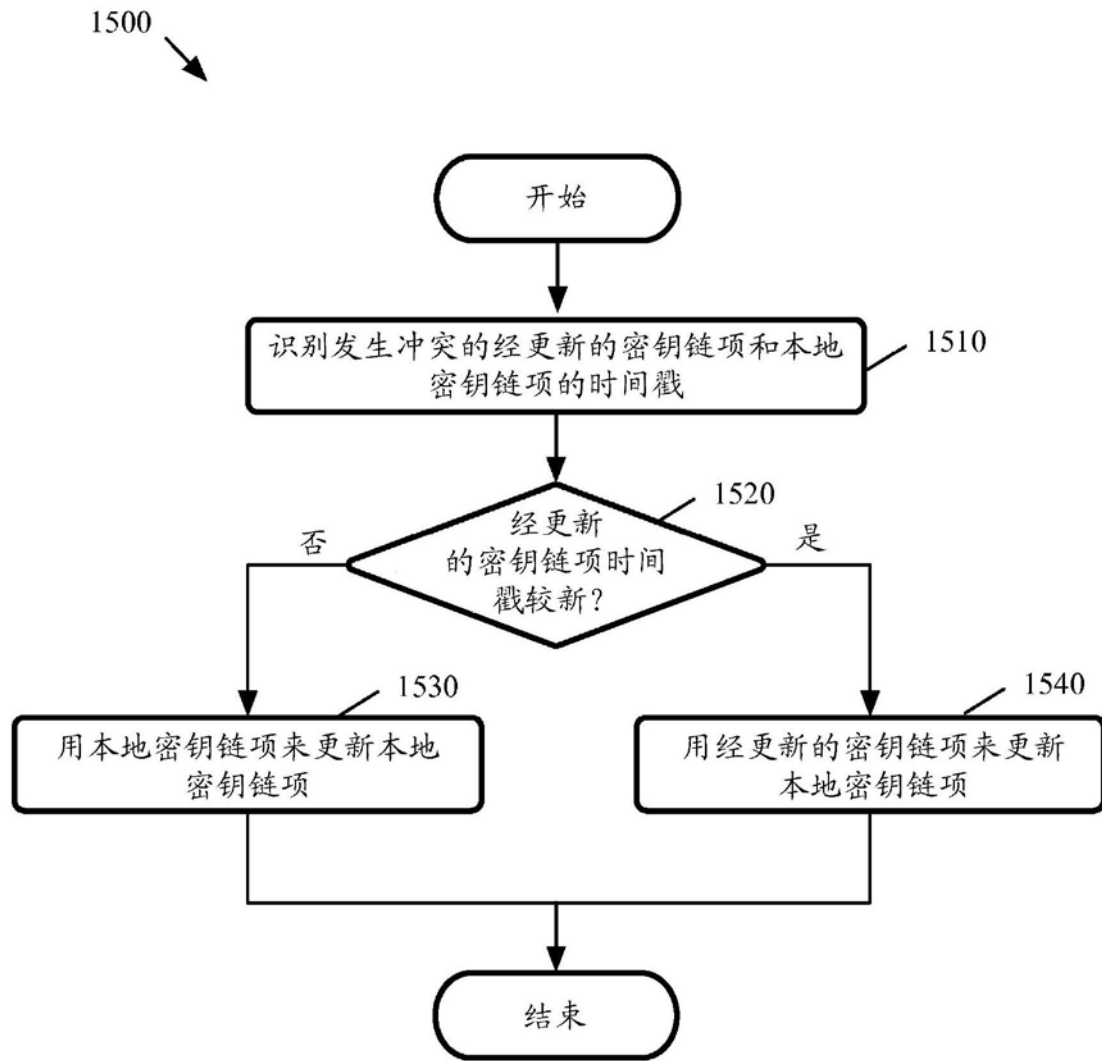


图15

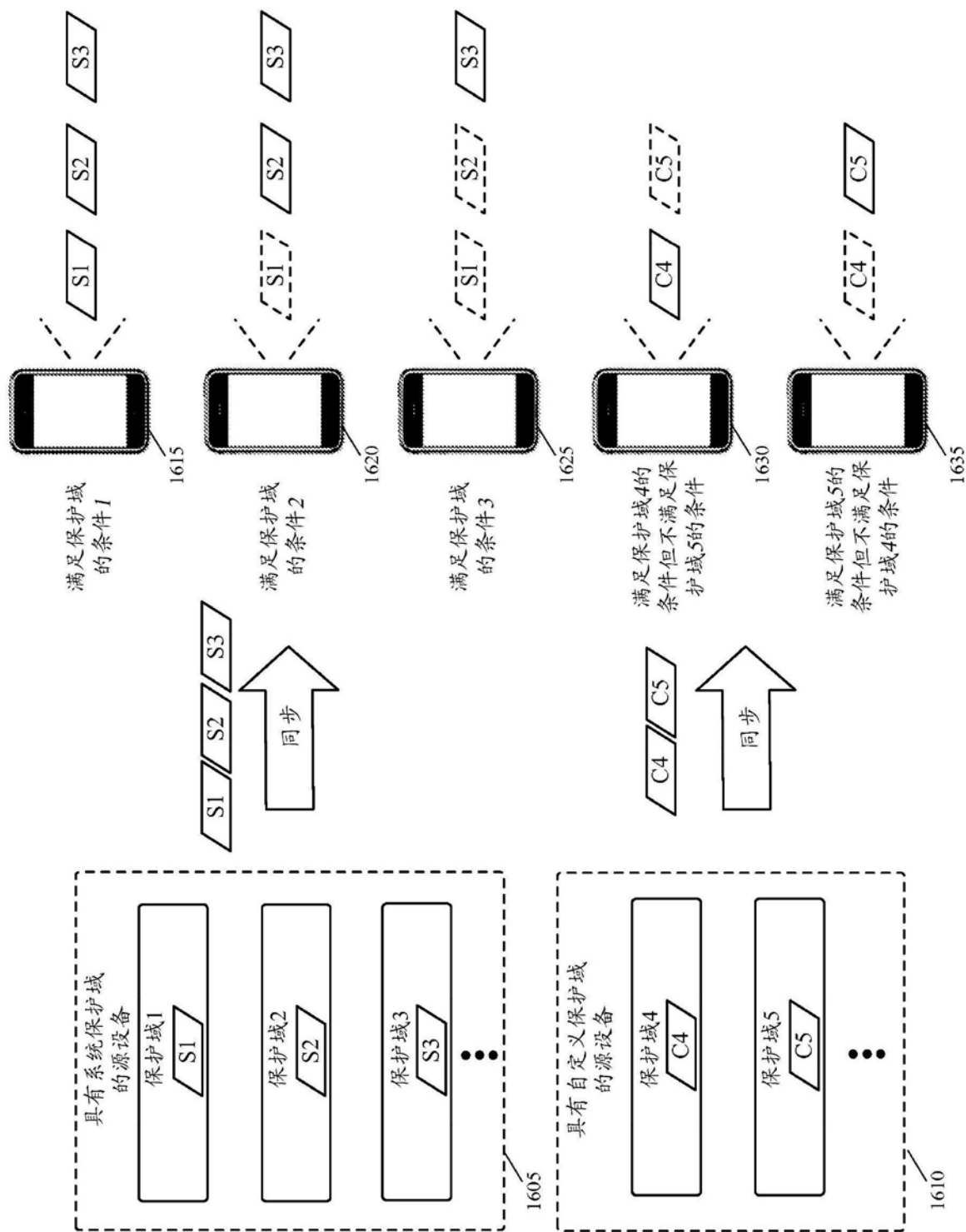


