(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 105144626 B
(45)授权公告日 2019.02.12

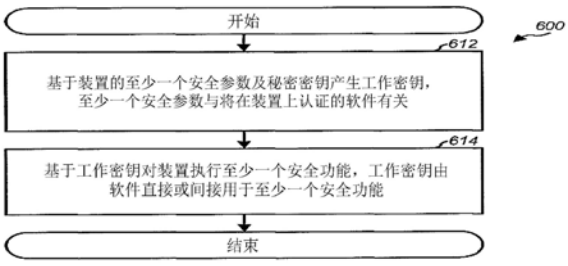
(21)申请号 201480022000.X
(22)申请日 2014.04.16
(65)同一申请的已公布的文献号
申请公布号 CN 105144626 A
(43)申请公布日 2015.12.09
(30)优先权数据
13/868,859 2013.04.23 US
(85)PCT国际申请进入国家阶段日
2015.10.13
(86)PCT国际申请的申请数据
PCT/US2014/034414 2014.04.16
(87)PCT国际申请的公布数据
WO2014/176101 EN 2014.10.30
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 阿萨夫·阿什克纳济
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 宋献涛
(51)Int.Cl.
H04L 9/08(2006.01)
G06F 21/10(2006.01)
H04L 9/32(2006.01)
(56)对比文件
US 2012201379 A1,2012.08.09,
CN 101379506 A,2009.03.04,
CN 101026455 A,2007.08.29,
CN 201181472 Y,2009.01.14,
US 2003163719 A1,2003.08.28,
审查员 李红玲
权利要求书2页 说明书8页 附图7页

(54)发明名称

提供安全性的方法和设备

(57)摘要

本发明揭示用于提高电子装置的安全性的技术。在本发明的一个方面中，装置的安全性可通过基于所述装置的硬件秘密密钥及至少一个安全参数(例如)用密钥导出函数产生工作密钥来提高。所述安全参数可与将在所述装置上认证的软件及/或无线装置的安全性的其它方面有关。所述安全参数可指示是否授权所述软件及/或经授权用于所述软件的至少一个操作功能。可基于所述工作密钥对所述装置执行至少一个安全功能。举例来说，所述工作密钥可用于对所述装置的数据进行加密、标志、解密或验证。所述工作密钥可由所述软件直接或间接用于所述至少一个安全功能。



CN 105144626 B

1.一种提供安全性的方法,其包括:

通过执行密钥导出函数来产生工作密钥,其中所述密钥导出函数的输入包括用于由安全机制使用以对软件进行认证的一组安全参数中的至少一个安全参数以及装置的秘密密钥,在所述工作密钥的所述产生之前将所述组安全参数及所述秘密密钥提供且存储在所述装置上;及

在激活所述安全机制以认证所述软件之前,所述软件基于所述工作密钥对所述装置执行至少一个安全功能,所述工作密钥由所述软件直接或间接用于所述至少一个安全功能。

2.根据权利要求1所述的方法,其中所述至少一个安全参数确定经授权用于所述装置上的所述软件的至少一个操作功能。

3.根据权利要求1所述的方法,其中所述至少一个安全参数包括用于确定是否授权所述软件用于所述装置的公共密钥。

4.根据权利要求3所述的方法,其中对应于私有密钥的所述公共密钥用于对所述软件进行标志。

5.根据权利要求1所述的方法,其中在不同时间将所述秘密密钥及所述至少一个安全参数加载到所述装置上。

6.根据权利要求1所述的方法,其中所述秘密密钥由第一实体载入到所述装置上,且所述至少一个安全参数由不同于所述第一实体的第二实体载入到所述装置上。

7.根据权利要求1所述的方法,其中所述执行至少一个安全功能包括通过所述工作密钥对所述装置的数据进行加密或标志。

8.根据权利要求1所述的方法,其中所述执行至少一个安全功能包括通过所述工作密钥对所述装置的数据进行解密或验证。

9.根据权利要求1所述的方法,其中所述执行至少一个安全功能包括在所述软件的控制下执行所述至少一个安全功能。

10.根据权利要求1所述的方法,其进一步包括:

在不经由安全机制认证所述软件的情况下在所述装置上执行所述软件。

11.根据权利要求1所述的方法,其进一步包括:

将所述秘密密钥存储在所述装置上的安全存储器中;及

将所述至少一个安全参数存储在所述装置上的所述安全存储器或不安全存储器中。

12.一种提供安全性的设备,其包括:

用于通过执行密钥导出函数来产生工作密钥的构件,其中所述密钥导出函数的输入包括用于由安全机制使用以对软件进行认证的一组安全参数中的至少一个安全参数以及装置的秘密密钥,在所述工作密钥的所述产生之前将所述组安全参数及所述秘密密钥提供且存储在所述装置上;及

用于在激活所述安全机制以认证所述软件之前基于所述工作密钥对所述装置执行至少一个安全功能的构件,所述工作密钥由所述软件直接或间接用于所述至少一个安全功能。

13.根据权利要求12所述的设备,其中在不同时间将所述秘密密钥及所述至少一个安全参数加载到所述装置上。

14.一种提供安全性的设备,其包括:

存储器，其经配置以存储装置的软件；及

处理器，其耦合到所述存储器且经配置以：

通过执行密钥导出函数来产生工作密钥，其中所述密钥导出函数的输入包括用于由安全机制使用以对软件进行认证的一组安全参数中的至少一个安全参数以及装置的秘密密钥，在所述工作密钥的所述产生之前将所述组安全参数及所述秘密密钥提供且存储在所述装置上；及

在激活所述安全机制以认证所述软件之前，基于所述工作密钥对所述装置执行至少一个安全功能，所述工作密钥由所述软件直接或间接用于所述至少一个安全功能。

15.根据权利要求14所述的设备，其中在不同时间将所述秘密密钥及所述至少一个安全参数加载到所述装置上。

16.一种包括指令非暂时性计算机可读媒体，所述指令在被至少一个计算机执行时致使所述至少一个计算机执行以下操作：

通过执行密钥导出函数来产生工作密钥，其中所述密钥导出函数的输入包括用于由安全机制使用以对软件进行认证的一组安全参数中的至少一个安全参数以及装置的秘密密钥，在所述工作密钥的所述产生之前将所述组安全参数及所述秘密密钥提供且存储在所述装置上；及

在激活所述安全机制以认证所述软件之前，基于所述工作密钥对所述装置执行至少一个安全功能，所述工作密钥由所述软件直接或间接用于所述至少一个安全功能。

17.根据权利要求16所述的非暂时性计算机可读媒体，其中在不同时间将所述秘密密钥及所述至少一个安全参数加载到所述装置上。

提供安全性的方法和设备

技术领域

[0001] 本发明大体上涉及电子设备，且更具体来说，涉及用于在电子装置上提供安全性的技术。

背景技术

[0002] 电子装置(例如，蜂窝电话或智能手机)通常基于控制装置上的硬件的操作且支持装置的各种功能的软件来操作。安全机制(例如，安全启动)可用于确保仅已授权用于装置的软件可在装置上执行。然而，在激活装置上的安全机制之前，装置可易受到恶意攻击(例如，在制造期间)。在此易受损时间段期间，未经授权的软件可被恶意地加载到装置上并且通过装置执行以访问装置上的安全信息(例如，安全密钥)及/或使用安全信息操纵数据。.

