(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 105308925 B
(45)授权公告日 2019.04.09

(21)申请号 201480007047.9

(22)申请日 2014.01.29

(65)同一申请的已公布的文献号
申请公布号 CN 105308925 A

(43)申请公布日 2016.02.03

(30)优先权数据
13/757561 2013.02.01 US

(85)PCT国际申请进入国家阶段日
2015.07.31

(86)PCT国际申请的申请数据
PCT/US2014/013465 2014.01.29

(87)PCT国际申请的公布数据
WO2014/120695 EN 2014.08.07

(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州

(72)发明人 H.克里什纳墨菲 M.朱
K.T.尼尔森 M.莫里斯

(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 29/06(2006.01)
H04W 12/06(2006.01)

(56)对比文件
US 2011126005 A1,2011.05.26,
US 2011271296 A1,2011.11.03,
US 2009187983 A1,2009.07.23,
US 2010169222 A1,2010.07.01,
US 2008196086 A1,2008.08.14,
US 2011167262 A1,2011.07.07,
CN 101464934 A,2009.06.24,
CN 102239675 A,2011.11.09,
CN 102546584 A,2012.07.04,

审查员 王相君

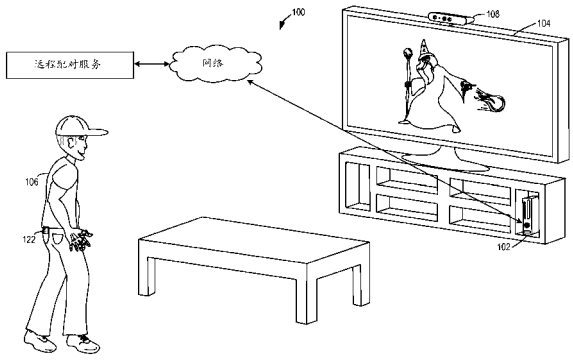
权利要求书1页 说明书10页 附图9页

(54)发明名称

保护计算设备配件

(57)摘要

所公开的各个实施例涉及计算机配件设备的安全。例如,一个非限制性实施例提供主机计算设备,其被配置成引导与配件设备的相互认证会话的初始部分,并且经由计算机网络将关于主机计算设备和配件设备的信息发送给远程配对服务。主机计算设备还被配置成:作为响应,从远程配对服务接收配对证书,该配对证书经由远程配对服务的私人密钥进行加密;并且使用来自远程配对服务的配对证书完成与配件设备的相互认证。



CN 105308925 B

1.一种主机计算设备,包括:

逻辑子系统;以及

存储子系统,其包括存储在其上的指令,所述指令可由逻辑子系统执行以:

引导与配件设备的相互认证会话的初始部分;

经由计算机网络将关于主机计算设备和配件设备的信息发送给远程配对服务;

作为响应,从远程配对服务接收配对证书,所述配对证书包括从主机计算设备被发送到远程配对服务的配对公钥和从配件设备接收的安全芯片证书的摘要,所述配对证书经由远程配对服务的私钥进行加密;

在完成相互认证会话的初始部分后,确定是否准许配件设备与主机计算设备一起使用;以及

在准许配件设备与主机计算设备一起使用时,使用来自远程配对服务的配对证书完成与配件设备的相互认证会话。

2.权利要求1的主机计算设备,其中引导相互认证会话的初始部分包括:

建立与配件设备的连接;

从配件设备接收安全芯片证书;以及

核实安全芯片证书有效。

3.权利要求2的主机计算设备,其中核实安全芯片证书是否有效包括联系发布所述安全芯片证书的证书授权机构。

4.权利要求1的主机计算设备,其中关于主机计算设备和配件设备的信息包括主机公钥和安全芯片证书。

5.权利要求4的主机计算设备,其中使用配对证书完成相互认证会话包括:

将配对证书发送给配件设备;

将经由配件设备公钥加密的预主秘密发送给配件设备;

从配件设备接收响应;

将由主机获取的配对私钥加密的主机证书核实消息发送给配件设备;以及

从配件设备接收针对主机证书核实消息的响应。

6.权利要求5的主机计算设备,其中指令还可执行以生成配对私钥和对应的配对公钥。

7.权利要求5的主机计算设备,其中配对私钥和对应的配对公钥被预先配置。

8.权利要求1的主机计算设备,其中所述指令还可执行:

如果不准许配件设备与主机计算设备一起使用,则拒绝完成相互认证会话。

9.权利要求8的主机计算设备,其中所述指令还可执行,如果不准许配件设备与主机计算设备一起使用,则执行不利用远程配对服务的单向认证。

10.权利要求9的主机计算设备,其中确定是否准许配件设备与主机计算设备一起使用包括在相互认证会话的初始部分期间检查从配件设备所接收的配置信息。

保护计算设备配件

背景技术

[0001] 伪造计算设备配件可能对合法配件的制造商和/或销售商具有负面影响。因此，已经使用各种策略来帮助防止计算机配件伪造。例如，一些伪造防止方案可以利用每一个可信设备上的安全芯片，其中安全芯片可以允许主机计算机对设备进行认证。

[0002] 即使是可信配件设备也可能易受未授权使用形式的影响。例如，一些配件设备可以以具有所启用的不同增值特征的不同价格点而得到，使得更昂贵的设备包括更多所启用的增值特征。这可允许消费者针对其需要和/或期望而选取适当或期望的产品，但是也可能会提供使伪造者和/或攻击者在不具有对设备的较低成本模型的授权的情况下解锁特征的机会。

发明内容

[0003] 所公开的各种实施例涉及计算机配件设备的安全性，从配件设备的组件的制造贯穿到配件的消费者使用。例如，一个非限制性实施例提供一种主机计算设备，其被配置成引导与配件设备的相互认证会话的初始部分，并且经由计算机网络将关于主机计算设备和配件设备的信息发送给远程配对服务。主机计算设备还被配置成：从远程配对服务接收配对证书，该配对证书经由远程配对服务的私钥进行加密；并且使用来自远程配对服务的配对证书完成与配件设备的相互认证。

[0004] 提供该发明内容来以简化形式介绍在下文具体实施方式中进一步描述的概念的选择。该发明内容不旨在标识所要求保护的主题的关键特征或必要特征，也不旨在用于限制所要求保护的主题的范围。此外，所要求保护的主题不限于解决本公开内容的任何部分中所指出的任何或全部缺陷的实现方式。

附图说明

[0005] 图1示出了计算设备和配件设备的示例实施例。

[0006] 图2示出示意性地图示了配件设备组件制造和最终使用之间的各种示例步骤的框图。

[0007] 图3示出了用于在组件制造、组件递送和设备制造期间保护配件设备的方法的实施例的流程图。

[0008] 图4示出描绘了用于在配件设备组装期间激活配件设备上的安全芯片的方法的实施例的流程图。

[0009] 图5A和5B示出描绘了用于经由第三方远程配对服务手动地认证配件设备和主机计算系统的方法的实施例的流程图。

[0010] 图6示出示意性地图示了手动认证期间图5A和5B的实施例的配件设备、主机计算设备和远程配对服务的实施例的框图。

[0011] 图7示出描绘了用于在认证配件设备之后解锁配件设备的方法的实施例的流程图。

[0012] 图8示出示意性地图示了图7的配件设备的实施例的框图。

[0013] 图9示出图示了计算系统的示例实施例的框图。

具体实施方式

[0014] 如上文所提及的，一些计算机配件伪造防止方案可以利用每一个可信设备上的安全芯片，其中安全芯片可以允许主机计算机对设备进行认证。然而，这样的伪造防止方案可以在不具有对于配件所连接到的主机计算设备的任何知识的情况下对配件进行认证。另外，如果安全芯片本身失窃或丢失，则安全芯片可以用于生产伪造设备。

[0015] 另外，如上文所描述的，即便是可信配件设备也可能易受未经授权的使用形式的影响。例如，一些配件设备可以以具有所启用的不同特征的不同价格点而得到，使得更昂贵的设备可以包括更多所启用的增值特征。这可以允许消费者针对其需要和/或期望而选取适当或期望的产品，但是也为伪造者和/或攻击者提供了这样的机会，即：使伪造者和/或攻击者在不具有对设备的较低成本模型的认证的情况下解锁特征，从而在没有进行支付的情况下获取增值特征。

[0016] 用于保护增值特征的先前解决方案可以依赖于在固件更新之前使用秘密密钥来核对固件图像的有效性以防止未经授权的更新。然而，采用单个密钥对每一个固件图像进行签名可能会允许所有系统在单个密钥变得已知的情况下受损。

[0017] 因此，本文所公开的实施例解决关于防止计算配件的伪造生产和/或使用的各种问题。例如，为了防止使用丢失或失窃的安全芯片，一些实施例针对在将安全芯片安装到配件设备中的工厂处激活各个安全芯片，使得丢失或失窃的安全芯片不能用于生产伪造设备。

[0018] 附加地，实施例针对计算设备配件和主机计算设备的相互认证。这可以促进计算机配件的SKU(库存单元)差异化。例如，相互认证可以用于对旨在与特定主机一起使用的SKU进行认证，而单向认证可以用于对旨在用于不同主机的不同SKU进行认证。这还可以允许具体配件设备与具体主机计算系统之间的“配对”能力。如下文更详细描述的，这样的配对可以由远程第三方服务控制，使得未经授权的配件和/或受损的控制台可以受约束以不能与生态系统的其他部分一起工作。