图16

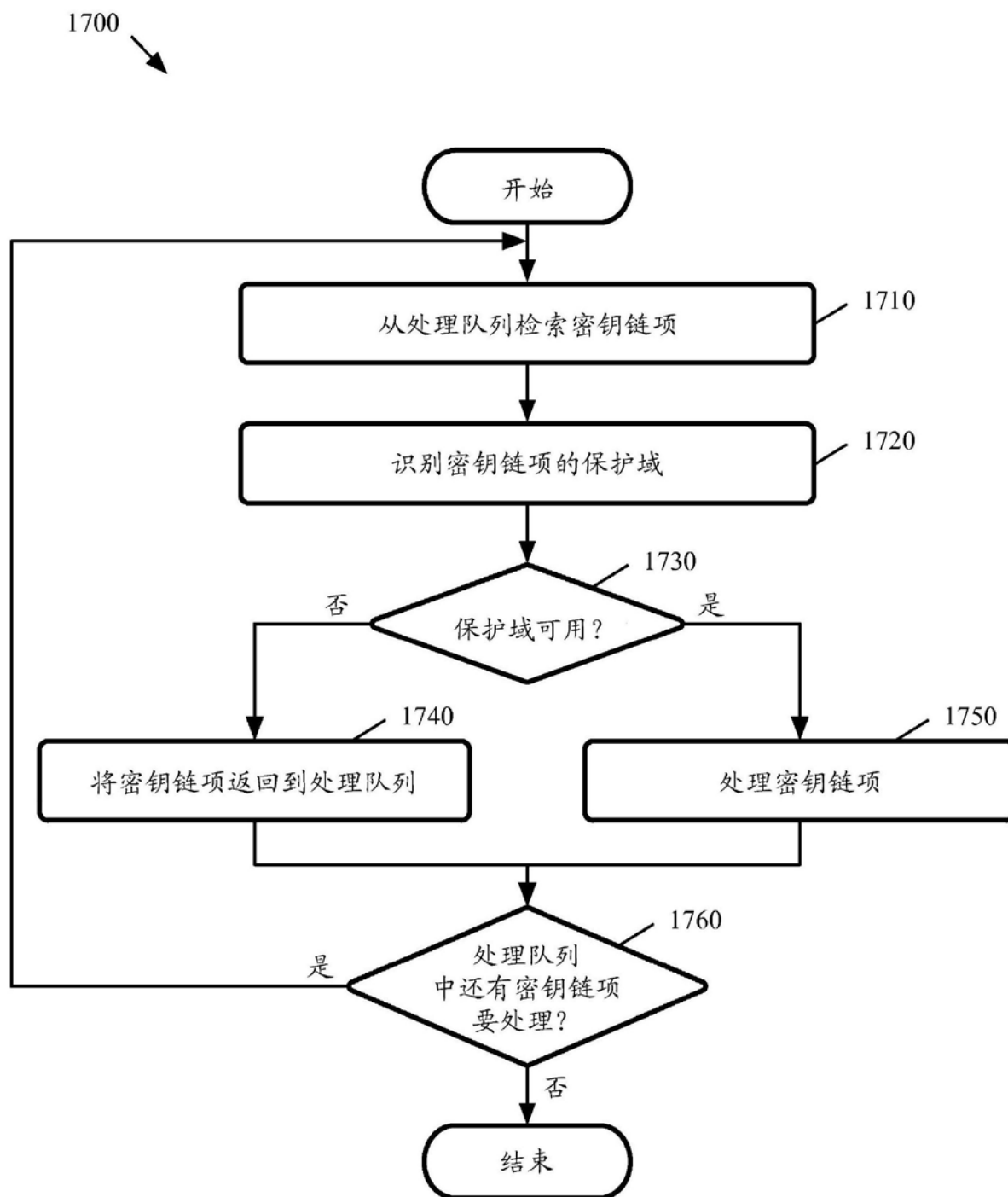


图17

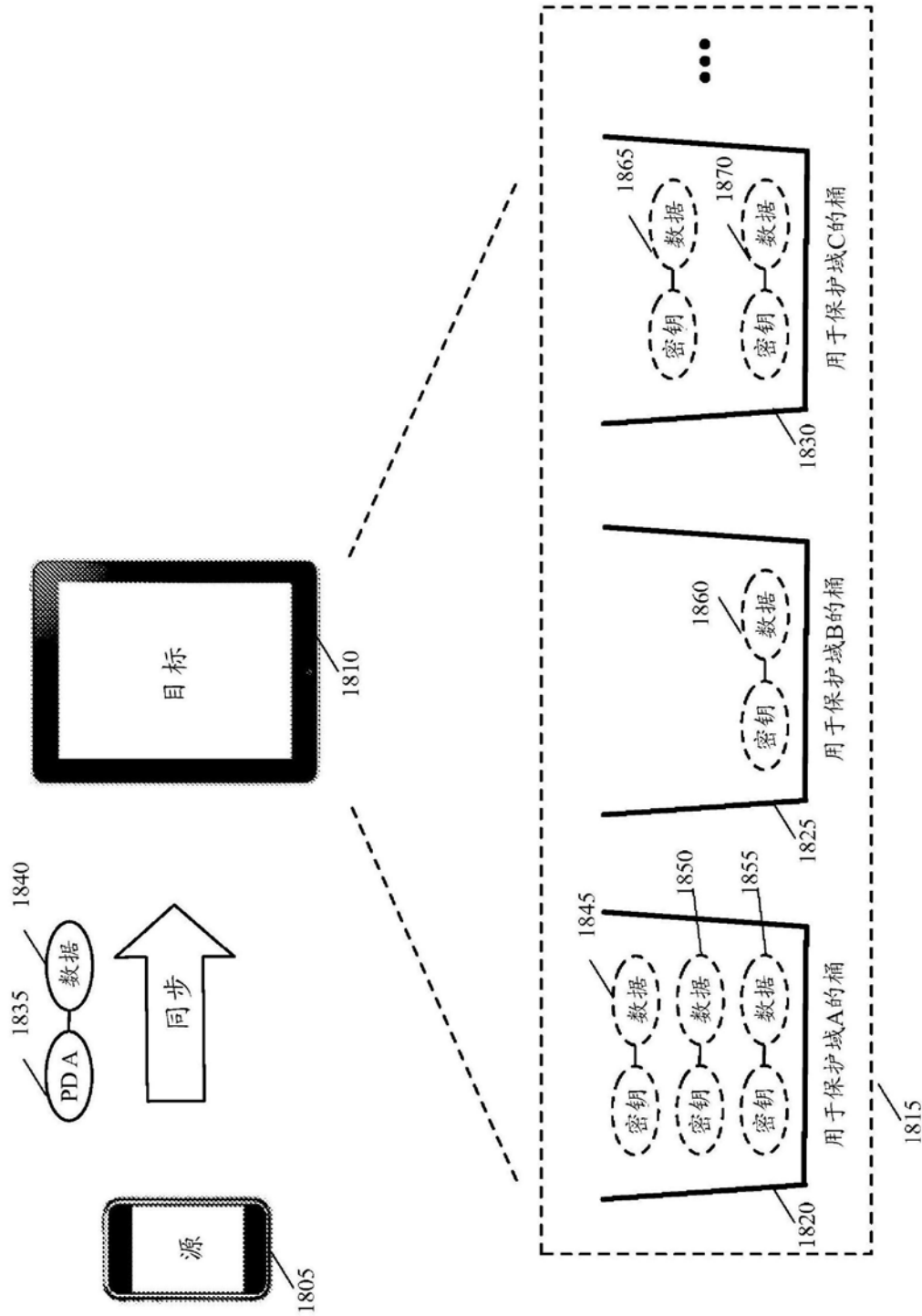