发明内容

[0003] 本文揭示用于提高电子装置的安全性的技术。在本发明的方面中，装置的安全性可通过基于所述装置的硬件秘密密钥及至少一个安全参数产生工作密钥来提高。所述工作密钥(而不是所述硬件秘密密钥)可用于在装置上执行安全功能(例如，对数据进行加密及解密)。

[0004] 在示例性设计中，可基于装置的至少一个安全参数及秘密密钥(例如)通过密钥导出函数产生工作密钥。所述至少一个安全参数可与将在所述装置上认证的软件及/或所述装置的安全性的其它方面有关。可基于工作密钥对所述装置执行至少一个安全功能。举例来说，所述工作密钥可用于对所述装置的数据进行加密、标志、解密或验证。所述工作密钥可由所述软件直接或间接用于所述至少一个安全功能。

[0005] 所述至少一个安全参数可控制所述装置的安全性的各个方面。举例来说，所述至少一个安全参数可确定是否授权所述软件在所述装置上执行、是否对所述软件授权至少一个操作功能等。在一个设计中，所述至少一个安全参数可包含用于确定是否授权所述软件用于所述装置的公共密钥。所述公共密钥可对应于用于标志所述软件的私有密钥。所述至少一个安全参数还可包括其它类型的信息。

[0006] 下文进一步描述本发明的各种方面及特征。

附图说明

[0007] 图1展示无线装置的方框图。

[0008] 图2展示无线装置的示范性制造过程。

[0009] 图3A展示用于存储关于无线装置的安全信息的过程。

[0010] 图3B展示用于执行无线装置的安全启动的过程。

[0011] 图4展示基于硬件秘密密钥对数据进行加密及解密的过程。

[0012] 图5展示基于工作密钥对数据进行加密及解密的过程。

[0013] 图6展示用于提供装置的安全性的过程。

具体实施方式

[0014] 本文中揭示的安全密钥产生技术可用于各种电子装置，例如，无线通信装置、手持式装置、游戏装置、计算装置、消费型电子装置、计算机等。为了清楚起见，下文描述用于无线通信装置的技术。

[0015] 图1展示能够实施本文中揭示的安全密钥产生技术的无线装置100的示范性设计的方框图。无线装置100可为蜂窝电话、智能手机、平板计算机、无线调制解调器、个人数字助理(PDA)、手持式装置、膝上型计算机、智能本、上网本、无绳电话、无线本地环路(WLL)站、蓝牙装置等。无线装置100可支持与一或多个无线通信系统的双向通信。

[0016] 对于数据发射，数字模块120可处理(例如，编码及调制)待发射的数据并且向发射器(TMTR)114提供输出基带信号。发射器114可放大、过滤及上变频输出基带信号以产生可经由天线112发射到基站的输出射频(RF)信号。

[0017] 对于数据接收，天线112可从基站及/或其它发射器站接收信号并且可向接收器(RCVR)116提供接收到的RF信号。接收器116可将接收到的RF信号从RF下变频至基带、过滤及放大经下变频信号并且向数字模块120提供输入基带信号。数字模块120可处理(例如，解调及解码)输入基带信号以恢复发送到无线装置100的数据。

[0018] 数字模块120可包含各种处理、接口及存储器单元以支持无线装置100的数字处理。在图1中展示的设计中，数字模块120包含调制解调器处理器122、中央处理单元(CPU)/精简指令集计算机(RISC)处理器124、主控制器126、内部存储器130、安全存储器140、存储器控制器148，及输入/输出(I/O)控制器158，所有这些装置可经由一或多个数据总线160彼此通信。

[0019] 调制解调器处理器122可执行对数据发射及接收的处理，例如，编码、调制、解调、解码等。CPU/RISC处理器124可对无线装置100执行通用处理，例如，对音频、视频、图形及/或其它应用程序的处理。主控制器126可指导数字模块120内的各种单元的操作。内部存储器130可存储由数字模块120内的处理器及控制器使用的软件132及/或数据。内部存储器130可实施有静态随机存取存储器(SRAM)或其它类型的存储器。

[0020] 安全存储器140可存储安全密钥142、安全参数144、启动代码146及/或其它安全信息。安全密钥142可用于无线装置100上的安全功能，例如，以对无线装置100发送的数据进行加密、对发送待无线装置100的经加密数据进行解密、认证被加载到内部存储器130中的软件等。安全参数144可控制与无线装置100的安全性有关的各个方面。启动代码146可执行安全启动以认证被加载到无线装置100上的软件。安全存储器140可实施有只读存储器(ROM)、一次性可编程(OTP)元件，及/或其它类型的存储器。

[0021] 存储器控制器148可促进数据在外部存储器150与数字模块120之间的传送。外部存储器150可为数字模块120内的处理单元提供大容量存储装置。举例来说，外部存储器150可存储可被加载到数字模块120中用于执行的软件152、数据等。外部存储器150可包括(i)大容量非易失性存储器，例如，NAND闪存及/或NOR闪存存储器、(ii)大容量易失性存储器，例如，同步动态随机存取存储器(SDRAM)或动态随机存储器(DRAM)，及/或(iii)其它类型的存储器。I/O控制器158可允许无线装置100与安全服务器及/或其它实体通信。

[0022] 图1展示数字模块120的示范性设计。一般来说，数字模块120可包含任何数目的处

理、接口及存储器单元。数字模块120还可实施有一或多个数字信号处理器(DSP)、微处理器、RISC处理器等。可在一或多个专用集成电路(ASIC)及/或其它集成电路(IC)上实施数字模块120。

[0023] 电子装置，例如，无线装置100通常经过一系列制造步骤。在一或多个制造步骤期间电子装置可易受安全攻击。

[0024] 图2展示用于无线装置100(或任何电子装置)的示范性制造过程200。密钥提供实体可安全地提供无线装置100上的硬件(HW)秘密密钥(步骤1)。密钥提供实体可为用于无线装置100(如图2中展示)中的IC芯片(例如，ASIC)的集成电路(IC)芯片产品或一些其它实体。可将硬件秘密密钥存储在无线装置100上的安全存储器140中。

[0025] 装置制造商可能在对所制造装置的接入无法仅限于可信员工的不安全制造环境中制造或构建无线装置100。装置制造商可为原始装置制造商(ODM)(如图2中展示)、原始设备制造商(OEM)，或构建、组装及提供无线装置100的任何实体。装置制造商通常加载软件、加载安全参数及启用无线装置100上的安全功能(步骤2)。

[0026] 安全服务器可使用硬件秘密密钥提供具有秘密数据的无线装置100(步骤3)。通常在安全设施中执行安全数据提供以将秘密数据加载到无线装置100上。对于安全数据提供，安全服务器可使用硬件秘密密钥与无线装置100安全地交换数据。可将所提供的秘密数据存储在无线装置100上的安全存储器140中。

[0027] 如图2中展示，在制造过程期间可将安全参数加载到无线装置100上。安全参数可控制无线装置100上的安全性的各个方面并且可包含以下项中的一或多者：

[0028] • 与装置的信任根(RoT)有关的信息，

[0029] • 控制哪个软件可在装置上执行及/或软件可如何在装置上操作的信息，

[0030] • 控制可在装置上启用还是停用某些安全特征的信息，及/或

[0031] • 其它与安全有关的信息。

[0032] 安全参数可包含与无线装置100的信任根有关的信息。信任根可为无线装置100上的所有安全机制的根本。与信任根有关的信息可包含对应于一或多个私有根密钥的一或多个公共根密钥、用于公共根密钥的一或多个证书等。私有根密钥可用于标志发送到无线装置100的数据。对应公共根密钥可用于认证已通过私有根密钥标志的数据。举例来说，公共根密钥可用于安全启动中以认证被加载到无线装置100上的软件，如下文所描述。

