(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113748698 B
(45)授权公告日 2024.09.10

(21)申请号 202080031420.X
(22)申请日 2020.03.09
(65)同一申请的已公布的文献号
申请公布号 CN 113748698 A
(43)申请公布日 2021.12.03
(30)优先权数据
16/362,786 2019.03.25 US
(85)PCT国际申请进入国家阶段日
2021.10.26
(86)PCT国际申请的申请数据
PCT/US2020/021628 2020.03.09
(87)PCT国际申请的公布数据
WO2020/197744 EN 2020.10.01

(73)专利权人 美光科技公司
地址 美国爱达荷州
(72)发明人 A·蒙代洛 A·特罗亚
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
专利代理师 王龙

(51)Int.Cl.
H04W 12/03(2021.01)
H04W 12/041(2021.01)
H04W 88/06(2009.01)

(56)对比文件
CN 101267631 A,2008.09.17
CN 104380807 A,2015.02.25

审查员 高凯

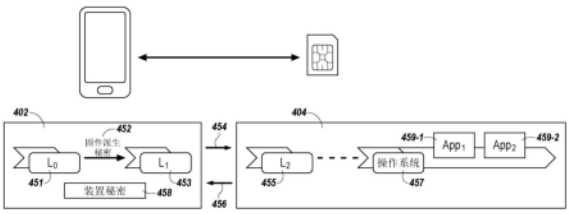
权利要求书3页 说明书14页 附图9页

(54)发明名称

存取网络时的安全通信

(57)摘要

本文中描述存取网络时的安全通信。实例设备可包含存储器及耦合到所述存储器的处理器。所述处理器可经配置以从标识装置接收标识公钥。可响应于向所述标识装置提供修改所述标识装置的内容的请求而接收所述标识公钥。所述处理器可进一步经配置以使用所述标识公钥对与订户信息对应的数据进行加密,(向所述标识装置)提供所述经加密数据以将所述订户信息存储在所述标识装置中,及经由存储在所述标识装置中的所述数据存取由网络运营商运营的网络。



CN 113748698 B

1.一种用于在存取网络(308)时进行安全通信的设备,其包括:

处理器(114);以及

存储器(112),其耦合到所述处理器并存储指令,其中当所述指令被所述处理器执行时,致使所述处理器:

从标识装置(204;304;404;804)接收与订户标识模块SIM相关联的标识公钥(784),其中:

所述标识装置是所述SIM;且

所述标识公钥是响应于向所述标识装置提供修改所述标识装置的内容的请求而被接收;

使用所述标识公钥对与订户信息对应的数据进行加密;

向所述标识装置提供所述经加密数据以将所述数据存储在所述标识装置中;及

经由存储在所述标识装置中的所述数据存取由网络运营商运营的所述网络。

2.根据权利要求1所述的设备,其中当所述指令被所述处理器执行时,进一步致使所述处理器:

从由所述网络运营商运营的服务器(306),连同与所述订户信息对应的所述数据一起接收装置秘密(458);

基于所述所接收到的装置秘密生成订户公钥(583;683;883);及

向所述标识装置提供所述订户公钥,其中至少基于所述订户公钥来验证所述设备的标识。

3.根据权利要求2所述的设备,其中响应于基于所述订户公钥验证所述设备,从所述标识装置接收所述标识公钥。

4.根据权利要求1到3中任一项所述的设备,其中所述网络运营商是第一网络运营商,且其中修改所述标识装置的所述内容的所述请求包括以下中的至少一个:

将网络运营商从第二网络运营商切换到所述第一网络运营商的请求;或

添加所述第一网络运营商的请求。

5.一种用于在存取网络(308)时进行安全通信的设备,其包括:

处理器(220);以及

存储器(218),其耦合到所述处理器并存储指令,其中当所述指令被所述处理器执行时,致使所述处理器:

响应于从订户装置(102;302;402;802)接收到修改所述存储器的内容的请求,生成与订户标识模块SIM相关联的标识公钥(784)及标识私钥(772),其中所述设备是所述SIM;

