



(12)发明专利

(10)授权公告号 CN 103999400 B

(45)授权公告日 2016.10.12

(21)申请号 201180074627.6

(22)申请日 2011.12.28

(65)同一申请的已公布的文献号

申请公布号 CN 103999400 A

(43)申请公布日 2014.08.20

(85)PCT国际申请进入国家阶段日

2014.05.04

(86)PCT国际申请的申请数据

PCT/KR2011/010253 2011.12.28

(87)PCT国际申请的公布数据

W02013/100224 EN 2013.07.04

(73)专利权人 仁荷大学校产学协力团

地址 韩国,仁川

(72)发明人 李文揆

(74)专利代理机构 北京市铸成律师事务所

11313

代理人 孟锐

(51)Int.Cl.

H04L 9/32(2006.01)

H04L 9/28(2006.01)

(56)对比文件

CN 1655498 A,2005.08.17,

WO 2007/114623 A1,2007.10.11,

CN 102187618 A,2011.09.14,

审查员 刘锐

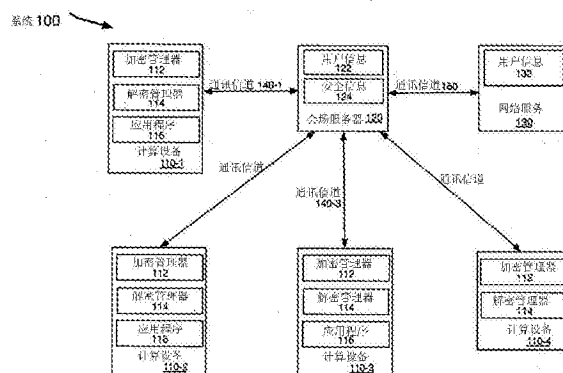
权利要求书4页 说明书16页 附图10页

(54)发明名称

用于安全地共享数据的基于喜好的认证方式

(57)摘要

实例被公开用于变换用于计算设备用户的与感兴趣领域相关的喜好的多维属性值,且通过使用被变换的多维属性值加密或解密密文,以与另一计算设备安全地共享数据。



1. 一种方法,包括:

产生第一化名,以至少暂时地识别第一计算设备,所述第一计算设备关联于具有与感兴趣领域相关的第一喜好的第一用户,所述第一喜好具有多维属性值;

产生第一会话密钥,以与所述化名一起使用,从而与一个或多个其他计算设备安全地共享在第一计算设备上维护的数据;

产生变换参数;

通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值;

通过使用一维属性值加密化名和会话密钥,以产生第一密文;以及

向第一计算设备和所述一个或多个其他计算设备都可访问的服务器传送第一密文和变换参数,其中,服务器维护第一密文和变换参数。

2. 如权利要求1所述的方法,还包括:

从在所述一个或多个其他计算设备之中的第二计算设备接收第二化名和第二会话密钥;以及

基于基本类似于第一化名的第二化名和基于基本类似于第一会话密钥的第二会话密钥建立与第二计算设备的安全会话。

3. 如权利要求2所述的方法,其中,建立与第二计算设备的安全会话包括共享与感兴趣领域关联的数据。

4. 如权利要求1所述的方法,其中,多维属性值包括至少部分地以对于将第一喜好特征化的两个或多个属性的单独分配值为基础的多维属性值。

5. 如权利要求4所述的方法,其中,所述对于将第一喜好特征化的两个或多个属性的单独分配值包括与第一轴线关联的第一值和与第二轴线关联的第二值,第一轴线正交于第二轴线。

6. 如权利要求5所述的方法,其中,通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值包括在预定义有限域上将多维属性值变换成一维属性值,并且将一维属性值映射到单一轴线。

7. 如权利要求1所述的方法,其中,产生变换参数包括响应于建立和完成与所述一个或多个其他计算设备之中的第二计算设备的安全会话而产生新的变换参数,所述建立和完成的安全会话用于包括共享与感兴趣领域关联的数据。

8. 如权利要求1所述的方法,其中,通过使用一维属性值加密化名和会话密钥包括实施至少一部分容错型加密方案以产生第一密文。

9. 如权利要求1所述的方法,其中,具有多维属性值的第一喜好包括从第一计算设备和所述一个或多个其他计算设备都可访问的服务器提供给第一计算设备的多维属性值,多维属性值至少部分地基于与第一用户关联的信息。

10. 如权利要求1所述的方法,其中,具有多维属性值的第一喜好包括由第一计算设备至少部分地以从第一计算设备和所述一个或多个其他计算设备都可访问的服务器提供给第一计算设备的一般问题为基础确定的多维属性值,所述一般问题与第一用户在感兴趣领域中的偏好相关。

11. 如权利要求1所述的方法,其中,具有多维属性值的第一喜好包括由被第一计算设备维护的应用程序至少部分地以与第一用户关联的信息为基础确定的多维属性值。

12.一种方法,包括:

在第一计算设备处,从服务器接收第一密文和变换参数,所述密文和变换参数由第二计算设备产生;

接收对于第一计算设备的第一用户的第一喜好,所述第一喜好与感兴趣领域相关且具有多维属性值;

通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值;

通过使用一维属性值解密第一密文,以获取识别第二计算设备的化名和获取与所述化名一起使用的会话密钥,从而与第二计算设备安全地共享数据;

确定解密质量;以及

至少部分地基于所确定的超过阈值的解密质量启动与第二计算设备的安全会话,从而共享数据。

13.如权利要求12所述的方法,其中,确定解密质量至少部分地基于第一喜好与对于第二计算设备的第二用户的第二喜好的相似性,所述第二喜好也与感兴趣领域相关。

14.如权利要求12所述的方法,其中,接收第一喜好包括从服务器接收第一喜好,所述第一喜好至少部分地基于与第一用户关联的信息。

15.如权利要求14所述的方法,其中,与第一用户关联的信息包括对于第一用户的购买历史、对于第一用户的搜索历史、或对于第一用户的人口统计特征中的一个或多个。

16.如权利要求12所述的方法,其中,接收第一喜好包括至少部分地基于从服务器提供给第一计算设备的一般问题接收第一喜好,所述一般问题与第一用户在感兴趣领域中的偏好相关。

17.如权利要求12所述的方法,其中,接收第一喜好包括从由第一计算设备至少部分地以与第一用户关联的信息为基础维护的应用程序接收第一喜好,所述与第一用户关联的信息包括对于第一用户的购买历史、对于第一用户的搜索历史、或第一用户的人口统计特征中的一个或多个。

18.如权利要求12所述的方法,其中,所述多维属性值包括至少部分地以对于将第一喜好特征化的两个或多个属性的单独分配值为基础的多维属性值。

19.如权利要求18所述的方法,其中,所述对于将第一喜好特征化的两个或多个属性的单独分配值包括与第一轴线关联的第一值和与第二轴线关联的第二值,第一轴线正交于第二轴线。

20.如权利要求19所述的方法,其中,通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值包括在预定义有限域上将多维属性值变换成一维属性值,并且将一维属性值映射到单一轴线。

21.如权利要求12所述的方法,其中,通过使用一维属性值解密第一密文以获取化名和会话密钥包括实施至少一部分容错型解密方案以获取化名和会话密钥。

22.一种设备,包括:

具有逻辑的加密管理器,所述逻辑配置成:

产生第一化名,以至少暂时地识别第一计算设备,所述第一计算设备关联于具有与感兴趣领域相关的第一喜好的第一用户,所述第一喜好具有多维属性值;

产生第一会话密钥,以与所述化名一起使用,从而与一个或多个其他计算设备安全地

共享在第一计算设备上维护的数据；

产生变换参数；

通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值；

通过使用一维属性值加密化名和会话密钥，以产生第一密文；以及

向第一计算设备和所述一个或多个其他计算设备都可访问的服务器传送第一密文和变换参数，其中，服务器维护第一密文和变换参数。

23. 如权利要求22所述的设备，还包括逻辑，所述逻辑配置成：

从所述一个或多个其他计算设备之中的第二计算设备接收第二化名和第二会话密钥；以及

基于基本类似于第一化名的第二化名和基于基本类似于第一会话密钥的第二会话密钥与第二计算设备建立安全会话。

24. 如权利要求23所述的设备，其中，与第二计算设备建立安全会话包括配置成将与感兴趣领域关联的数据共享的逻辑。

25. 如权利要求22所述的设备，其中，所述多维属性值包括至少部分地以对于将第一喜好特征化的两个或多个属性的单独分配值为基础的多维属性值。

26. 如权利要求25所述的设备，其中，所述对于将第一喜好特征化的两个或多个属性的单独分配值包括与第一轴线关联的第一值和与第二轴线关联的第二值，第一轴线正交于第二轴线。

27. 如权利要求26所述的设备，其中，通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值包括配置成在预定义有限域上将多维属性值变换成一维属性值的逻辑，并且所述逻辑也配置成将一维属性值映射到单一轴线。

28. 如权利要求22所述的设备，其中，通过使用一维属性值加密化名和会话密钥包括配置成实施至少一部分容错型加密方案以产生第一密文的逻辑。

29. 一种计算设备，包括：

应用程序，其具有逻辑，以产生对于计算设备用户的第一喜好，所述第一喜好与感兴趣领域相关且具有多维属性值；以及

具有逻辑的解密管理器，所述逻辑配置成：

从服务器接收密文和变换参数，所述密文和变换参数由其他计算设备产生；

从应用程序接收多维属性值；

通过使用变换参数将用于所述喜好的多维属性值变换成一维属性值；

通过使用一维属性值解密密文，以获取识别其他计算设备的化名和获取与所述化名一起使用的会话密钥，从而与所述其他计算设备安全地共享数据；

确定解密质量；以及

至少部分地基于所确定的超过阈值的解密质量启动与所述其他计算设备的安全会话，从而共享数据。

30. 如权利要求29所述的计算设备，其中，至少部分地基于对于所述用户的所述喜好与对于所述其他计算设备的其他用户的其他喜好相比的相似性确定解密质量，所述其他喜好也与感兴趣领域相关。

31. 如权利要求30所述的计算设备，其中，所述多维属性值包括至少部分地以对于将喜

好特征化的两个或多个属性的单独分配值为基础的多维属性值。

32. 如权利要求31所述的计算设备,其中,所述对于将用户的喜好特征化的两个或多个属性的单独分配值包括与第一轴线关联的第一值和与第二轴线关联的第二值,第一轴线正交于第二轴线。

33. 如权利要求32所述的计算设备,其中,通过使用变换参数将用于喜好的多维属性值变换成一维属性值包括配置成在预定义有限域上将多维属性值变换成一维属性值且将一维属性值映射到单一轴线的逻辑。

34. 如权利要求29所述的计算设备,其中,通过使用一维属性值解密密文以获取化名和会话密钥包括配置成实施至少一部分容错型解密方案以获取化名和会话密钥的逻辑。

35. 一种在第一计算设备实施的装置,包括:

具有逻辑的解密管理器,所述逻辑配置成:

从服务器接收第一密文和变换参数,第一密文和变换参数由第二计算设备产生;

接收对于第一计算设备的第一用户的第一喜好,所述第一喜好与感兴趣领域相关且具有多维属性值;

通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值;

通过使用一维属性值解密第一密文,以获取识别第二计算设备的化名和获取与所述化名一起使用的会话密钥,从而与第二计算设备安全地共享数据;

确定解密质量;以及

至少部分地基于所确定的超过阈值的解密质量启动与第二计算设备的安全会话,从而共享数据。

36. 如权利要求35所述的装置,其中,确定解密质量至少部分地基于第一喜好与对于第二计算设备的第二用户的第二喜好的相似性,第二喜好也与感兴趣领域相关。

37. 如权利要求35所述的装置,其中,接收第一喜好包括从服务器接收第一喜好,第一喜好至少部分地基于与第一用户关联的信息,所述与第一用户关联的信息包括对于第一用户的购买历史、对于第一用户的搜索历史、或第一用户的人口统计特征中的一个或多个。

38. 如权利要求35所述的装置,其中,接收第一喜好还包括从由第一计算设备至少部分地基于与第一用户关联的信息维护的应用程序接收第一喜好,所述与第一用户关联的信息包括对于第一用户的购买历史、对于第一用户的搜索历史、或第一用户的人口统计特征中的一个或多个。