图18

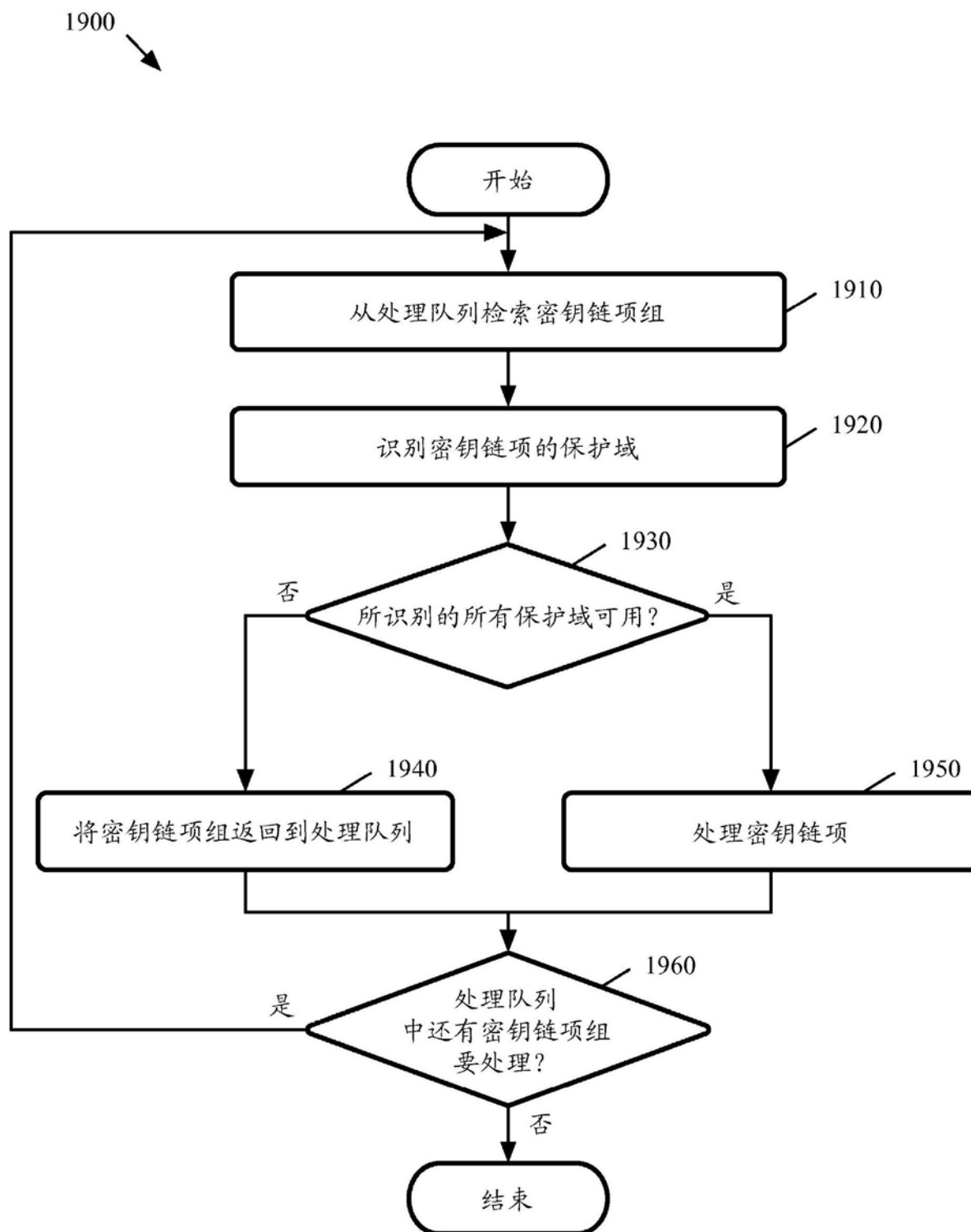


图19