向所述订户装置提供所述标识公钥;

响应于提供所述标识公钥,从所述订户装置接收数据,其中通过所述订户装置使用所述标识公钥对所述所接收到的数据进行加密;

使用所述标识私钥对所述所接收到的数据进行解密;及

基于所述经解密数据,修改所述存储器的所述内容。

6.根据权利要求5所述的设备,其中连同修改所述存储器的所述内容的所述请求一起从所述订户装置接收订户公钥(583;683;883),且其中当所述指令被所述处理器执行时,进一步致使所述处理器:

在生成标识公钥及所述标识私钥之前,至少基于所述订户公钥验证所述订户装置的标识;及

响应于验证所述订户装置的所述标识,生成所述标识公钥及所述标识私钥。

7.根据权利要求6所述的设备,其中当所述指令被所述处理器执行时,进一步致使所述处理器响应于未验证所述订户装置,丢弃从所述订户装置接收的所述数据。

8.根据权利要求6所述的设备,其中当所述指令被所述处理器执行时,进一步致使所述处理器:

连同所述订户公钥一起从所述订户装置接收订户公共标识(565;665)及订户证书(581;681);及

将所述订户公钥与解密组件的输出进行比较,以验证所述订户装置的所述标识,其中所述订户公共标识、所述订户证书及所述订户公钥被输入到所述解密组件中。

9.根据权利要求8所述的设备,其中所述解密组件包括第一解密器(685)及第二解密器(687),且其中:

所述订户公钥及所述订户证书被输入到所述第一解密器中;且

所述第一解密器的输出及所述订户公钥被输入到所述第二解密器中,其中将所述第二解密器的输出与所述订户公钥进行比较。

10.一种用于在存取网络(308)时进行安全通信的方法,其包括:

响应于接收到修改标识装置(204;304;404;804)的内容的请求及来自订户装置(102;302;402;802)的订户公钥(583;683;883),至少基于所述订户公钥验证所述订户装置的标识,其中所述标识装置是订户标识模块SIM;

响应于验证所述订户装置的所述标识,生成与所述SIM相关联的标识公钥(784)及标识私钥(772);

响应于向所述订户装置提供所述标识公钥,接收与基于所述标识公钥加密的订户信息对应的数据;以及

响应于使用所述标识私钥对所述数据进行解密,基于所述经解密订户信息修改所述标识装置的所述内容。

11.根据权利要求10所述的方法,其中基于所述经解密订户信息修改所述标识装置的所述内容包括:

向所述标识装置添加与所述经解密订户信息相关联的网络运营商,使得通过所述订户装置使用存储在所述标识装置中的所述经解密订户信息来存取由所述网络运营商运营的所述网络。

12.根据权利要求10所述的方法,其中所述经解密订户信息对应于第一网络运营商,且其中基于所述经解密订户信息修改所述标识装置的所述内容包括:

将网络运营商从第二网络运营商切换到所述第一网络运营商。

13.根据权利要求10到12中任一项所述的方法,其进一步包括使用装置标识组合引擎(DICE)-稳健物联网(RIOT)协议对所述订户信息进行加密及解密。

14.根据权利要求10到12中任一项所述的方法,其进一步包括响应于所述订户装置未被验证,阻止生成所述标识公钥及所述标识私钥。

15.一种用于在存取网络(308)时进行安全通信的系统,其包括:

订户装置(102;302;402;802),其经配置以从由网络运营商运营的服务器(306)接收与订户信息对应的数据;及

订户标识模块SIM(204;304;404;804),其与所述订户装置无线通信,所述SIM经配置以:

从所述订户装置接收订户公钥(583;683;883)及修改存储在所述SIM中的数据的内容的请求;以及

响应于基于接收到的所述订户公钥验证所述订户装置的标识,向所述订户装置提供与所述SIM相关联的标识公钥(784);

其中所述订户装置经配置以:

基于所述标识公钥对与所述订户信息对应的所述数据进行加密;以及

向所述SIM提供所述经加密数据;