用于安全地共享数据的基于喜好的认证方式

背景技术

[0001] 除非在本文中另有说明,否则在这部分内容描述的方法对于本申请中的权利要求而言并非现有技术,并且不通过包含在这部分内容中而被承认是现有技术。

[0002] 在各计算设备之间安全地共享数据可能是计算设备用户的理想目标。所述用户也可能想要基于对感兴趣领域的类似偏好或喜好与其他用户共享数据。这些用户还可能想要在共享数据的同时与其他实体维持可接受程度的隐私和/或安全。这些其他实体可以包括非期望的登广告者、垃圾邮件发送者或恶意行为者。

[0003] 概述

[0004] 在多个实施方式中,本申请描述了用于加密密文和向服务器传送密文的示例性方法。所述方法可以包括产生第一化名以至少暂时地识别第一计算设备,所述第一计算设备关联于具有与感兴趣领域相关的第一喜好的第一用户。第一喜好可以具有多维属性值。然后可以产生第一会话密钥以与所述化名一起使用,从而与一个或多个其他计算设备安全地共享在第一计算设备上维护的数据。也可以产生变换参数,而后所述变换参数被用于将用于第一喜好的多维属性值变换成一维属性值。然后可以通过使用一维属性值加密所述化名和会话密钥,以产生第一密文。在一些实例中,第一密文和变换参数可以被传送到第一计算设备和所述一个或多个其他计算设备都可访问的服务器。对于这些实例,所述服务器可以维护第一密文和变换参数。

[0005] 在多个实施方式中,本申请也描述了用于解密密文和启动安全会话的示例性方法。所述方法可以包括从服务器接收第一密文和变换参数的第一计算设备。第二计算设备可以产生所述密文和变换参数。也可以接收对于第一计算设备的第一用户的第一喜好。然后通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值。也可以通过使用一维属性值解密第一密文,以获取识别第二计算设备的化名和获取与所述化名一起使用的会话密钥,从而与第二计算设备安全地共享数据。在一些实例中,然后可以确定解密质量。对于这些实例,可以至少部分地基于所确定的超过阈值的解密质量启动与第二计算设备的安全会话,从而共享数据。

[0006] 在多个实施方式中,本申请也描述了用于加密密文和向服务器传送密文的示例性装置。所述示例性装置可以具有加密管理器,所述加密管理器具有逻辑。所述逻辑可以配置成产生第一化名以至少暂时地识别第一计算设备,所述第一计算设备关联于具有与感兴趣领域相关的第一喜好的第一用户。第一喜好可以具有多维属性值。逻辑也可以配置成产生第一会话密钥。第一会话密钥可以与所述化名一起使用,以与一个或多个其他计算设备安全地共享在第一计算设备上维护的数据。所述逻辑也可以配置成产生变换参数,所述变换参数然后可以被用于将用于第一喜好的多维属性值变换成一维属性值。所述逻辑也可以配置成通过使用一维属性值加密化名和会话密钥,以产生第一密文。在一些实例中,所述逻辑可以配置成向第一计算设备和所述一个或多个其他计算设备都可访问的服务器传送第一密文和变换参数。对于这些实例,服务器可以维护第一密文和变换参数。

[0007] 在多个实施方式中,本申请也描述了用于解密密文和启动安全会话的示例性计算

设备。所述示例性计算设备可以包括应用程序和解密管理器。所述应用程序可以具有逻辑，以产生对于计算设备用户的喜好。第一喜好可以与感兴趣领域相关且可以具有多维属性值。加密管理器可以具有配置成从服务器接收密文和变换参数的逻辑，可以通过其他计算设备产生密文和变换参数。加密管理器也可以具有逻辑，所述逻辑配置成从应用程序接收多维属性值且通过使用变换参数将用于所述喜好的多维属性值变换成一维属性值。加密管理器也可以具有逻辑，所述逻辑配置成通过使用一维属性值而解密密文，以获取识别所述其他计算设备的化名和获取与所述化名一起使用的会话密钥，从而与所述其他计算设备安全地共享数据。在一些实例中，加密管理器还可以具有逻辑，所述逻辑配置成确定解密质量且至少部分地基于所确定的超过阈值的解密质量启动与所述其他计算设备的安全会话，从而共享数据。

[0008] 在多个实施方式中，本申请也描述了示例性计算机程序产品。在一些实例中，所述计算机程序产品可以包括信号承载介质，所述信号承载介质具有待在第一计算设备实施的指令。当由逻辑执行时，所述指令可以引起所述逻辑从服务器接收第一密文和变换参数。第二计算设备可以产生所述密文和变换参数。所述指令也可以引起所述逻辑接收对于第一计算设备的第一用户的第一喜好。第一喜好可以与感兴趣领域相关且可以具有多维属性值。所述指令也可以引起所述逻辑通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值。所述指令也可以引起所述逻辑通过使用一维属性值而解密第一密文，以获取识别第二计算设备的化名和获取与所述化名一起使用的会话密钥，从而与第二计算设备安全地共享数据。在一些实例中，所述指令可以引起所述逻辑确定解密质量且至少部分地基于所确定的超过阈值的解密质量启动与所述其他计算设备的安全会话，从而共享数据。

[0009] 前述总结内容仅是示例性的且并非旨在以任何方式具有限定性。除了上述示例性的方面、实施方式、以及特征，其他方面、实施方式以及特征将通过参考附图和以下详细说明变得明显。

附图说明

[0010] 通过以下结合附图的说明内容和所附权利要求，本申请的前述和其他特征将变得更加完全明显。因此，将被理解的是，这些附图仅描绘了根据本公开的数个实施方式且并非被考虑成限定本申请的范围，通过利用附图以附加的具体性和详细性描述本申请。

[0011] 图1示出用于在各计算设备之间共享数据的示例性系统；

[0012] 图2示出对于加密管理器的示例性结构的方框示意图；

[0013] 图3示出对于解密管理器的示例性结构的方框示意图；

[0014] 图4示出示例性多维属性值的示意图；

[0015] 图5示出示例性容错型加密方案；

[0016] 图6示出用于加密密文和向服务器传送密文的示例性方法的流程图；

[0017] 图7示出示例性容错型解密方案；

[0018] 图8示出用于解密密文和启动安全会话的示例性方法的流程图；

[0019] 图9示出示例性计算机程序产品的方框示意图；以及

[0020] 图10示出示例性计算设备；

[0021] 所有这些附图都根据本申请的至少一些实施方式设置。

具体实施方式

[0022] 在以下详细说明中,将参考作为本文一部分的附图。在附图中,除非文中另有说明,否则类似的附图标记通常标示类似的部分。在详细说明、附图和权利要求中描述的示例性实例或实施方式并不意味着具有限定性。在不偏离本文所展现的保护主题的精神和范围的情况下,可以利用其他实例或实施方式且可以作出其他变型。将易于被理解的是,本申请的如同在本文中大体描述的在附图中展示的方面能够以各种不同的配置方式设置、替换、结合以及设计,所有这些都是构思明确的且构成本申请的一部分。

[0023] 本申请尤其涉及基于喜好认证(taste-based authentication)以在各计算设备之间安全地共享数据的方法、设备、系统以及计算机程序产品。

[0024] 如在本申请中构思的,计算设备用户可能想要基于对于感兴趣领域的类似偏好或喜好与其他计算设备用户不公开地和/或安全地共享数据。这些用户也可能想要在不使得其他实体(诸如非期望的登广告者、垃圾邮件发送者或恶意行为者)也能够共享数据的情况下寻找对所述感兴趣领域具有类似喜好的其他用户。因此,可能存在问题的是在排除非期望的登广告者、垃圾邮件发送者或恶意行为者的同时寻找具有类似偏好或喜好的用户而后与之安全地共享数据。

[0025] 在一些实例中,可以实施多种方法以产生第一化名(pseudonym),从而至少暂时地识别第一计算设备,所述第一计算设备关联于具有与感兴趣领域相关的第一喜好的第一用户。第一喜好可以具有多维属性值或由之代表。然后,可以产生第一会话密钥(session key),以与所述化名一起使用,从而与一个或多个其他计算设备安全地共享在第一计算设备上维护的数据。也可以产生变换参数,所述变换参数而后被用于将用于第一喜好的多维属性值变换成一维属性值。然后,可以通过使用一维属性值加密所述化名和会话密钥,以产生第一密文(ciphertext)。在一些实例中,第一密文和变换参数可以被传送到第一计算设备和所述一个或多个其他计算设备都可访问的服务器。对于这些实例,服务器可以维护第一密文和变换参数。所述一个或多个其他计算设备然后可以接收第一密文和变换参数。所述一个或多个其他计算设备然后可以解密第一密文,并且使用变换参数以确定第一密文的解密质量。至少部分地基于所确定的第一密文的解密质量,所述一个或多个其他计算设备可以启动与第一计算设备的安全会话,从而安全地共享数据。

[0026] 图1示出根据本申请的至少一些实施方式设置的用于计算设备之间共享数据的示例性系统100。如图1所示,系统100包括计算设备110-1至110-4、会场(venue)服务器120以及网络服务130。在一些实例中,如图1所示,通讯信道140-1至140-4可以分别将计算设备110-1至110-4通讯地连接到会场服务器120。虽然在图1中示出四个计算设备,但是本申请并非限于四个计算设备,而是可以包括任何数量的通讯地连接到会场服务器120的计算设备。同样如图1所示,通讯信道150可以将会场服务器120通讯地连接到网络服务130。

[0027] 如图1所示,根据一些实例,计算设备110-1至110-4可以分开地包括加密管理器112和解密管理器114。如以下更加详细描述地,加密管理器112和解密管理器114可以包括配置成至少部分地以基于喜好认证方式为基础而安全地共享数据的逻辑和/或特征。所述基于喜好的认证可以结合对于计算设备(例如,计算设备110-1)的给定用户而言的与感兴趣领域有关的喜好。同样如图1所示,各计算设备中的至少一部分单独地包括应用程序116。

对于一些实例,应用程序116可以包括配置成产生对于计算设备的给定用户的喜好的逻辑和/或特征。

[0028] 在一些实例中,如图1所示,会场服务器120可以包括用户信息122和安全信息124。用户信息122可以包括由会场服务器120维护的会场特定的用户信息。例如,会场可以是商贸场所(有形的或虚拟的),计算设备用户可以参观所述商贸场所,从而可能购买物品(例如,书本、电影、专辑、歌曲、衣物、饮料等等)。会场特定用户信息可以包括在计算设备用户参观会场时搜集的信息(例如,购买历史、搜索历史、用户人口统计学特征等等),且可以被用于产生或确定对于用户而言的与感兴趣领域相关的喜好。如以下进一步描述的,安全信息124可以包括在会场服务器120维护或利用所述会场服务器120维护的信息,所述信息可以被用于允许计算设备110-1至110-4安全地共享数据。

[0029] 根据一些实例,如图1所示,网络服务130可以包括用户信息132。用户信息132可以包括与计算设备用户关联的用户特定信息。在用户信息132中包含的用户特定信息可以补充或代替由会场服务器120维护的用户信息122中包含的会场特定信息使用。例如,对于给定计算设备用户的用户特定信息可以被包含在用户信息132中。给定计算设备用户可能在与会场服务器120关联的会场具有很少到没有在先购买或搜索历史。会场服务器120可以配置成从网络服务130获取或接收对于用户的用户特定信息,以补充在用户信息122中维护的任何会场特定用户信息。

[0030] 根据一些实例,计算设备110-1的用户可以物理地或虚拟地引起计算设备110-1进入与会场服务器120关联的会场。例如,会场可以是书店,并且一旦计算设备110-1经由通讯信道140-1与会场服务器120通讯地连接,计算设备110-1就可以被视为进入书店。如以下将更加详细描述地,加密管理器112、解密管理器114或应用程序116可以配置成与也通讯地连接到会场服务器120的其他计算设备(例如,计算设备110-4)安全地共享在计算设备110-1维护或利用所述计算设备110-1维护的数据。同样如以下将更加详细描述地,计算设备110-1用户可以具有与感兴趣领域相关的喜好,诸如特定类型的书本。这些喜好可以被利用,以与在感兴趣领域中具有类似喜好的其他计算设备的用户选择性地和安全地共享数据。

