(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109194465 B
(45)授权公告日 2022.02.18

(21)申请号 201811161190.X

(22)申请日 2018.09.30

(65)同一申请的已公布的文献号
申请公布号 CN 109194465 A

(43)申请公布日 2019.01.11

(73)专利权人 巍乾全球技术有限责任公司
地址 卢森堡市

(72)发明人 张磊 马帮亚 顾建良

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 101166089 B,2010.10.20
US 2018109372 A1,2018.04.19
CN 101546407 A,2009.09.30
CN 101753298 A,2010.06.23
CN 101425902 A,2009.05.06
CN 103856478 B,2017.11.24
US 2008095375 A1,2008.04.24

审查员 刘慧敏

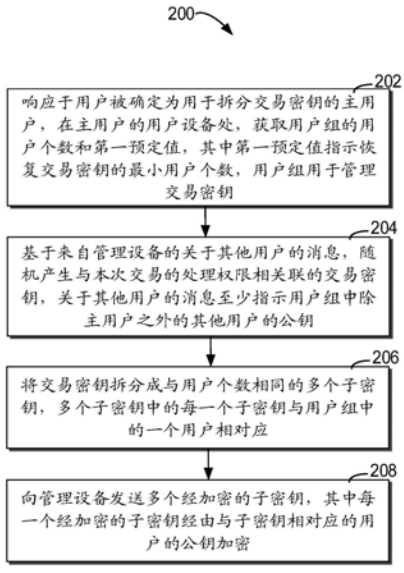
权利要求书3页 说明书12页 附图6页

(54)发明名称

用于管理密钥的方法、用户设备、管理设备、存储介质

(57)摘要

本公开提供了用于管理密钥的方法、用户设备、管理设备、存储介质和计算机程序产品。该用于管理密钥的方法包括:响应于用户被确定用于拆分交易密钥的主用户,在主用户的用户设备处,获取用户组的用户个数和第一预定值,其中第一预定值指示恢复交易密钥的最小用户个数,用户组用于管理交易密钥;基于来自管理设备的关于其他用户的消息,随机产生与本次交易的处理权限相关联的交易密钥,关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥;将交易密钥拆分成与用户个数相同的多个子密钥,多个子密钥中的每一个子密钥与用户组中的一个用户相对应;以及向管理设备发送多个经加密的子密钥,其中每一个经加密的子密钥经由与子密钥相对应的用户的公钥加密。



CN 109194465 B

1.一种用于管理密钥的方法,包括,在用于拆分交易密钥的主用户的用户设备处:

响应于用户被确定为所述主用户,获取用户组的用户个数和第一预定值,其中所述第一预定值指示恢复所述交易密钥的最小用户个数,所述用户组用于管理所述交易密钥;

基于来自管理设备的关于其他用户的消息,随机产生与本次交易的处理权限相关联的所述交易密钥,所述关于其他用户的消息至少指示所述用户组中除所述主用户之外的其他用户的公钥;

将所述交易密钥拆分成与所述用户个数相同的多个子密钥,所述多个子密钥中的每一个子密钥与所述用户组中的一个用户相对应;以及

向所述管理设备发送多个经加密的子密钥,其中每一个所述经加密的子密钥经由与所述子密钥相对应的用户的公钥加密,

其中随机产生所述交易密钥包括:

响应于确认所述管理设备的证书通过验证,基于所述其他用户的公钥的签名信息,确认所述其他用户的公钥是否通过验证;以及

响应于所述其他用户的公钥通过验证,随机产生与所述第一预定值相同的多个用于构建拆分多项式的随机数,所述多个用于构建拆分多项式的随机数包括所述交易密钥。

2.根据权利要求1所述的方法,其中所述主用户由所述管理设备在所述用户组中指定或随机确定。

3.根据权利要求1所述的方法,其中所述关于其他用户的消息还指示以下至少一项:

所述管理设备的证书;

用于验证所述其他用户的公钥的签名信息;

所述其他用户的标识;

所述其他用户的合并数据的哈希值的签名信息;以及

所述关于其他用户的消息的有效期。

4.根据权利要求1所述的方法,其中将所述交易密钥拆分成所述多个子密钥包括:

基于所述用户组的所述用户个数和所述多个用于构建拆分算法的随机数,确定所述多个子密钥,其中每一个子密钥包括第一子密钥数据和第二子密钥数据。

5.根据权利要求1所述的方法,其中经由与所述子密钥对应的用户的公钥加密包括:

基于与所述子密钥对应的用户的公钥和所述关于其他用户的消息的有效期,加密所述子密钥。

6.根据权利要求1所述的方法,还包括:

响应于确认来自所述管理设备的签名数据通过验证,基于预置在所述用户设备中的私钥,对所述签名数据进行签名,所述签名数据至少包括经由所述管理设备签名的随机数;以及

响应于用户被确定为用于组建所述用户组的组队主用户,向所述管理设备发送关于所述用户组的业务信息、所述用户设备的公钥和经由所述用户设备私钥签名的所述签名数据,所述业务信息至少包括所述用户组的用户个数和所述第一预定值。

7.根据权利要求1所述的方法,其中所述用户设备包括具有处理单元的硬件USB KEY。

8.一种用于管理密钥的方法,包括,在用于恢复交易密钥的恢复用户的用户设备处:

响应于用户被确定为所述恢复用户,获取来自管理设备的、用于恢复所述交易密钥的

恢复消息,其中所述恢复消息至少指示用户组中同意本次交易的确认用户的个数和所述恢复用户的标识,其中所述用户组用于管理所述交易密钥,所述交易密钥由用于拆分交易密钥的主用户的用户设备响应于所述用户组中的其他用户的公钥通过验证,随机产生与第一预定值相同的多个用于构建拆分多项式的随机数,所述多个用于构建拆分多项式的随机数包括所述交易密钥,并且所述交易密钥与本次交易的处理权限相关联,其中所述第一预定值指示恢复交易密钥的最小用户个数;

响应于确认所述确认用户的个数大于或等于所述第一预定值,基于从所述管理设备获取的确认用户的子密钥,确定所述交易密钥,所述确认用户的子密钥是经由所述主用户的用户设备事先拆分所述交易密钥而生成的并且经由所述恢复用户的公钥签名;以及

基于所确定的所述交易密钥,对关于所述本次交易的交易请求进行签名。

9.根据权利要求8所述的方法,其中所述恢复用户由所述管理设备在所述用户组中指定或随机确定。

10.根据权利要求8所述的方法,其中所述确认用户的子密钥由所述确认用户发送给所述管理设备,并且所述确认用户的子密钥经由所述恢复用户的公钥加密。

11.根据权利要求10所述的方法,其中所述确认用户的子密钥经由所述恢复用户的公钥加密包括:

在所述确认用户的用户设备处,基于经由所述管理设备获取的所述恢复用户的公钥,对所述确认用户的子密钥和与所述本次交易相关联的关联随机数进行加密。

12.根据权利要求8所述的方法,其中所述恢复消息还指示以下至少一项:

与所述本次交易相关联的关联随机数;

经由所述恢复用户的公钥签名的所述确认用户的子密钥和所述关联随机数;

所述确认用户的签名信息;

所述管理设备的证书;以及

所述恢复消息的哈希值的签名信息。

13.一种用于管理密钥的方法,包括,在管理设备处:

从用于创建用户组的组队主用户的用户设备获取关于所述用户组的业务信息,所述业务信息至少指示所述用户组的用户个数和第一预定值,所述第一预定值指示恢复交易密钥的最小用户个数,所述用户组用于管理所述交易密钥;

向用于拆分所述交易密钥的主用户的用户设备发送关于其他用户的消息,其中所述关于其他用户的消息至少指示所述用户组中除所述主用户之外的其他用户的公钥;

获取来自所述主用户的、与所述用户组的用户个数相同的多个子密钥,其中所述多个子密钥经由所述主用户对所述交易密钥拆分而生成,并且所述多个子密钥经由对应的用户的公钥加密,并且所述交易密钥由用于拆分所述交易密钥的主用户的用户设备响应于所述其他用户的公钥通过验证,随机产生与所述第一预定值相同的多个用于构建拆分多项式的随机数,所述多个用于构建拆分多项式的随机数包括所述交易密钥;以及

将所述多个子密钥缓存,以用于发送给相对应的用户。

14.根据权利要求13所述的方法,还包括:

在所述用户组中指定或随机确定以下各项中的至少一项:

所述主用户;以及

用于恢复所述交易密钥的恢复用户。

15.根据权利要求14所述的方法,还包括:

响应于接收到关于本次交易的请求,向所述用户组的用户发送用于确认是否同意所述本次交易的交易信息,其中所述交易信息至少指示所述本次交易的交易内容和所述恢复用户的标识;