其中所述SIM经配置以对与所述订户信息对应的所述数据进行解密,使得所述订户装置经配置以经由存储在所述SIM中的所述订户信息存取由所述网络运营商运营的所述网络。

16.根据权利要求15所述的系统,其中:

所述订户装置经配置以:

连同所述订户公钥一起生成订户公共标识(565;665)及订户证书(581;681);及

向所述SIM提供所述订户公共标识、所述订户证书及所述订户公钥;且

所述SIM经配置以在所述订户公共标识、所述订户证书及所述订户公钥之间执行比较,以验证所述订户装置的所述标识。

17.根据权利要求16所述的系统,其中所述SIM经配置以:

至少基于从所述订户装置接收的所述订户公钥,连同所述标识公钥一起生成标识公共标识(766)及标识证书(782);及

将所述标识公共标识、所述标识证书及所述标识公钥提供回到所述订户装置。

18.根据权利要求15所述的系统,其中所述订户装置包括非对称标识生成器(561),且其中所述订户装置经配置以:

使用所述非对称标识生成器连同公共订户标识一起生成私有订户标识(567)。

19.根据权利要求15到18中任一项所述的系统,其中所述订户装置包括非对称密钥生成器(563),且其中所述订户装置经配置以:

使用所述非对称密钥生成器连同所述订户公钥一起生成订户私钥(571;871)。

20.根据权利要求15到18中任一项所述的系统,其中所述SIM经配置以:

基于所述SIM的装置秘密(458)连同所述标识公钥一起生成标识私钥(772);及

向所述订户装置提供所述标识公钥;

其中所述订户装置经配置以基于所述标识公钥验证所述SIM的标识。

存取网络时的安全通信

技术领域

[0001] 本公开大体上来说涉及设备、方法及系统,且更特定来说,涉及存取网络中的安全通信。

背景技术

[0002] 存储器装置通常被提供作为计算机或其它电子装置中的内部半导体集成电路及/或外部可装卸式装置。存在许多不同类型的存储器,包含易失性及非易失性存储器。易失性存储器可需要电力来维持其数据,且可包含随机存取存储器(RAM)、动态随机存取存储器(DRAM)及同步动态随机存取存储器(SDRAM),以及其它存储器。非易失性存储器可通过在未供电时留存所存储数据而提供永久数据,且可包含NAND快闪存储器、NOR快闪存储器、只读存储器(ROM),及电阻可变存储器,例如相变随机存取存储器(PCRAM)、电阻式随机存取存储器(RRAM)及磁阻式随机存取存储器(MRAM),以及其它存储器。

[0003] 可将存储器装置组合在一起以形成固态驱动器(SSD)、嵌入式多媒体卡(e.MMC),及/或通用快闪存储(UFS)装置。SSD、e.MMC及/或UFS装置可包含非易失性存储器(例如,NAND快闪存储器及/或NOR快闪存储器),及/或可包含易失性存储器(例如,DRAM及/或SDRAM)以及各种其它类型的非易失性及易失性存储器。非易失性存储器可用于广泛范围的电子应用中,例如个人计算机、便携式存储棒、数码相机、蜂窝式电话、例如MP3播放器等便携式音乐播放器、电影播放器及其它电子装置。

[0004] 例如,快闪存储器装置可包含将数据存储于例如浮动栅极等电荷存储结构中的存储器单元。快闪存储器装置通常使用允许高存储器密度、高可靠性及低功耗的单晶体管存储器单元。电阻可变存储器装置可包含电阻存储器单元,其可基于存储元件(例如,具有可变电阻的电阻存储器元件)的电阻状态来存储数据。

[0005] 存储器单元可经布置成阵列,且可将阵列架构中的存储器单元编程为目标(例如,所要)状态。举例来说,可将电荷置放在快闪存储器单元的电荷存储架构(例如,浮动栅极)上或从所述电荷存储架构移除以将所述单元编程为特定数据状态。单元的电荷存储架构上的所存储电荷可指示所述单元的阈值电压(Vt)。快闪存储器单元的状态可通过感测所述单元的电荷存储架构上的所存储电荷(例如,Vt)而确定。