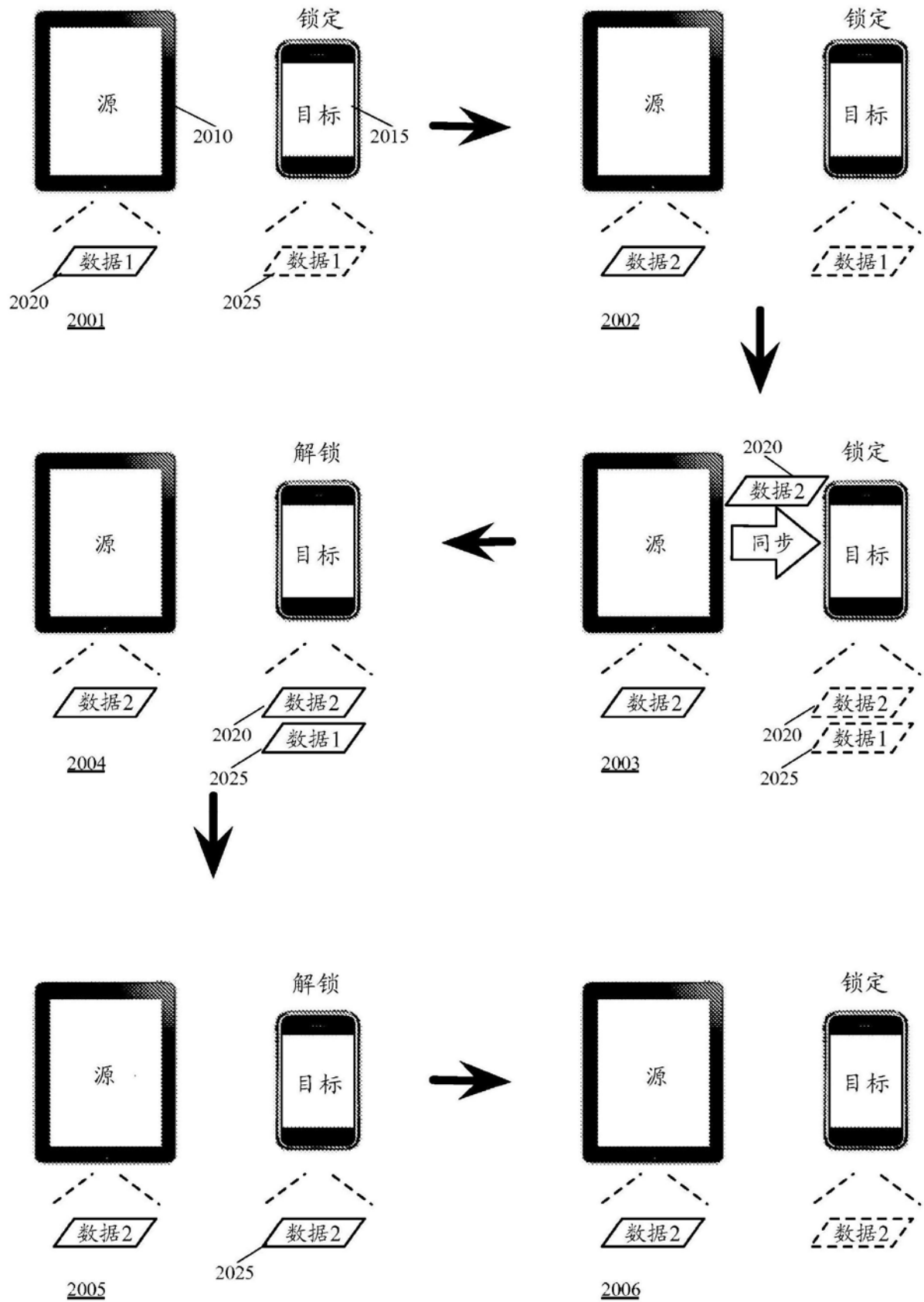


图20

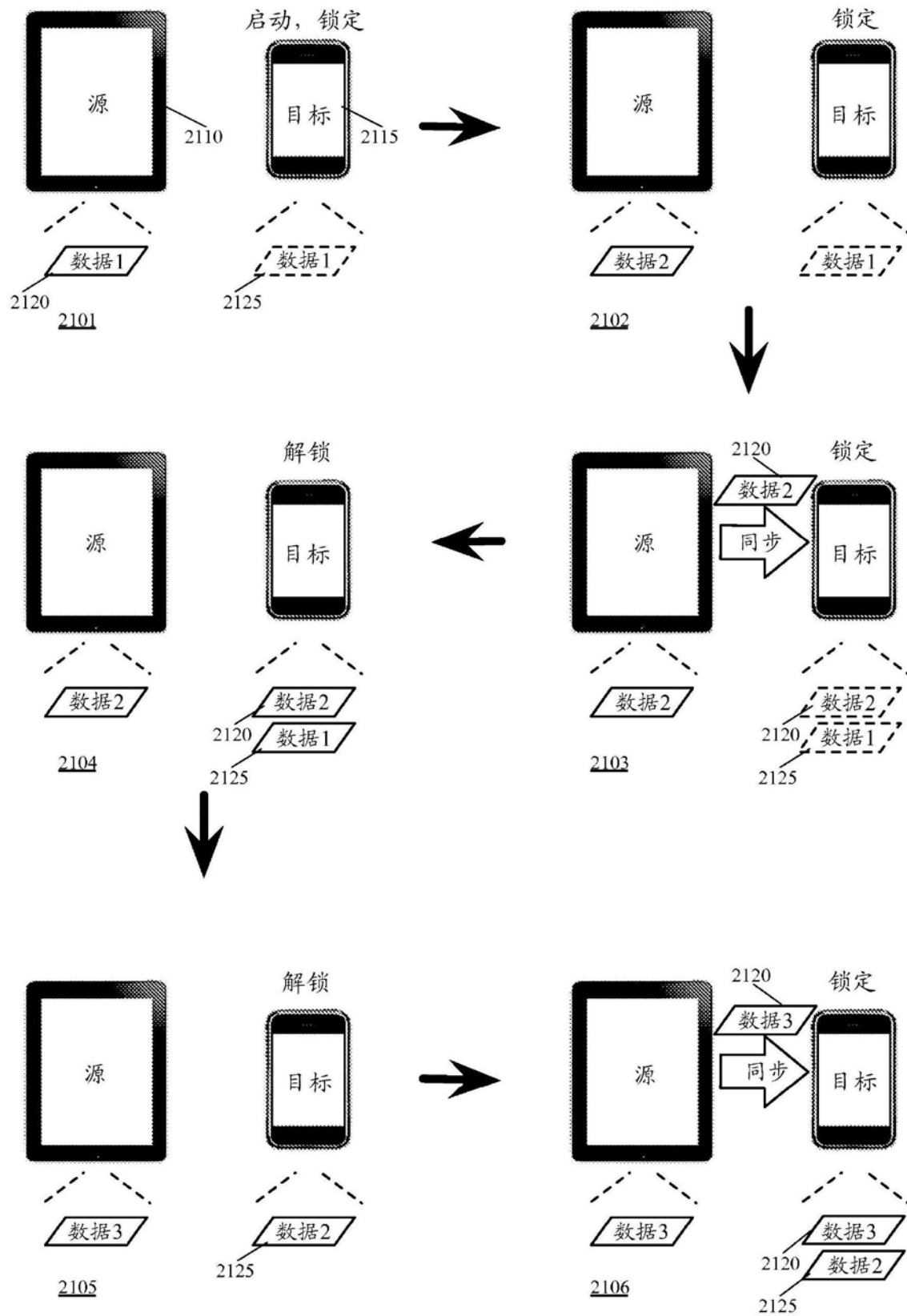


图21