[0033] 安全参数可控制哪一个软件可在无线装置100上执行及/或软件可如何在无线装置100上操作。举例来说，安全参数可包含用于认证经授权用于在无线装置100上执行的软件的公共密钥。所述软件可基于对应于公共密钥的私有密钥进行标志并且可存储在无线装置100上。所述软件可在于无线装置100上执行之前基于公共密钥进行认证，如下文所描述。

[0034] 安全参数可控制可在无线装置100上启用还是停用某些安全特征。举例来说，安全参数可控制是否启用无线装置100的安全启动、是否可停用无线装置100的调试能力以允许在测试或调试期间接入无线装置100的内部状态等。

[0035] 一些安全参数可用于多个目的。举例来说，公共根密钥可用作无线装置100的信任根以及用于控制哪一个软件可在无线装置100上执行。

[0036] 可将安全参数存储在无线装置100上的安全存储器140中。举例来说，可使用无线装置100的处理器的IC芯片上的OTP元件存储安全参数。所述OTP元件可实施有可在制造期

间被一次烧断的熔丝以经由熔丝的状态永久地存储数据。

[0037] 可通过允许无线装置100在执行软件之前认证软件的方式将软件及安全信息存储在无线装置100上。下文描述存储在无线装置100上的用于认证软件的示范性安全机制。

[0038] 图3A展示用于将安全信息存储在无线装置100上以支持被加载到无线装置100上的软件的认证的过程300的示范性设计。过程300可通过安全服务器或一些其它实体执行。

[0039] 在安全服务器处，符号函数320可在公共密钥X'上产生数字签名SR且使用私有根密钥R产生可能的其它信息。签名SR可用于认证为安全服务器的源实体。符号函数320可实施RSA(非对称密钥)算法、数字签名算法(DSA)，或一些其它密码编译(数字签名或加密)算法。证书产生器322可形成含有公共密钥X'、签名SR及可能其它信息的证书CR，所述其它信息例如，源实体的标识符、选择供使用的密码编译算法、证书的有效期等。可将此证书作为X.509证书存储在无线装置100上的安全存储器140(或一些其它存储器)中。公共根密钥R'可通过安全方式可用于无线装置100并且可存储在无线装置100上的安全存储器140(例如，OTP存储器或ROM)中。

[0040] 安全散列函数330可散列被加载到无线装置100上的软件并且可提供散列摘要S。安全散列函数330可实施SHA-1、SHA-2、MD-5或一些其它安全散列算法。符号函数332可使用私有密钥X在摘要S上产生数字签名SX。可将签名SX存储在外部存储器150中。符号函数332可实施RSA、DSA或一些其它密码编译算法。可将软件存储在无线装置100上的外部存储器150(或一些其它存储器)中。

[0041] 图3B展示用于无线装置100的安全启动的过程350的示范性设计。过程350可通过无线装置100执行，如下文所描述。在无线装置100处，验证函数370可从安全存储器140接收证书CR及公共根密钥R'。验证函数370可从证书CR提取签名SR及公共密钥X'、用公共根密钥R'验证签名SR及在签名SR得到验证的情况下提供公共密钥X'。由第三方对证书CR的任何篡改可由签名SR而不是通过验证容易地检测到。

[0042] 安全散列函数380可从外部存储器150接收软件、散列软件及提供散列摘要S'。安全散列函数380可实施由图3A中的安全散列函数330使用的相同安全散列算法。验证函数390可接收来自安全散列函数380的摘要S'、来自外部存储器150的数字签名SX及来自验证函数370的公共密钥X'。验证函数390可通过公共密钥X'及摘要S'验证数字签名SX且可指示数字签名SX是否得到验证。公共密钥X'通过公共根密钥R'进行认证。因此，由第三方对数字签名SX及/或软件的任何篡改可由数字签名SX而不是通过验证容易地检测到。如果数字签名SX得到验证，那么可提供软件以供使用。否则，可提供错误消息。

[0043] 图3A展示示范性安全启动软件标志过程。图3B展示示范性安全启动软件认证过程。还可通过其它方式实施安全启动。

[0044] 在正常操作期间，无线装置100可执行安全启动以在执行软件之前认证被加载到无线装置100上的软件。对于安全启动，无线装置100可首先通过公共根密钥R'认证签名SR以确定公共密钥X'的真实性。如果公共密钥X'得到认证，那么无线装置100可通过公共密钥X'认证签名SX以确定软件的真实性。安全启动可确保仅已授权用于无线装置100的软件可在无线装置100上执行。

[0045] 硬件秘密密钥通常提供于例如片上系统(SoC)IC等的ASIC上且用于对存储在ASIC外部的存储器中的数据进行加密及解密。此安全机制还称为安全文件系统或经加密文件系

统。通常将硬件秘密密钥与公共/私有密钥分开。硬件秘密密钥通常是用于对装置中的秘密进行加密及解密的对称密钥。举例来说，硬件秘密密钥可用于在将经加密数据存储在不受保护的数据存储装置(例如，固态磁盘(SSD)、多媒体卡(MMC)、eMMC等)中之前对数据进行加密。许多OEM并不信任其生产车间员工或ODM员工。因此，大部分安全实施方案并不允许软件访问ASIC上的硬件秘密密钥。然而，这些安全实施方案通常允许由软件间接使用硬件秘密密钥。此使用可包含数据的解密或加密。

[0046] 在软件已通过连接至ASIC的信任根(RoT)的认证机制认证及验证之后，所述软件可被视为可信的。此认证机制通常称为安全启动。然而，安全启动可能在制造过程期间不可用。

[0047] 通常的做法是提供具有通用ASIC的OEM/ODM，其中提供硬件秘密密钥、不启用安全启动及不提供信任根。可将硬件秘密密钥提供在装置或ASIC上的安全存储器中。在此阶段，在启用可保护装置上的软件的完整性的安全启动及/或其它安全机制之前，未经授权的软件可被加载到装置上且通过装置执行。提供于装置上的任何安全密钥可通过未经授权的软件操纵。这为不可信的ODM/OEM生产工人打开使用硬件秘密密钥操纵数据、曝露机密信息或危害通过硬件秘密密钥保护的数据的完整性的大门。

[0048] 无线装置100因此在从(i)在图2中在步骤1中硬件秘密密钥例如通过IC芯片制造商提供于无线装置100上的时候至(ii)在图2中在步骤3中例如通过OEM将安全性锁定在无线装置100上的时候可易受攻击。在此易受损时间段期间，未经授权的软件可被恶意地加载到无线装置100上并且通过无线装置执行以(i)访问硬件秘密密钥及/或(ii)使用硬件秘密密钥操纵数据，例如，在硬件秘密密钥不可由无线装置100上的软件访问的情况下。

[0049] 在本发明的一方面中，可通过基于可与经授权用于装置的软件有关的硬件秘密密钥以及至少一个安全参数产生工作密钥来提高装置的安全(并且可有效地寻址上文所描述的安全弱点)。工作密钥(而不是硬件秘密密钥)可用于对装置上的数据进行加密及/或解密。

[0050] 图4展示基于硬件秘密密钥以常规方式对数据进行加密及解密的过程400。在安全服务器410(其可属于OEM)处，密码引擎430可通过装置450的硬件秘密密钥442对数据进行加密以获得经加密数据。密码引擎430可如通过安全服务器410中的软件440引导那样操作。可将经加密数据发送到装置450。

[0051] 在装置450处，密码引擎470可从安全服务器410接收经加密数据且可通过装置450的硬件秘密密钥442对经加密数据进行解密。密码引擎470可如通过装置450中的软件480引导那样操作。如上所述，软件480在启用装置450上的安全启动之前可能是不安全的。在这种情况下，恶意软件可被加载到装置450上并且可经执行以(i)引导密码引擎470对经加密数据进行解密及/或(ii)操纵经解密数据。