[0019] 另外的其他实施例针对配件设备的安全解锁以防止增值特征的未经授权的解锁。如下文更详细描述的，这些实施例可以利用另外的非安全芯片(例如片上系统(SOC))上的安全硬件模块来提供安全芯片和SOC之间的安全交互，使得安全芯片而不是SOC芯片上的固件控制解锁过程。这可以通过将硬件安全模块并入到SOC设计中而使得可能不具有安全方面的专业技术的SOC生产商能够生产安全SOC芯片。

[0020] 图1示出了根据本公开内容的实施例的用于计算系统和配件设备的示例使用环境100。使用环境100包括以视频游戏控制台的形式的计算设备102，其与显示设备104通信使得计算设备102可以将视频内容输出到显示设备104。用户106被图示为经由以传感器系统的形式的配件设备108与计算设备102交互，该传感器系统被配置成经由一个或多个使用环境传感器对用户106进行感测。配件设备108可以包括任何适当的一个或多个传感器，其包括但不限于二维图像传感器(例如RGB或灰度级传感器)、深度图像传感器(例如飞行时间或结构化光深度传感器)、立体摄像机系统、一个或多个麦克风(例如定向麦克风阵列)和/或

任何其他适合的传感器。尽管本文在主机视频游戏控制台和配件传感器系统的上下文中进行描述，但是将理解到，所公开的实施例可以应用于任何适当的主机和配件系统。

[0021] 图2示出描绘了制造和使用配件设备的示例方法200中的各种步骤的框图。首先，方法200包括在组件制造商处制造配件设备的安全芯片和其他组件，如分别由202和204所指示的。将理解到，可以在不同位置处制得各种组件，并且然后将其输运到组装设施以用于配件设备生产。因此，方法200包括将用于组装配件的安全芯片和其他组件输运到配件设备制造商，如在206处所指示的。如上文将描述的，安全芯片可以制造成使得它们未激活直到在配件设备生产设施处被激活为止，使得它们在配件设备制造之前丢失或失窃的情况下不能被用于伪造配件中。

[0022] 在配件设备制造设施处，由接收自组件制造商的组件来制造配件。如下文所描述的，用于每一个配件的安全芯片可以在制造将该芯片并入在内的配件期间或之后被激活。然后，分别在208和210处，所制造的配件被传递到配件的设计者/销售商，并且然后销售给消费者。消费者然后可以将经授权的配件设备连接到适当的主机设备。在认证和解锁后，获取经认证和激活的配件设备以用于使用和享用。

[0023] 图3图示了用于防止在配件设备制造之前丢失、失窃或以其他方式不恰当地获取的安全芯片的未经授权使用的方法300的实施例。简要地说，方法300利用了私钥/公钥对，其中在安全条件之下，将公钥提供给安全芯片制造商并且将私钥提供给配件设备制造商。私钥可以以智能卡或具有适当安全特性的其他计算设备(例如其难以进行逆向工程)的形式提供给安全芯片制造商，该智能卡或具有适当安全特性的其他计算设备在本文中被称为“安全模块”。另外，安全模块还可以包括可执行以限制可由安全模块激活的安全芯片数目的代码。以此方式，安全的任何破坏，例如经由存储在安全模块上的私钥的破坏，可以受限于经授权的激活数目，并且因而可以限制安全受损的影响。另外，在一些实施例中，安全模块可以包括用于配件设备的不同SKU的不同私钥(每一个具有对应的公钥)。

[0024] 方法300示出在安全芯片制造商、配件设备制造商、以及利用配件设备制造商来制造用于销售的配件设备的设备设计者/销售商中的每一个处发生的过程。方法300包括：在302处，将用于配件设备安全芯片的公钥，或者在一些实施例中用于每一个SKU的公钥发送给安全芯片制造商；以及在304处，在安全芯片制造商处接收(一个或者多个)公钥。方法300还包括在306处将具有用于每一个公钥的私钥的安全模块发送给配件设备制造商，其中在308处对其进行接收。

[0025] 方法300还包括在310处制造安全芯片，其中每一个安全芯片包括适当的公钥(例如用于配件设备的意图SKU的正确公钥)。安全芯片被制造为处于未激活状态，使得芯片固件最初仅对“激活”命令做出响应，并且不会执行除激活过程中所使用的那些操作之外的其他安全芯片操作，直到激活已经完成为止。将理解到，并入了安全芯片的配件设备可以不操作，直到安全芯片得以激活并且配件设备得以认证为止。

[0026] 在制造具有适当的公钥的未激活安全芯片后，方法300包括在312处将安全芯片发送给配件设备制造商，其中在314处对其进行接收。接下来，在316处，方法300包括组装配件设备并且然后激活安全芯片。关于示例安全芯片激活过程的细节在下文参照图4进行描述。在完成配件设备的制造并且激活安全芯片后，方法300包括在318处将配件设备发送给设计者/销售商，其在320处将设备销售给消费者。

[0027] 如上文所提及的，在一些实施例中，安全模块或其他私钥存储设备可以包括可执行代码，其限制可以由该安全模块执行的安全芯片解锁的数目。因此，在激活经授权数目的安全芯片之后，方法300包括在322处达到针对该安全模块的经授权安全芯片激活的限制。在该实例中，没有附加的安全芯片可以被激活，除非从配件设备设计者/销售商(或者负责安全芯片公钥/私钥的其他方)获取新的安全模块，或者增加用于当前安全模块和(一个或多个)当前公钥/私钥的限制。对每个安全模块上可以被激活的安全芯片的数目强加限制可以帮助限制私钥的破坏对安全模块的负面影响。

[0028] 在一些实施例中，安全通信信道可以用于将安全芯片激活限制的更新传送到安全模块。因此，方法300包括传送指令以增加用于该安全模块的芯片激活限制(假定尚未发生安全模块的破坏)。方法300然后包括在326处在安全模块处接收限制增加，并且在328处激活附加的安全芯片。将理解到，如果确定安全模块上的私钥已经被破坏，则新的公钥/私钥对可以被生成以代替每一个被破坏的私钥，并且新的私钥可以经由新的安全模块传递到配件设备制造商。

[0029] 安全芯片可以在配件制造位置处以任何适合的方式被激活。图4示出描绘了用于在配件设备制造商位置处激活安全芯片的方法的示例实施例的流程图。图4示出了在配件设备上的安全芯片、安全模块、以及被配置成使得能够与安全模块通信的应用(例如运行在计算机上的智能卡接口应用)中的每一个处发生的过程。

[0030] 方法400包括在402处从应用向安全芯片发送针对芯片标识号的请求，并且在一些实施例中针对安全芯片的SKU的请求。安全芯片在404处接收该请求。作为响应，安全芯片在406处生成随机数，并且在408处向应用发送该随机数、芯片标识号和SKU。在410处，应用接收该信息并且将其转发给安全模块，其中在412处对其进行接收。在接收后，安全模块在414处利用适当的私钥(例如对应于SKU的私钥)对随机数、芯片ID和SKU签名，并且在416处向应用发送已签名的值。安全模块还可以使激活限制计数器减量(或增量，这取决于特定实现方式)，如在417处所指示的。在其他实施例中，激活限制计数器可以在芯片激活完成之后减量。

[0031] 继续，方法400包括在418处接收信号值，并且将已签名的值转发给安全芯片。接下来，在420处，安全芯片使用在制造时包括于安全芯片上的公钥来核实已签名的值，并且然后在422处确定所核实的值是否与之前发送给安全模块的正确值匹配。如果值正确，则方法400包括在424处激活安全芯片。在另一方面，如果值不匹配，则方法400包括在426处不激活安全芯片。

[0032] 一旦安全芯片被激活，则准备将配件设备销售给消费者。如上文所提及的，配件设备可以包括安全措施，其防止配件设备被使用，直到附加安全条件得以满足为止。例如，配件设备可以被配置成在首次连接到主机设备时不起作用直到该配件设备已经被认证为止。在一些实施例中，这样的认证过程可以由主机来驱动，使得配件设备简单地响应于主机命令或消息。例如，取决于命令，配件设备要么将数据发送给主机以用于核实，要么对发送自主机的数据进行处理以核实其正确地遵循相关认证协议。仅在认证已经成功完成的时候，设备才将开始进行正常的功能性。

[0033] 在一些实例中，认证可以是单向认证，其中配件设备不对主机进行认证。在其他实施例中，认证可以是相互的使得主机和配件设备彼此认证。这可以允许建立主机和配件设

备的“配对”，使得配件设备具体地与该主机相关联。

[0034] 图5A和5B示出描绘了用于相互认证主机计算设备和配件设备的方法500的实施例的流程图。适当的主机和配件设备的示例包括但不限于权利要求1中所图示的视频游戏控制台和传感器系统。简要地参照图6，方法500图示了在以下每一个处执行的过程，即：包括安全芯片602的配件设备600、主机计算设备604、以及调解相互认证的远程配对服务606。尽管相互认证协议的各种部分可以被描述为由配件设备执行，但是将理解到，处理消息的实体可以实际上为设备内的安全芯片，并且配件设备固件简单地在主机和安全芯片之间输运消息。这可以帮助防止中间人攻击。