获取所述用户组中同意所述本次交易的每个确认用户的子密钥,其中所述确认用户的所述子密钥经由所述恢复用户的公钥签名;以及

响应于确认满足本次交易的条件,向所述恢复用户发送用于恢复交易密钥的恢复消息。

16.根据权利要求13所述的方法,还包括:

响应于来自所述用户组中用户的用户设备的报到请求,向所述用户设备发送所述管理设备的签名数据,所述签名数据至少包括经由所述管理设备签名的随机数;

基于来自所述用户设备的签名数据,确认所述用户设备是否通过验证,所述签名数据由所述用户设备响应于确认所述管理设备通过验证,基于预置在所述用户设备中的私钥,对所述随机数进行签名而生成的;以及

响应于确认所述用户组中每一个用户的用户设备通过验证,确认所述用户组通过验证。

17.根据权利要求13所述的方法,其中所述用户设备包括具有处理单元的硬件USB KEY。

18.一种用于管理密钥的用户设备,所述用户设备包括:

存储器,被配置为存储一个或多个计算机程序;

处理单元,耦合至所述存储器并且被配置为执行所述一个或多个计算机程序使所述设备执行权利要求1-12中任一项所述的方法。

19.一种用于管理密钥的管理设备,所述管理设备包括:

存储器,被配置为存储一个或多个计算机程序;

处理单元,耦合至所述存储器并且被配置为执行所述一个或多个计算机程序使所述设备执行权利要求13-17中任一项所述的方法。

20.一种非瞬态计算机可读存储介质,其上存储有机器可执行指令,所述机器可执行指令在被执行时使机器执行根据权利要求1-17中任一项所述的方法的步骤。

用于管理密钥的方法、用户设备、管理设备、存储介质

技术领域

[0001] 本公开涉及权限管理的方法和设备，更具体地，涉及用于管理密钥的方法、用户设备、管理设备、非瞬态计算机可读存储介质和计算机程序产品。

背景技术

[0002] 在电子商务、资产分割、资金管理等诸多场景下，需要多个用户对待处理的交易具有支配与管理权限。在传统的权限管理方案中，为了提高安全性，防止密钥被个别拥有权限的用户所泄露，通常会采用多重签名的解决手段，例如，由多个拥有权限的用户分别利用各自的密钥依次对同一交易进行加密或签名。

[0003] 在上述传统的权限管理方案中，需要多个拥有权限的用户依次对同一交易进行签名或授权，因此使得整个交易流程比较冗长；另外，各拥有权限的用户持有各自的密钥，当任一用户丢失其密钥或者因故拒绝使用其密钥时，都有可能拖延或阻止交易的进行；此外，由于拥有权限的用户所持有的密钥通常在一段时间内是固定的，因此存在被破译的较高概率。

[0004] 有鉴于此，有必要构建一种用于管理密钥的方案，使得涉及多个拥有权限的用户的密钥支配与管理更加安全和易用。

发明内容

[0005] 本公开提供一种用于管理密钥的方法和设备，能够使得密钥的支配与管理更加安全、可靠与方便使用。

[0006] 根据本公开的第一方面，提供了一种用于管理密钥的方法。该方法包括：响应于用户被确定为用于拆分交易密钥的主用户，在主用户的用户设备处，获取用户组的用户个数和第一预定值，其中第一预定值指示恢复交易密钥的最小用户个数，用户组用于管理交易密钥；基于来自管理设备的关于其他用户的消息，随机产生与本次交易的处理权限相关联的交易密钥，关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥；将交易密钥拆分成与用户个数相同的多个子密钥，多个子密钥中的每一个子密钥与用户组中的一个用户相对应；以及向管理设备发送多个经加密的子密钥，其中每一个经加密的子密钥经由与子密钥相对应的用户的公钥加密。

[0007] 根据本发明的第二方面，还提供一种用于管理密钥的方法。该方法包括：响应于用户被确定为用于恢复交易密钥的恢复用户，在恢复用户的用户设备处，获取来自管理设备的、用于恢复交易密钥的恢复消息，其中恢复消息至少指示用户组中同意本次交易的确认用户的个数和恢复用户的标识，其中用户组用于管理交易密钥；响应于确认确认用户的个数大于或等于第一预定值，基于从管理设备获取的确认用户的子密钥，确定交易密钥，确认用户的子密钥是经由事先拆分交易密钥而生成的；以及基于所确定的交易密钥，对关于本次交易的交易请求进行签名。

[0008] 根据本发明的第三方面，还提供一种用于管理密钥的方法。该方法包括：在管理设

备处，从用于创建用户组的组队主用户的用户设备获取关于用户组的业务信息，业务信息至少指示用户组的用户个数和第一预定值，第一预定值指示恢复交易密钥的最小用户个数，用户组用于管理交易密钥；向用于拆分交易密钥的主用户的用户设备发送关于其他用户的消息，其中关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥；获取来自主用户的、与用户组的用户个数相同的多个子密钥，其中多个子密钥经由主用户对交易密钥拆分而生成，并且多个子密钥经由对应的用户的公钥加密；以及将多个子密钥缓存，以用于发送给相对应的用户。

[0009] 根据本发明的第四方面，还提供用于管理密钥的用户设备。该用户设备包括：存储器，被配置为存储一个或多个计算机程序；处理单元，耦合至该存储器并且被配置为执行该一个或多个计算机程序使该设备执行本公开的第一和二中任一方面的方法。

[0010] 根据本发明的第五方面，还提供一种用于管理密钥的管理设备。该管理设备包括：存储器，被配置为存储一个或多个计算机程序；处理单元，耦合至该存储器并且被配置为执行该一个或多个计算机程序使该设备执行本公开的第三方面的方法。

[0011] 根据本发明的第六方面，还提供一种非瞬态计算机可读存储介质。该非瞬态计算机可读存储介质上存储有机器可执行指令，该机器可执行指令在被执行时使机器执行本公开的第一、二和三中任一方面的方法。

[0012] 根据本公开的第七方面，提供了一种计算机程序产品。该计算机程序产品被有形地存储在非瞬态计算机可读介质上并且包括机器可执行指令，机器可执行指令在被执行时使机器执行本公开的第一、二和三中任一方面的方法。

[0013] 提供发明内容部分是为了以简化的形式来介绍对概念的选择，它们在下文的具体实施方式中将被进一步描述。发明内容部分无意标识本公开的关键特征或主要特征，也无意限制本公开的范围。

附图说明

[0014] 通过结合附图对本公开示例性实施例进行更详细的描述，本公开的上述以及其它目的、特征和优势将变得更加明显，其中，在本公开示例性实施例中，相同的参考标号通常代表相同部件。

[0015] 图1示出了根据本公开的实施例的用于管理密钥的管理系统100 的架构图；

[0016] 图2示出了根据本公开的实施例的用于管理密钥的方法200的流程图；

[0017] 图3示出了根据本公开的实施例的用于管理密钥的方法300的流程图；

[0018] 图4示出了根据本公开的实施例的用于管理密钥的方法400的流程图；

[0019] 图5示出了根据本公开的实施例的用于管理密钥的管理系统500 的数据流向图；

[0020] 图6示意性示出了适于用来实现本公开实施例的电子设备600的框图。

[0021] 在各个附图中，相同或对应的标号表示相同或对应的部分。

具体实施方式

[0022] 下面将参照附图更详细地描述本公开的优选实施例。虽然附图中显示了本公开的优选实施例，然而应该理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了使本公开更加透彻和完整，并且能够将本公开的范围完整

地传达给本领域的技术人员。

[0023] 在本文中使用的术语“包括”及其变形表示开放性包括，即“包括但不限于”。除非特别申明，术语“或”表示“和/或”。术语“基于”表示“至少部分地基于”。术语“一个示例实施例”和“一个实施例”表示“至少一个示例实施例”。术语“另一实施例”表示“至少一个另外的实施例”。术语“第一”、“第二”等等可以指代不同的或相同的对象。下文还可能包括其他明确的和隐含的定义。

[0024] 如上文所描述的，传统的权限管理方案中，由于用户所持有的的密钥长时间固定不变、并且多个用户需依次利用各自持有的密钥对同一交易进行签名，任一用户出现问题(例如丢失其密钥或者拒绝使用其密钥)，将导致交易无法被顺利处理。因此，传统的权限管理方案的签名过程不够安全和方便，而且系统的可靠性较低，容易受制于一些涉及权限使用的不当行为。