[0006] 许多威胁可影响存储器装置的操作及/或存储在存储器装置的存储器单元中的数据。此类威胁可导致重大的经济损失,及/或可带来重大的安保及/或安全性问题。

发明内容

[0007] 在一个方面中,本申请案提供一种用于在存取网络时进行安全通信的设备,其包括:存储器;及处理资源,其耦合到所述存储器,所述处理资源经配置以:从标识装置接收标识公钥,其中所述标识公钥是响应于向所述标识装置提供修改所述标识装置的内容的请求而被接收;使用所述标识公钥对与订户信息对应的数据进行加密;向所述标识装置提供所述经加密数据以将所述数据存储在所述标识装置中;及经由存储在所述标识装置中的所述

数据存取由网络运营商运营的所述网络。

[0008] 在另一方面中,本申请案提供一种用于在存取网络时进行安全通信的设备,其包括:存储器;及处理资源,其耦合到所述存储器,所述处理资源经配置以:响应于从订户装置接收到修改所述存储器的内容的请求,生成标识公钥及标识私钥;向所述订户装置提供所述标识公钥;响应于提供所述标识公钥,从所述订户装置接收数据,其中通过所述订户装置使用所述标识公钥对所述所接收到的数据进行加密;使用所述标识私钥对所述所接收到的数据进行解密;及基于所述经解密数据,修改所述存储器的所述内容。

[0009] 在又一方面中,本申请案提供一种用于在存取网络时进行安全通信的方法,其包括:响应于接收到修改标识装置的内容的请求及来自订户装置的订户公钥,至少基于所述订户公钥验证所述订户装置的标识;响应于验证所述订户装置的所述标识,生成标识公钥及标识私钥;响应于向所述订户装置提供所述标识公钥,接收与基于所述标识公钥加密的订户信息对应的数据;响应于使用所述标识私钥对所述数据进行解密,基于所述经解密订户信息修改所述标识装置的所述内容。

[0010] 在又一方面中,本申请案提供一种用于在存取网络时进行安全通信的系统,其包括:订户装置,其经配置以从由网络运营商运营的服务器接收与订户信息对应的数据;及订户标识模块(SIM),其与所述订户装置无线通信,所述SIM经配置以:从所述订户装置接收订户公钥及修改存储在所述SIM中的数据的内容的请求;响应于验证所述订户装置的标识,向所述订户装置提供标识公钥,其中基于所述所接收到的订户公钥来验证所述订户装置的所述标识;其中所述订户装置经配置以:基于所述标识公钥对与所述订户信息对应的所述数据进行加密;向所述SIM提供所述经加密数据;其中所述SIM经配置以对与所述订户信息对应的所述数据进行解密,使得所述订户装置经配置以经由存储在所述SIM中的所述订户信息存取由所述网络运营商运营的所述网络。

附图说明

[0011] 图1为根据本公开的实施例的实例订户装置的框图。

[0012] 图2为根据本公开的实施例的实例标识装置的框图。

[0013] 图3为根据本公开的实施例的能够与服务器及网络无线通信的实例计算系统的框图。

[0014] 图4为根据本公开的实施例的包含订户装置及标识装置的实例系统的框图。

[0015] 图5为根据本公开的实施例的用于确定多个参数的实例过程的框图。

[0016] 图6为根据本公开的实施例的验证证书的实例过程的框图。

[0017] 图7为根据本公开的实施例的用于确定多个参数的实例过程的框图。

[0018] 图8为根据本公开的实施例的验证签名的实例过程的框图。

[0019] 图9说明流程图,所述流程图说明根据本公开的实施例的用于存取网络的实例方法的流程图。

[0020] 图10为根据本公开的实施例的包含主机及呈存储器装置形式的设备的计算系统的框图。

[0021] 图11为根据本公开的实施例的实例存储器装置的框图。

具体实施方式

[0022] 本文中描述存取网络时的安全通信。实例设备可包含存储器及耦合到所述存储器的处理器。所述处理器可经配置以从标识装置接收标识公钥。可响应于向所述标识装置提供修改所述标识装置的内容的请求而接收所述标识公钥。所述处理器可进一步经配置以使用所述标识公钥对与订户信息对应的数据进行加密,(向所述标识装置)提供所述经加密数据以将所述订户信息存储在所述标识装置中,及经由存储在所述标识装置中的所述数据存取由网络运营商运营的网络。