[0035] 方法502包括在502处从主机计算设备向配件设备发送“主机问候(host hello)”消息，其中主机问候消息包括随机现时。在504处，配件设备接收主机问候消息，并且在506处发送具有另一随机现时的“设备问候”消息，其由主机在508处接收。另外，在510处，配件设备还将安全芯片证书发送给主机设备，该证书由主机在512处接收和核实(例如通过联系发布设备证书的证书授权机构)以确认安全芯片证书有效。另外，在一些实施例中，在相互认证会话的初始部分期间，主机可以在认证的该初始部分期间从配件设备接收配置信息，并且如果经由检查配置信息而确定不准许配件设备与主机设备一起使用(例如配件设备是不正确的SKU)，则拒绝认证。

[0036] 接下来，如513和514处所示，主机和远程配对服务建立安全连接，以发起配对过程。主机然后获取配对私钥/公钥对以帮助配对功能，如516处所示。配对私钥/公钥对可以作为配对过程的一部分而被生成，或者可以被预先配置。在获取配对私钥/公钥对之后，在518处，主机将安全芯片证书和配对私钥发送给远程配对服务，在520处对其进行接收。

[0037] 在接收到该信息后，在522处，远程配对服务可以确定是否应当允许主机和配件设备的配对。例如，如果已知任一设备已经受损、如果配件是用于主机的不正确SKU、和/或如果已知其他潜在问题，那么可以拒绝配对，如524处所指示的。在另一方面，如果在522处确定准许主机和配件设备之间的配对，那么在526处，远程配对服务可以将配对证书发送给主机，其中配对证书包括配对公钥和安全芯片证书的摘要(digest)，其所有都经由配对服务的私钥(其要与主机在516处所获取的配对密钥区分开)进行签名。远程配对服务还可以存储关于主机服务和配件设备的标识信息以用于在确定是否允许涉及主机设备和配件设备中的一个或多个的未来配对时使用，如527处所示。

[0038] 主机在528处接收配对证书，并且然后在530处将配对证书作为“主机证书”转发给配件设备。配件设备在532处接收主机证书，并且在534处经由远程配对服务的公钥核实主机证书。该公钥对应于用来在526处对配对证书进行加密的私钥。在经由公钥核实主机证书之后，配件设备可以核实主机证书中所包含的信息，如536处所指示的。如果配对证书中的信息未被核实，那么配对过程可以中止。

[0039] 主机还在538处生成“预主秘密(pre-master secret)”，并且经由配件设备上的安全芯片的公钥对预主秘密进行加密，使得只有私钥持有者(例如配件设备上的安全芯片)可以对其进行解码。预主秘密可以包括任何适合的信息，诸如随机数。主机在541处将预主秘密发送给配件设备，配件设备在542处接收预主秘密。主机还在544处经由预主秘密以及在主机/配件“问候”消息交换期间所交换的两个现时来生成“主秘密”。

[0040] 在接收到预主秘密后，配件设备可以经由配件设备的私钥对预主秘密进行解密，

如548处所指示的，并且可以从该值和两个“问候”现时导出主秘密，如550处所示。接下来，主机在552处生成“主机证书核实”消息并且利用在516处所获取的私有配对密钥来对该消息签名。主机然后在554处将主机证书核实消息发送给配件设备。配件设备在556处接收主机证书核实消息，并且在558处经由包括于主机证书中的配对公钥对其进行核实。这允许配件设备确认主机证书中的配对公钥由向远程服务提供配对公钥的相同设备来发送。

[0041] 继续在560处，主机生成并且发送“主机完成”消息给配件设备，其在562处接收该消息。同样地，配件设备在564处生成并且发送“设备完成消息”，其由主机在566处接收。当完成相互认证过程后，配件设备可以解锁并且开始正常功能运行。方法500的相互认证过程可以提供优于诸如TLS(传输层安全协议)相互认证之类的其他相互认证过程的优点。例如，利用方法500，每一个主机和设备对具有其自身的密钥，因此令某个主机和设备对受损将不会引起生态系统的大幅崩溃。另外，因为配对是由在线服务控制，所以离线攻击对于该过程可能不会成功。附加地，由于安全芯片本身控制配件设备侧上的过程，因而安全芯片可以用在各种各样的不同设备中，由此允许认证过程适配于其他配件。

[0042] 如上文所提及的，在一些实例中，单向认证可以用于对配件设备的解锁进行授权。这样的认证可以类似于参照图5A-5B所描述的那种认证，但是其中省略涉及远程服务和配对证书的步骤，使得预主秘密消息是在主机处接收和核实安全芯片证书之后从主机发送到配件的第一消息。另外，在一些实施例中，不同配件SKU可以利用不同认证过程。例如，旨在用于与特定主机一起使用的SKU可以利用相互认证，而旨在用于与更宽范围的计算设备(例如PC型设备)一起使用的SKU可以利用单向认证。在这样的实施例中，如果主机由于设备是非正确SKU而拒绝相互认证，则主机可以执行单向认证以使得能够使用配件设备。将理解到，可以使用任何适当的单向认证过程。

[0043] 图7示出描绘了用于在认证之后解锁配件设备的方法700的示例实施例的流程图。简要地参照图8，方法700图示了在配件设备804内的片上系统(SOC)802和安全芯片800上执行的过程。SOC包括非安全的固件805，以及被实现为SOC上的硬件以将安全芯片800的安全域扩展到SOC 802中的安全硬件模块806。安全硬件模块806可以并入到任何期望的非安全组件中，以增加将安全状态信息从安全芯片安全地直接传递到安全硬件模块的能力。安全硬件模块然后可以使用安全状态来启用或禁用SOC内的具体特征。

[0044] 通过限定安全硬件模块，减小了确认SOC安全的工作的范围。SOC的大部分可以被视为不受信的，而安全硬件模块是受信的。使用安全硬件模块硬件块可以进一步使得能够将该硬件块并入到由卖主所限定的设备，该卖主可能不具有开发安全产品方面的技术能力和/或经验。

[0045] 安全硬件模块806可以包括任何适合的组件。例如，在所描绘的实施例中，安全硬件模块806包括随机数生成器808或其他适合的熵源、硬件测错(sniffing)接口810和非易失性存储器812。随机数生成器808可以用来制定发送给安全芯片800的质询消息(challenge message)。硬件测错接口810可以用来确定在安全硬件模块806处所接收的消息是否是从SOC外部的安全芯片800接收的，而不是来自SOC上的潜在受损的固件。非易失性存储器812可以用于存储用来对与安全芯片的通信进行加密的密钥。在一些实施例中，密钥可以是对称密钥，使得相同密钥存储在安全芯片上，并且可以特定于该安全芯片/SOC对，使得每一个配件设备具有其自身的对称密钥对。在其他实施例中，可以使用任何其他适合的

密钥。

[0046] 返回到图7，方法700包括在701处接收解锁请求(例如在认证已经完成之后来自主机的请求)，并且在702处，从SOC上的固件向SOC上的安全硬件模块发送针对随机数的生成的请求。作为响应，安全硬件模块在704处生成随机数，并且在706处经由共享密钥对随机数进行加密。经加密的随机数然后在708处被提供给固件，使得固件仅看到该数的经加密版本。固件接收经加密的随机数，并且然后将经加密的随机数转发给安全芯片，如在710处所指示的。安全芯片在712处接收经加密的随机数，在714处利用共享密钥对随机数进行解密，并且然后在716处对经解密的随机数执行操作以形成新值。可以执行任何适合的操作。一个非限制性示例是二进制补码操作。

[0047] 在对随机数执行操作以产生新值之后，安全芯片在718处经由共享密钥对新值进行加密，并且在720处将经加密的新值发送给SOC。SOC在722处接收经加密的新值，并且将其转发给安全硬件模块。安全硬件模块在724处经由硬件测错接口确认经加密的新值是从SOC外部接收到的，而不是源自SOC上的位置。接下来，安全硬件模块在728处经由共享密钥对经加密的新值进行解密，并且执行在716处所执行的那个操作的逆操作以获取随机数的原始值。安全硬件模块然后可以将逆操作的结果与原始随机数相比较，以确保安全芯片是可信的。如果比较正确，那么安全硬件模块可以解锁SOC，由此使得配件设备能够起作用。

[0048] 在一些实施例中，由安全芯片发送的解锁指令可以包括指示设备要被解锁的单个比特。在其他实施例中，可以由安全芯片发送多个比特以解锁SOC的不同特征(例如其中每一个比特控制不同特征)。这可以提供用于SKU区分的附加机制。

[0049] 将理解到，上述实施例是出于示例的目的而呈现的，并且可以使用用于安全芯片激活、相互或单向认证、以及设备解锁的任何其他适当的方法。例如，用于激活安全芯片的方法的另一实例实施例如下。首先，在芯片制造时，针对安全芯片的每个SKU生成随机主密钥。然后，通过使用该随机主密钥并且还使用每个芯片的ID，可以使用诸如HMAC-SHA256之类的HMAC算法来导出每个芯片的激活密钥。