[0025] 为了至少部分地解决上述问题以及其他潜在问题中的一个或者多个，本公开的示例实施例提出了一种用于管理密钥的方案。在该方案中，响应于用户被确定为用于拆分交易密钥的主用户，在该主用户的用户设备处，获取用户组的用户个数和第一预定值，其中第一预定值指示恢复交易密钥的最小用户个数，用户组用于管理交易密钥；基于来自管理设备的关于其他用户的消息，随机产生与本次交易的处理权限相关联的交易密钥，关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥；将交易密钥拆分成与用户个数相同的多个子密钥，多个子密钥中的每一个子密钥与用户组中的一个用户相对应；以及向管理设备发送多个经加密的子密钥，其中每一个经加密的子密钥经由与子密钥相对应的用户的公钥加密。

[0026] 在上述方案中，通过将主用户随机产生的交易密钥拆分成与用户组中的用户个数相同的多个子密钥，并且每一个子密钥经由与子密钥对应的用户的公钥加密，本公开的示例实施例所提出方案不仅降低了因交易密钥固定而导致的易被破解的风险。而且，由于拥有子密钥的单个用户无法独立恢复交易密钥，需要多个用户一同协作才能恢复交易密钥，因此分散了密钥过于集中的风险、进一步提高了交易密钥的安全性。此外，通过设置恢复交易密钥的最小用户个数，使得能够在个别用户出现问题的情况下(例如丢失子密钥或者拒绝使用子密钥)，依然可以通过其他用户的协作而恢复交易密钥，因而，提高了权限管理系统的可靠性和强健性。另外，通过将经加密的多个子密钥发送给管理设备，管理设备可以缓存经加密的子密钥，不需要用户组的其他用户同步操作，因而能够实现交易密钥在多个用户之间进行拆分与分发的异步处理，提高了权限管理系统的方便性。

[0027] 图1示出了根据本公开的实施例的用于管理密钥的管理系统100 的架构图。如图1所示，管理系统100包括管理设备110、多个用户设备120-1、120-2、120-3、120-4至120-N(以下有时也统称为用户设备120)，该多个用户设备例如与管理交易密钥的多个用户140-1、140-2、140-3、140-4至140-N(以下有时也统称为用户140)相关联，以作为对应用户用于管理交易密钥的终端设备。用户140-1至140-N 例如对交易或资产处置等事项共同拥有权限，因此可以组建成管理密钥的用户组。上述管理设备110和多个用户设备120-1、120-2、120-3、 120-4至120-N经由网络150进行数据交互。

[0028] 关于管理设备110，其例如是但不限个人计算机、服务器或其他计算设备。管理设备110用于通过与用户设备交互，实现各用户的用户设备的初始化、指定或随机确定用户组

中的主用户或恢复用户、协助组队主用户组建用于管理交易密钥的用户组、协助拆分主用户将交易密钥拆分成与用户组中用户个数相同的多个子密钥、缓存并分发子密钥、以及协助恢复用户进行交易密钥恢复。在一些实施例中，管理设备110响应于用户设备的报到请求，确认用户设备是否通过验证，以及通过确认用户组中的每一个用户的用户设备是否通过验证，进而确认整个用户组是否通过验证。在一些实施例中，管理设备110还可以用于从用于组建用户组的主用户处获取用户组的用户个数和恢复交易密钥的最小用户个数(即第一预定值)，以及协助随机选定的用于拆分交易密钥的主用户的用户设备构建拆分多项式。

[0029] 关于用户设备120-1、120-2、120-3、120-4至120-N，其例如是但不限于常规的手机、个人计算机等。每个用户设备120具有与其相关联的硬件安全设备130(例如130-1、130-2、130-3、130-4或130-N)。硬件安全设备130例如而不限于USB KEY，其例如可以即插即用到用户设备120上。硬件安全设备130主要承担涉及交易密钥产生、拆分或恢复的主要功能。在一些实施例中，该硬件安全设备130可以创建自己的用于非对称加密的公钥K和私钥P对。该硬件安全设备130 可以用于创建用户组的密码、随机产生交易密码、以及构建用于拆分交易密码的多项式等等。

[0030] 为了方便描述起见，在本文中，也将如图1中所示的每个用户设备120和与该用户设备120相关联的硬件安全设备130的组合称为用户设备120。

[0031] 然而，本发明并不局限于此。本发明中所述的用户设备120也可以是单独设计的、通信和处理功能模块与通用的硬件安全设备130的集成。这样的用户设备120可以创建自己的用于非对称加密的私钥K 和公钥P，还通过与管理设备110相互验证来建立互信、以便交换密钥和交易信息。此外，用户设备120还可以被管理设备指定或随机确定为用户组中的主用户、恢复用户或其他用户。

[0032] 在一些实施例中，用户设备(例如120-1)被管理设备110随机确定为用于组建用户组的主用户的用户设备。该用户设备120-1可以确定用户组的业务信息(例如包括用户个数N和用户指示恢复交易密钥的最小用户个数的第一预定值M)，以及向管理设备110发送该业务信息。

[0033] 在一些实施例中，用户设备(例如120-2)被管理设备110指定或随机确定为用于拆分交易密钥的主用户的用户设备。该用户设备 120-2可以随机产生与本次交易的处理权限相关联的交易密钥，并基于来自管理设备的业务信息(例如包括用户个数N和第一预定值M)，将交易密钥拆分成与用户组中的用户个数相同的多个子密钥，然后向所述管理设备发送经对应用户公钥加密的子密钥。

[0034] 在一些实施例中，用户设备(例如120-3)被管理设备110指定或随机确定为用于恢复交易密钥的恢复用户的用户设备。该用户设备 120-3可以获取恢复消息(例如包括同意本次交易的确认用户的个数和恢复用户的标识)，以及当确认确认用户的个数大于或等于第一预定值时，基于确认用户的子密钥，恢复交易密钥，以便对本次交易的交易请求进行签名。

[0035] 图2示出了根据本公开的实施例的用于管理密钥的方法200的流程图。在图2中，各个动作例如由用于管理密钥的主用户的用户设备所执行。方法200还可以包括未示出的附加动作和/或可以省略所示出的动作，本公开的范围在此方面不受限制。

[0036] 在框202处，响应于用户被确定为用于拆分交易密钥的主用户，在该主用户的用户

设备120处，获取用户组的用户个数N和第一预定值，其中第一预定值指示恢复交易密钥的最小用户个数M，用户组用于管理交易密钥。在一些实施例中，M小于用户组中的用户个数N。在一些实施例中，主用户例如是由管理设备在用户组中指定或随机确定。在一些实施例中，用于拆分交易密钥的主用户与用于创建用户组时的组队主用户可以是同一用户，也可以是不同的用户。在一些实施例中，用户设备包括具有处理单元的硬件USB KEY。

[0037] 在框204处，基于来自管理设备的关于其他用户的消息，随机产生与本次交易的处理权限相关联的交易密钥，关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥。在上述方案中，通过在主用户的用户设备处，随机产生与本次交易的处理权限相关联的交易密钥，能够降低因交易密钥固定不变或者被重复使用而导致的易被破解的风险。

[0038] 在一些实施例中，关于其他用户的消息还指示以下至少一项：管理设备的证书、用于验证其他用户的公钥的签名信息、其他用户的标识、其他用户的合并数据的哈希值的签名信息、以及关于其他用户的消息的有效期。关于其他用户的合并数据的哈希值的签名信息，在一些实施例中，管理设备首先对用户组中的每一个其他用户哈希计算以下合并数据：管理设备证书的哈希值、其他用户在用户组的编号的哈希值、其他用户的公钥的哈希值和其他用户对用户组密码的签名哈希值；然后利用管理设备的公钥对该合并数据的哈希值进行签名，以便主用户的用户设备对关于其他用户的消息中各项数据进行验证。在上述方案中，通过在关于其他用户的消息中包括经签名的其他用户合并数据的哈希值，以方便主用户验证所接收的该关于其他用户的消息的各项数据是否经过篡改。

[0039] 关于随机产生交易密钥，在一些实施例中，其包括：响应于确认管理设备的证书通过验证，基于其他用户的公钥的签名信息，确认其他用户的公钥是否通过验证；以及响应于其他用户的公钥通过验证，随机产生与第一预定值相同的多个用于构建拆分多项式的随机数，该多个用于构建拆分多项式的随机数包括交易密钥。

[0040] 在框206处，将交易密钥拆分成与用户个数相同的多个子密钥，多个子密钥中的每一个子密钥与用户组中的一个用户相对应。在一些实施例中，其中将交易密钥拆分成多个子密钥包括：基于用户组用户个数和多个用于构建拆分算法的随机数，确定多个子密钥，其中每一个子密钥包括第一子密钥数据和第二子密钥数据。

[0041] 关于交易密钥的拆分，可以采用多种方式。在一些实施例中，可以而不限于基于以下拆分多项式(1)，将交易密钥拆分成多个子密钥。

[0042] $Y=A_0+A_1*X+A_2*X^2+\cdots\cdots+A_{N-1}*X^{M-1}$ (1)