[0052] 图5展示用于基于工作密钥以新颖方式对数据进行加密及解密的过程500的示范性设计。在安全服务器510处，单向密钥导出函数(KDF)522可基于可与在装置550上授权的软件有关的硬件秘密密钥542及至少一个安全参数544产生装置550的工作密钥。密码引擎530可通过工作密钥对数据进行加密以获得可发送到装置550的经加密数据。

[0053] 在装置550处，密钥导出函数522可基于装置550的硬件秘密密钥542及至少一个安全参数544产生装置550的工作密钥。密码引擎570可从安全服务器510接收经加密数据且可

通过工作密钥对经加密数据进行解密以获得经解密数据。

[0054] 在安全服务器510处，可将硬件秘密密钥542及/或安全参数544存储在安全服务器510内的安全存储装置541中。密钥导出函数522及密码引擎530可用硬件、软件及/或固件实施并且可通过(例如，执行于)安全服务器510内的处理器521实施。

[0055] 在装置550处，可将硬件秘密密钥542及/或安全参数544存储在装置550的安全存储器540中。举例来说，安全存储器540可包括OTP存储器并且可通过烧断OTP存储器的熔丝存储硬件秘密密钥542及/或安全参数544。密钥导出函数522及密码引擎570可用硬件、软件及/或固件实施并且可通过(例如，执行于)装置550内的处理器520实施。装置550可为图1中的无线装置100的一个示范性设计。安全存储器540可对应于图1中的无线装置100内的安全存储器140。处理器520可对应于图1中的无线装置100内的处理器122或124。

[0056] 多个密钥导出函数可用于在安全服务器510及装置550处的密钥导出函数522。密钥导出函数可利用一或多个密码编译散列函数，例如，SHA-1(安全散列算法)、SHA-2(其包含SHA-224、SHA-256、SHA-384及SHA-512)、MD-4(信息摘要)、MD-5等。安全散列算法具有密码编译特性，使得输入消息与输出摘要(其为伪随机位串)之间的函数不可逆并且两个输入消息映射到同一摘要的可能性极小。可如NIST 800-108中所描述实施公开可用的密钥导出函数522。

[0057] 如图2中展示，可将安全参数(例如，与信任根有关的安全信息及与安全启动有关的安全信息)提供于无线装置的安全存储器中作为制造过程的一部分。通常在硬件秘密密钥已提供于无线装置上之后完成安全参数的提供。安全参数通常不是秘密的且可通过未经授权的实体(例如，生产工人)提供。

[0058] 如图5中展示，密钥导出函数可用于基于在装置上提供的硬件秘密密钥及至少一个安全参数产生工作密钥。安全参数可与经授权用于装置的软件有关。安全参数还可确定装置上的系统密级及/或特定信任根。在已例如通过将安全参数提供于装置上之后可适当地产生工作密钥。工作密钥可由OEM用来保护秘密数据。未经授权的软件可在提供装置上的安全参数之前被恶意地加载到装置上。然而，未经授权的软件将不能够在不具有正确的安全参数集合的情况下产生正确的工作密钥。此外，可通过未经授权的实体(例如，不可信的员工)将不正确的安全参数加载到装置上。然而，在不具有正确的安全参数集合的情况下将不会产生正确的工作密钥且数据仍将受到保护。在任何情况下，不能够利用正确的工作密钥的软件将不能够对装置上的数据适当地进行加密或解密。

[0059] 图6展示用于提供安全性的过程600的示范性设计。过程600可通过装置，或安全服务器，或一些其它实体执行。可基于装置的至少一个安全参数及秘密密钥(例如，硬件秘密密钥)产生工作密钥(例如，通过密钥导出函数)(块612)。至少一个安全参数可与将在装置上认证的软件及/或无线装置的安全性的其它方面有关。可基于工作密钥执行对装置执行至少一个安全功能(块614)。工作密钥可由软件直接或间接用于至少一个安全功能。可将至少一个安全参数及/或秘密密钥存储在装置上的安全存储器中，例如，OTP元件中。

[0060] 至少一个安全参数可控制装置的安全性的各个方面。在一个设计中，至少一个安全参数可确定软件是否(或哪一个软件)经授权用于在装置上执行。在另一设计中，至少一个安全参数可确定经授权用于装置上的软件的至少一个操作功能(或软件可如何用于装置上)。在又一设计中，至少一个安全参数可包括用于确定是否授权软件用于装置的公共密

钥。公共密钥可对应于用于标志软件的私有密钥，例如，如图3A及3B中展示。至少一个安全参数还可包括其它类型的信息。

[0061] 在一个设计中，可通过第一实体(例如，IC芯片制造商，在IC芯片的制造期间)将秘密密钥加载到装置上。可通过第二实体(例如，OEM或ODM装置制造商)将至少一个安全参数加载到装置上，所述第二实体可不同于第一实体。在一个设计中，可在不同时间将秘密密钥及至少一个安全参数加载到装置上。秘密密钥及至少一个安全参数可具有其它不同的特性。

[0062] 在框614的一个设计中，装置的数据可通过工作密钥进行加密或标志。在框614的另一设计中，装置的数据可通过工作密钥进行解密或验证。在一个设计中，可在软件的控制下执行至少一个安全功能。

[0063] 至少一个安全功能可在激活安全机制(例如，安全启动)以认证软件之前通过软件执行。在不经由安全机制认证软件的情况下，工作密钥的使用可使软件能够在装置上执行。

[0064] 在示范性设计中，设备(例如，ASIC、无线装置、电子装置等)可包含存储器及处理器。存储器(例如，图1中的外部存储器150)可存储用于装置的软件。处理器(例如，图1中的处理器122或124)可以操作方式耦合到存储器(例如，经由一或多个数据总线)。处理器可(i)基于装置的至少一个安全参数及秘密密钥产生工作密钥及(ii)基于工作密钥执行装置的至少一个安全功能(例如，加密、解密、签名、验证等)。处理器可在激活安全机制(例如，安全启动)以认证软件之前执行至少一个安全功能。至少一个安全参数可与存储在存储器中的软件的认证有关。工作密钥可由软件直接或间接用于至少一个安全功能。可通过不同实体及/或在不同时间将秘密密钥及至少一个安全参数加载到装置上。第一实体可将秘密密钥加载到装置上，并且第二实体可稍后将至少一个安全参数加载到装置上。第一实体可为IC芯片制造商，并且第二实体可为OEM或ODM。或者，第一实体可为可信员工，并且第二实体可为不可信员工，例如，在同一生产车间或在不同位置处。设备可进一步包含存储秘密密钥及/或至少一个安全参数的安全存储器。还可将至少一个安全参数存储在设备上的不安全存储器中，只要至少一个安全参数的完整性受存储器保护。

[0065] 本文中揭示的安全密钥产生技术可提供各种优点。所述技术可防止在激活安全启动之前在制造中的易受损时间段期间未经授权的软件利用硬件秘密密钥或操纵数据。这可以使OEM/ODM不必实施各种过程来使生产车间安全。可存在通过本文中揭示的技术提供的其它优点。

[0066] 所属领域的技术人员将理解，可使用多种不同技术及技艺中的任一个来表示信息及信号。举例而言，可通过电压、电流、电磁波、磁场或磁粒子、光场或光粒子或其任何组合来表示贯穿以上描述可能参考的数据、指令、命令、信息、信号、位、符号及芯片。