[0031] 根据一些实例,通讯信道140-1至140-4、或通讯信道150可以根据一个或多个有线或无线标准操作,所述有线或无线标准使得计算设备110-1至110-4、会场服务器120或网络服务130能够通讯地连接。这些有线或无线标准可以被描述在一个或多个工业标准中,诸如那些与IEEE802.1、IEEE802.11、IEEE802.16、GSM、GPRS、EDGE、W-CDMA、HSPA、CDMA-2000、EV-DO、LTE或TD-LTE关联的标准,但是本申请并非仅限于上述有线或无线标准。

[0032] 虽然在图1中未示出,但是计算设备110-1至110-4也可以直接相互之间或通过会场服务器120建立单独的通讯信道。在一些实例中,单独的通讯信道可以在设立或建立安全会话时建立,以安全地共享与类似感兴趣领域相关的数据。这些单独的通讯信道可以根据上述有线或无线标准操作。

[0033] 图2示出根据本申请的至少一些实施方式的设置的对于加密管理器112的示例性结构的方框示意图。如对于图1中的系统100的以上描述,计算设备110-1至110-4可以包括加密管理器112。在一些实例中,加密管理器112包括特征和/或逻辑,所述特征和/或逻辑被配置或设置成使得计算设备能够通讯地连接到会场服务器120,并且与也通讯地连接到会场服务器120的其他计算设备安全地共享数据。

[0034] 图2的示例性加密管理器112包括加密逻辑210、控制逻辑220、存储器230、输入/输出(I/O)接口240以及可选地一个或多个应用程序250。如图2所示,加密逻辑210可以被连接到控制逻辑220、存储器230以及I/O接口240。同样如图2所示,可选的应用程序250可以被设置成与控制逻辑220通讯。加密逻辑210还可以包括喜好特征211、产生特征213,变换特征215、加密特征217、或传送特征219中的一个或多个或它们的任何合理组合。

[0035] 在一些实例中,在图2的方框示意图中描绘的元件配置成支持或使能如本申请中描述的加密管理器112。给定加密管理器112可以包括图2中描绘的那些元件中的一些、所有,或比图2中描绘的那些元件更多的元件。例如,加密逻辑210和控制逻辑220可以分开地或共同地代表用于实施加密管理器112特征的各种逻辑装置(一个或多个)。示例性逻辑装置可以包括计算机、微处理器、微控制器、现场可编程门阵列(FPGA)、专用集成电路、(ASIC)、多核/多线程微处理器的隔离的(sequestered)线程或核中的一个或多个或它们的组合。

[0036] 在一些实例中,如图2所示,加密逻辑210包括喜好特征211、产生特征213、变换特征215、加密特征217、或传送特征219。加密逻辑210可以配置成使用这些特征中的一个或多个执行操作。如以下将更加详细描述地,示例性操作可以包括通过使用计算设备用户的与感兴趣领域相关的喜好(一个或多个)以产生密文。所述操作也可以包括向计算设备可访问的服务器(例如,会场服务器120)传送密文,以与服务器也可以访问的其他计算设备安全地共享数据。

[0037] 在一些实例中,控制逻辑220可以配置成控制加密管理器112的整体操作。如以上所述,控制逻辑220可以代表各种逻辑装置(一个或多个)中的任何一种,所述逻辑装置配置成结合可执行内容或指令操作,以实施对加密管理器112的控制。在一些替换性实例中,控制逻辑220的特征和功能可以在加密逻辑210内实施。

[0038] 根据一些实例,存储器230被设置成存储可执行内容或指令。可执行内容或指令可以被控制逻辑220和/或加密逻辑210使用,以实施或激活加密管理器112的特征或元件。如以下将更加详细描述地,存储器230也可以被设置成暂时地维护信息,所述信息关联于通过使用计算设备用户的与感兴趣领域相关的喜好而产生密文。

[0039] 存储器230可以包括各种存储介质,其包括但不限于易失存储器、非易失存储器、闪存、可编程变量或状态、随机存取存储器(RAM)、只读存储器(ROM)、或其他静态或动态存储介质中的一个或多个。

[0040] 在一些实例中,I/O接口240可以经由局域有线和/或无线通讯介质或链路在加密管理器112与驻留在计算设备上或与所述计算设备设置的元件之间提供接口,所述计算设备诸如如图1中描绘的计算设备110-1至110-4。I/O接口240可以包括根据多个通讯协议操作以在局域有线或无线通讯介质或链路(例如,I2C、SMBus、SPI、PCI-Express、USB等等)上通讯的接口。I/O接口240也可以在加密管理器112与远离计算设备定位的元件之间提供接口。例如,如以上对于图1所述,具有加密管理器112的计算设备110-1可以经由通讯信道140-1通讯地连接到会场服务器120。具有加密管理器112的计算设备110-1也可以通过会场服务器120且经由通讯信道140-2至140-4、或通过单独建立的通讯信道通讯地连接到计算设备110-2至110-4。I/O接口240例如包括配置成根据多种有线或无线通讯协议操作以允许加密管理器112经由这些通讯信道通讯的接口。这些有线或无线通讯协议可以包括但不限于

IEEE802.1、IEEE802.11、IEEE802.16、GSM、GPRS、EDGE、W-CDMA、HSPA、CDMA-2000、EV-DO、LTE、TD-LTE。

[0041] 在一些实例中,加密管理器112包括一个或多个应用程序250,以向控制逻辑220和/或加密逻辑210提供指令。这些指令例如可以包括用于加密管理器112以实施或使用喜好特征211、产生特征213、变换特征215、加密特征217、或传送特征219中的一个或多个的指令。

[0042] 图3示出根据本申请的至少一些实施方式的设置的对于解密管理器114的示例性结构的方框示意图。如以上对于图1中的系统100所述,计算设备110-1至110-4可以包括加密管理器112。在一些实例中,解密管理器114包括特征和/或逻辑,所述特征和/或逻辑被配置或设置成使得计算设备能够通讯地连接到会场服务器120且启动与通讯地连接到会场服务器120的其他计算设备的安全会话,从而安全地共享数据。

[0043] 图3的示例性解密管理器114包括解密逻辑310、控制逻辑320、存储器330、输入/输出(I/O)接口340、以及可选地一个或多个应用程序350。如图3所示,解密逻辑310可以被连接到控制逻辑320、存储器330以及I/O接口340。同样如图3所示,可选的应用程序350可以被设置成与控制逻辑320协作。解密逻辑310还可以包括接收特征311、喜好特征313、变换特征315、解密特征317、或启动特征319中的一个或多个或它们的任何合理组合。

[0044] 在一些实例中,在图3的方框示意图中描绘的元件配置成支持或使能如在本申请中描述的解密管理器114。给定解密管理器114可以包括图3中描绘的那些元件中的一些、全部,或比图3中描绘的那些元件更多的元件。例如,解密逻辑310和控制逻辑320可以分开地或共同地代表用于实施解密管理器114特征的各种逻辑装置(一个或多个)。示例性逻辑装置可以包括计算机、微处理器、微控制器、现场可编程门阵列(FPGA)、专用集成电路(ASIC)、多核/多线程微处理器的隔离线程或核中的一个或多个或它们的组合。

[0045] 在一些实例中,如图3所示,解密逻辑310包括接收特征311、喜好特征313、变换特征315、解密特征317、或启动特征319。解密逻辑310可以配置成使用这些特征中的一个或多个执行操作。如以下将更加详细描述地,示例性操作可以包括解密从服务器(例如,会场服务器120)接收的密文,并且基于所确定的解密密文的质量启动安全会话,从而在各计算设备之间共享数据。

[0046] 在一些实例中,控制逻辑320可以配置成控制解密管理器114的整体操作。如以上所述,控制逻辑320可以代表各种逻辑装置(一个或多个)中的任何一种,所述逻辑装置配置成结合可执行内容或指令操作,以实施对解密管理器114的控制。在一些替换性实例中,控制逻辑320的特征和功能可以在解密逻辑310内实施。

[0047] 根据一些实例,存储器330被设置成存储可执行内容或指令。可执行内容或指令可以被控制逻辑320和/或解密逻辑310使用,以实施或激活解密管理器114的特征或元件。如以下进一步描述的,存储器330也可以被设置成暂时地维护信息,所述信息关联于解密密文以启动安全会话,以在各计算设备之间共享数据。这种信息例如可以包括对于包括解密管理器114的计算设备的用户而言的与感兴趣领域相关的用户喜好信息。

[0048] 存储器330可以包括各种存储介质,其包括但不限于易失存储器、非易失存储器、闪存、可编程变量或状态、RAM、ROM、或其他静态或动态存储介质中的一个或多个。

[0049] 在一些实例中,I/O接口340可以经由局域有线和/或无线通讯介质或链路在解密

管理器114和驻留在计算设备上或与计算设备定位的元件之间提供接口,所述计算设备诸如如图1中描绘的计算设备110-1至110-4。I/O接口340可以包括根据多种通讯协议操作以在局域有线或无线通讯介质或链路(例如,I2C、SMBus、SPI、PCI-Express、USB,等等)上通讯的接口。I/O接口340也可以在解密管理器114与远离计算设备定位的元件之间提供接口。例如,如以上对于图1所述,具有解密管理器114的计算设备110-1可以经由通讯信道140-1通讯地连接到会场服务器120。具有解密管理器114的计算设备110-1也可以通过会场服务器120且经由通讯信道140-2至140-4、或通过分开地建立的通讯信道通讯地连接到计算设备110-2至110-4。I/O接口340例如包括配置成根据多种有线或无线通讯协议操作以允许解密管理器114经由这些通讯信道通讯的接口。这些有线或无线通讯协议可以包括但不限于IEEE802.1、IEEE802.11、IEEE802.16、GSM、GPRS、EDGE、W-CDMA、HSPA、CDMA-2000、EV-DO、LTE、TD-LTE。

[0050] 在一些实例中,解密管理器114包括一个或多个应用程序350,以向控制逻辑320和/或解密逻辑310提供指令。这些指令例如可以包括用于解密管理器114以实施或使用接收特征311、喜好特征313、变换特征315、解密特征317、或启动特征319中的一个或多个的指令。

[0051] 图4示出根据本申请的至少一些实施方式的设置的示例性多维属性值的示意图。如图4所示,三个多维属性值在绘图400上被描绘成多维属性值405、415以及425。根据一些实例,这三个多维属性值均可以特征化对于计算平台用户的各个喜好。所述各个喜好例如可以由用户在会场购买的书本。对于这些实例,如图4所示,由多维属性值405、415以及425特征化的各个喜好可以包括两个值。第一值可以基于给定被购书本的平均读者类别(rating),而第二值可以基于给定被购书本的类型。同样如图4所示,基于平均读者类别的第一值可以与轴线410或(x)关联,而基于类型的第二值可以与轴线420或(y)关联。如图4所示,在一些实例中,轴线410和轴线420可以相互正交。虽然在图4中未示出,但是附加属性可以在其他轴线上描绘,所述其他轴线也可以正交于轴线410和轴线420(例如,(z)轴线)。

[0052] 在一些实例中,基于平均读者类别的第一值可以被缩放成允许在轴线410上描绘所有数值。对于多维属性415的被购书本例如可以具有基于比例1至5的平均读者类别。对于这个实例,对于多维属性415的被购书本可以具有平均等级3.9。平均等级3.9可以被缩放成值39。基于类型的第二值也可以基于给被购书本类型的分配数值。例如,冒险类型可以具有分配值1,而喜剧、奇幻、历史、神秘以及浪漫类型可以分别具有分配值2、3、4、5以及6。对于这个实例,对于多维属性415的被购书本可以是喜剧类型。因此,多维属性415可以具有二维值,所述二维值可以被描绘或映射到如图4所示的在绘图400上的坐标值(39,2)。对于多维属性405和435的被购书本也可以分别是奇幻类型(分配值3)和冒险类型(分配值1)。这些被购书本也可以具有缩放为10和40的平均读者类别1和4,并且可以如所示图4地描绘和映射。

[0053] 图5示出根据本申请的至少一些实施方式的设置的示例性容错型加密(FTE)方案500。在一些实例中,如图1所示或如图2描述的与计算设备设置的加密管理器112可以包括逻辑和/或特征,以实施至少部分的FTE方案500。但是FTE方案500并非限于由加密管理器112的逻辑和/或特征实施。包括于计算设备中或布置在所述计算设备上的其他逻辑和/或特征也可以实施至少一部分FTE方案500。