[0043] 在上述拆分多项式中，M表示恢复所述交易密钥的最小用户个数。A_0、$A_1\cdots\cdots A_{M-1}$表示用于构建拆分算法的随机数，上述随机数是由主用户的用户设备随机产生的与恢复所述交易密钥的最小用户个数M相同的随机数。例如，A_0可以表示用于本次交易的交易密钥。当A_0至A_{M-1}、M已经确定时，可以用于构建N个(X,Y)对，例如确定与用户组的用户个数N相同的X_1至X_N，可以基于上述拆分多项式获得N个确定的Y值，例如是Y_1至Y_N。上述基于多项式所确定N个(X,Y)对，即：(X_1,Y_1)、$(X_2,Y_2)\cdots\cdots(X_N,Y_N)$表示被拆分的与用户组的N个用户对应的N个子密钥。基于上述拆分多项式、用户组的用户个数N、恢复所述交易密钥的最小用户个数M和主用户的用户设备随机产生的随机数A_0至A_{M-1}，可以将交易密钥A_0拆分成与用户组中的用户个数相同的N个子密钥(X_1,Y_1)、$(X_2,Y_2)\cdots\cdots(X_N, Y_N)$。其中，每一个子密钥(X,Y)包括第一子密

钥数据X和第二子密钥数据Y。在上述方案中，通过将主用户随机产生的交易密钥A_0拆分成与用户组中的用户个数相同的多个子密钥，不仅能够有效避免因交易密钥固定而导致的易被破解的风险，而且由于拥有子密钥的单个用户无法独立恢复交易密钥，只有最小用户个数(M)个用户协作才能恢复交易密钥，因此显著地提高了交易密钥的安全性。在一些实施例中，M也可以小于用户组中的用户个数N。通过设置恢复交易密钥的最小用户个数M，并且使得M<N，能够使得本公开的示例实施例所提出的用于管理密钥的方案即便在个别用户出现问题的情况下，依然可以通过M个用户的协作而恢复交易密钥。因而提高了权限管理系统的可靠性。

[0044] 在框208处，向管理设备发送多个经加密的子密钥，其中每一个经加密的子密钥经由与子密钥相对应的用户的公钥加密。在一些实施例中，经由与子密钥对应的用户的公钥加密包括：基于与子密钥对应的用户的公钥和关于其他用户的消息的有效期，加密子密钥。在上述方案中，通过利用对应用户的公钥加密的子密钥，提高了每个子密钥的安全性，即便他人获知该经加密的子密钥，也会因为无法获得对应用户的私钥，而不能破译该子密钥。因此提高了交易密钥的安全性。另外，由于将上述经加密的子密钥发送给管理设备，管理设备可以缓存上述经加密的子密钥，因此，不需要用户组的其他用户同步操作以便接收子密钥，因而实现了交易密钥拆分与分发的异步。

[0045] 在一些实施例中，方法200还包括主用户的用户设备的初始化动作。例如，主用户的用户设备响应于确认来自管理设备的签名数据通过验证，基于预置在用户设备中的私钥，对签名数据进行签名，签名数据至少包括经由管理设备签名的随机数；以及响应于用户被确定为用于组建用户组的组队主用户，向管理设备发送关于用户组的业务信息、用户设备的公钥和经由用户设备私钥签名的签名数据，业务信息至少包括用户组的用户个数和第一预定值。在上述方案中，通过对管理设备的签名信息进行验证，以及将经由主用户的用户设备私钥签名的签名信息发给管理设备以便验证，能够实现主用户的用户设备与管理设备之间的互信，提高权限管理系统的安全性。另外，通过将包括用户组的用户个数N和第一预定值M的业务信息发送给管理设备，以方便管理设备协助进行交易密钥的拆分与恢复过程。

[0046] 图3示出了根据本公开的实施例的用于管理密钥的方法300的流程图。在图3中，各个动作例如由用于管理密钥的恢复用户的用户设备执行。方法300还可以包括未示出的附加动作和/或可以省略所示出的动作，本公开的范围在此方面不受限制。

[0047] 在框302处，响应于用户被确定为用于恢复交易密钥的恢复用户，在该恢复用户的用户设备处，获取来自管理设备的、用于恢复交易密钥的恢复消息，其中恢复消息至少指示用户组中同意本次交易的确认用户的个数和恢复用户的标识，其中用户组用于管理交易密钥。在一些实施例中，恢复用户由管理设备在用户组中指定或随机确定。在一些实施例中，恢复消息还指示以下至少一项：与本次交易相关联的关联随机数、经由恢复用户的公钥签名的确认用户的子密钥和关联随机数、确认用户的签名信息、管理设备的证书、以及恢复消息的哈希值的签名信。

[0048] 在框304处，响应于确认确认用户的个数大于或等于第一预定值，基于从管理设备获取的确认用户的子密钥，确定交易密钥，确认用户的子密钥是经由事先拆分交易密钥而生成的。在一些实施例中，其中确认用户的子密钥由确认用户发送给管理设备，并且确认用户的子密钥经由恢复用户的公钥加密。在一些实施例中，其中确认用户的子密钥经由恢复

用户的公钥加密包括:在确认用户处,基于经由管理设备获取的恢复用户的公钥,对确认用户的子密钥和与本次交易相关联的关联随机数进行加密。在上述方案中,通过利用与本次交易相关联的关联随机数对子密钥签名,使得子密钥仅能用于本次交易的交易密码的恢复,而不能被重复用在其他交易的交易密码的恢复。

[0049] 在一些实施例中,可以而不限于基于以下上文提及的拆分多项式 (1)来恢复交易密钥。鉴于拆分多项式(1)中随机数的个数为M 个,即A_0至A_{M-1}。因此在获取至少M个确认用户的子密钥(X_1,Y_1)、(X_2,Y_2)……(X_M,Y_M)的情况下,可以通过求解M个随机数A_0至 A_{M-1},进而获取交易密钥A_0。

[0050] 在框306处,基于所确定的交易密钥,对关于本次交易的交易请求进行签名。在一些实施例中,恢复用户的用户设备向管理设备发送该经签名的本次交易请求,以用于本次交易的执行。

[0051] 在上述方案中,通过设置恢复交易密钥的最小用户个数(即,第一预定值),并响应于确认用户的个数大于或等于第一预定值,基于恢复用户的子密钥和确认用户的子密钥来恢复交易密钥,使得能够基于用户组中部分用户的协作而恢复交易密钥,因而,提高了权限管理系统的可靠性和强健性,使其能够抵抗一些涉及权限使用的不当行为。

[0052] 图4示出了根据本公开的实施例的用于管理密钥的方法400的流程图。在图4中,各个动作例如由用于管理密钥的管理设备110所执行。方法400还可以包括未示出的附加动作和/或可以省略所示出的动作,本公开的范围在此方面不受限制。

[0053] 在框402处,在管理设备处,从用于创建用户组的组队主用户的用户设备获取关于用户组的业务信息,业务信息至少指示用户组的用户个数和第一预定值,第一预定值指示恢复交易密钥的最小用户个数,用户组用于管理交易密钥。在一些实施例中,管理设备在用户组中随机确定以下各项中的至少一项:主用户和用于恢复交易密钥的恢复用户。在一些实施例中,该主用户是创建用户组时的组队主用户,也是用于拆分交易密钥的主用户。在一些实施例中,用户设备包括具有处理单元的硬件USB KEY。

[0054] 在框404处,向用于拆分交易密钥的主用户的用户设备发送关于其他用户的消息,其中关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥。

[0055] 关于用户组通过验证,在一些实施例中,其包括:响应于来自用户组中用户的用户设备的报到请求,向用户设备发送管理设备的签名数据,签名数据至少包括经由管理设备签名的随机数;基于来自用户设备的签名数据,确认用户设备是否通过验证,签名数据由用户设备响应于确认管理设备通过验证,基于预置在用户设备中的私钥,对随机数进行签名而生成的;以及响应于确认用户组中每一个用户的用户设备通过验证,确认用户组通过验证。在一些实施例中,用户设备包括具有处理单元的硬件USB KEY。在上述方案中,通过管理设备与用户组中每一个用户的用户设备的相互验证,能够实现用户组的各用户设备与管理设备之间的互信,以便提高信息交换的安全性。

[0056] 在框406处,获取来自主用户的、与用户组的用户个数相同的多个子密钥,其中多个子密钥经由主用户对交易密钥拆分而生成,并且多个子密钥经由对应的用户的公钥加密。

[0057] 在框408处,将多个子密钥缓存,以用于发送给相对应的用户。在上述方案中,由于管理设备能够缓存来自主用户的用户设备的经加密的子密钥,因此,不需要用户组的其他