[0050] 每个芯片的激活密钥(PerChipActivationKey)=HMAC-SHA256(主密钥(MasterKey)，PUID)。

[0051] 每个芯片的激活密钥安全地存储在安全芯片内，并且不能在安全芯片之外读出。因为这是针对每一个安全芯片而执行的，因而每一个芯片具有所存储的不同激活密钥。因而，在特定芯片的激活密钥受损的情况下，其他芯片不受影响。这可以帮助提供抵抗针对激活密钥的攻击的额外安全。

[0052] 接下来。在配件设备制造时，主密钥经由安全模块(例如智能卡)从安全芯片工厂安全地传递到配件设备工厂。智能卡可以接受安全芯片标识号作为输入，使用与安全芯片制造时所用的相同算法导出每芯片激活密钥，并且使用激活密钥生成另一摘要：

[0053] 激活摘要(ActivationDigest)=HMAC-SHA256(每个芯片的激活密钥(PerChipActivationKey)，PUID+附加追踪信息(AdditionalTrackingInfo))。

[0054] 激活摘要是“激活(Activate)”命令对安全芯片的输入。当安全芯片接收该输入时，其可以被配置成使用其自身的激活密钥的副本来计算相同摘要。如果摘要与输入匹配，则安全芯片可以激活其自身并且开始常规功能。

[0055] 在计算激活摘要时，值“附加追踪信息”可以用于追踪每一个芯片的激活。可以使

用任何适当的值。例如，在一些实施例中，附加追踪信息可以是记录安全模块已经激活了多少个安全芯片的序号(序号(SquenceNumber))。该信息也可以作为激活命令的输入而传递给安全芯片：

[0056] 激活(SMID,序号,激活摘要)。

[0057] 另外，该信息还可以在激活之后安全地存储在芯片内，使得随后安全芯片可以可选地将该信息报告给在线系统，并且在线系统也可以追踪每一个芯片及其激活状态。这可以增加又一安全层，因为如果安全模块也失窃(但是主密钥尚未公开)，则在线系统可以知晓失窃安全模块的多少个芯片已经被激活。另外，如上文所描述的，每一个安全模块还可以在其可以激活多少个芯片方面受限制，由此帮助减小由失窃安全模块所引起的损害。安全模块可以是密码保护的，以提供附加的安全。因为对于该激活过程而言，激活密钥是针对每个芯片的，所以失窃芯片将不会使其他芯片受损。

[0058] 在一些实施例中，上文所描述的方法和过程可以依赖于一个或多个计算设备的计算系统。特别地，这样的方法和过程可以实现为计算机应用程序或服务、应用编程接口(API)、库和/或其他计算机程序产品。

[0059] 图9示意性地示出了可以制定上述方法和过程中的一个或多个的计算系统900的非限制性实施例。计算系统900以简化形式示出。将理解到，实际上可以在不脱离本公开内容的范围的情况下使用任何计算机架构。在不同实施例中，计算系统900可以采取大型计算机、服务器计算机、台式计算机、膝上型计算机、平板计算机、家用娱乐计算机、配件设备、网络计算设备、游戏设备、移动计算设备、移动通信设备(例如，智能电话)、智能卡等形式。计算系统的示例包括但不限于各种配件设备、主机设备、和智能卡、和上述其他计算设备。

[0060] 计算系统900包括逻辑子系统902和存储子系统904。计算系统900可以可选地包括显示子系统906、输入子系统908、通信子系统910和/或未在图9中示出的其他组件。

[0061] 逻辑子系统902包括被配置成执行指令的一个或多个物理设备。例如，逻辑子系统可以被配置成执行指令，其作为一个或多个应用、服务、程序、例程、库、对象、组件、数据结构或其他逻辑构造的一部分。这样的指令可以实现为执行任务、实现数据类型、变换一个或多个组件的状态、或者以其他方式到达期望结果。

[0062] 逻辑子系统可以包括被配置成执行软件指令的一个或多个处理器。附加地或可替换地，逻辑子系统可以包括被配置成执行硬件或固件指令的一个或多个硬件或固件逻辑机器。逻辑子系统的处理器可以是单核或多核的，并且在其上执行的程序可以配置用于串行、并行或分布式处理。逻辑子系统可以可选地包括分布于两个或更多个设备之中的单个组件，其可以位于远程位置和/或配置用于协同处理。逻辑子系统的方面可以是虚拟化的并且由配置在云计算配置中的远程可访问的联网计算设备执行。

[0063] 存储子系统904包括一个或多个物理、非瞬时性设备，其被配置成保存由逻辑子系统可执行以实现本文所描述的方法和过程的数据和/或指令。当实现这样的方法和过程时，存储子系统904的状态可以变换--例如变换为保存不同数据。

[0064] 存储子系统904可以包括可移除介质和/或内置设备。存储子系统904可以包括除了其他方面之外的光学存储器设备(例如CD、DVD、HD-DVD、蓝光盘等)、半导体存储器设备(例如RAM、EPROM、EEPROM等)和/或磁性存储器设备(例如硬盘驱动器、软盘驱动器、磁带驱动器、MRAM等)。存储子系统904可以包括易失性、非易失性、动态、静态、读/写、只读、随机存

取、顺序存取、位置可寻址、文件可寻址、和/或内容可寻址的设备。

[0065] 将了解到，存储子系统904包括一个或多个物理设备。然而，在一些实施例中，本文所描述的指令的方面可以经由通信介质通过纯信号(例如电磁信号、光信号等)传播，这与存储设备相反。此外，涉及本公开内容的数据和/或其他形式的信息可以通过纯信号传播。

[0066] 在一些实施例中，逻辑子系统902和存储子系统904的方面可以一起集成到一个或多个硬件逻辑组件中，通过该硬件逻辑组件，可以制定本文所描述的功能性。这样的硬件逻辑组件可以包括例如现场可编程门阵列(FPGA)、特定于编程和应用的集成电路(PASIC/ASIC)、特定于程序和应用的标准产品(PSSP/ASSP)、片上系统(SOC)系统、以及复杂可编程逻辑设备(CPLD)。

[0067] 术语“模块”、“程序”和“引擎”可以用于描述被实现为执行特定功能的计算系统900的方面。在一些情形中，模块、程序或引擎可以经由执行由存储子系统904所保存的指令的逻辑子系统902而实例化。将理解的是，可以从相同应用、服务、代码块、对象、库、例程、API、功能等实例化不同模块、程序和/或引擎。同样地，可以通过不同应用、服务、代码块、对象、例程、API、功能等实例化相同模块、程序和/或引擎。术语“模块”、“程序”和“引擎”可以涵盖单独或成组的可执行文件、数据文件、库、驱动器程序、脚本、数据库记录等。

[0068] 将了解到，本文所使用的“服务”是可跨多个用户会话执行的应用程序。服务可以可用于一个或多个系统组件、程序和/或其他服务。在一些实现方式中，服务可以运行在一个或多个服务器计算设备上。

[0069] 当包括显示子系统906时，该显示子系统906可以用于呈现由存储子系统904保存的数据的虚拟表示。该虚拟表示可以采取图形用户接口(GUI)的形式。因为本文所描述的方法和过程改变了由存储子系统保存的数据，并且因而变换了存储子系统的状态，所以显示子系统906的状态同样可以被变换成虚拟地表示底层数据中的改变。显示子系统906可以包括实际上利用任何类型的技术的一个或多个显示设备。这样的显示设备可以与逻辑子系统902和/或存储子系统904组合在共享外壳中，或者这样的显示设备可以是外围显示设备。

[0070] 当包括输入子系统908时，该输入子系统908可以包括诸如键盘、鼠标、触摸屏、游戏控制器之类的一个或多个用户输入设备或者与这种用户输入设备交互。在一些实施例中，输入子系统可以包括诸如上文所描述的配件设备实施例之类的所选自然用户输入(NUI)元件部分或者与所选自然用户输入元件部分交互。这样的元件部分可以是集成的或外围的，并且输入动作的转导和/或处理可以在板上或板外处置。示例NUI元件部分可以包括用于话音和/或语音识别的麦克风；用于机器视觉和/或手势识别的红外、颜色、立体和/或深度相机；用于运动检测和/或意图识别的头部追踪器、眼部追踪器、加速度计和/或陀螺仪；以及用于评估脑部活动的电场感测元件部分。

[0071] 当包括通信子系统910时，该通信子系统910可以被配置成使计算系统900与一个或多个其他计算设备通信耦合。通信子系统910可以包括与一个或多个不同通信协议兼容的有线和/或无线通信设备。作为非限制性示例，通信子系统可以被配置用于经由无线电话网络、或有线或无线局域网或广域网进行通信。在一些实施例中，通信子系统可以允许计算系统900经由诸如互联网之类的网络向其他设备发送消息和/或从其他设备接收消息。

[0072] 将理解到，本文所描述的配置和/或方法在本性上是示例性的，并且这些具体实施例或示例不应被视为是限制意义的，因为众多变化是可能的。本文所描述的具体例程或方

法可以表示任何数目的处理策略中的一个或多个。因此，所图示和/或描述的各种动作可以以所图示和/或描述的序列、以其他序列、并行地执行或者被省略。同样地，上述过程的次序可以改变。