[0054] 从示例性步骤5.1开始(提供喜好(T);提供变换参数(P)),喜好特征211可以提供

对于计算平台(例如,计算平台110-1)的用户而言的与感兴趣领域相关的喜好(T),而产生特征213可以提供变换参数(P)。在一些实例中,T和P均可以被提供给变换特征215。与T相关的感兴趣领域例如可以是计算平台用户购买的被购书本。在一些实例中,T可以是类似于图4中示出的多维属性值(例如,(39,2))的多维属性值。同样对于这些实例,P可以由产生特征213新近产生,而后被提供给变换特征215。

[0055] 移动到示例性步骤5.2(提供被变换的喜好(T')),变换特征215可以将被变换的喜好(T')提供给加密特征217。根据一些实例,变换特征215可以在预定义有限域(F)上将多维属性值T变换成一维属性值T'。换言之,通过使用由P定义的不可逆变换,可以将T变换成一维离散集合 $T' \subseteq F$ 。这种变换到T'的结果然后可以被映射到一维数据中。

[0056] 继续示例性步骤5.3(提供作为纯文本(X)的化名和会话密钥),产生特征213可以将纯文本(X)提供给加密特征217。在一些实例中,产生特征213可以产生化名,以作用于计算平台(例如,计算平台110-1)的唯一识别符。对于这些实例,化名可以随机产生。同样,产生特征213也可以产生会话密钥。会话密钥也可以随机产生。产生特征213可以将化名和会话密钥结合或联系起来以形成X。X然后可以被提供给加密特征217。

[0057] 移动到示例性步骤5.4(提供密文Y),加密特征217可以将密文Y提供给传送特征219。在一些实例中,加密特征217可以配置成基于以下参数产生和提供Y:在F上的 $k, r(k \neq r)$ 。对于这些实例,X可以被分成k个区段,以使得每个区段代表F中的一个元素,其中F代表有限域。可以定义在F上具有阶次 $k-1$ 的多项式(f),并且f可以具有由这些k值定义的系数。加密特征217也可以配置成通过使用f估算T'中的每个元素,以获取 $\text{set}(S) = \{(x, f(x)) : x \in T'\}$ 。同样对于这些实例,加密特征217可以配置成与 $r - |T'|$ 元素产生噪声集合 $(N) = \{(x, y) : x \notin T', y \neq f(x)\}$ 。加密特征217然后可以形成或产生 $(S \oplus N)$ 作为Y,而后将Y提供给传送特征219。根据一些实例,传送特征219然后可以向通信地连接到计算平台(例如,会场服务器120)的服务器传送Y。

[0058] 图6示出根据本申请的至少一些实施方式的设置的用于加密密文和向服务器传送密文的示例性方法的流程图。在一些实例中,系统100的元件可以被用于示出与在图6中描绘的流程图相关的示例性方法。如图2所示的加密管理器112也可以被用于示出示例性方法。但是所描述的方法并非限于实施在系统100上或对图2中示出的加密管理器112实施。示例性方法可以实施在其他系统上,所述其他系统具有图1或2中描绘的元件中的一个或多个。

[0059] 从开始之处移动到方框605(进入会场),计算设备(诸如计算设备110-1)可以进入会场。在一些实例中,计算设备110-1可以在进入会场时经由通信信道140-1与会场服务器120通信地连接。

[0060] 从方框605行进到方框610(接收喜好),与计算设备110-1设置的加密管理器112可以包括接收或获取与感兴趣领域相关的喜好(例如,经由喜好特征211)的逻辑和/或特征。在一些实例中,喜好可以与对于计算设备110-1用户的感兴趣领域相关。喜好也可以由多维属性值代表,诸如以上对于图4描述的多维属性值。如果计算设备110-1用户想要对会场服务器120保持匿名,则可以从驻留在或与计算设备110-1设置的应用程序116接收用于喜好的多维属性值。否则,可以从会场服务器120或通过所述会场服务器120接收用于喜好的多维属性值。

[0061] 从方框610行进到方框615(产生第一化名、第一会话密钥以及变换参数),加密管理器112可以包括逻辑和/或特征,所述逻辑和/或特征配置成产生(例如,经由产生特征213)第一化名以至少暂时地识别计算设备110-1,并且产生第一会话密钥以及变换参数。对于这些实例,第一会话密钥可以与第一化名一起使用,以与和会场服务器120通讯地连接的其他计算设备安全地共享数据。

[0062] 从方框615行进到方框620(变换喜好),加密管理器112可以包括配置成变换用于被接收喜好的多维属性值(例如,经由变换特征215)的逻辑和/或特征。根据一些实例,可以如以上对于FTE方案500所述地变换多维属性值。对于这些实例,可以通过使用所产生的变换参数将多维属性值变换成一维属性值。

[0063] 从方框620行进到方框625(产生密文),加密管理器112可以包括配置成产生密文(例如,经由加密特征217)的逻辑和/或特征。根据一些实例,可以如以上对于FTE方案500所述地产生密文。例如,被变换的多维属性值可以被用于产生密文。

[0064] 从方框625行进到方框630,(向服务器传送密文),加密管理器112可以包括逻辑和/或特征,所述逻辑和/或特征配置成向会场服务器120传送所产生的密文(例如,经由传送特征219)。在一些实例中,所产生的变换参数也可以被传送到会场服务器120。对于这些实例,会场服务器120可以包括逻辑和/或特征,以利用安全信息或以安全信息124维护用于计算设备110-1的密文和变换参数。在计算设备110-2至110-4之中的其他计算设备能够从会场服务器120访问密文和变换参数。

[0065] 从方框630行进到判定方框635(密文解密是适当的?),加密管理器112可以包括逻辑和/或特征,所述逻辑和/或特征配置成确定:要求安全地共享数据的请求是否指示被传送到会场服务器120的密文适当解密(例如,经由加密特征217)。如以下将更加详细描述地,所述其他计算设备可以经由会场服务器120访问密文和变换参数,并且利用变换参数以尝试解密该密文以及确定解密质量。在一些实例中,如果密文被适当解密,则另一个计算设备(例如,计算设备110-2)可以将第二化名和第二会话密钥传递到计算设备110-1,所述第二化名和第二会话密钥可以基本类似于由计算设备110-1初始产生的第一化名和第一会话密钥。第二化名和会话密钥也可以包括质量值,以指示所述其他计算机的评估,所述评估针对所述其他计算机的用户的喜好与计算设备110-1用户的喜好的类似程度。如果密文被适当解密(例如,具有高质量值、和/或化名和会话密钥正确),则流程移动到方框640。否则,流程移动到方框645。

[0066] 从判定方框635移动到方框640(安全地共享数据),加密管理器112可以包括与所述其他计算设备安全地共享数据的逻辑和/或特征(例如,经由喜好特征211)。在一些实例中,被共享的数据可以与对于计算设备110-1用户的感兴趣领域相关。所述感兴趣领域例如可以是用户已经购买的书本、电影、歌曲等等的类型。对于这些实例,数据可以被存储于在计算设备110-1维护的存储器中或可以被存储在通过计算设备110-1可访问的存储器(例如,云存储器或网络存储器)中。同样对于一些实例,数据可以经由在两个计算设备之间单独地建立的通讯信道被安全地共享。可替换地,数据可以由已经建立的通讯信道(例如,通讯信道140-1至140-4)通过会场服务器120被安全地共享。

[0067] 从判定方框635移动到方框645(不要共享数据),加密管理器112可以包括逻辑和/或特征,以由于不正确的化名或会话密钥而拒绝与其他计算设备共享数据(例如,经由喜好

特征211)。从另外计算设备接收的与其他质量值相比的低质量值也可以导致拒绝与所述其他计算设备共享数据。在一些实例中,要求共享数据可以被简单地忽略。在其他实例中,拒绝信息可以被传递到所述其他计算设备。

[0068] 从方框640或方框645行进到判定方框650(仍然在会场中?),加密管理器112可以包括逻辑和/或特征,以确定计算设备110-1是否仍然在与会场服务器120关联的会场中。在一些实例中,计算设备110-1用户可能已经将计算设备110-1关掉。在其他实例中,用户可能已经将通讯信道140-1与会场服务器120断开。对于所述其他实例,被断开的通讯信道可能已经由用户离开与会场服务器120关联的虚拟会场(例如,网站)或物理地离开有形会场(例如,实体书店)引起。如果计算设备110-1仍然在会场中,则流程移动回到判定方框635。否则,流程结束。

[0069] 图7示出根据本申请的至少一些实施方式的设置的示例性容错型解密(FTD)方案700。在一些实例中,如图1所示或如图3描述地与计算设备设置的解密管理器114可以包括逻辑和/或特征,以实施至少部分的FTD方案700。但是FTD方案700并非限于由解密管理器114的逻辑和/或特征实施。包括于计算设备或布置在计算设备上的其他逻辑和/或特征也可以实施至少一部分FTD方案700。

[0070] 从示例性步骤7.1开始(提供密文(Y)和变换参数(P);提供喜好(一个或多个)),接收特征311可以提供密文(Y)和变换参数(P),而喜好特征313可以提供对于计算平台(例如,计算平台110-4)的用户的与感兴趣领域相关的喜好(一个或多个)。在一些实例中,Y和P均可以从会场服务器120由接收特征311接收,而后提供给变换特征315。Y和P例如可以由也通讯地连接到会场服务器120的其他计算设备的逻辑和/或特征初始产生。所述其他计算设备可以类似于以上对于图5和图6描述的步骤/流程地产生Y和P。所述其他计算设备然后可以传送待在会场服务器120维护的Y和P。同样对于这些实例,S可以被提供给变换特征315。与S相关的感兴趣领域例如可以是由计算平台用户购买的书本。在一些实例中,S可以是类似于图4中示出的多维属性值(例如,(39,2))的多维属性值。

[0071] 移动到示例性步骤7.2(提供被变换的喜好(S')),变换特征315可以将被变换的喜好(S')提供给解密特征317。根据一些实例,变换特征315可以在预定义有限域(F)上将多维属性值S变换成一维属性值S'。换言之,S可以通过使用由P定义的不可逆变换被变换成一维离散集合S'?F。这个变换到S'的结果然后可以被映射成一维数据。

[0072] 继续示例性步骤7.3(基于解密质量提供化名和会话密钥),解密特征317可以基于对解密质量的评估而将被解密的化名和被解密的会话密钥提供给启动特征319。在一些实例中,从由如以上所述的接收特征311提供的Y获取化名和会话密钥。对于这些实例,化名可以识别所述其他计算设备,而会话密钥可以被用于启动与所述其他计算设备的安全会话。解密特征217可以配置成基于以下参数确定Y的解密质量:在F上的 $k, r(k \neq r)$ 。

[0073] 在一些实例中,如果对于计算平台用户的S类似于对于初始产生Y的计算平台的喜好(T),将同样的P应用到S和T的变换结果(即,S'和T')将会是几乎相同的。对于这些实例,质量确定流程可以包括以下两个步骤过程:

[0074] 步骤1:对于Y中的每个(x,y)执行

[0075] 如果x不在S'中,则从Y中消除(x,y)。

[0076] 步骤2:如果可能

[0077] 构造在 F 上具有阶次 $k-1$ 的多项式 g

[0078] 以使得 g 可以覆盖被减少的 Y 的最大数目的点。

[0079] 然后搜集 g 的 k 系数且构造位串 Z 。

[0080] 计数在被减少的 Y 中的实际位于 g 中的数对 (x, y) 的数量 Q 。

[0081] 输出 (Z, Q) 。

[0082] 如果这不可能,则输出“解密失败”。

[0083] 在一些实例中,质量确定流程可以包括从 Y 中消除那些 x 坐标不在 S' 中的点。对于这些实例, Y 可能起始包含随机噪声点以及通过使用集合 T' 中的所有元素作为 x 值而被估算的点 $(x, f(x))$ 。同样,如果有许多 S' 和 T' 的重叠值,则这些噪声点中的大部分可以在质量确定流程的第一步骤被消除。同样,许多初始函数值 $(x, f(x))$ 将剩下。质量确定流程的步骤2可以包括由通过拉格朗日插值结合这些有序数对 (x, y) 而重新构造曲线的过程。然而,如果 S' 和 T' 并非精确匹配且二者之间具有微小差异,这些误差可以被移除以实现正确插值。对于移除误差,可以使用在译码理论中广泛使用的译码算法,诸如里德-所罗门算法(Reed-Solomon algorithm)。