[0023] 用户装置可存储与可在网络内标识自身的个人信息对应的数据,使得网络的服务提供商可基于个人信息对其进行授权。通常,个人信息可存储在用户装置内及/或在用户装置可无线存取的远程存储器装置中。在任一状况下,个人信息可暴露于来自黑客及/或其它恶意的许多威胁,且此类黑客活动可导致重大的经济损失,及/或可带来重大的安保及/或安全性问题。

[0024] 一些先前的方法提供反黑客机制,所述反黑客机制可包含例如时间戳、随机数生成器及/或计数器(例如,单调计数器),其可提供每次存取及/或交换个人信息时都会改变的一条信息。然而,此类先前的反黑客机制可需要专门专用于反黑客功能性的额外组件及/或电路系统,此可增加存储器的电路系统的大小及/或复杂性。

[0025] 相比之下,本公开的实施例可提供反黑客机制,所述反黑客机制确保安全存储器,同时不需要专门专用于反重放功能性的额外电路系统,此如与利用先前反黑客机制的存储器相比可减小存储器的电路系统的大小及/或复杂性。例如,此类反黑客机制可利用存储器的现有电路系统(例如,存储器装置的现有固件)来提供反黑客功能性,而不必添加专门专用于反黑客功能性的额外(例如,新)组件或电路系统。

[0026] 本文中的图遵循其中第一个数字或前几个数字对应于图式的图编号且剩余数字标识图式中的元件或组件的编号惯例。可通过使用类似的数字来标识不同图之间的类似元件或组件。例如,102可在图1中指代元件“02”,且类似元件可在图3中被称作为302。

[0027] 图1为根据本公开的实施例的实例订户装置102的框图。如本文中所使用,订户装置可指代特定网络运营商的订户(例如,用户)用来存取由特定网络运营商运营的网络(例如,网络308)的装置。如本文中所使用的,网络运营商可指代经由网络向用户提供存取及/或服务的实体。术语“网络运营商”、“移动运营商”、“服务提供商”及“运营商”在本文中可互换使用,且可具有相同的含义,视上下文而定。

[0028] 订户装置102可包含用户设备(UE)装置,例如膝上型计算机、个人计算机、数码相机、数字记录及播放装置、移动电话、PDA、存储卡读取器、接口集线器或具有物联网(IoT)能力的装置,例如汽车(例如,车辆及/或运输基础设施)具有IoT能力装置或医疗(例如,可植入及/或运行状况监测)具有IoT能力的装置,以及其它主机系统,且可包括存储器存取装置(例如,处理器)。所属领域的普通技术人员将了解,“处理器”可意指一或多个处理器,例如并行处理系统,多个协处理器等。

[0029] 订户装置102可包含存储器资源112、处理资源114及收发器资源116,如在图1中所说明。存储器资源112(其也可被称为“存储器”)可包含存储器(例如,存储器单元),所述存储器经布置成例如多个存储器装置的多个存储体组、存储体、存储体区段、子阵列,及/或行。在一些实施例中,存储器资源112可包含多个存储器装置,例如形成及/或可操作为RAM、

DRAM、SRAM、SDRAM及/或TRAM以及其它类型的易失性存储器的多个易失性存储器装置的多个存储器装置。在一些实施例中,存储器资源112可包含多个非易失性存储器装置,所述非易失性存储器装置经形成及/或可操作为PCRAM、RRAM、FeRAM、MRAM及/或STT RAM、相变存储器、3DXPoint及/或快闪存储器装置,以及其它类型的非易失性存储器装置。在一些实施例中,存储器资源112可包含多个易失性存储器装置及多个非易失性存储器装置的组合,如本文中所描述。