[0073] 本公开内容的主题包括本文所公开的各种过程、系统和配置、以及其他特征、功能、动作和/或属性的所有新颖且非显而易见的组合和子组合，以及其任何和全部等同形式。

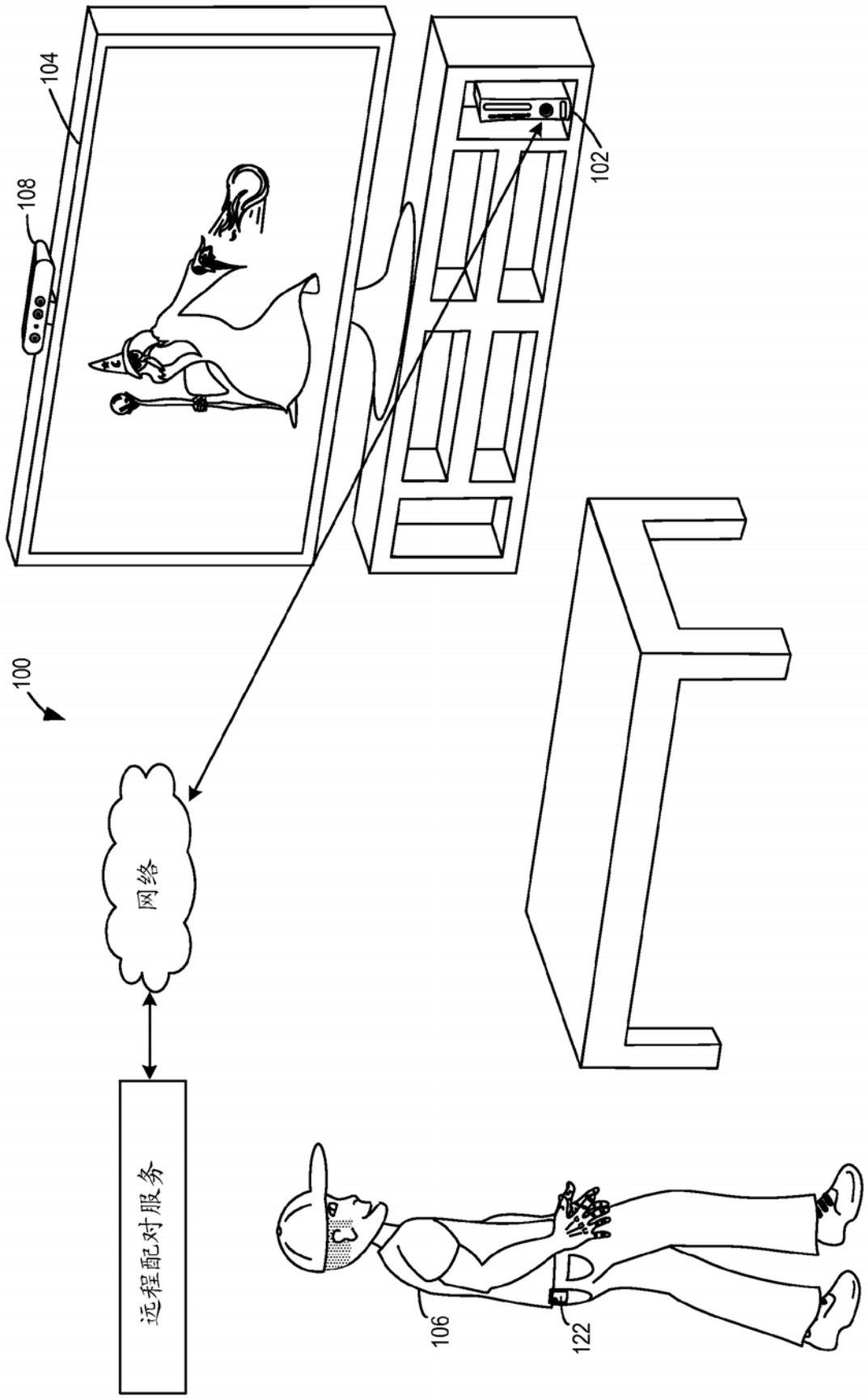


图 1

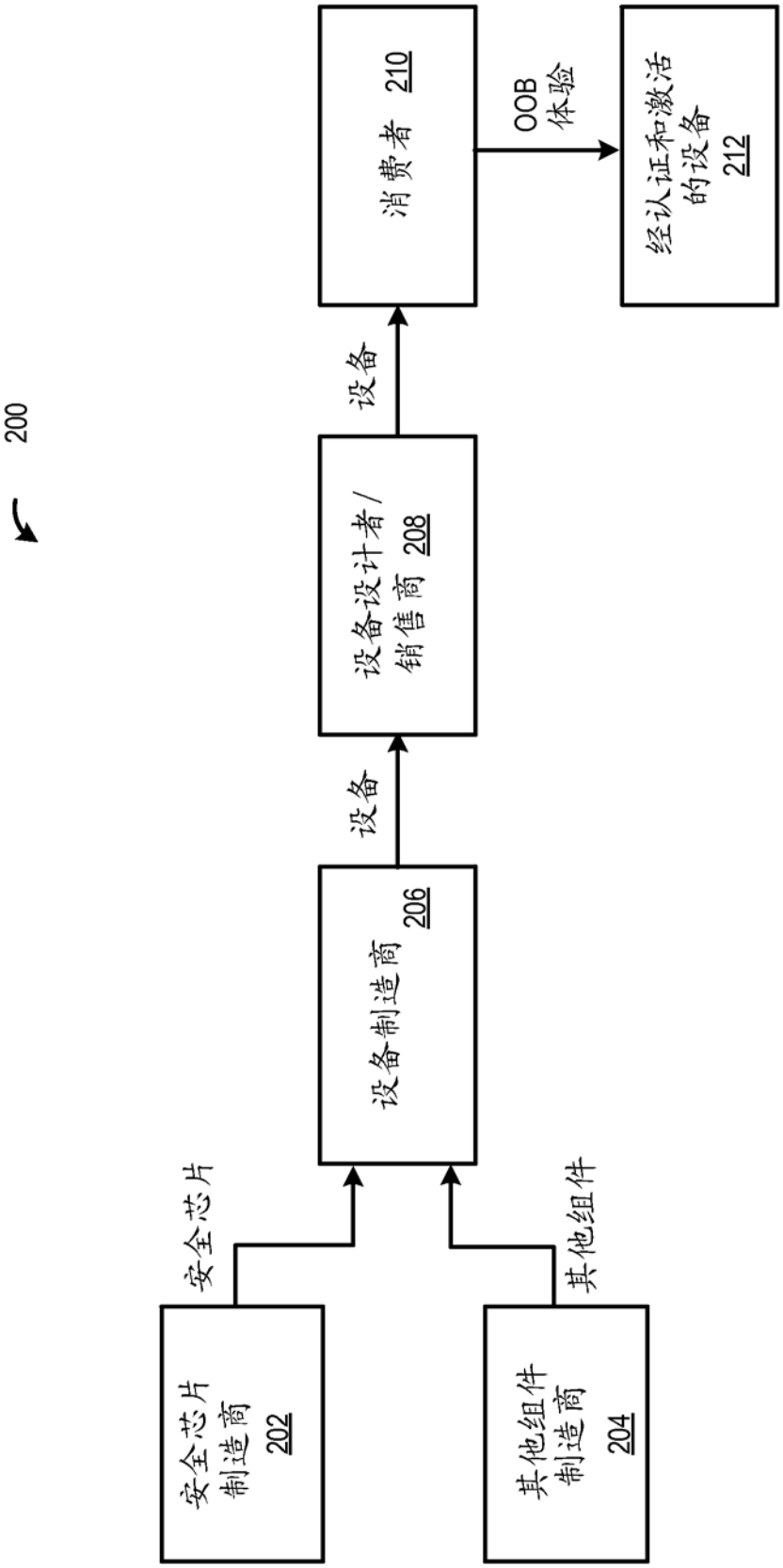

200
安全芯片
制造商
202
其他组件
制造商
204
安全芯片
其他组件
设备制造商
206
设备
设备设计者/
销售商 208
设备
消费者 210
OOB
体验
经认证和激活
的设备
212