[0084] 当译码是成功或适合的质量时,能够重新构造多项式 g 。多项式 g 可以基本类似于以上描述的多项式 f ,所述多项式 f 用于产生如对于图5描述的密文。当 S 非常不同于 T 时,在 S' 和 T' 中可能有明显差异。由于 S' 和 T' 中的明显差异,所以实施质量确定流程的步骤2可以消除在多项式 g 上的许多点,而许多随机噪声将剩下。许多随机噪声的存在可能导致译码失败或质量劣等。

[0085] 在一些实例中,如果解密是适当的或可接受的,则输出 (Z, Q) 可以由质量确定流程产生。对于这些实例, Z 可以包括纯文本会话密钥和化名以识别其他计算设备,而 Q 可以包括与解密关联的质量值。 Q 值可以基于在实施步骤2之后仍然剩下的随机噪声量。例如,大量的随机噪声等同于 Q 的较低值,而少量的随机噪声等同于 Q 的较高值。如以上所述,更少量的随机噪声可能意味着 S 和 T 基本类似。

[0086] 图8示出根据本申请的至少一些实施方式设置的用于解密密文和启动安全会话的示例性方法的流程图。在一些实例中,系统100的元件可以被用于示出与图8中描绘的流程图相关的示例性方法。如图3所示,解密管理器114也可以被用于示出示例性方法。但是所描述的方法并非限于在系统100上实施或对图3中示出的解密管理器114实施。示例性方法可以在具有在图1或3中描绘的元件中的一个或多个的其他系统上实施。

[0087] 从开始之处移动到方框810(进入会场),诸如计算设备110-4的计算设备可以进入会场。在一些实例中,计算设备110-4可以在进入会场时经由通讯信道140-4与会场服务器120通讯地连接。

[0088] 从方框810行进到方框820(接收密文和变换参数),与计算设备110-4一起设置的解密管理器114可以包括配置成接收密文和变换参数(例如,经由接收特征311)的逻辑和/或特征。在一些实例中,可以从会场服务器120经由通讯信道140-4接收密文和变换参数。对于这些实例,密文和变换参数可以从也通讯地连接到会场服务器120的另一计算设备(例如,计算设备110-1)传送到会场服务器120,而后在会场服务器120维护(例如,利用安全信息124)。

[0089] 从方框820行进到方框830(接收喜好),解密管理器114可以包括配置成接收或获

取与感兴趣领域相关的喜好(例如,经由喜好特征311)的逻辑和/或特征。在一些实例中,喜好可以与对于计算设备110-4用户的感兴趣领域相关。喜好也可以具有多维属性值或由之代表,所述多维属性值诸如以上对于图4描述的多维属性值。对于这些实例,计算设备110-4不包括应用程序116,且因此可以依赖于会场服务器120提供用于喜好的多维属性值。

[0090] 从方框830行进到方框840(变换喜好),解密管理器114可以包括配置成变换对于被接收喜好的多维属性值(例如,经由变换特征315)的逻辑和/或特征。根据一些实例,可以如以上对于FTD方案700所述地变换多维属性值。对于这些实例,可以通过使用产生的变换参数将多维属性值变换成一维属性值。

[0091] 从方框840行进到方框850(解密密文),解密管理器114可以包括配置成解密被接收的密文(例如,经由解密特征317)的逻辑和/或特征。根据一些实例,可以如以上对于FTD方案700所述地解密密文。例如,被变换的多维属性值可以被用于通过使用一维属性值由被接收的密文解密化名和会话密钥。

[0092] 从方框840行进到判定方框850(质量适合?),解密管理器114可以包括配置成确定被解密的密文的质量是否适合(例如,经由解密特征317)的逻辑和/或特征。在一些实例中,两个步骤质量确定流程可以如以上对于FTD方案700所述地实施,以确定解密质量是否适合。如果质量适合(例如,很少到没有随机噪声剩下),则流程移动到方框870。否则,流程移动到判定方框880。

[0093] 从判定方框860移动到方框870(启动安全会话),解密管理器114可以包括配置成启动与其他计算设备(例如,计算设备110-1)的安全会话(例如,启动特征319)的逻辑和/或特征。在一些实例中,可以通过将被解密的会话密钥和被解密的化名传送到所述其他计算设备以启动安全会话。对于这些实例中的一些,已经与会场服务器120建立的通讯信道(例如,通讯信道140-1至140-4)可以被用于启动与所述其他计算设备的安全会话。在其他实例中,单独建立的通讯信道可以被用于启动与所述其他计算设备的安全会话。

[0094] 根据一些实例,所述其他计算设备可以至少部分地基于与初始被加密的化名和会话密钥基本匹配的化名和会话密钥建立安全会话。一旦安全会话建立,计算设备110-4就可以与所述其他计算设备安全地共享与感兴趣领域关联的数据。数据可以经由两个计算设备之间单独建立的通讯信道、或经由已经建立的通讯信道(例如,通讯信道140-1至140-4)通过会场服务器120安全地共享。

[0095] 从方框870行进到判定方框880(仍然在会场中),解密管理器114可以包括配置成确定计算设备110-4是否仍然在与会场服务器120关联的会场中的逻辑和/或特征。在一些实例中,计算设备110-4用户可能已经使得计算设备110-4关掉。在其他实例中,用户可能已经将与会场服务器120的通讯信道140-4断开。对于所述其他实例,被断开的通讯信道可以由用户离开与会场服务器120关联的虚拟会场(例如,网站)或物理地离开有形会场(例如,实体书店)引起。如果计算设备110-4仍然在会场中,则流程移动回到方框820。否则,流程结束。

[0096] 图9示出根据本申请的至少一些实施方式的设置的示例性计算机程序产品900的方框示意图。在一些实例中,如图9所示,计算机程序产品900包括信号承载介质902,所述信号承载介质也可以包括待在第一计算设备实施的指令904。当由逻辑(例如,加密逻辑210)执行时,指令904可以引起所述逻辑从服务器接收第一密文和变换参数。第二计算设备可以

已经产生密文和变换参数。指令904也可以引起所述逻辑接收对于第一计算设备的第一用户的第一喜好。第一喜好可以与感兴趣领域相关和可以具有多维属性值。指令904也可以引起所述逻辑通过使用变换参数将用于第一喜好的多维属性值变换成一维属性值。指令904也可以引起所述逻辑通过使用一维属性值解密第一密文,以获取识别第二计算设备的化名和获取与所述化名一起使用的会话密钥,从而与第二计算设备安全地共享数据。在一些实例中,指令904可以引起所述逻辑确定解密质量,并且至少部分地基于所确定的超过阈值的解密质量启动与所述其他计算设备的安全会话,从而共享数据。

[0097] 同样在图9中描绘地,在一些实例中,计算机产品900可以包括计算机可读介质906、可记录介质908、以及通讯介质910中的一个或多个。围绕这些元件的虚线框描绘出不同类型的介质,其包括在信号承载介质902内但不限于此。这些类型的介质可以分配待由逻辑(例如,加密逻辑210)执行的指令904。计算机可读介质906和可记录介质908可以包括但不限于软盘、硬盘驱动器(HDD)、压缩盘(CD)、数字多用光盘(DVD)、数字磁带、计算机存储器等等,通讯介质910可以包括但不限于数字和/或模拟通讯介质(例如,光纤、波导、有线通讯链路、无线通讯链路等等)。

[0098] 图10示出根据本申请的至少一些实施方式的设置的示例性计算设备1000。在一些实例中,图1、2或3中描绘的加密管理器112或解密管理器114可以在计算设备1000上实施。在这些实例中,计算设备1000的元件可以被设置或配置成实施基于喜好的认证,以在各计算设备之间安全地共享数据。就在这个基本构型1001中,计算设备1000通常包括一个或多个处理器1010和系统存储器1020。存储器总线1030能够被用于使处理器1010与系统存储器1020之间通讯。

[0099] 根据理想构型,处理器1010能够是任何类型,其包括但是不限于微处理器(μ P)、微控制器(μ C)、数字信号处理器(DSP)、或它们的任何组合。处理器1010能够包括多于一级的缓存(诸如一级缓存1011和二级缓存1012)、处理器内核1013、以及寄存器1014。处理器内核1013能够包括算术逻辑单元(ALU)、浮点单元(FPU)、数字信号处理内核(DSP内核)、或它们的任何组合。存储器控制器1015也能够被用于处理器1010,或在一些实施方式中,存储器控制器1015能够是处理器1010的内件。

[0100] 根据理想构型,系统存储器1020能够是任何类型,其包括但是不限于易失存储器(诸如RAM)、非易失存储器(诸如ROM、闪存,等等)、或它们的任何组合。系统存储器1020通常包括操作系统1021、一个或多个应用程序1022、以及程序数据1024。应用程序1022包括设置成执行这里描述的功能的指令1023,所述功能包括就图2或3中示出的加密管理器112或解密管理器114结构而言描述的动作或就图5-8中示出的方案和流程图而言描述的动作。程序数据1024包括用于实施指令1023(例如,基于喜好的认证以共享数据)的共享数据1025。在一些实例中,应用程序1022能够被设置成利用程序数据1024在操作系统1021上操作,以使得可以如本文描述地提供实施方式,所述实施方式用于实施基于喜好的认证以在各计算设备之间安全地共享数据的指令。这种被描述的基本构型在图10中由虚线1001内的那些部件示出。

[0101] 计算设备1000能够具有附加特征或功能、以及附加接口,用于协助基本构型1001与任何所需装置和接口之间的通讯。例如,总线/接口控制器1040能够被用于有助于基本构型1001和一个或多个数据存储装置1050之间经由存储器接口总线1041通讯。数据存储装置

1050能够是可移除存储装置1051、不可移除存储装置1052、或它们的组合。可移除存储和不可移除存储装置的实例包括,举例而言:磁盘装置,诸如软盘驱动器和硬盘驱动器(HDD);光盘驱动器,诸如压缩盘(CD)驱动器或数字多用光盘(DVD)驱动器;固态驱动器(SSD);以及磁带驱动器。示例性计算机存储介质能够包括为存储信息以任何方法或技术实施的易失和非易失介质、可移除和不可移除介质,所述信息诸如计算机可读指令、数据结构、程序模块、或其他数据。

[0102] 系统存储器1020、可移除存储器1051以及不可移除存储器1052都是计算机存储介质的实例。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多用光盘(DVD)或其他光学存储器、盒式磁带、磁带、磁盘存储器或其他磁性存储装置、或能够被用于存储所需信息且能够由计算设备1000访问的任何其他介质(例如,信号的基带表达)。任何这种计算机存储介质都能够是装置1000的一部分。

[0103] 计算设备1000也能够包括接口总线1042,所述接口总线1042用于协助经由总线/接口控制器1040从多种接口装置(例如,输出接口、外围接口、以及通讯接口)到基本构型1001的通讯。示例性输出接口1060包括图形处理单元1061和音频处理单元1062,其能够配置成经由一个或多个A/V端口1063通讯到多种外部装置,诸如显示器或扬声器。示例性外围接口1060包括串行接口控制器1071或并行接口控制器1072,其能够配置成经由一个或多个I/O端口1073通讯于外部装置,诸如输入装置(例如,键盘、鼠标、笔、声音输入装置、触摸输入装置等等)或其他外围装置(例如,打印机、扫描器等等)。示例性通讯接口1080包括网络控制器1081,其能够被设置成协助经由一个或多个通讯端口1082在网络通讯上与一个或多个其他计算设备1090通讯。网络通讯连接是通讯介质的一个实例。通讯介质通常可以由计算机可读指令、数据结构、程序模块、或调制数据信号中的其他数据(诸如载波或其他传输机制)实施,并且可包括任何信息传递介质。“调制数据信号”能够是这样一种信号,所述信号使得其特性中的一个或多个被设定或改变成编码所述信号中的信息。以示例性且非限定性的方式,通讯介质能够包括有线介质诸如有线网络或直接有线连接,并且无线介质诸如声学、射频(RF)、红外(IR)以及其他无线介质。在本文中使用的术语计算机可读介质能够包括存储介质和通讯介质。