[0067] 所属领域的技术人员将进一步了解，在本文中结合揭示内容而描述的各种说明性逻辑区块、模块、电路及算法步骤可实施为电子硬件、计算机软件，或两者的组合。为清晰地说明硬件与软件的此可互换性，上文已大体就其功能性而言描述了各种说明性组件、块、模块、电路及步骤。此功能性是实施为硬件还是软件取决于具体应用及施加于整个系统的设计约束。所属领域的技术人员可针对每一特定应用以不同的方式实施所描述的功能性，但此类实施决策不应被解释为会引起偏离本发明的范围。

[0068] 可使用通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门

阵列信号(FPGA)或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或其经设计以执行本文所描述的功能的任何组合来实施或执行结合本发明而描述的各种说明性逻辑块、模块及电路。通用处理器可为微处理器，但在替代方案中，处理器可为任何常规处理器、控制器、微控制器或状态机。处理器还可实施为计算装置的组合，例如，DSP与微处理器的组合、多个微处理器、结合DSP核心的一或多个微处理器，或任何其它此类配置。

[0069] 结合本文中的揭示内容而描述的方法或算法的步骤可直接在硬件中、由处理器执行的软件模块中或此两者的组合中体现。软件模块可驻留在RAM存储器、闪存存储器、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可装卸式磁盘、CD-ROM或此项技术中已知的任何其它形式的存储媒体中。示范性存储媒体耦合到处理器，使得处理器可从存储媒体读取信息及将信息写入到存储媒体。在替代方案中，存储媒体可与处理器一体化。处理器及存储媒体可驻留在ASIC中。ASIC可驻留在用户终端中。在替代方案中，处理器及存储媒体可作为离散组件驻留在用户终端中。

[0070] 在一或多个示范性设计中，所描述的功能可在硬件、软件、固件或其任何组合中实施。如果以软件实施，则可将功能作为一或多个指令或代码而存储在计算机可读媒体上或经由计算机可读媒体发射。计算机可读媒体包含计算机存储媒体及通信媒体两者，通信媒体包含促进将计算机程序从一处传送到另一处的任何媒体。存储媒体可为可由通用或专用计算机访问的任何可用媒体。借助于实例而非限制，这些计算机可读媒体可包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储装置、磁盘存储装置或其它磁性存储装置，或可用于运载或存储指令或数据结构的形式的所需程序代码装置并且可由通用或专用计算机或通用或专用处理器访问的任何其它媒体。此外，任何连接被恰当地称为计算机可读媒体。举例来说，如果使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)或例如红外线、无线电及微波的无线技术从网站、服务器或其它远程源传输软件，那么同轴电缆、光纤电缆、双绞线、DSL或例如红外线、无线电及微波等无线技术包含于媒体的定义中。如本文中所使用的磁盘及光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字影音光盘(DVD)、软磁盘及蓝光光盘，其中磁盘通常是以磁性方式再现数据，而光盘是用激光以光学方式再现数据。上述各项的组合也应包含在计算机可读媒体的范围内。

[0071] 提供本发明的先前描述以使所属领域的技术人员能够制造或使用本发明。所属领域的技术人员将易于了解对本发明的各种修改，且本文中界定的一般原理可应用于其它变体而不脱离本发明的范围。因此，本发明并不希望限于本文中所描述的实例及设计，而应被赋予与本文中所揭示的原理及新颖特征相一致的最广范围。

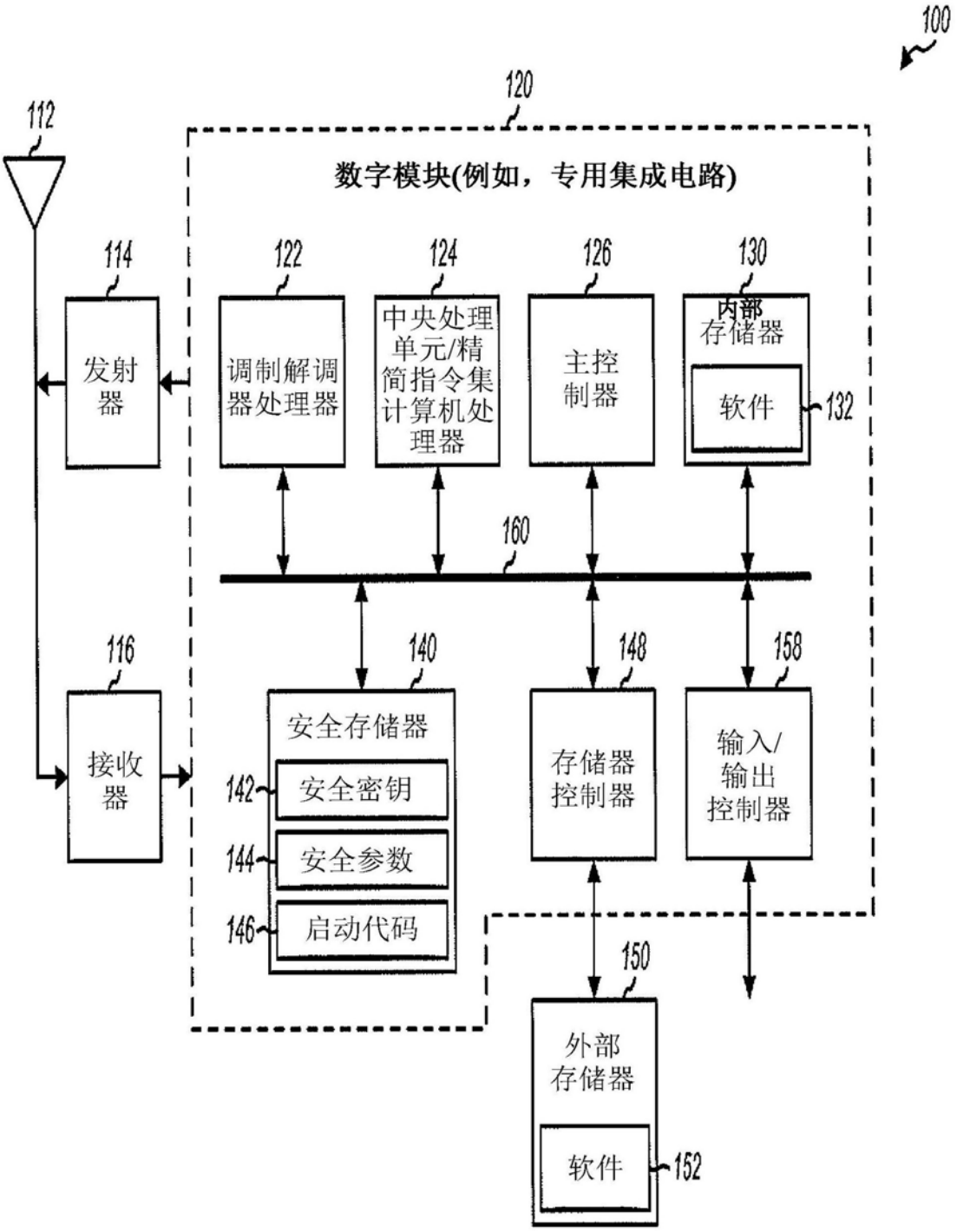

100
120
112
数字模块(例如，专用集成电路)
114
发射器
122
调制解调器处理器
124
中央处理单元/精简指令集计算机处理器
126
主控制器
130
内部存储器
软件
132
160
116
接收器
140
安全存储器
142
安全密钥
144
安全参数
146
启动代码
148
存储器控制器
158
输入/输出控制器
150
外部存储器
软件
152