图 2

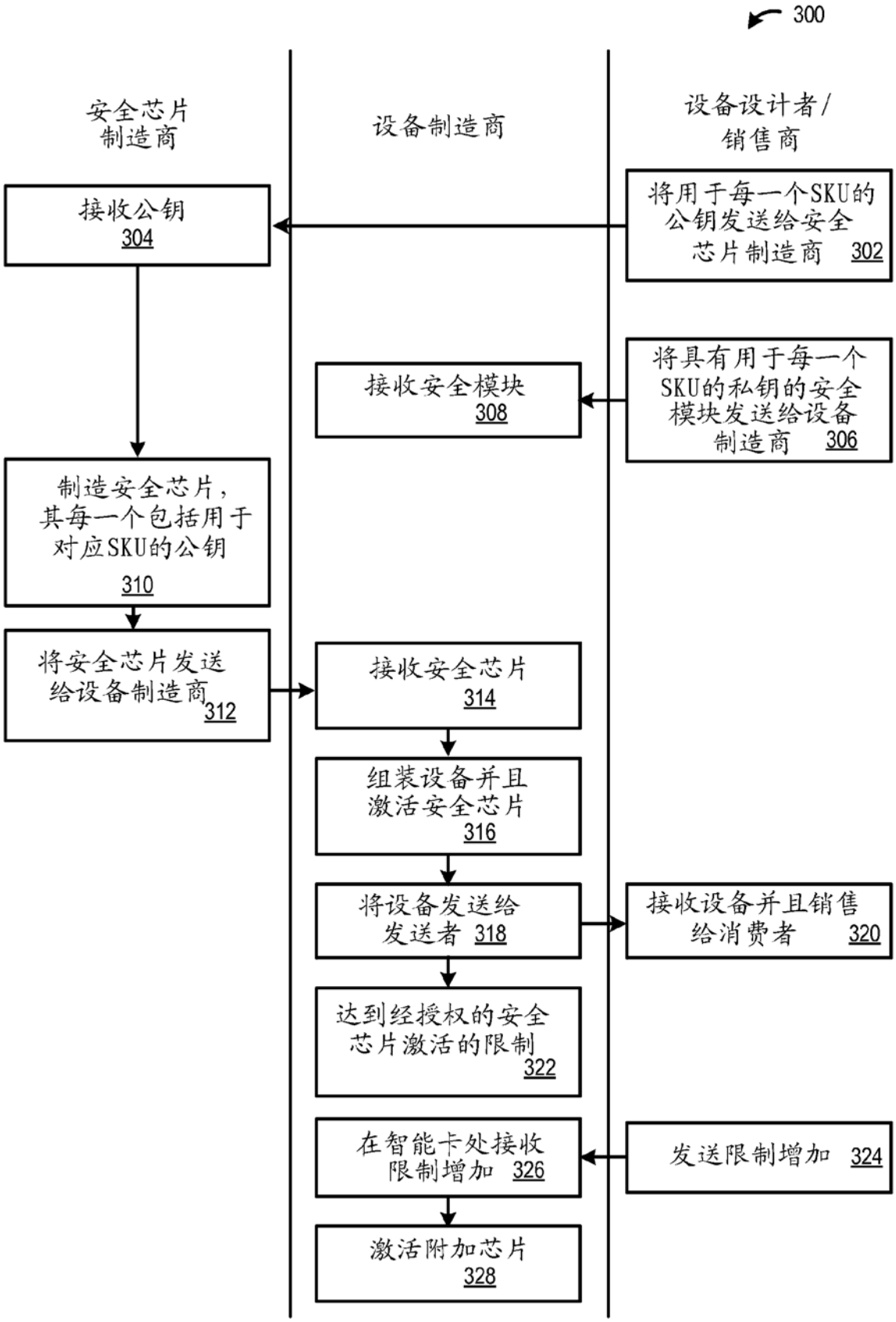

300
安全芯片制造商
设备制造商
设备设计者/销售商
接收公钥 304
将用于每一个SKU的公钥发送给安全芯片制造商 302
接收安全模块 308
将具有用于每一个SKU的私钥的安全模块发送给设备制造商 306
制造安全芯片，其每一个包括用于对应SKU的公钥 310
将安全芯片发送给设备制造商 312
接收安全芯片 314
组装设备并且激活安全芯片 316
将设备发送给发送者 318
接收设备并且销售给消费者 320
达到经授权的安全芯片激活的限制 322
在智能卡处接收限制增加 326
发送限制增加 324
激活附加芯片 328

图 3

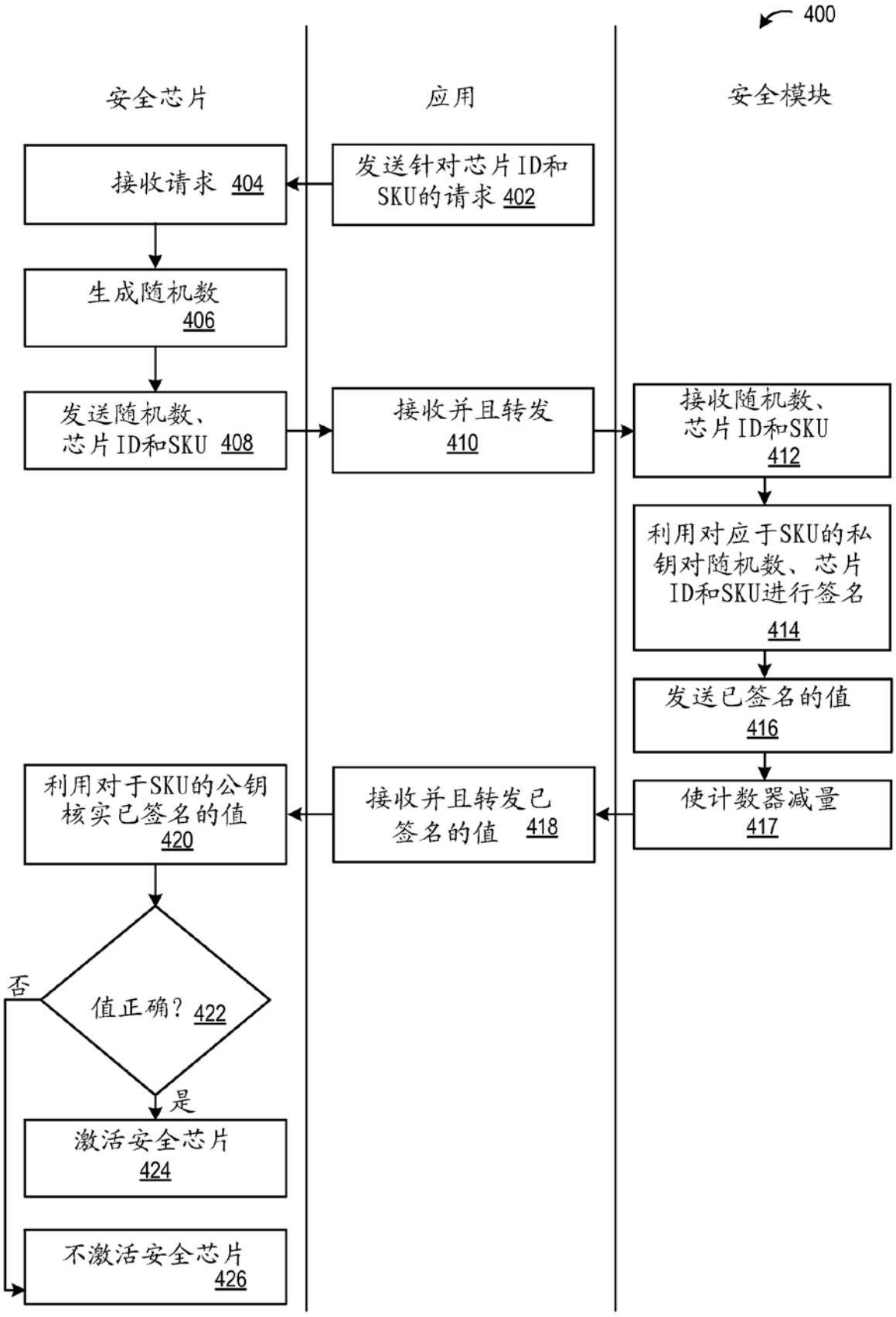

400
安全芯片
应用
安全模块
发送针对芯片ID和SKU的请求 402
接收请求 404
生成随机数 406
发送随机数、芯片ID和SKU 408
接收并且转发 410
接收随机数、芯片ID和SKU 412
利用对应于SKU的私钥对随机数、芯片ID和SKU进行签名 414
发送已签名的值 416
使计数器减量 417
接收并且转发已签名的值 418
利用对于SKU的公钥核实已签名的值 420
值正确? 422
否
是
激活安全芯片 424
不激活安全芯片 426