[0104] 计算设备1000能够被实施为个人计算机的一部分,所述计算机包括在工作站或服务器构型中配置或实施的便携式计算机和非便携式计算机。

[0105] 在本申请中引用的术语“回应于”或“响应于”并非限于对特定特征和/或结构回应。特征也可以回应于另一特征和/或结构,并且也可以位于所述另一特征和/或结构内。此外,当在本文中或以下权利要求中使用诸如“连接”或“回应”或“响应于”或“通讯于”等等的术语或短语时,应该广义地解释这些术语。例如,如对于短语使用的情景合适,短语“连接到”可以涉及通讯地、电气地和/或操作地连接。

[0106] 本领域技术人员将认识到,在本领域中常见的是,以本文列出的方式描述各装置和/或流程,而后利用工程实践将所述装置(例如,发射器、接收器、无线装置、计算平台、计算设备等等)和/或方法集成到数据处理系统中。换言之,至少一部分在本文中描述的装置和/或方法能够经由合理数量的实验被集成到数据处理系统中。本领域技术人员将认识到,通常数据处理系统大体包括以下部件中的一个或多个:系统单元壳体;视频显示装置;存储器,诸如易失和非易失存储器;处理器,诸如微处理器和数字信号处理器;计算实体,诸如操

作系统、驱动器、图形用户接口、以及应用程序；一个或多个互动装置，诸如触控板或触屏；和/或控制系统，其包括反馈环和控制电机（例如，用于感应位置和/或速度的反馈；用于移动和/或调整部件和/或量的控制电机）。通常数据处理系统可以利用任何合适的商用部件被实施，诸如那些通常在数据计算/通讯和/或网络计算/通讯系统中找到的部件。

[0107] 在本文中描述的保护主题有时示出包含在不同其他部件或元件内或与之连接的不同部件或元件。应该被理解的是，这种被描绘的结构仅是实例，并且事实上能够实施实现相同功能的许多其他结构。从概念意义上，用于实现相同功能的任何部件的配置方式被有效地“关联”，以实现所需功能。因此，无论结构或中间部件如何，在本文中结合以实现特定功能的任何两个部件能够被视为“关联于”彼此以实现所需功能。同样地，如此关联的任何两个部件也能够被视为“可操作地接合”或“可操作地连接”到彼此以实现所需功能，并且能够如此关联的任何两个部件也能够被视为“可操作地可连接”到彼此以实现所需功能。可操作地可连接的特定实例包括但不限于物理可匹配和/或物理相互作用部件、和/或可无线相互作用和/或无线相互作用部件、和/或逻辑相互作用和/或可逻辑相互作用部件。

[0108] 就在本文中使用的任何复数和/或单数术语而言，如对于情景和/或应用情况合适，本领域技术人员能够将复数转化成单数和/或将单数转化成复数。为了清楚起见，可以在本文中明确地列出多种单数/复数排列方式。

[0109] 本领域技术人员将理解的是，概括而言，在本文中且尤其在所附权利要求（例如，所附权利要求的主体）中使用的术语大体旨在用作“开放”术语（例如，术语“包括”应该被解释为“包括但不限于”，术语“具有”应该被解释为“至少具有”，术语“包含”应该被解释为“包含但不限于”等等）。本领域技术人员还将理解的是，如果意图在权利要求中引入具体数量，则会在权利要求中明确记载这样的意图，如果没有记载，则不存在这样的意图。例如，为了帮助理解，以下所附权利要求可以包含对引导短语“至少一个”以及“一个或多个”的使用，以引导权利要求记载(recitation)。然而，这种短语的使用不应该被理解为隐含着通过不定冠词“一”或“一个”引导的权利要求记载将包含这样引导的权利要求记载的任何特定权利要求限制为仅包含这种记载的公开，即使当同样的权利要求包括引导短语“一个或多个”或“至少一个”以及诸如“一”或“一个”（例如“一”和/或“一个”通常应该被理解为指“至少一个”或“一个或多个”）的不定冠词时也是如此；这同样适用于使用定冠词来引导权利要求记载的情况。此外，即使明确记载了引导的权利要求记载的特定数目，本领域的技术人员也将认识到，这样的记载通常应该被理解为是至少所记载的数目（例如，仅记载“两个记载”而没有其它修饰词通常表示至少两个记载，或者两个或更多个记载）。而且，在使用类似于“A、B或C等中的至少一个”的习惯表达的情况下，一般地，这样的句式的意图是本领域的技术人员理解该习惯表达的意思（例如，“具有A、B或C中的至少一个的系统”将包括但不限于仅具有A、仅具有B、仅具有C、具有A和B、具有A和C、具有B和C、和/或具有A、B和C的系统等等）（本句又重复了一遍）。本领域的技术人员还将理解，表示两个或更多个替代词汇的几乎任何连接词和/或短语，不论在说明书、权利要求或附图中，都应被理解为考虑到包括所述词汇之一、所述词汇中的任一、或两个词汇都包括的可能性。例如，词组“A或B”将被理解为包括“A”或“B”或“A和B”的可能性。

[0110] 虽然在本文中已经公开多个方面和实施方式，但是其他方面和实施方式对本领域技术人员而言将是明显的。在本文中公开的多个方面和实施方式仅用作示例性且并非旨在