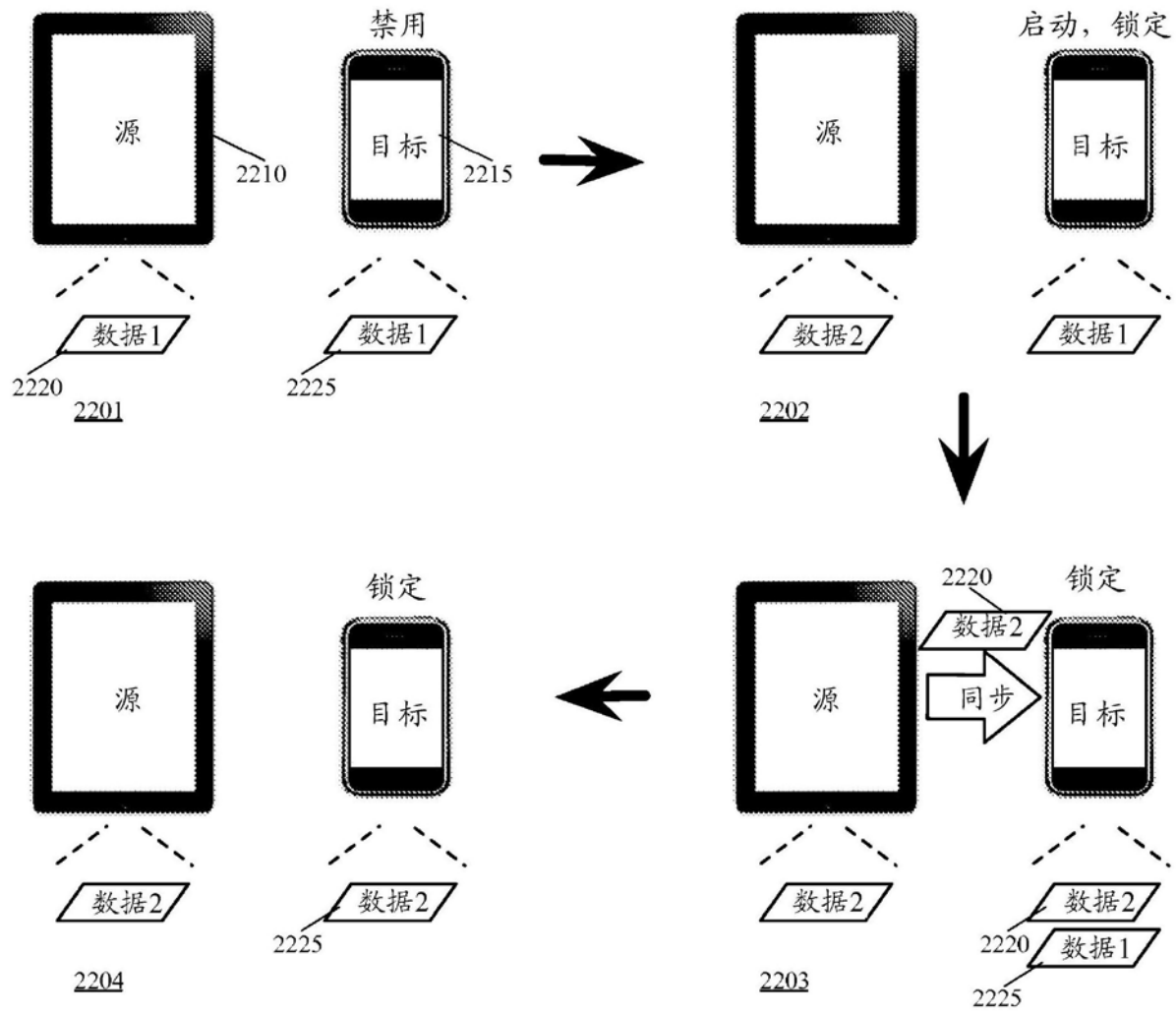


图22

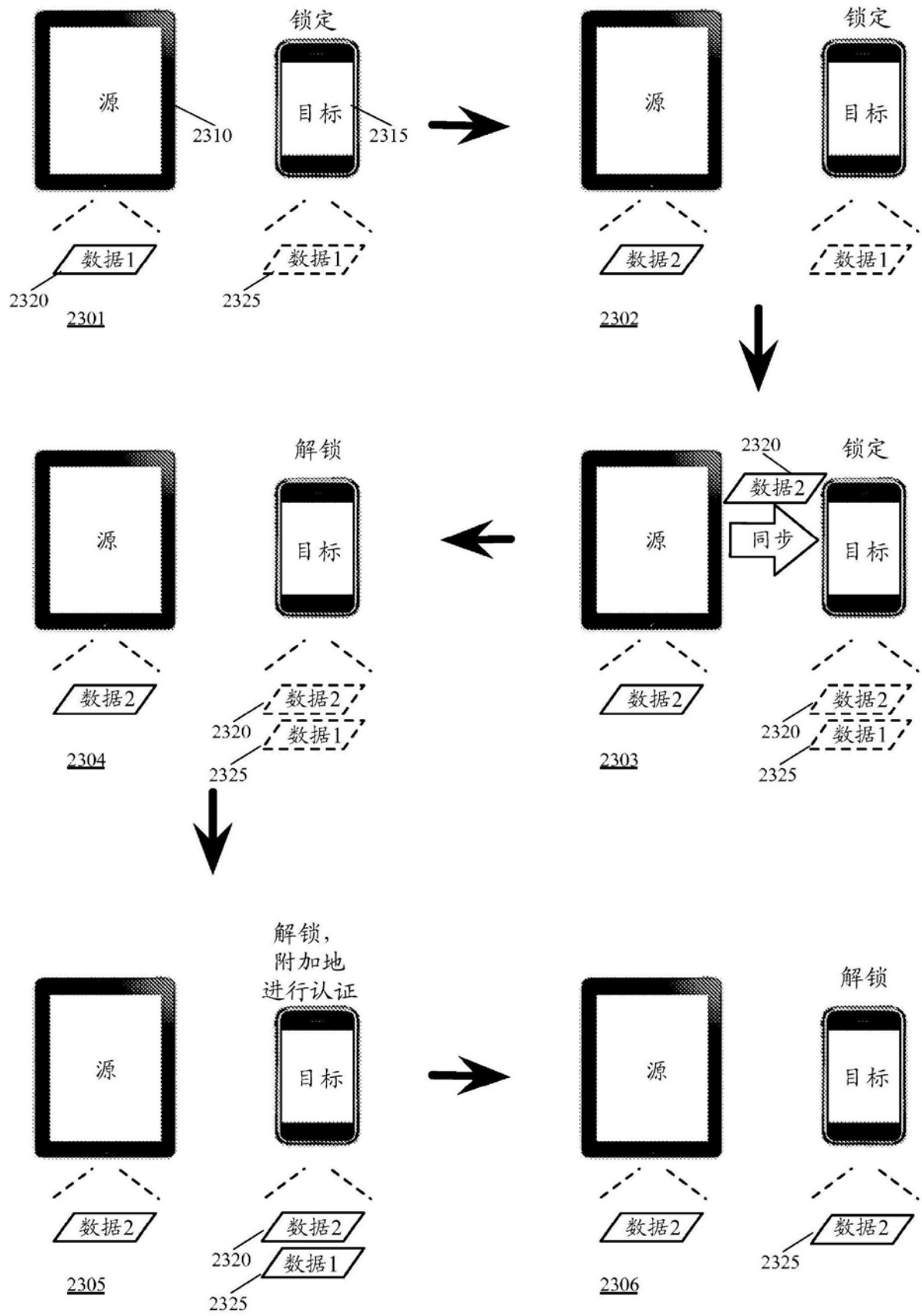