图 4

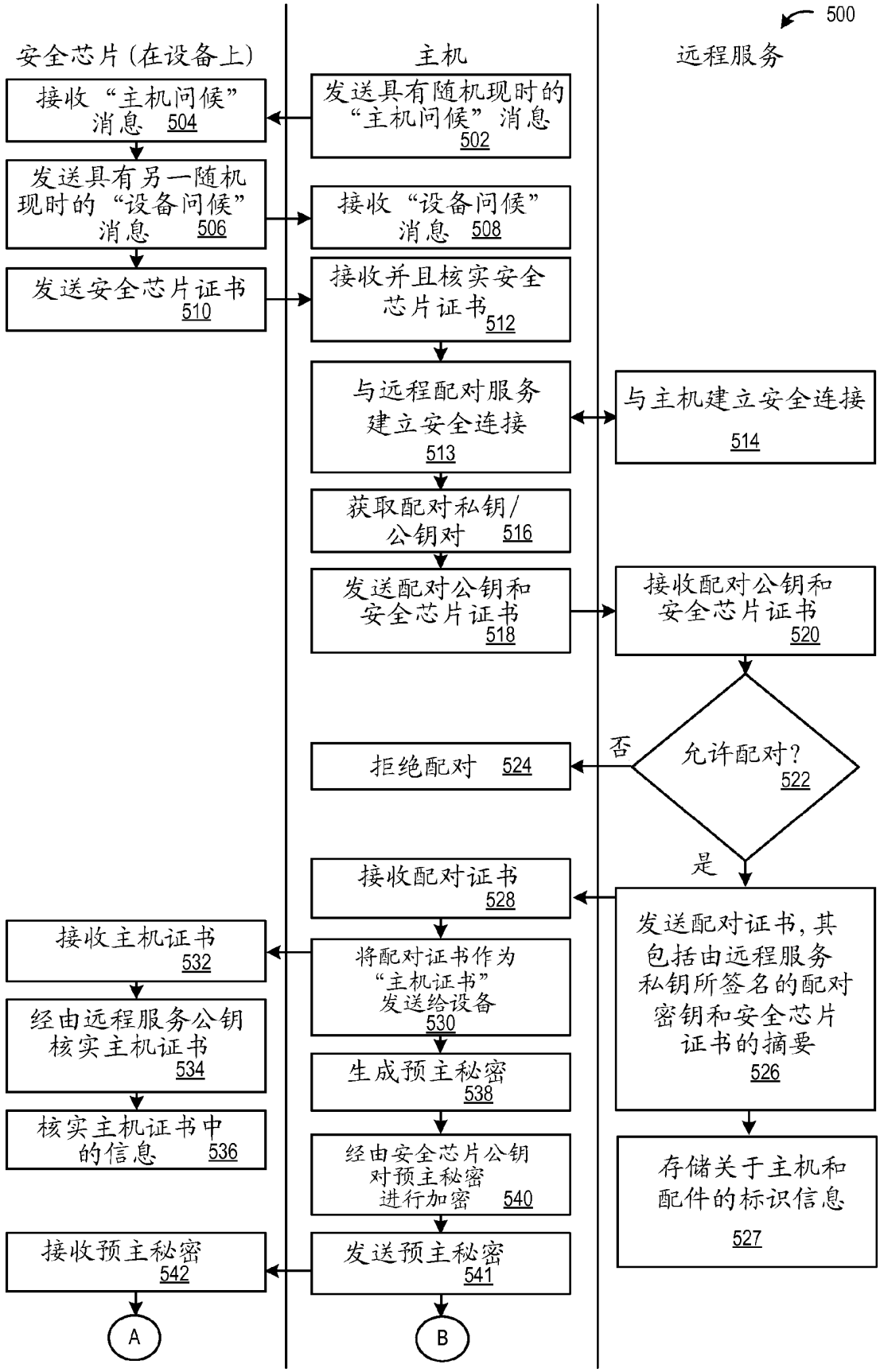

500
安全芯片(在设备上)
主机
远程服务
接收“主机问候”消息 504
发送具有随机现时的“主机问候”消息 502
发送具有另一随机现时的“设备问候”消息 506
接收“设备问候”消息 508
发送安全芯片证书 510
接收并且核实安全芯片证书 512
与远程配对服务建立安全连接 513
与主机建立安全连接 514
获取配对私钥/公钥对 516
发送配对公钥和安全芯片证书 518
接收配对公钥和安全芯片证书 520
允许配对? 522
否
拒绝配对 524
是
接收配对证书 528
发送配对证书,其包括由远程服务私钥所签名的配对密钥和安全芯片证书的摘要 526
接收主机证书 532
将配对证书作为“主机证书”发送给设备 530
经由远程服务公钥核实主机证书 534
生成预主秘密 538
存储关于主机和配件的标识信息 527
核实主机证书中的信息 536
经由安全芯片公钥对预主秘密进行加密 540
接收预主秘密 542
发送预主秘密 541
A
B

图 5A

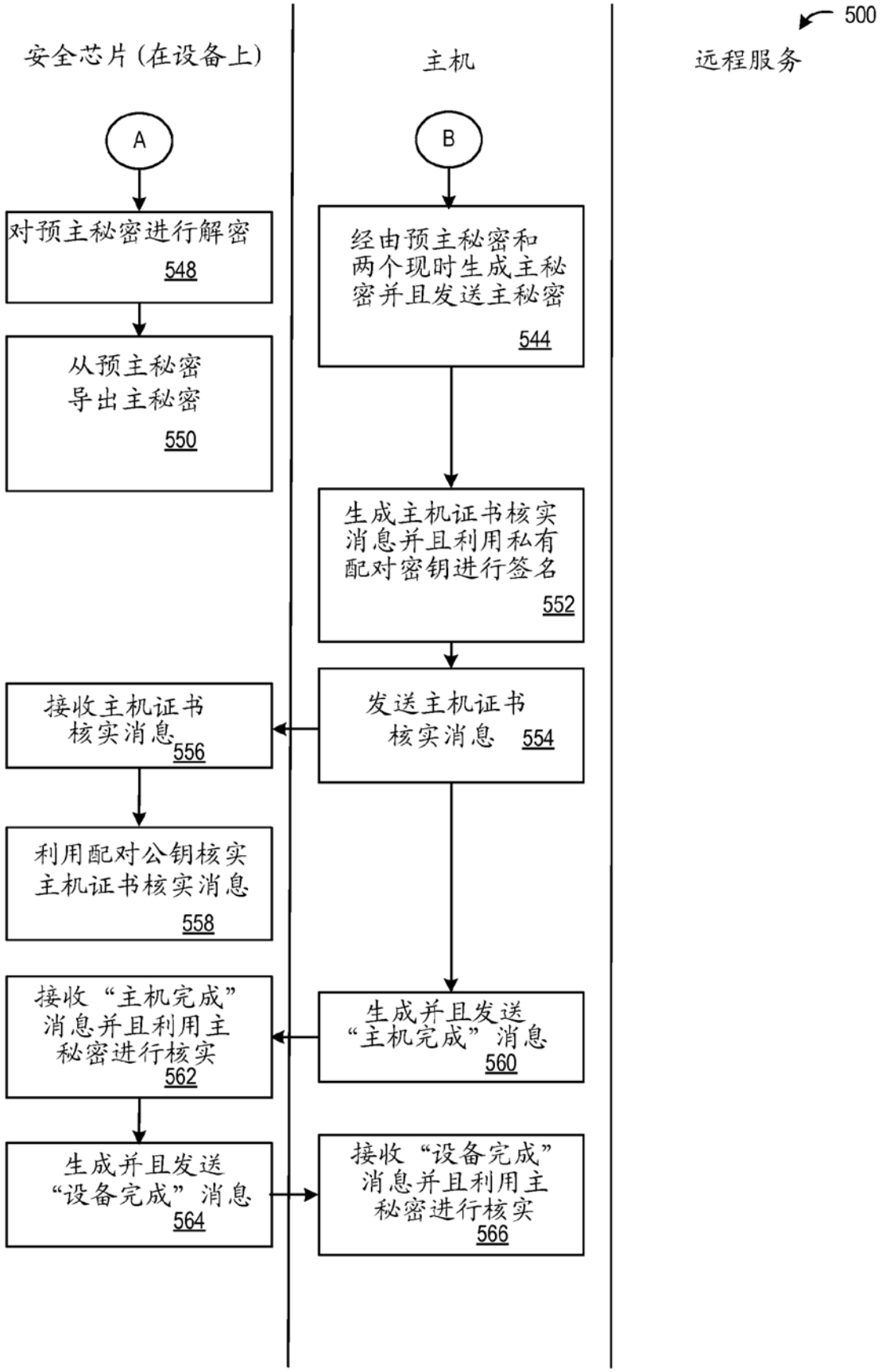

500
安全芯片(在设备上)
主机
远程服务
A
B
对预主秘密进行解密
548
经由预主秘密和
两个现时生成主秘
密并且发送主秘密
544
从预主秘密
导出主秘密
550
生成主机证书核实
消息并且利用私有
配对密钥进行签名
552
接收主机证书
核实消息
556
发送主机证书
核实消息 554
利用配对公钥核实
主机证书核实消息
558
接收“主机完成”
消息并且利用主
秘密进行核实
562
生成并且发送
“主机完成”消息
560
生成并且发送
“设备完成”消息
564
接收“设备完成”
消息并且利用主
秘密进行核实
566