具有限定性,通过以下权利要求阐明实际保护范围和精神。

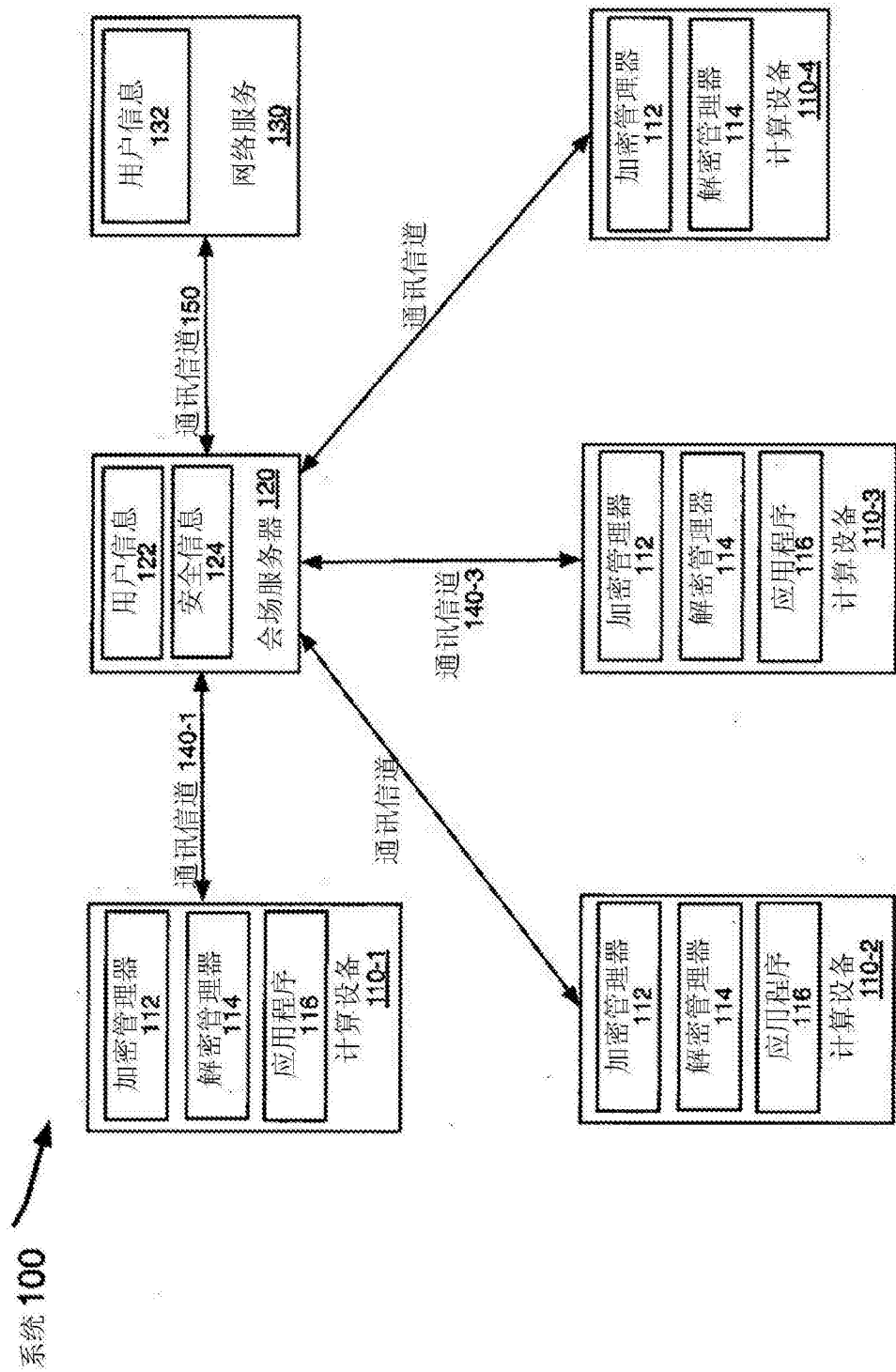


图1

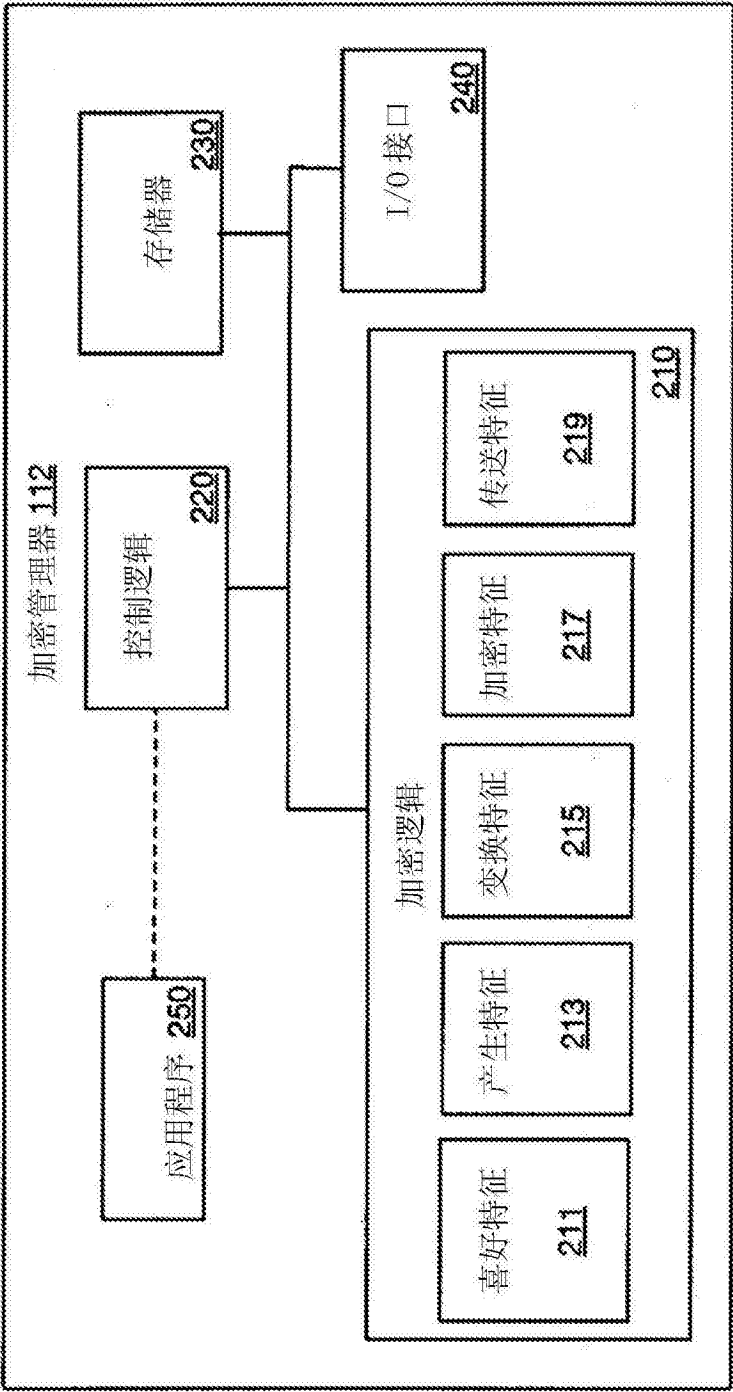


图2

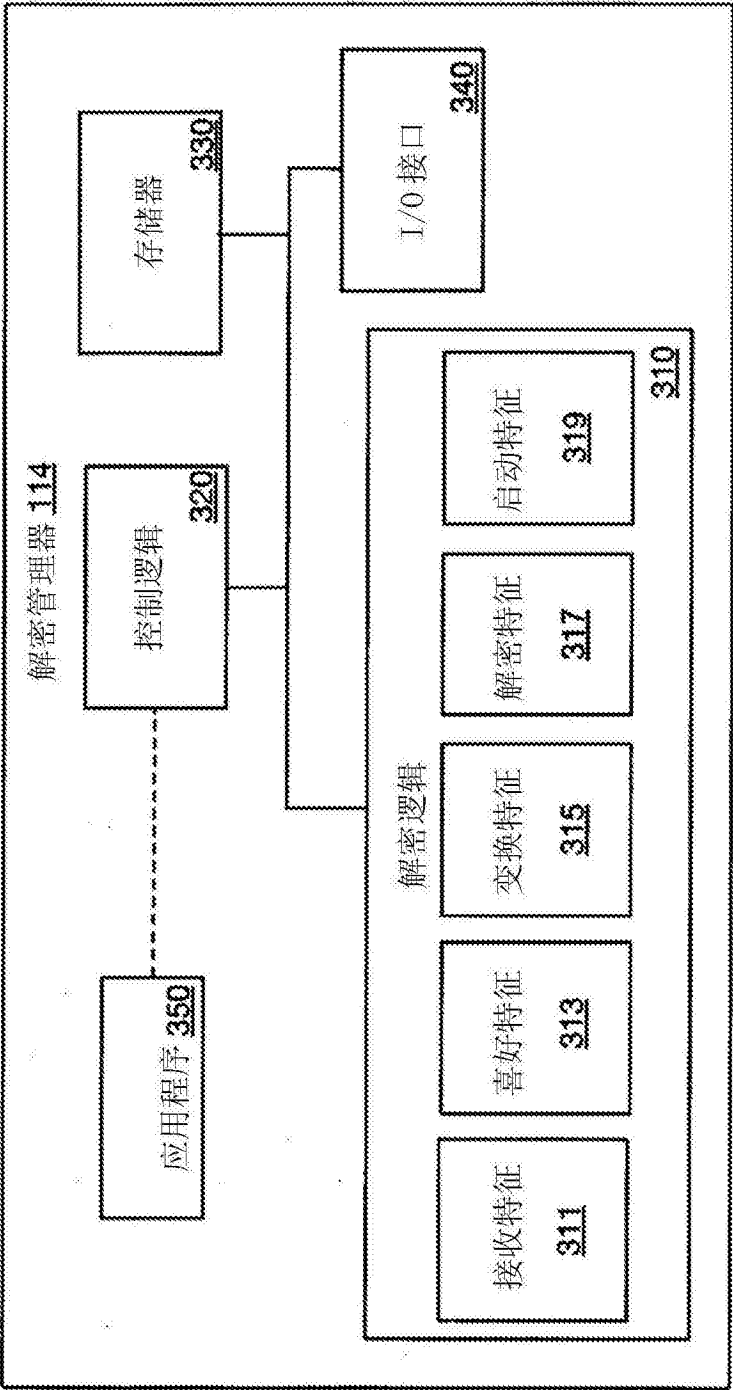
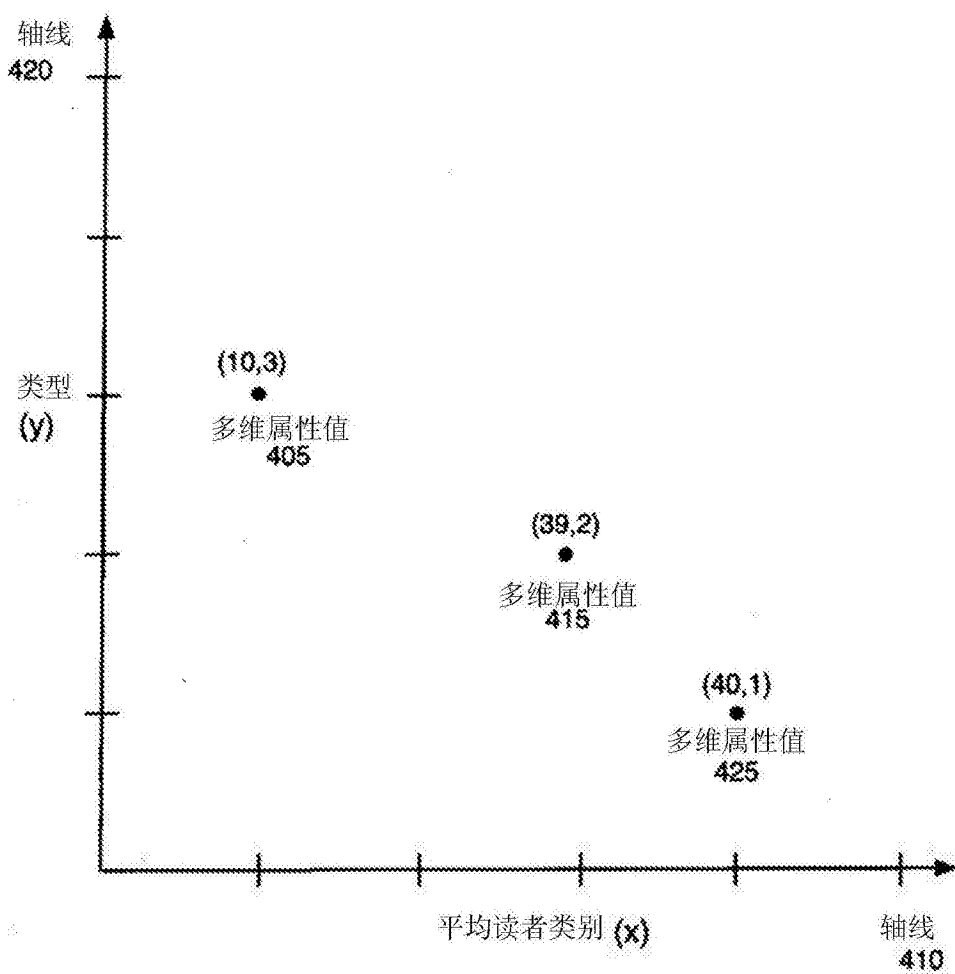


图3



绘图 400

图4

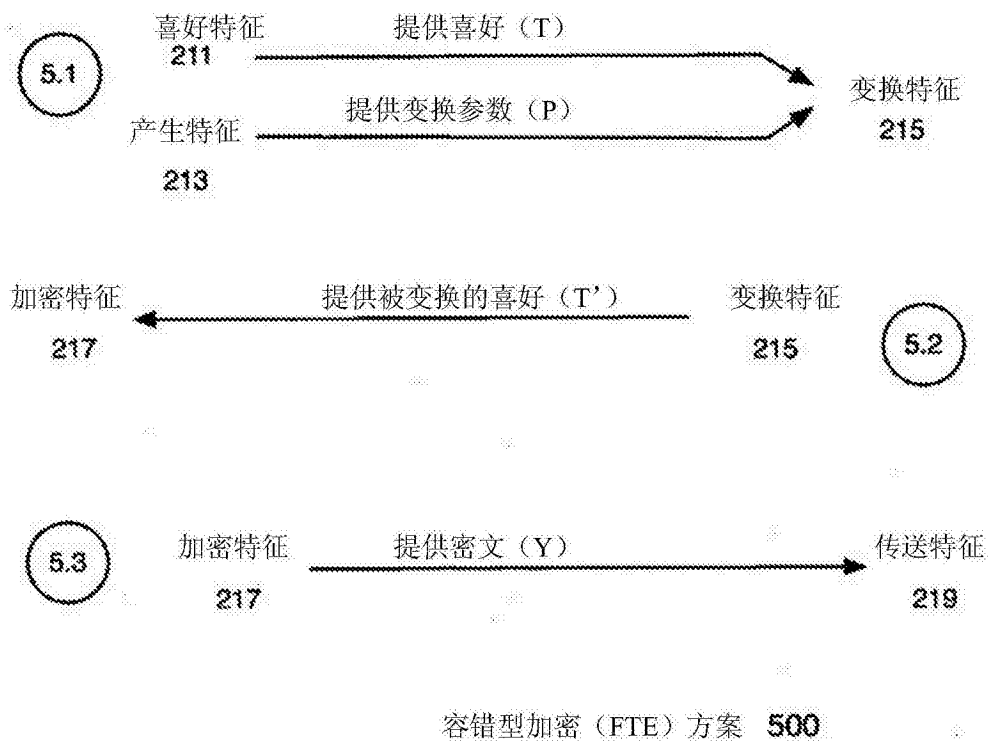


图5

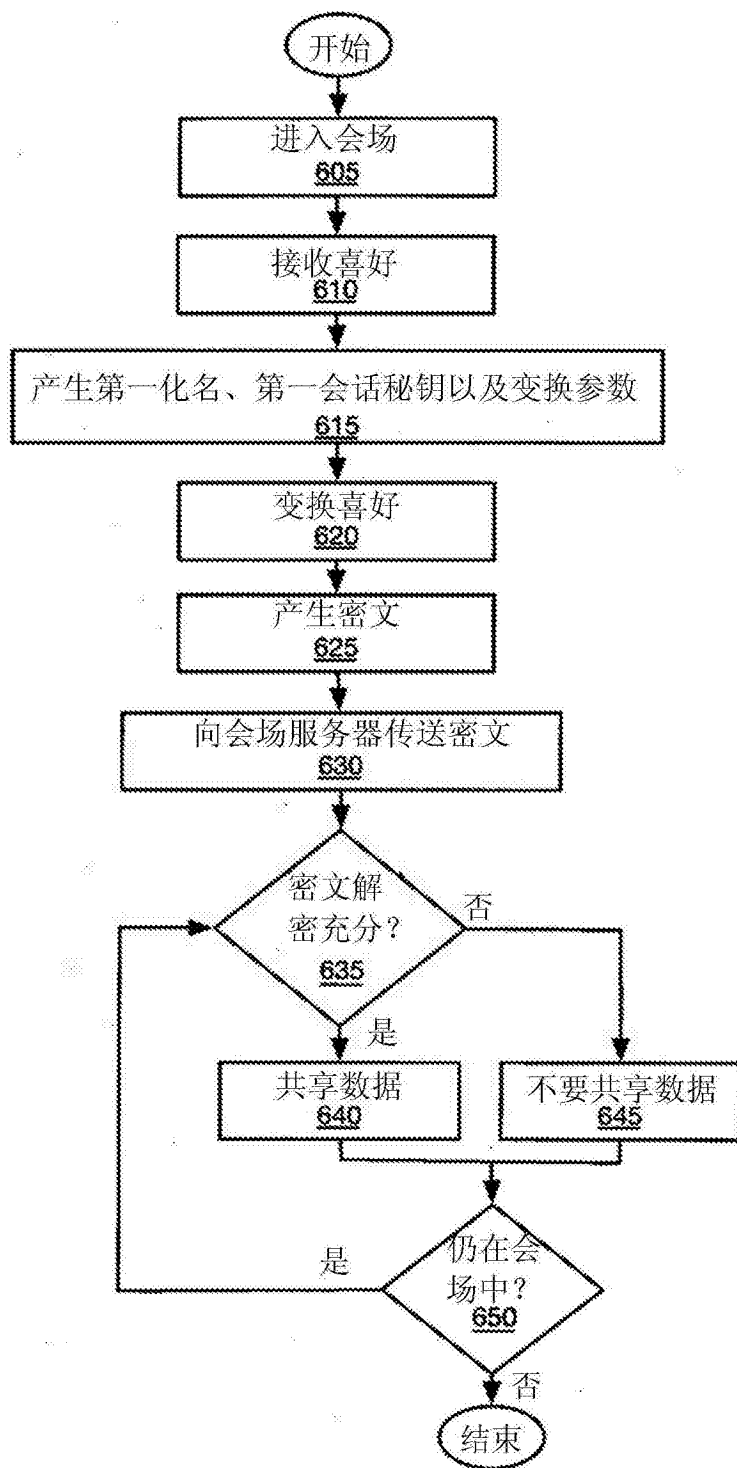
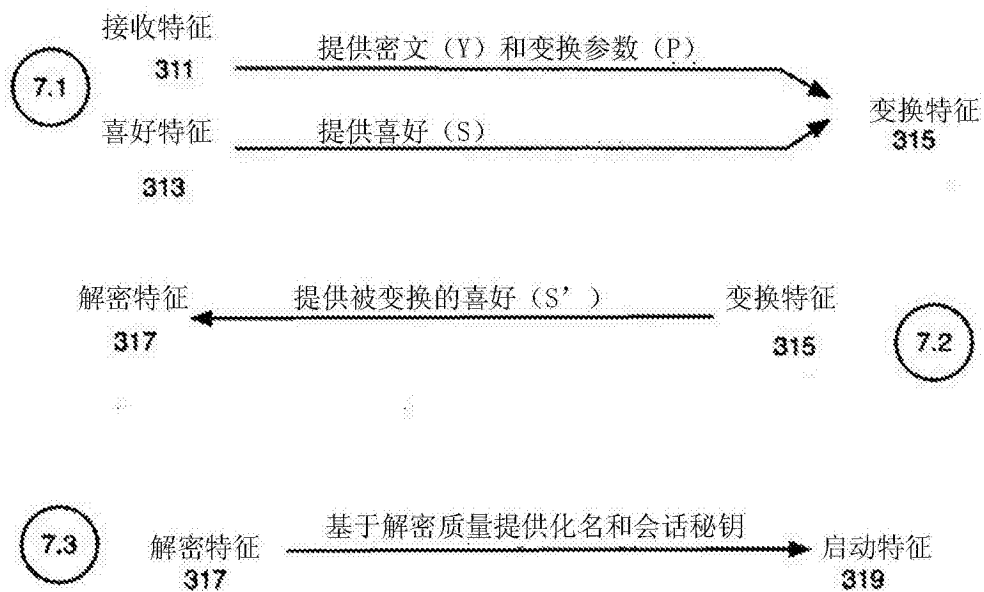