图23

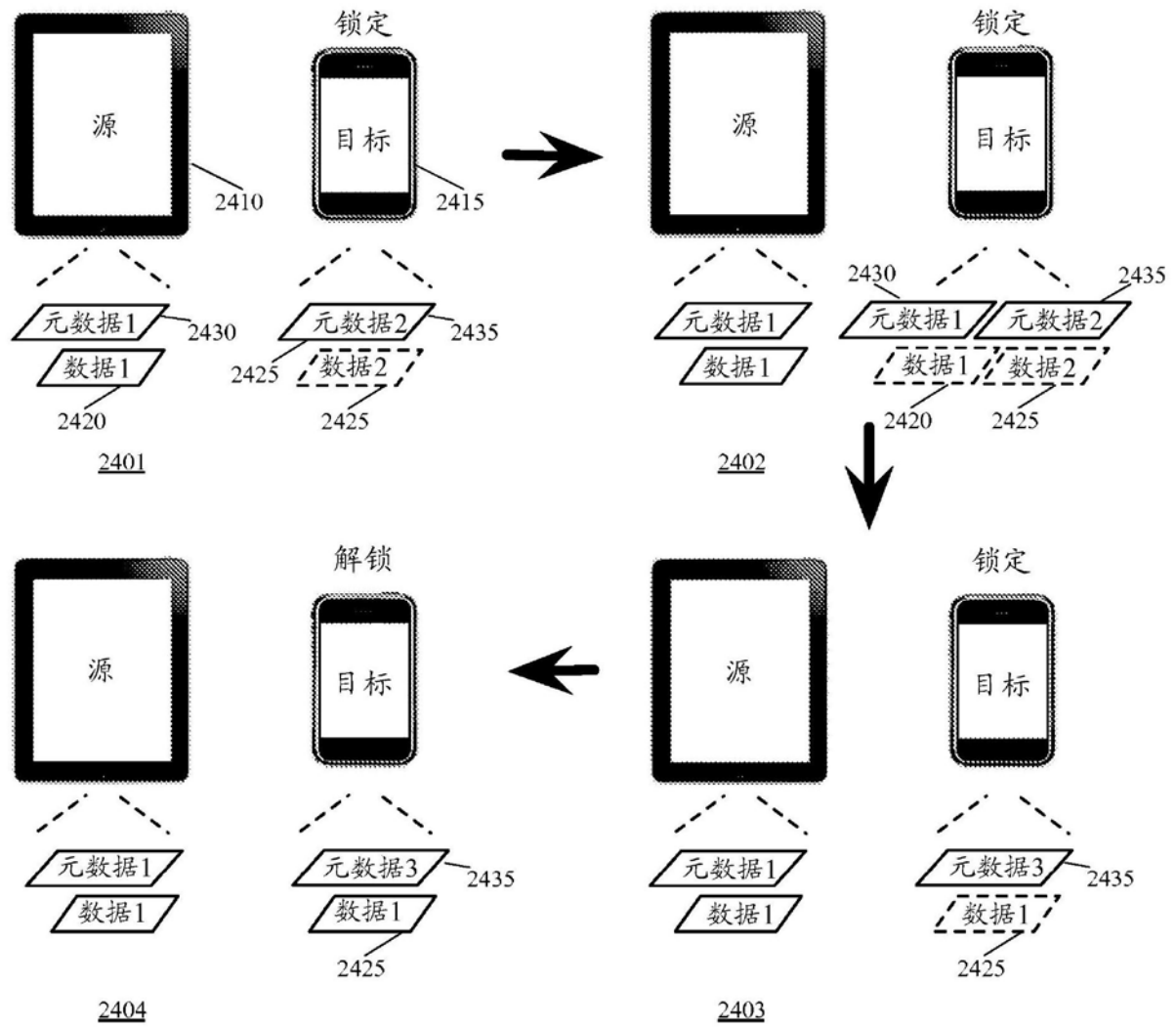


图24

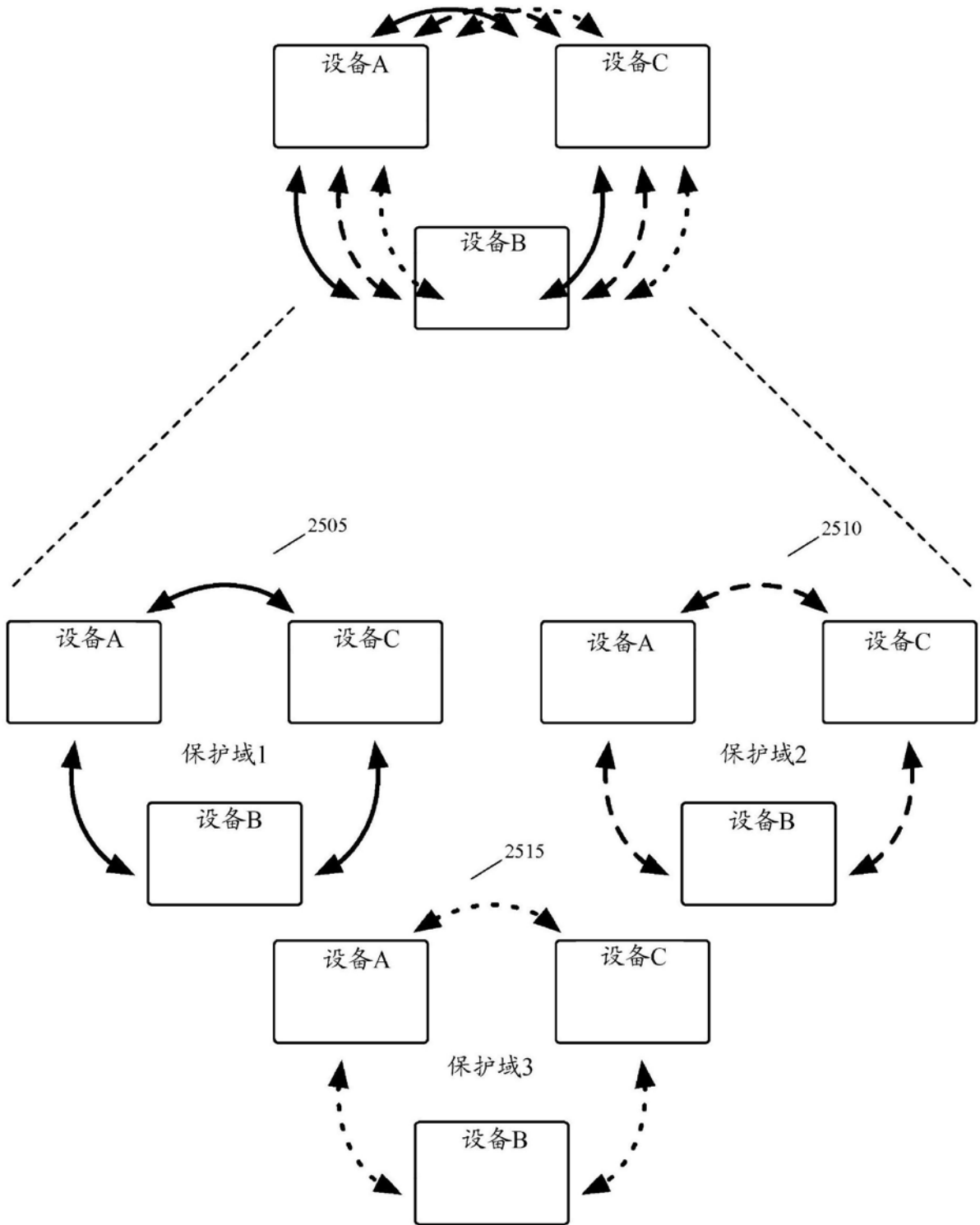