用户同步操作以便接收子密钥,因而实现了交易密钥拆分和分发的异步。

[0058] 在一些实施例中,方法400还包括:响应于接收到关于本次交易的请求,向用户组的用户发送用于确认是否同意本次交易的交易信息,其中交易信息至少指示本次交易的交易内容和恢复用户的标识;获取用户组中同意本次交易的每个确认用户的子密钥,其中确认用户的子密钥经由恢复用户的公钥签名;以及响应于确认满足本次交易的条件,向恢复用户发送用于恢复交易密钥的恢复消息。前文提及的"满足本次交易的条件"例如是:用户组中同意本次交易的确认用户的个数大于或等于第一预定值;也可以是:满足关于本次交易的其他预设条件,例如,达到本次交易的预设执行时间。在一些实施例中,确认用户的子密钥经由确认用户的公钥和与所述本次交易相关联的关联随机数进行加密。在上述方案中,对确认用户的子密钥和与本次交易相关联的关联随机数进行加密,使得子密钥仅能用于本次交易的交易密码的恢复,因而提高了权限管理的安全性。

[0059] 图5示出了根据本公开的实施例的用于管理密钥的管理系统500 的数据流向图。在图5中,各个动作例如由管理设备502、主用户的用户设备504、恢复用户的用户设备506、和其他用户的用户设备508 来实现。方法500主要包括用户组组队(例如包括组队主用户初始化、其他用户初始化)、交易密钥拆分和交易密钥恢复的阶段。应当理解,方法500还可以包括未示出的附加动作和/或可以省略所示出的动作,本公开的范围在此方面不受限制。这里,管理设备502例如可以是如上结合图1所描述的管理设备110,用户设备504、506、508例如可以是如上结合图1所描述的用户设备120。

[0060] 以下示例用户组组队阶段的各个动作。用户组组队阶段主要包括组队主用户的初始化、用户组的其他用户的初始化的阶段。

[0061] 以下示例用户组组队阶段的主用户的初始化阶段的各个动作。

[0062] 主用户的用户设备504处,在510,创建主用户的私钥K1和公钥P1。在512,创建用户组的密码。在514,向管理设备502发送验证请求。其中主用户例如是被指定或随机确定为用于组建用户组的组队主用户。

[0063] 管理设备502处,在516,利用管理设备的私钥K0对管理设备 502所产生的、用于主用户身份验证的随机数R1进行签名。在518,向主用户的用户设备504发送签名数据,该签名数据例如包括随机数 R1、经签名的随机数R1和管理设备502的证书,其中管理设备502 的证书例如包括管理设备502的公钥P0。

[0064] 主用户的用户设备504处,在520,确认来自管理设备502的签名数据是否通过验证。例如,确认所接收的管理设备502的证书和经管理设备502签名的随机数是否通过验证。在522,响应于确认来自管理设备502的签名数据通过验证,利用主用户的用户设备504的私钥K1对随机数R1和用户组的密码进行签名。在524,向管理设备 502发送关于用户组的业务信息、用户设备504的公钥P1、经由用户设备504的私钥K1签名的签名数据,其中该业务信息至少包括用户组的用户个数N和第一预定值M。

[0065] 管理设备502处,在526,基于所获取的用户设备504的公钥P1,验证经由用户设备504的私钥K1签名的随机数R1,以及缓存用户组的密码。

[0066] 以下示例用户组组队阶段的其他用户的初始化阶段的各个动作。

[0067] 在一些实施例中,主用户的用户设备504可以通过多种方式向用户组的其他用户分享所组建的用户组的链接和用户组的密码。例如。主用户的用户设备504通过局域网将用

户组的链接和用户组的密码分享给用户组中的其他用户。例如，其他用户的用户设备508是用户组中除主用户之外的任一用户的用户设备。

[0068] 其他用户的用户设备508处，在530，创建其他用户的用户设备 508的私钥K2和公钥P2。在532，基于用户组的链接和用户组的密码，与管理设备502建立联系，以及向管理设备502发送验证请求。

[0069] 管理设备502处，在534，合并以下数据：管理设备的证书的哈希值、主用户的用户设备504的公钥P1的哈希值、主用户对用户组密码的签名的哈希值和用于其他用户身份验证的随机数R2。在536，利用管理设备502的私钥KO对该合并数据的哈希值进行签名。在538，向其他用户设备508发送管理设备502的证书、主用户的用户设备504的公钥P1、主用户对用户组密码的签名和随机数R2、以及对合并数据的哈希值的签名。

[0070] 用户设备508处，在540，确认管理设备502是否通过验证。在 542，确认主用户的用户设备504的公钥P1是否通过验证。在544，利用用户设备508的私钥K2对用户组的密码签名，以及利用用户设备508的私钥K2对随机数R2签名。在546，向管理设备发送用户设备508的公钥P2和经由私钥K2签名的签名数据，该签名数据例如包括经由私钥K2签名的用户组密码和随机数R2。

[0071] 管理设备502处，在548，基于所获取的用户设备508的公钥P2，验证经由用户设备508的私钥K2签名的随机数R2，以及缓存用户组的密码。在550，对用户组的所有用户进行编号。

[0072] 以下示例拆分交易密钥的阶段的各个动作。

[0073] 管理设备502处，在552，响应于接收到拆分交易密钥的请求，在用户组中随机确定用于拆分交易密钥的主用户。该用于拆分交易密钥的主用户与创建用户组的组队主用户可以是同一用户，也可以是不同的用户，以下示例为同一用户，其用户设备为504。在554，对用户组中的每一个其他用户哈希计算以下合并数据：管理设备502的证书的哈希值、其他用户在用户组中的编号的哈希值、其他用户的公钥的哈希值和其他用户对用户组密码的签名的哈希值。在556，向主用户的用户设备502发送关于其他用户的消息，该关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥。在一些实施例中，关于其他用户的消息还指示以下至少一项：管理设备502的证书、其他用户的公钥、其他用户对用户组密码的签名、合并数据哈希值的签名以及关于其他用户的消息的有效期。在558，向主用户的用户设备 504发送用户组的业务信息，该业务信息至少包括用户组的用户个数 N和第一预定值M。

[0074] 主用户的用户设备504处，在560，响应于确认管理设备502的证书通过验证，基于其他用户的公钥的签名信息，确认其他用户的公钥是否通过验证。在562，响应于其他用户的公钥通过验证，随机产生与恢复所述交易密钥的最小用户个数M相同的随机数A_0至A_{M-1}。A_0表示用于本次交易的交易密钥。在564，基于恢复所述交易密钥的最小用户个数M和主用户的用户设备504随机产生的随机数A_0至 A_{M-1}，构建用于拆分交易密钥的多项式。在566，将交易密钥A_0拆分成与用户组中的用户个数相同的N个子密钥(X_1,Y_1)、(X_2,Y_2)……(X_N, Y_N)，其中每一个子密钥与用户组中的一个用户相对应。在568，用户设备504基于与子密钥对应的用户的公钥和有效期，分别加密各子密钥。在570，向管理设备502发送多个经加密的子密钥。

[0075] 管理设备502处，在572，缓存多个经加密的子密钥(X_1,Y_1)、$(X_2, Y_2)\cdots\cdots(X_N,Y_N)$。在一些实施例中，在574，通知其他用户的用户设备508，例如可以通知用户设备508插入相对应的硬件安全设备(如 USB KEY)130。在576，响应于接收到来自其他用户设备508的关于下发子密钥的请求，向其他用户的用户设备508发送以下至少一项：管理设备502的证书、其他用户的编号、主用户的公钥、子密钥、有效期和上述合并数据的哈希值签名。在上述方案中，由于管理设备502 缓存经加密的子密钥，以及响应于用户组的其他用户的下发子密钥的请求而发送相应子密钥，因此能够实现交易密钥拆分与分发的异步。不需要用户组的其他用户同步或实时操作，因而提高了权限管理系统的方便性。

[0076] 其他用户的用户设备508处，在578，验证管理设备502的证书和公钥，以及保存经解密的相应的子密钥。以下示例恢复交易密钥的阶段的各个动作。

[0077] 管理设备502处，在580，在用户组中指定或者随机确定恢复用户。在582，响应于接收到关于本次交易的请求，向用户组的用户发送用于确认是否同意本次交易的交易信息，其中交易信息至少指示本次交易的交易内容和恢复用户的标识。在584，获取所述用户组中同意本次交易的每个确认用户的子密钥，其中确认用户的子密钥经由恢复用户的公钥签名。在586，响应于确认满足本次交易的条件(例如用户组中同意本次交易的确认用户的个数大于或等于第一预定值)，向恢复用户发送用于恢复交易密钥的恢复消息，其中恢复消息至少包括以下一项：确认用户的个数和恢复用户的标识、管理设备的证书、交易数据、与本次交易相关联的关联随机数、经由恢复用户的公钥签名的其他用户的子密钥和关联随机数、用于验证恢复消息的哈希值。