图6



容错型解密 (FTD) 方案 700

图7

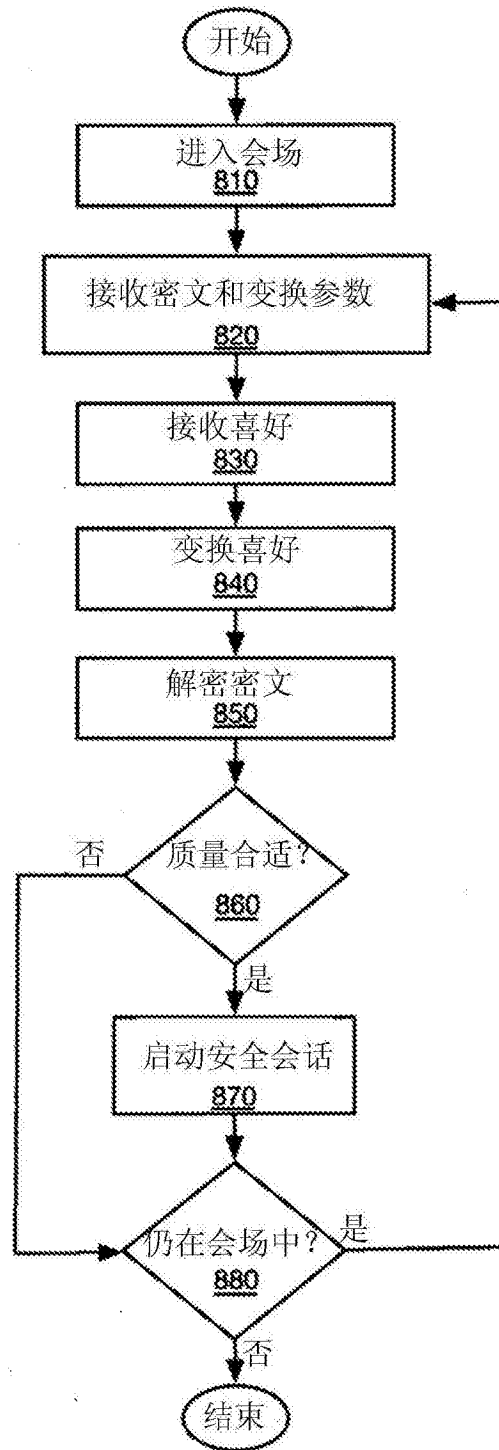


图8

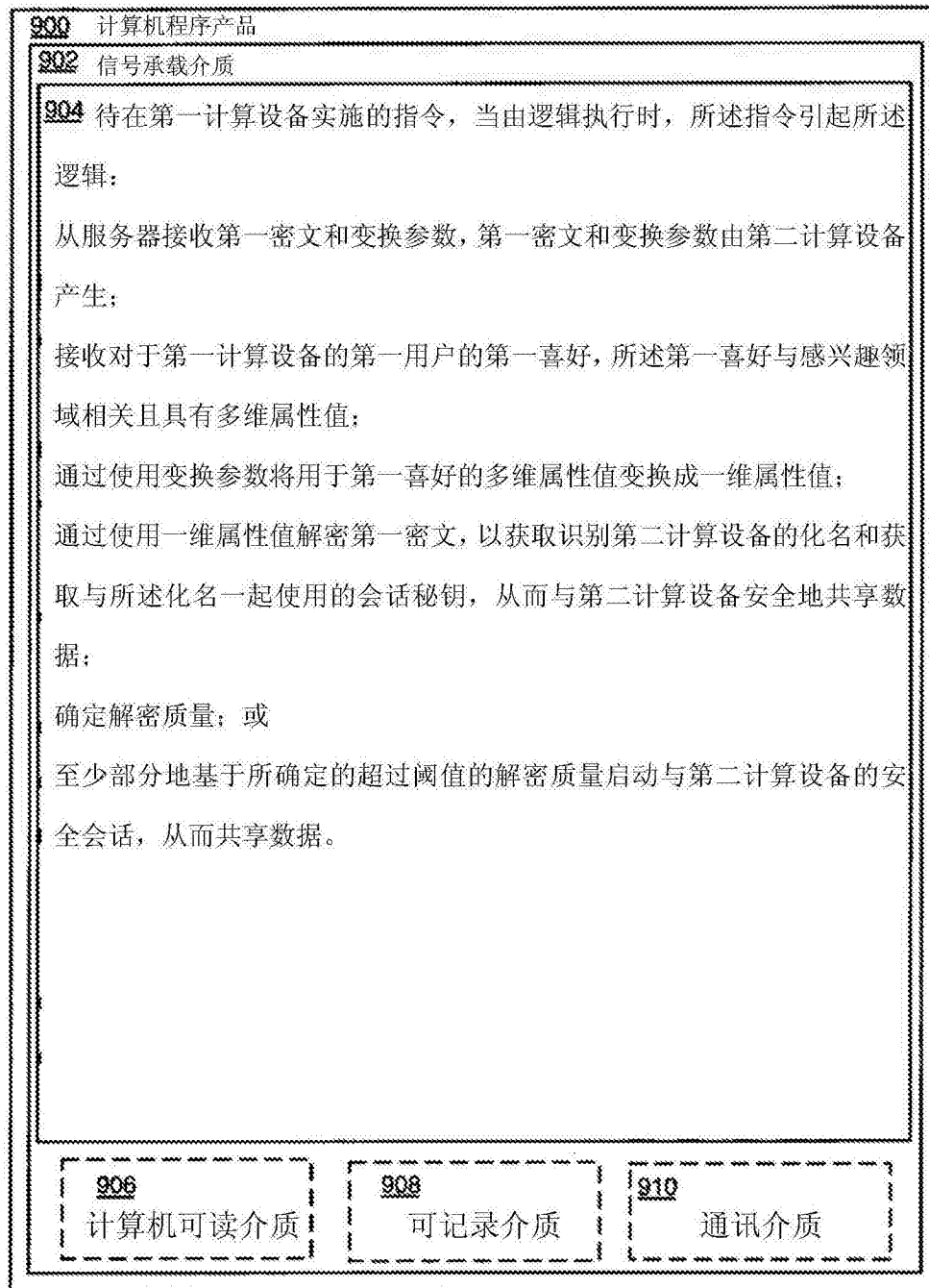


图9

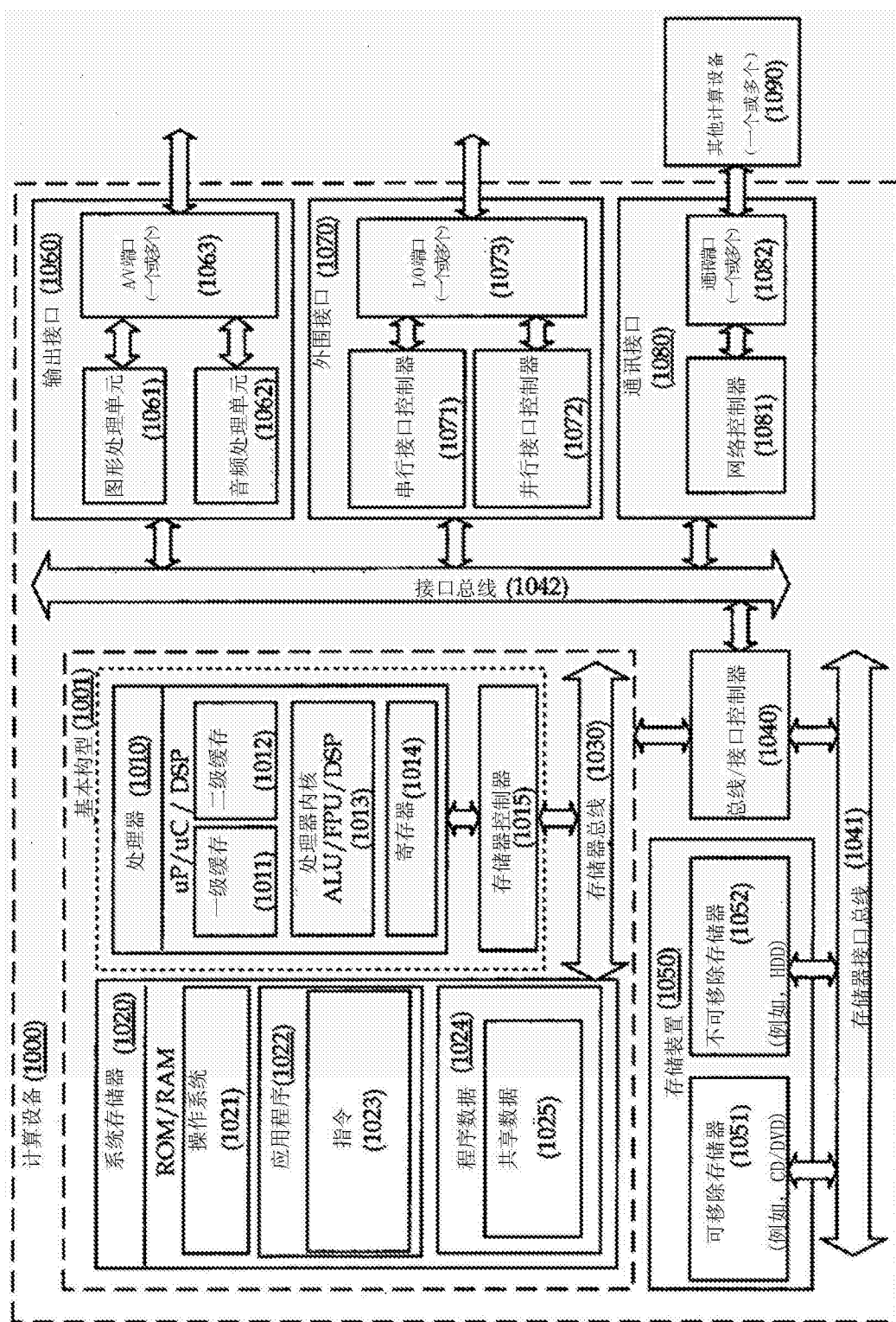


图10