图1

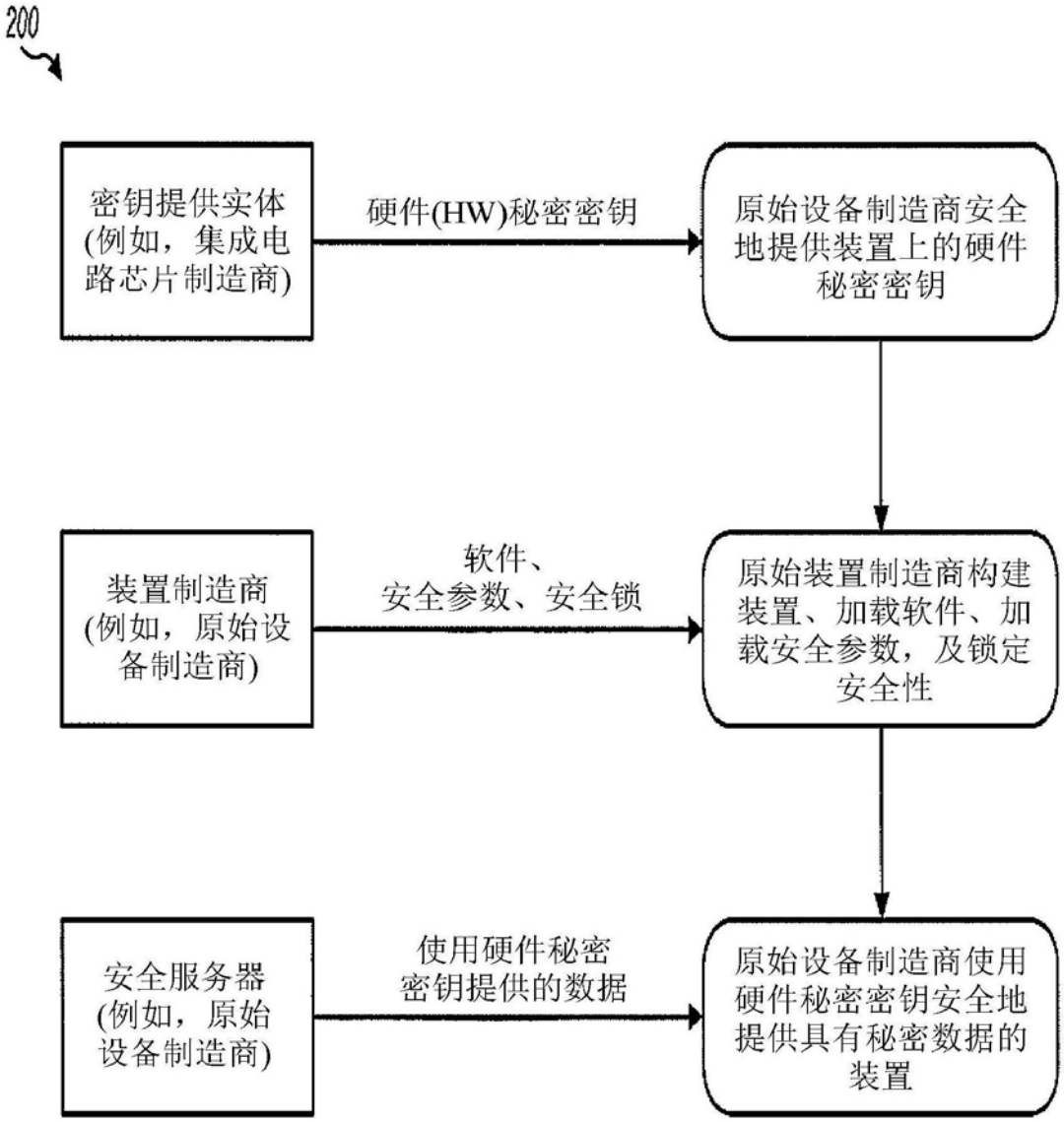

200
密钥提供实体(例如，集成电路芯片制造商)
硬件(HW)秘密密钥
原始设备制造商安全地提供装置上的硬件秘密密钥
装置制造商(例如，原始设备制造商)
软件、安全参数、安全锁
原始装置制造商构建装置、加载软件、加载安全参数，及锁定安全性
安全服务器(例如，原始设备制造商)
使用硬件秘密密钥提供的数据
原始设备制造商使用硬件秘密密钥安全地提供具有秘密数据的装置

图2

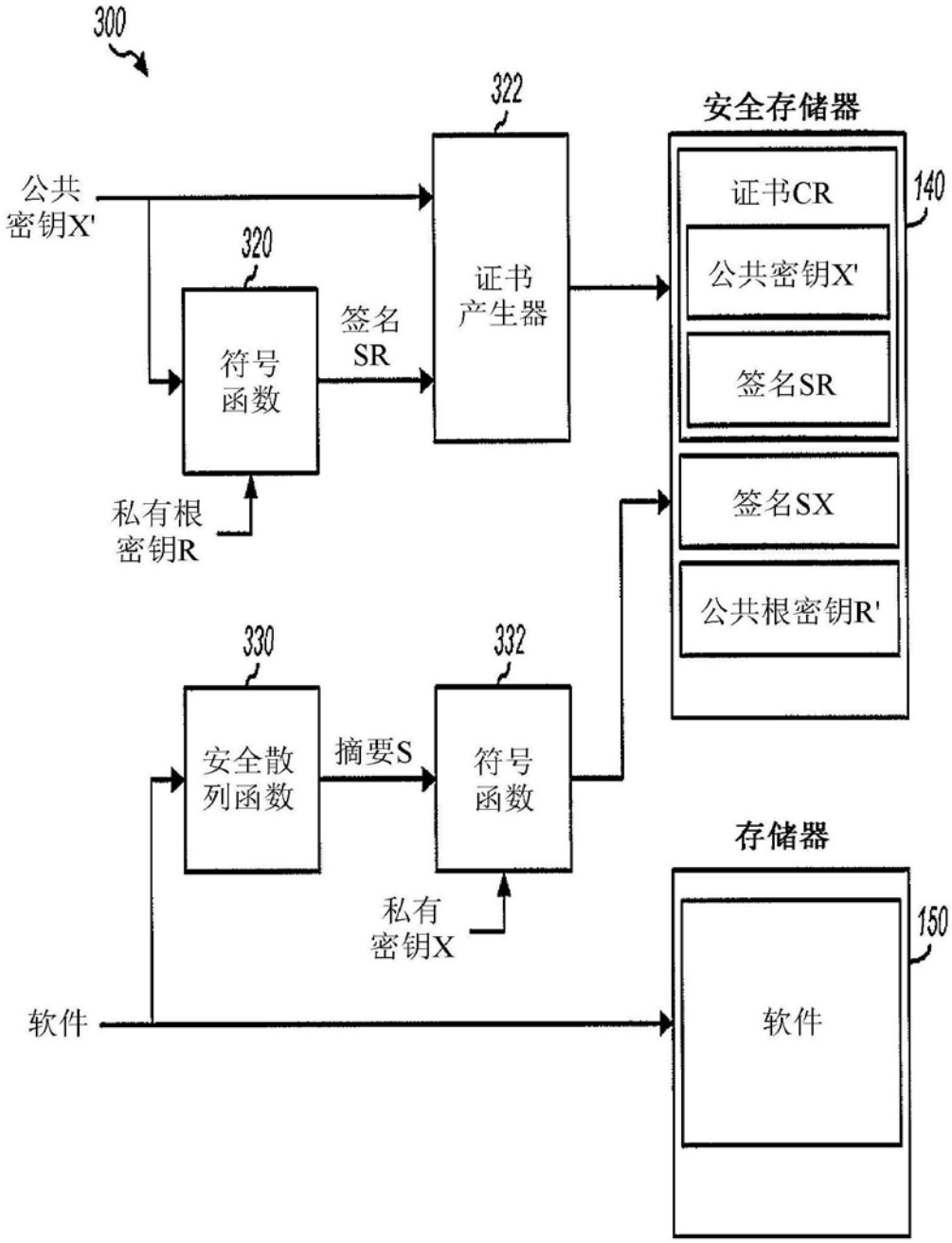

300
322
安全存储器
公共
密钥X'
证书
产生器
证书CR
140
320
公共密钥X'
符号
函数
签名
SR
签名SR
私有根
密钥R
签名SX
公共根密钥R'
330
332
安全散
列函数
摘要S
符号
函数
存储器
私有
密钥X
150
软件
软件