[0078] 恢复用户的用户设备506处，在获取来自管理设备的、用于恢复交易密钥的恢复消息之后。在588，响应于确认确认用户的个数大于或等于第一预定值，从管理设备获取的确定用户的子密钥，确定交易密钥，确定用户的子密钥是经由事先拆分交易密钥而生成的。在590，基于所确定的交易密钥，对关于本次交易的交易请求进行签名，以用于本次交易的执行。

[0079] 通过采用上述方法500，不仅能够显著地提高了交易密钥的安全性，而且能够在个别用户出现问题的情况下，依然可以通过M个用户的协作而恢复交易密钥，因而提高了权限管理系统的可靠性。

[0080] 图6示意性示出了适于用来实现本公开实施例的电子设备600的框图。设备600可以用于实现图1和图5的用户设备和管理设备中的一个或多个主机。如图所示，设备600包括中央处理单元(CPU)601，其可以根据存储在只读存储器(ROM)602中的计算机程序指令或者从存储单元608加载到随机访问存储器(RAM)603中的计算机程序指令，来执行各种适当的动作和处理。在RAM603中，还可存储设备 600操作所需的各种程序和数据。CPU 601、ROM 602以及RAM603 通过总线604彼此相连。输入/输出(I/O)接口605也连接至总线604。

[0081] 设备600中的多个部件连接至I/O接口605，包括：输入单元606，例如键盘、鼠标等；输出单元607，例如各种类型的显示器、扬声器等；存储单元608，例如磁盘、光盘等；以及通信单元609，例如网卡、调制解调器、无线通信收发机等。通信单元609允许设备600通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/ 数据。

[0082] 处理单元601执行上文所描述的各个方法和处理，例如执行用于管理密钥的方法200、300、400、500。例如，在一些实施例中，方法 200、300、400和500可被实现为计算机软件

程序,其被存储于机器可读介质,例如存储单元608。在一些实施例中,计算机程序的部分或者全部可以经由ROM 602和/或通信单元609而被载入和/或安装到设备600上。当计算机程序加载到RAM 603并由CPU 601执行时,可以执行上文描述的方法200、300、500的一个或多个操作。备选地,在其他实施例中,CPU 601可以通过其他任何适当的方式(例如,借助于固件)而被配置为执行方法200、300、400和500的一个或多个动作。

[0083] 然而,本领域技术人员可以理解,在根据本公开中所述的用户设备是集成有通信和处理功能模块的硬件安全设备130的情况下,该用户设备可以不包含如上结合图6所述的一个或多个组件。

[0084] 本公开可以是方法、装置、系统和/或计算机程序产品。计算机程序产品可以包括计算机可读存储介质,其上载有用于执行本公开的各个方面的计算机可读程序指令。

[0085] 计算机可读存储介质可以是可以保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以是但不限于电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。计算机可读存储介质的更具体的例子 (非穷举的列表)包括:便携式计算机盘、硬盘、随机存取存储器 (RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM 或闪存)、静态随机存取存储器(SRAM)、便携式压缩盘只读存储器(CD-ROM)、数字多功能盘(DVD)、记忆棒、软盘、机械编码设备、例如其上存储有指令的打孔卡或凹槽内凸起结构、以及上述的任意合适的组合。这里所使用的计算机可读存储介质不被解释为瞬时信号本身,诸如无线电波或者其他自由传播的电磁波、通过波导或其他传输媒介传播的电磁波(例如,通过光纤电缆的光脉冲)、或者通过电线传输的电信号。

[0086] 这里所描述的计算机可读程序指令可以从计算机可读存储介质下载到各个计算/处理设备,或者通过网络、例如因特网、局域网、广域网和/或无线网下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光纤传输、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配卡或者网络接口从网络接收计算机可读程序指令,并转发该计算机可读程序指令,以供存储在各个计算/处理设备中的计算机可读存储介质中。

[0087] 用于执行本公开操作的计算机程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、或者以一种或多种编程语言的任意组合编写的源代码或目标代码,所述编程语言包括面向对象的编程语言—诸如Smalltalk、C++等,以及常规的过程式编程语言—诸如“C”语言或类似的编程语言。计算机可读程序指令可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络—包括局域网(LAN)或广域网(WAN)—连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。在一些实施例中,通过利用计算机可读程序指令的状态信息来个性化定制电子电路,例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA),该电子电路可以执行计算机可读程序指令,从而实现本公开的各个方面。

[0088] 这里参照根据本公开实施例的方法、装置(系统)和计算机程序产品的流程图和/

或框图描述了本公开的各个方面。应当理解，流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合，都可以由计算机可读程序指令实现。

[0089] 这些计算机可读程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理单元，从而生产出一种机器，使得这些指令在通过计算机或其它可编程数据处理装置的处理单元执行时，产生了实现流程图和/或框图中的一个或多个方框中规定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中，这些指令使得计算机、可编程数据处理装置和/或其他设备以特定方式工作，从而，存储有指令的计算机可读介质则包括一个制造品，其包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的各个方面的指令。

[0090] 也可以把计算机可读程序指令加载到计算机、其它可编程数据处理装置、或其它设备上，使得在计算机、其它可编程数据处理装置或其它设备上执行一系列操作步骤，以产生计算机实现的过程，从而使得在计算机、其它可编程数据处理装置、或其它设备上执行的指令实现流程图和/或框图中的一个或多个方框中规定的功能/动作。

[0091] 附图中的流程图和框图显示了根据本公开的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分，所述模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0092] 以上已经描述了本公开的各实施例，上述说明是示例性的，并非穷尽性的，并且也不限于所披露的各实施例。在不偏离所说明的各实施例的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择，旨在最好地解释各实施例的原理、实际应用或对市场中的技术改进，或者使本技术领域的其它普通技术人员能理解本文披露的各实施例。

[0093] 以上所述仅为本公开的可选实施例，并不用于限制本公开，对于本领域的技术人员来说，本公开可以有各种更改和变化。凡在本公开的精神和原则之内，所作的任何修改、等效替换、改进等，均应包含在本公开的保护范围之内。