图 5B

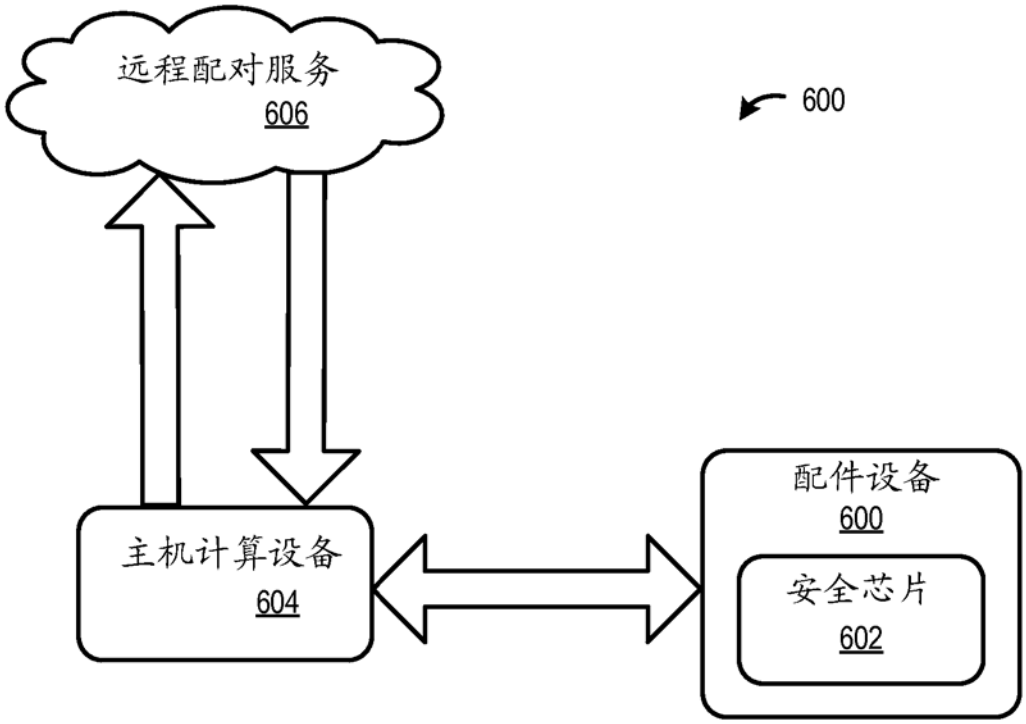


图 6

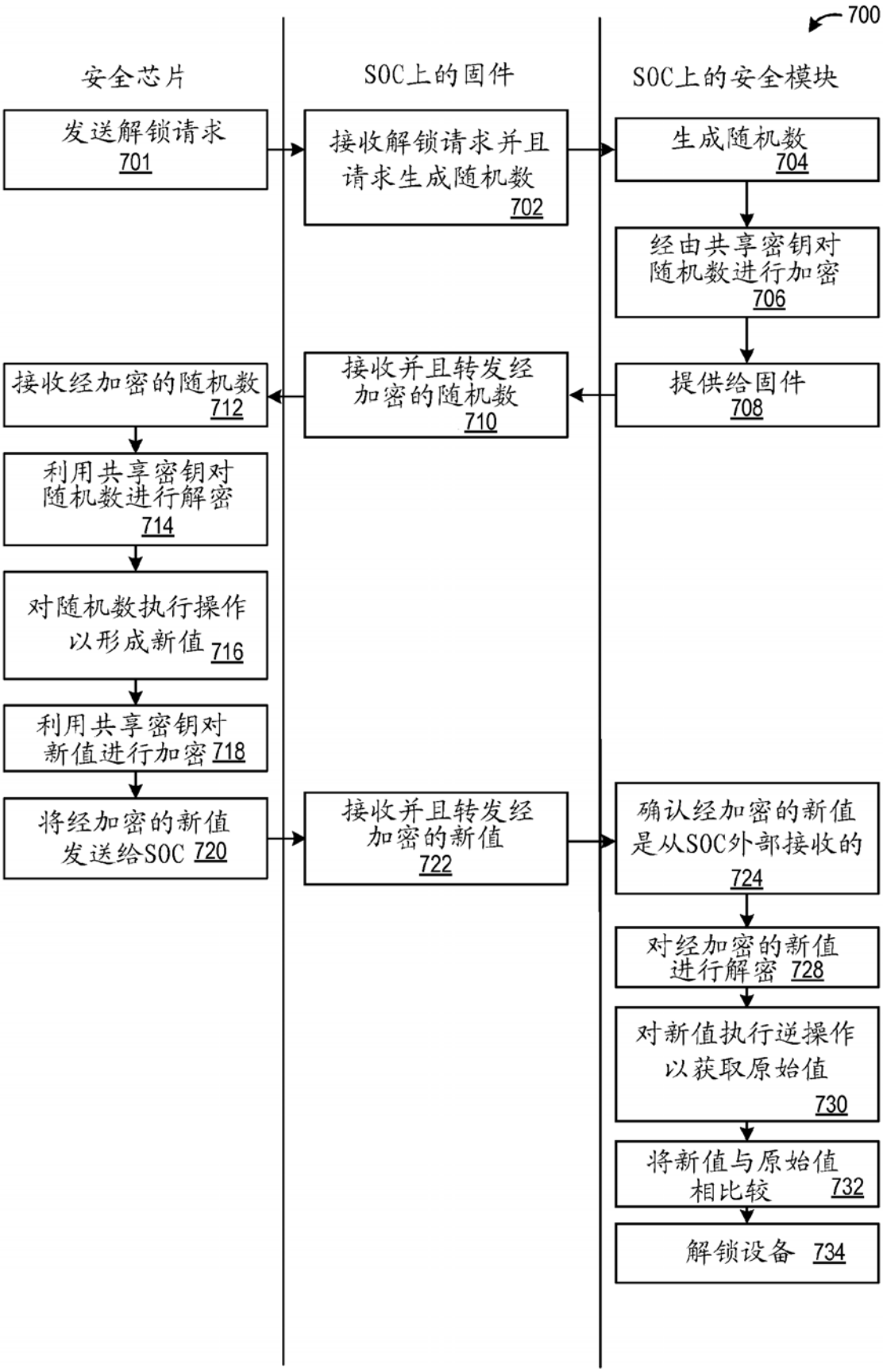

700
安全芯片
SOC上的固件
SOC上的安全模块
发送解锁请求 701
接收解锁请求并且请求生成随机数 702
生成随机数 704
经由共享密钥对随机数进行加密 706
提供给固件 708
接收并且转发经加密的随机数 710
接收经加密的随机数 712
利用共享密钥对随机数进行解密 714
对随机数执行操作以形成新值 716
利用共享密钥对新值进行加密 718
将经加密的新值发送给SOC 720
接收并且转发经加密的新值 722
确认经加密的新值是从SOC外部接收的 724
对经加密的新值进行解密 728
对新值执行逆操作以获取原始值 730
将新值与原始值相比较 732
解锁设备 734

图 7

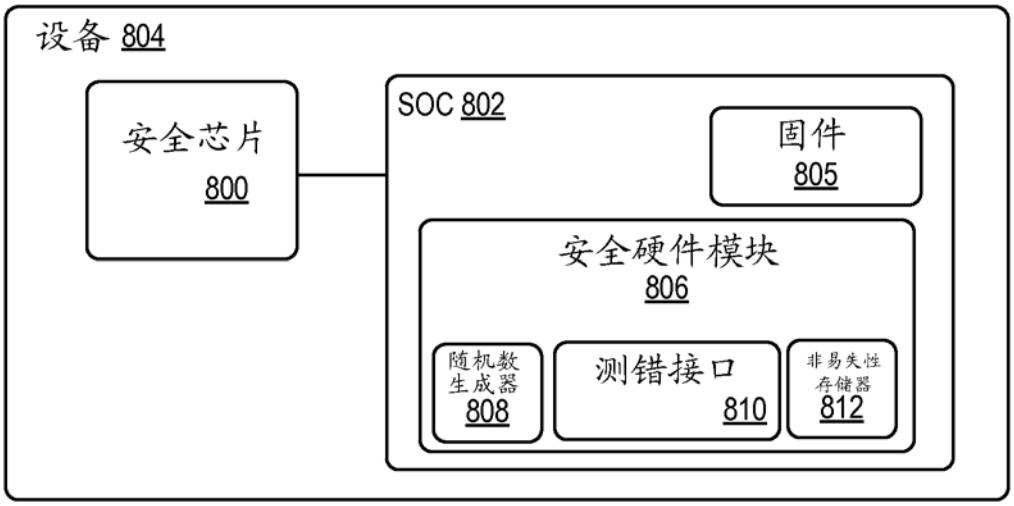

设备 804
安全芯片
800
SOC 802
固件
805
安全硬件模块
806
随机数生成器
808
测错接口
810
非易失性存储器
812

图 8

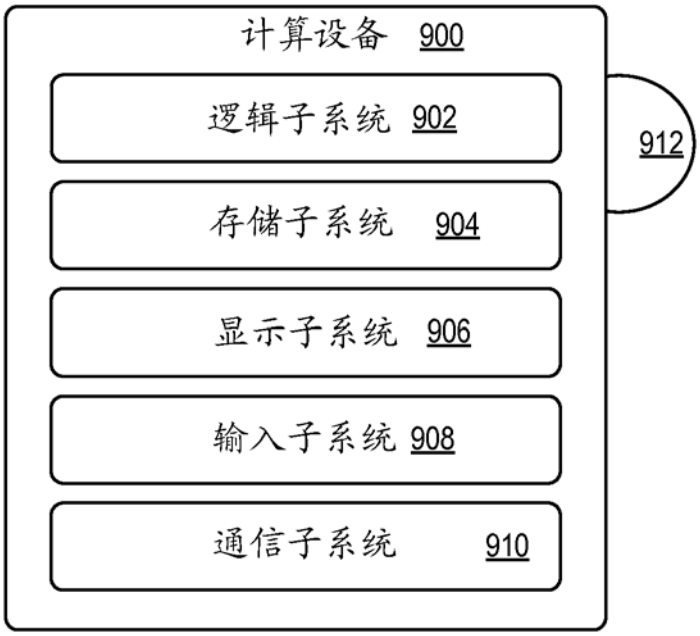

计算设备 900
逻辑子系统 902
存储子系统 904
显示子系统 906
输入子系统 908
通信子系统 910
912

图 9