图3A

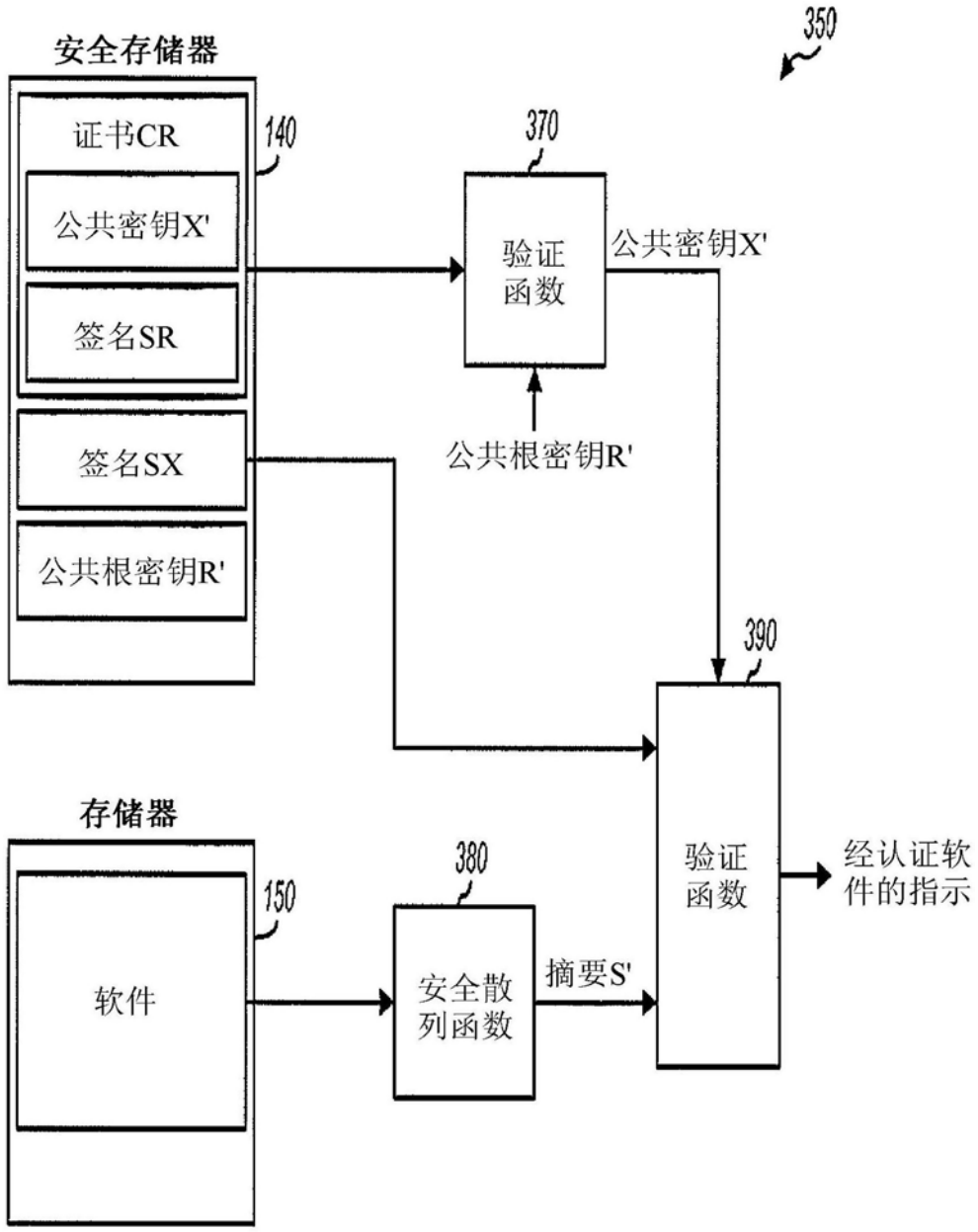

350
安全存储器
证书CR
140
公共密钥X'
签名SR
签名SX
公共根密钥R'
370
验证函数
公共密钥X'
公共根密钥R'
390
验证函数
经认证软件的指示
存储器
150
软件
380
安全散列函数
摘要S'

图3B

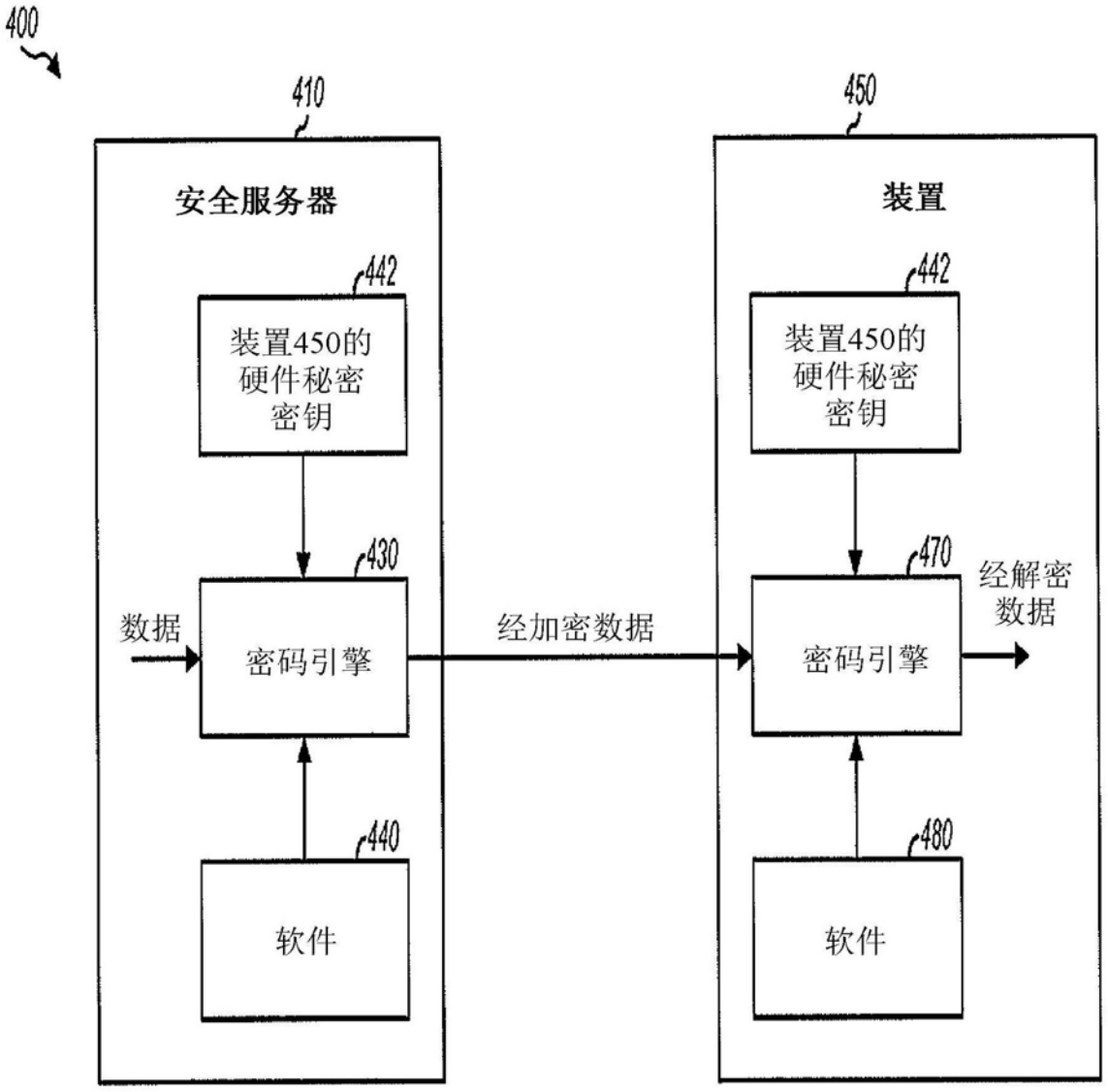

400
410
安全服务器
442
装置450的硬件秘密密钥
430
数据
密码引擎
440
软件
经加密数据
450
装置
442
装置450的硬件秘密密钥
470
密码引擎
经解密数据
480
软件