图25

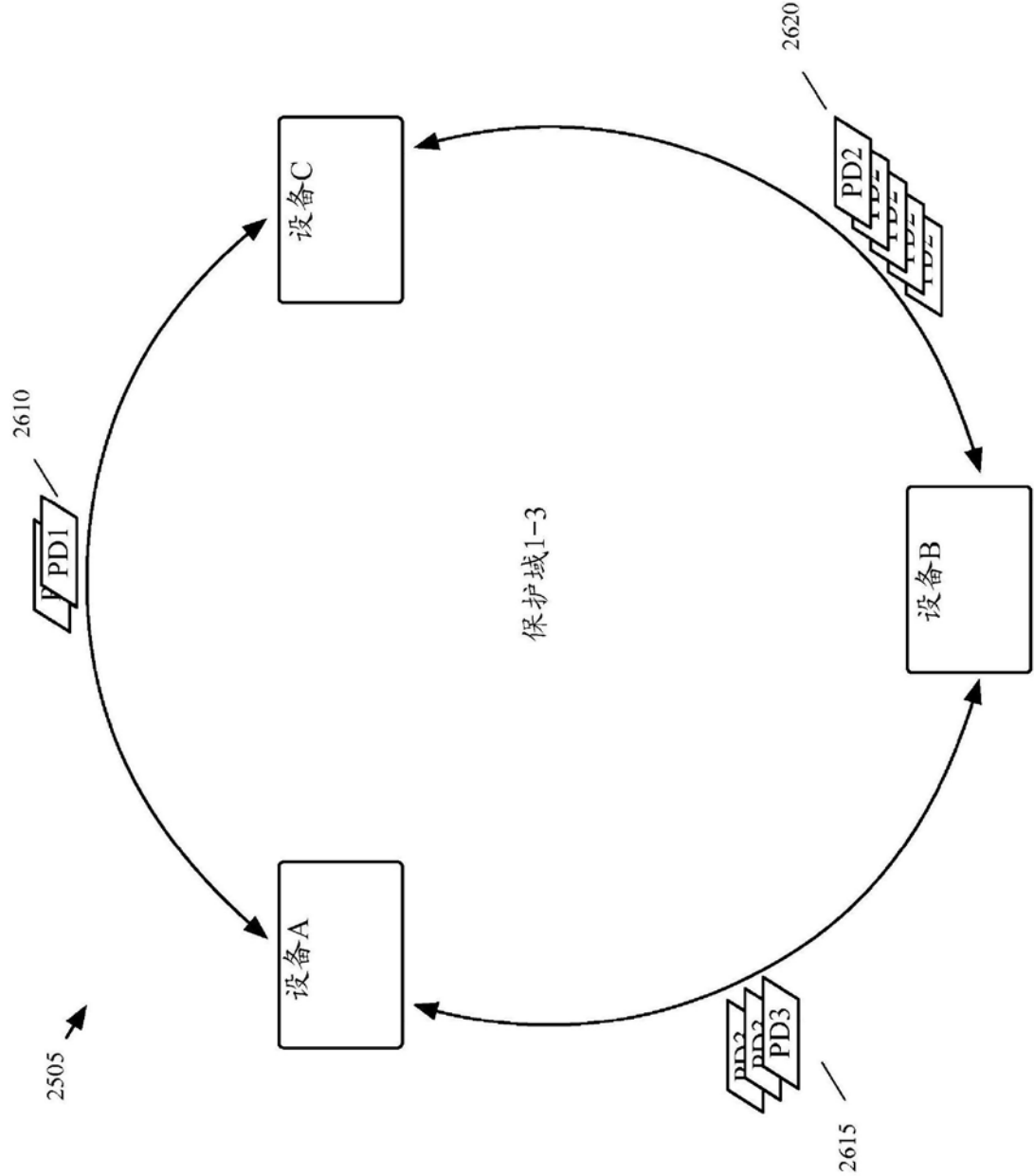


图26