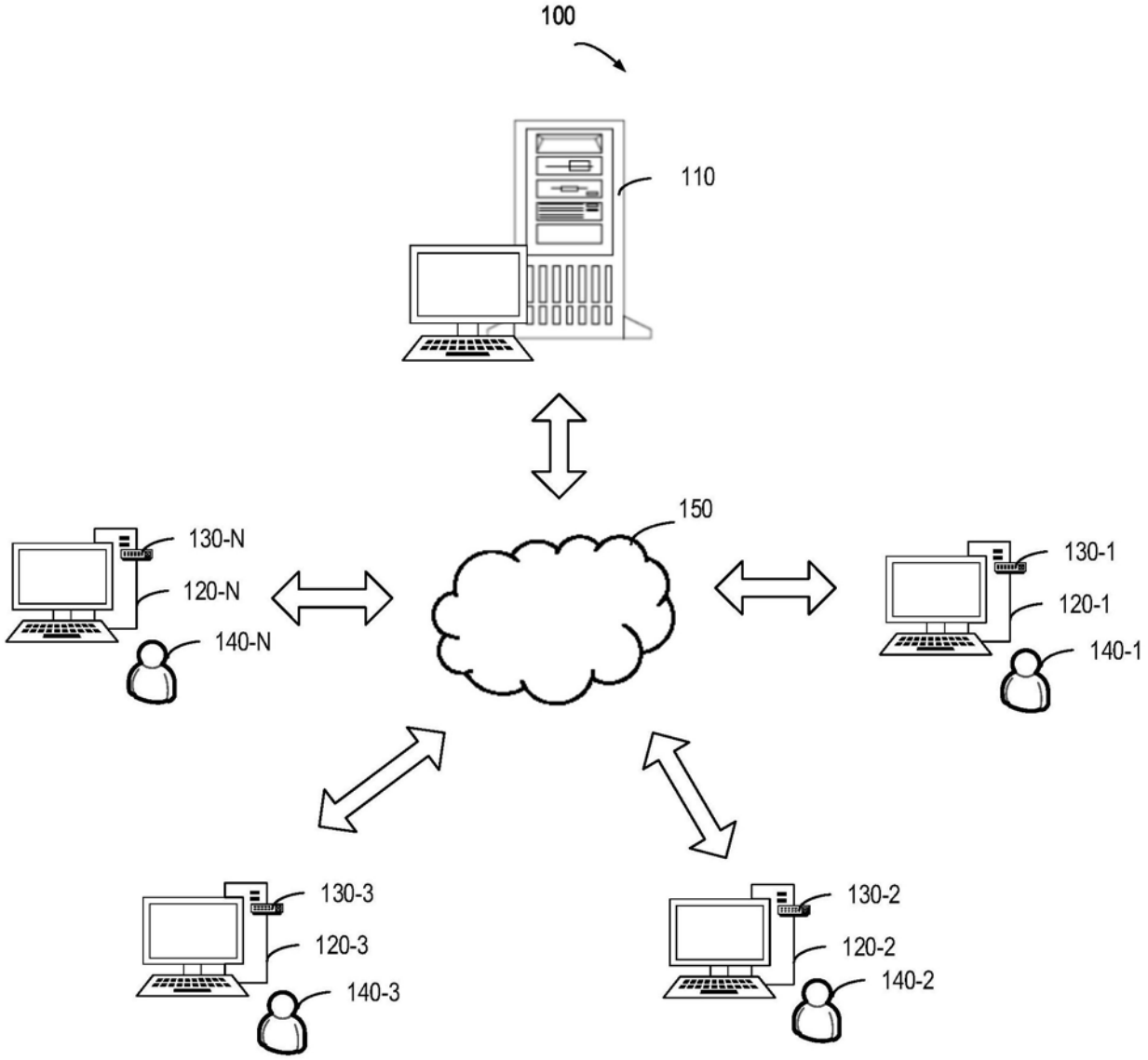

100
110
150
130-N
120-N
140-N
130-1
120-1
140-1
130-3
120-3
140-3
130-2
120-2
140-2

图1

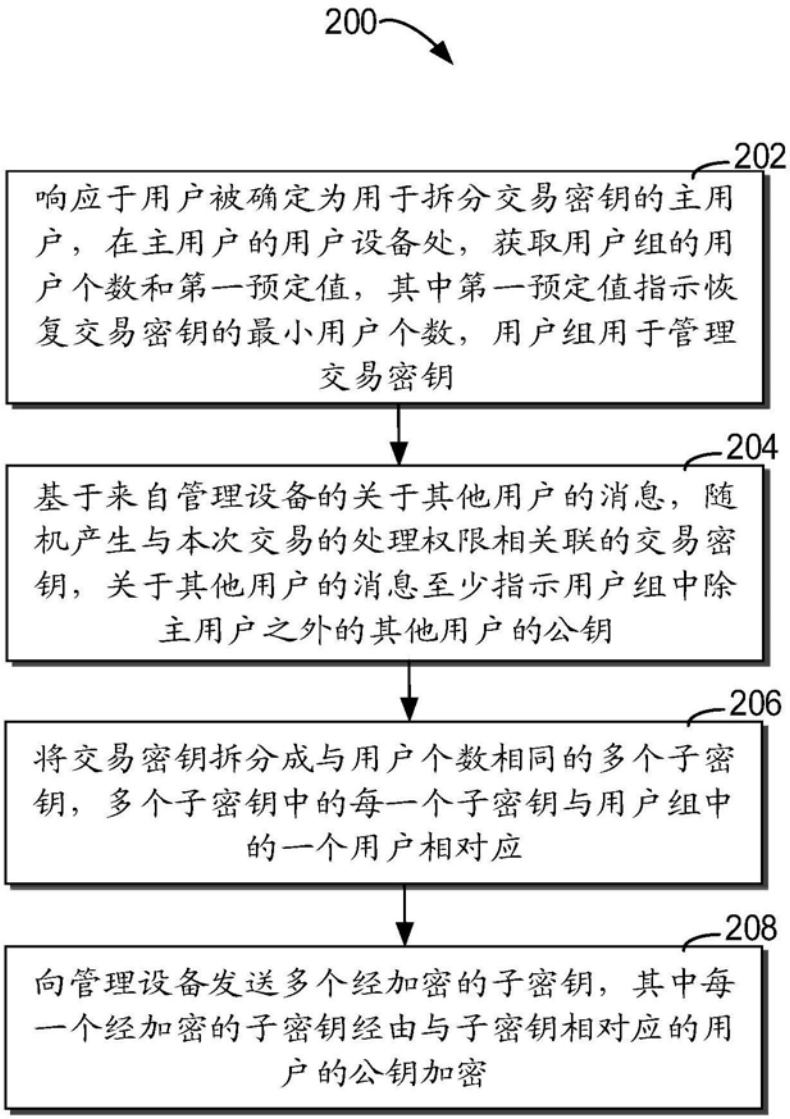

200
202
响应于用户被确定为用于拆分交易密钥的主用户，在主用户的用户设备处，获取用户组的用户个数和第一预定值，其中第一预定值指示恢复交易密钥的最小用户个数，用户组用于管理交易密钥
204
基于来自管理设备的关于其他用户的消息，随机产生与本次交易的处理权限相关联的交易密钥，关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥
206
将交易密钥拆分成与用户个数相同的多个子密钥，多个子密钥中的每一个子密钥与用户组中的一个用户相对应
208
向管理设备发送多个经加密的子密钥，其中每一个经加密的子密钥经由与子密钥相对应的用户的公钥加密

图2

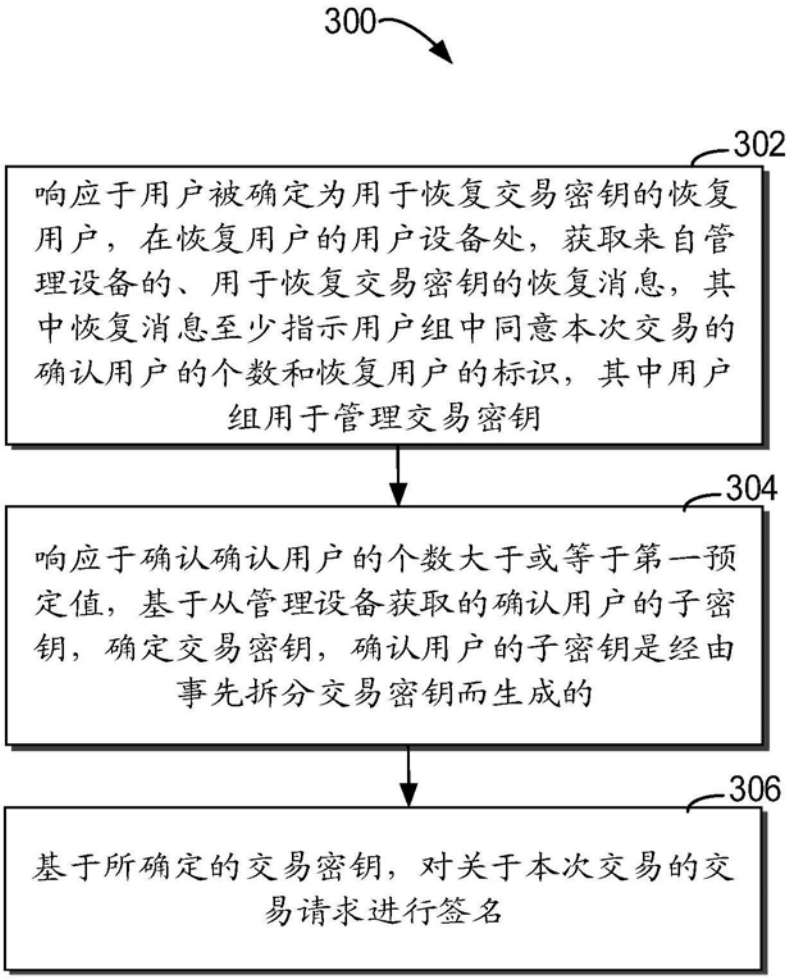

300
302
响应于用户被确定为用于恢复交易密钥的恢复用户，在恢复用户的用户设备处，获取来自管理设备的、用于恢复交易密钥的恢复消息，其中恢复消息至少指示用户组中同意本次交易的确认用户的个数和恢复用户的标识，其中用户组用于管理交易密钥
304
响应于确认确认用户的个数大于或等于第一预定值，基于从管理设备获取的确认用户的子密钥，确定交易密钥，确认用户的子密钥是经由事先拆分交易密钥而生成的
306
基于所确定的交易密钥，对关于本次交易的交易请求进行签名