图4

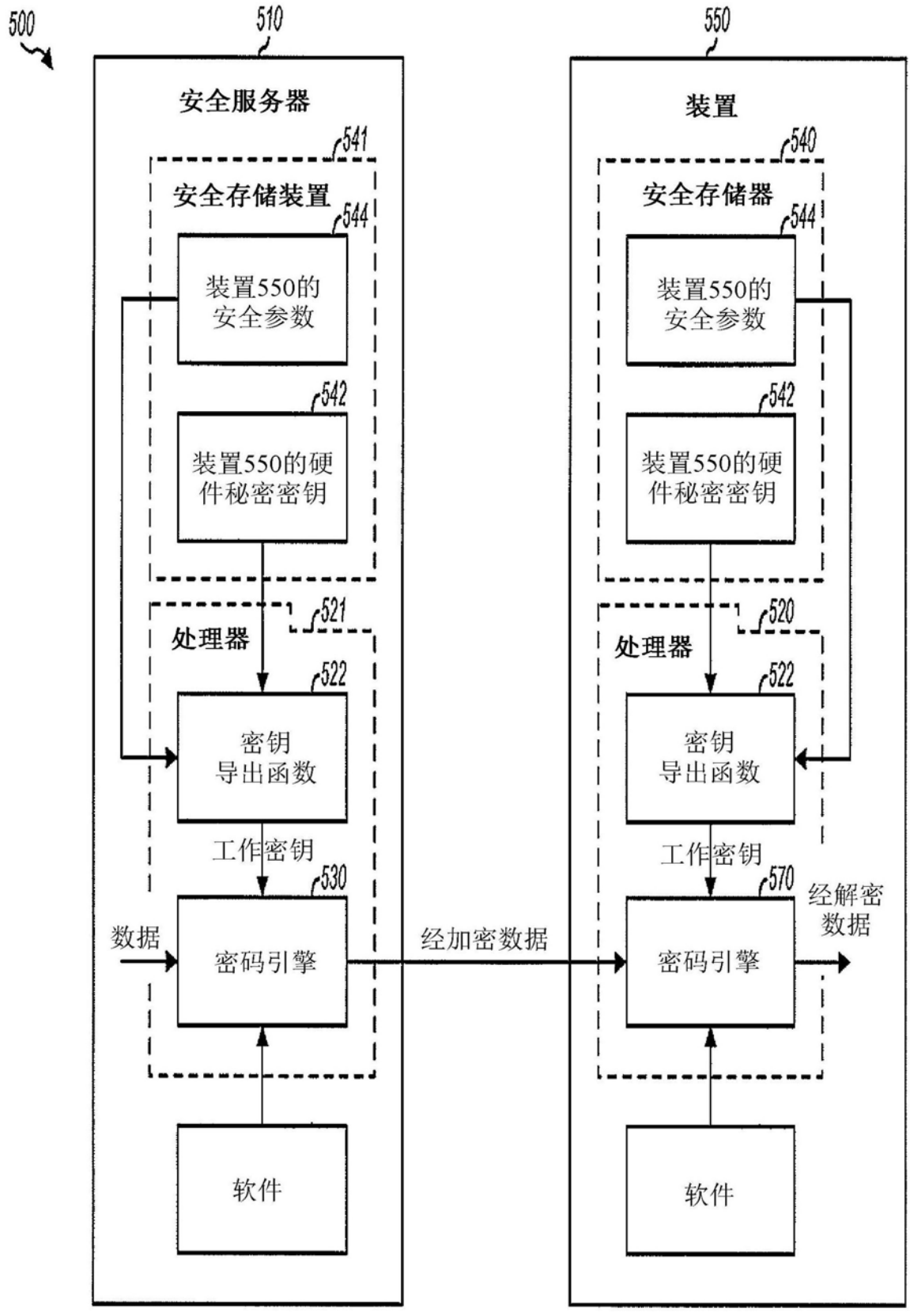

500
510
安全服务器
541
安全存储装置
544
装置550的安全参数
542
装置550的硬件秘密密钥
521
处理器
522
密钥导出函数
工作密钥
530
数据
密码引擎
软件
经加密数据
550
装置
540
安全存储器
544
装置550的安全参数
542
装置550的硬件秘密密钥
520
处理器
522
密钥导出函数
工作密钥
570
密码引擎
经解密数据
软件

图5

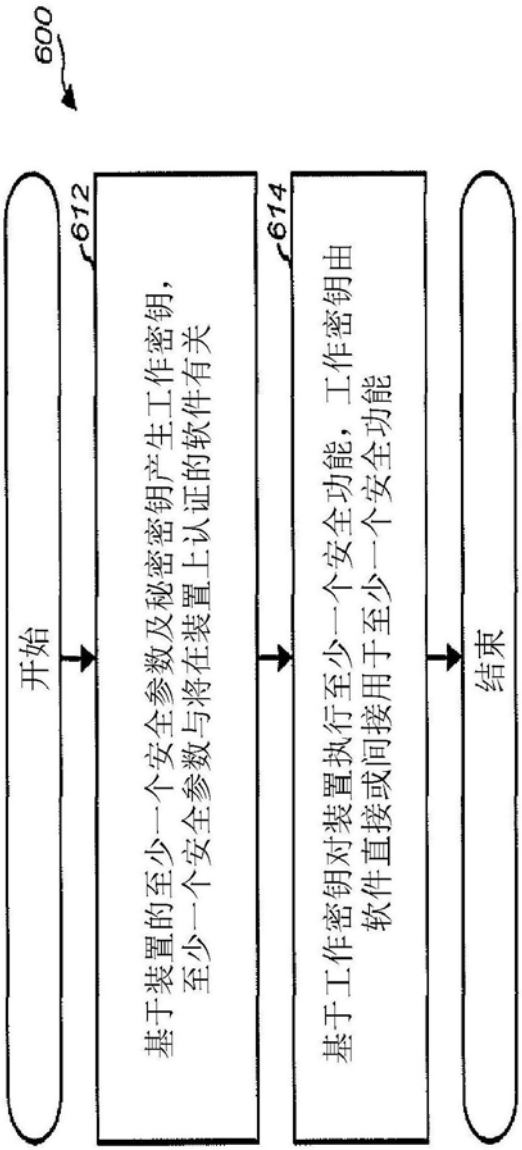

600
开始
612
基于装置的至少一个安全参数及秘密密钥产生工作密钥，
至少一个安全参数与将在装置上认证的软件有关
614
基于工作密钥对装置执行至少一个安全功能，工作密钥由
软件直接或间接用于至少一个安全功能
结束

图6