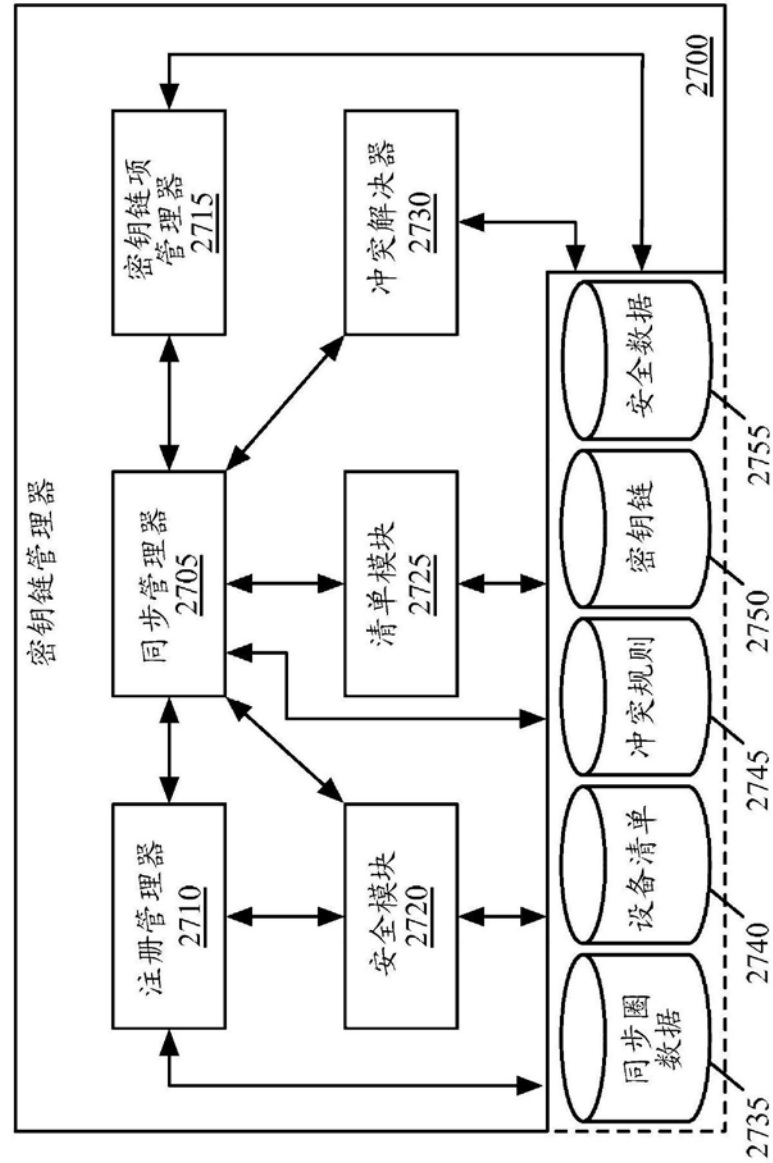


图27

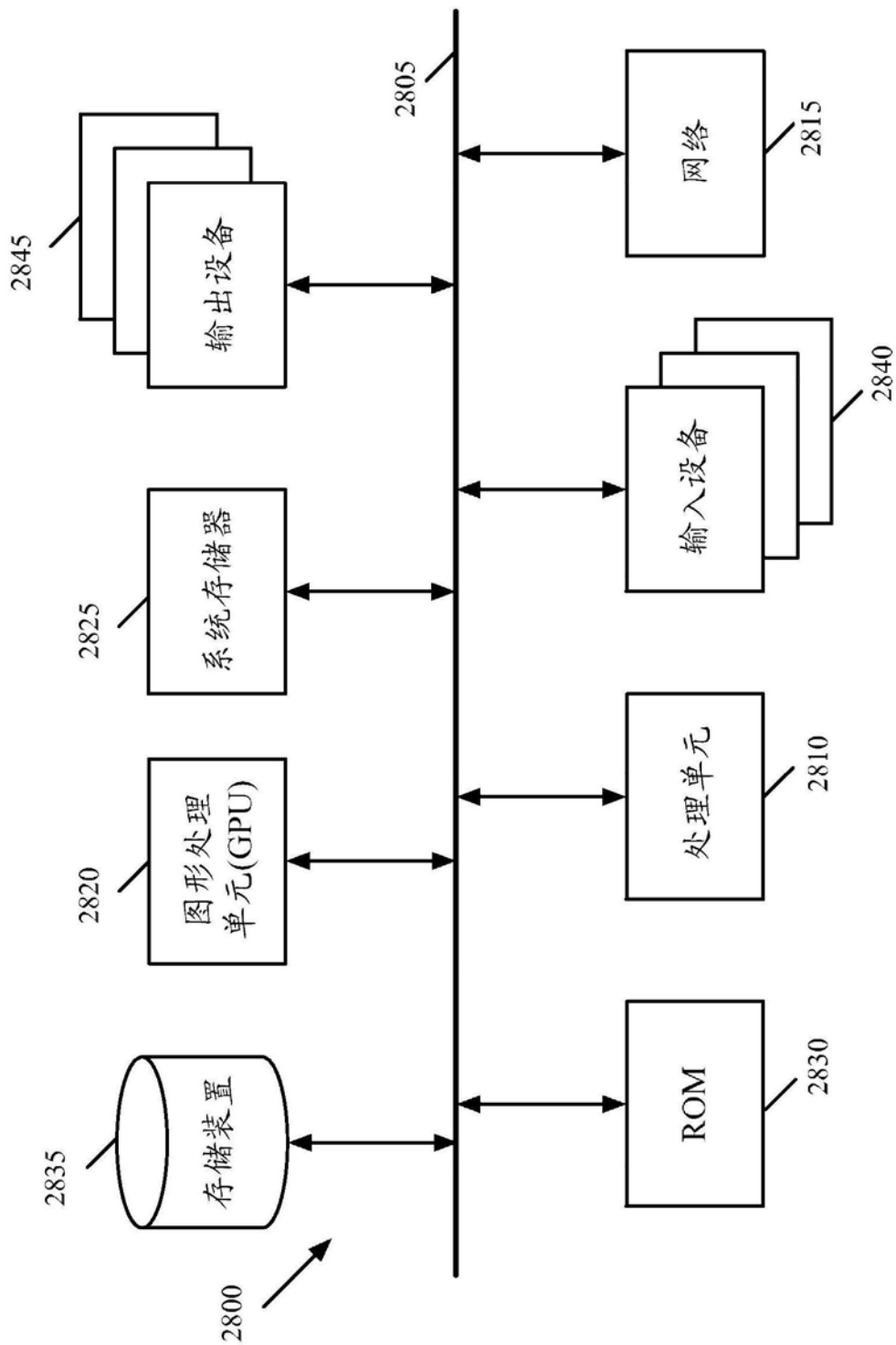


图28