图3

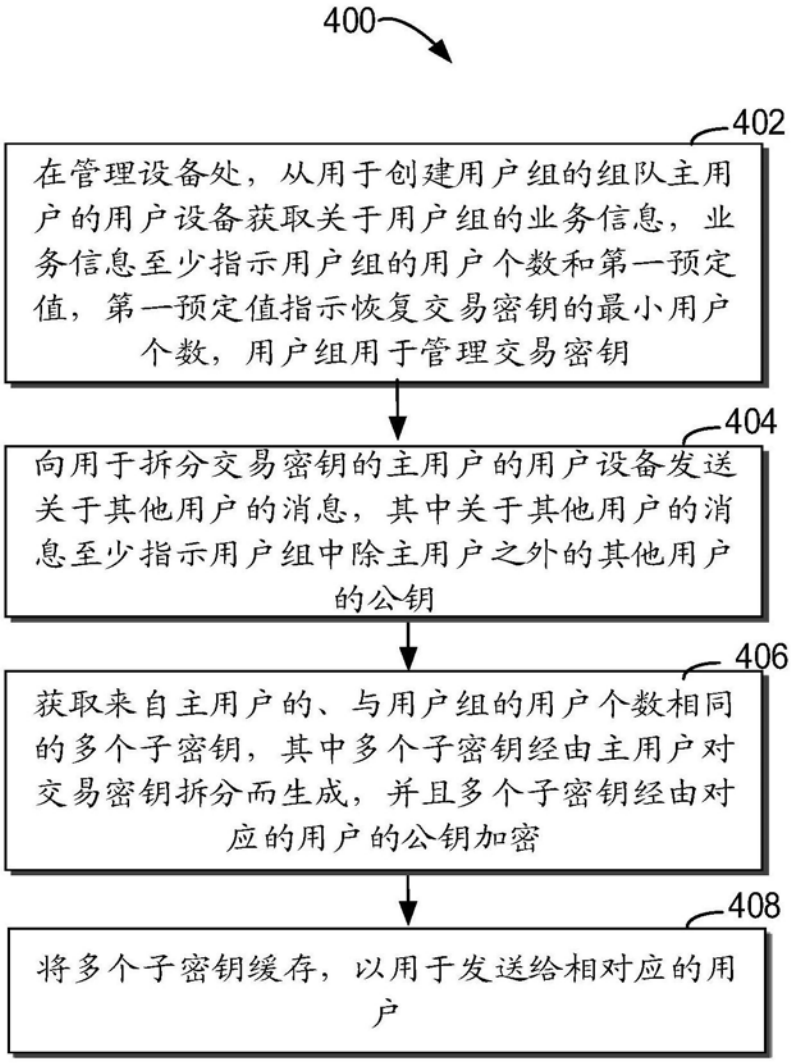

400
402
在管理设备处，从用于创建用户组的组队主用户的用户设备获取关于用户组的业务信息，业务信息至少指示用户组的用户个数和第一预定值，第一预定值指示恢复交易密钥的最小用户个数，用户组用于管理交易密钥
404
向用于拆分交易密钥的主用户的用户设备发送关于其他用户的消息，其中关于其他用户的消息至少指示用户组中除主用户之外的其他用户的公钥
406
获取来自主用户的、与用户组的用户个数相同的多个子密钥，其中多个子密钥经由主用户对交易密钥拆分而生成，并且多个子密钥经由对应的用户的公钥加密
408
将多个子密钥缓存，以用于发送给相对应的用户

图4

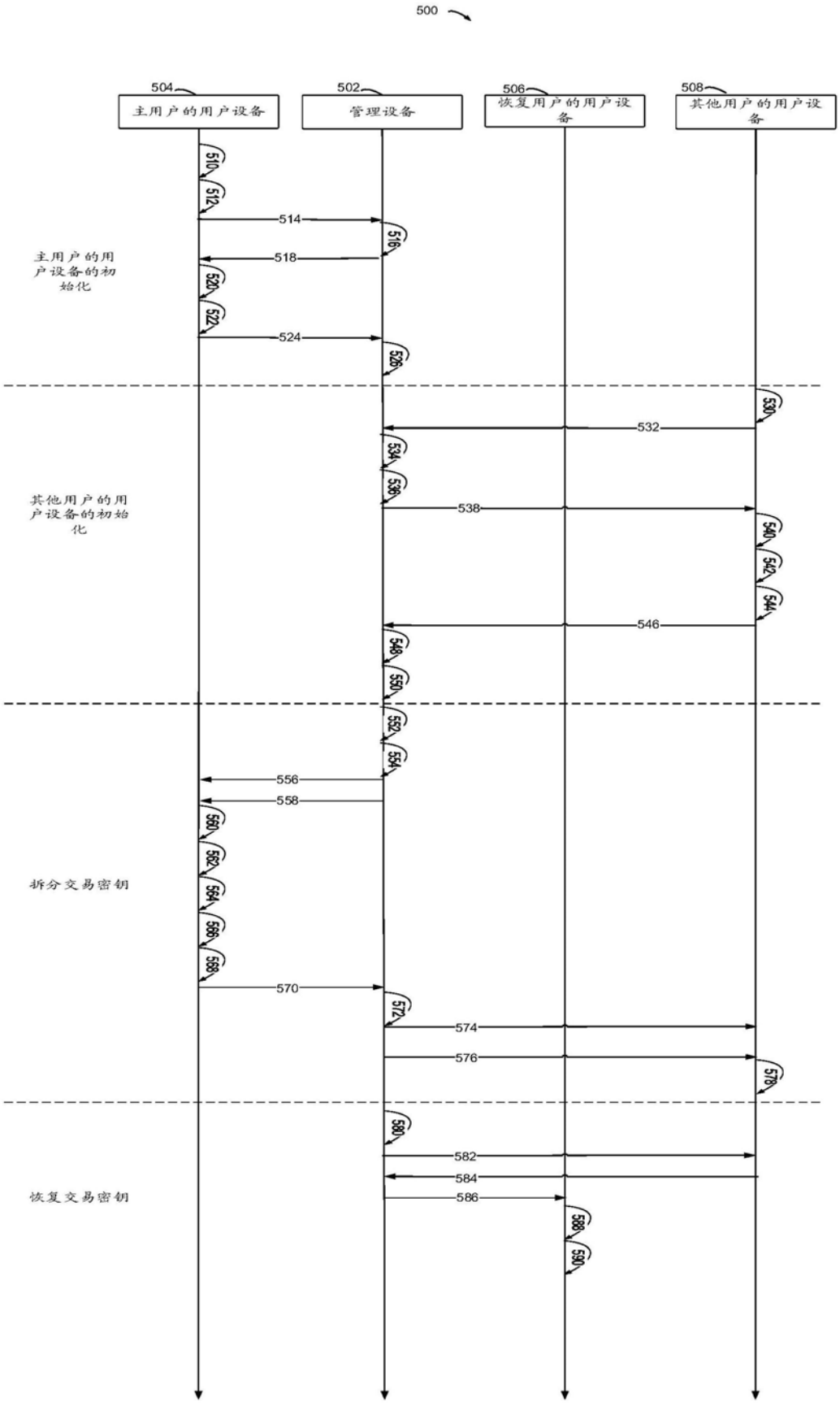

500
504
主用户的用户设备
502
管理设备
506
恢复用户的用户设备
508
其他用户的用户设备
510
512
514
516
518
主用户的用户设备的初始化
520
522
524
526
530
532
534
536
538
其他用户的用户设备的初始化
540
542
544
546
548
550
552
554
556
558
560
562
564
566
568
拆分交易密钥
570
572
574
576
578
580
582
584
586
588
590
恢复交易密钥

图5

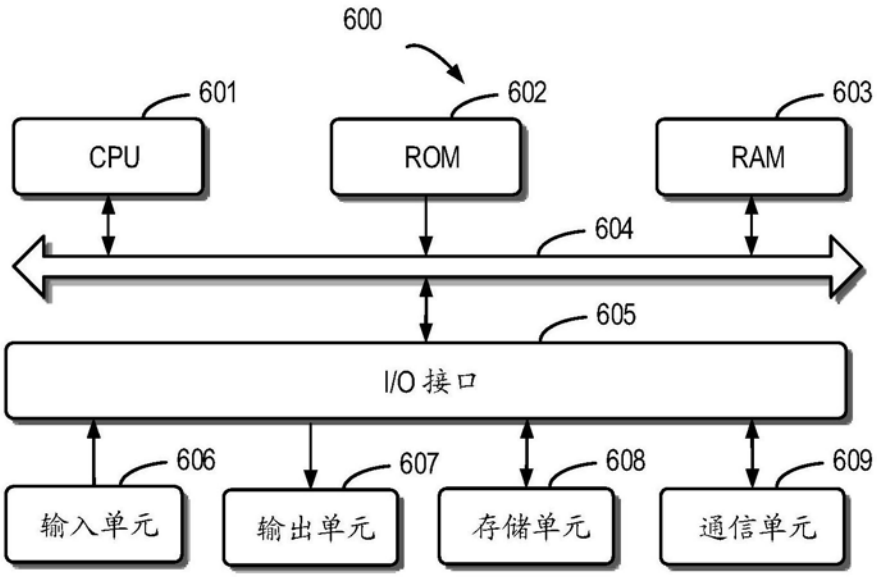

600
601
602
603
CPU
ROM
RAM
604
605
I/O 接口
606
607
608
609
输入单元
输出单元
存储单元
通信单元

图6