[0030] 尽管未在图1中所展示,但存储器资源112可耦合到控制器及/或包含控制器,所述控制器可发送命令以对存储器资源112执行操作,包含感测(例如,读取)、编程(例如,写入)、移动及/或擦除数据的操作。

[0031] 处理资源114可耦合到存储器资源112及收发器资源116,且经配置以经由收发器(例如,收发器资源116)存取存储在存储器资源112中的数据及/或存储在服务器(例如,服务器306)、网络(例如,网络308),及/或标识装置(例如,标识装置304)的数据。

[0032] 如本文中所使用,“收发器”可被称为包含发射器及接收器两者的装置。在一实施例中,收发器可为及/或包含多个射频(RF)收发器。在多个实施例中,发射器及接收器可组合及/或共享共用电路系统。在实施例中,无任何电路系统可在发射功能与接收功能之间共用,且所述装置可被称为发射器-接收器。与本公开一致的其它装置可包含转发器、转换器及/或中继器,以及类似装置。如本文中所使用,术语“收发器资源”及“收发器”在本文中可互换使用且可具有相同含义,视上下文而定。

[0033] 各种无线通信技术可用于经由收发器资源116与不同实体(例如,服务器306、网络308及/或标识装置304)进行通信。例如,不同代的宽带移动电信技术(例如,第一代到第五代(1G到5G))、装置到装置通信,包含蓝牙、Zigbee、1G到5G及/或长期演进(LTE)装置到装置通信技术及/或利用中间装置的其它无线通信(例如,利用接入点AP的WiFi)可用于与不同实体通信。

[0034] 在一些实施例中,订户装置102可存取标识装置(例如,标识装置304)以无线地利用存储在标识装置中的数据。作为实例,订户装置102可存取存储在标识装置中的数据以进一步存取由特定网络运营商运营的网络(例如,网络308)。结合图3描述存取标识装置的更多细节。

[0035] 图2为根据本公开的实施例的实例标识装置204的框图。标识装置204可为订户标识模块(SIM)。如本文中所使用,SIM可指代存储数据(例如,信息)的模块,所述数据可由订户装置用于存取网络(例如,网络108)。在一个实例中,标识装置204可实施为智能卡上的应用程序,例如通用集成电路卡(UICC),其可以可移除方式耦合到订户装置102。在另一实例中,标识装置204不需要物理存在于订户装置102内及/或可移除地耦合到订户装置102。在此实例中,订户装置102可经由收发器资源116无线地存取标识装置204。

[0036] 标识装置204可包含存储器资源218、处理资源220及收发器资源222,如在图2中所说明。存储器资源218(其也可被称为“存储器”)可包含存储器(例如,存储器单元),所述存储器经布置成例如多个存储器装置的多个存储体组、存储体、存储体区段、子阵列,及/或行。在一些实施例中,存储器资源218可包含多个存储器装置,例如形成及/或可操作为RAM、DRAM、SRAM、SDRAM及/或TRAM以及其它类型的易失性存储器的多个易失性存储器装置的多个存储器装置。在一些实施例中,存储器资源218可包含多个非易失性存储器装置,所述非

易失性存储器装置经形成及/或可操作为PCRAM、RRAM、FeRAM、MRAM及/或STT RAM、相变存储器、3DXPoint及/或快闪存储器装置,以及其它类型的非易失性存储器装置。在一些实施例中,存储器资源218可包含多个易失性存储器装置及多个非易失性存储器装置的组合,如本文中所描述。

[0037] 尽管未在图2中所展示,但存储器资源218可耦合到控制器及/或包含控制器,所述控制器可发送命令以对存储器资源218执行操作,包含感测(例如,读取)、编程(例如,写入)、移动及/或擦除数据的操作。

[0038] 存储器资源218可存储对应于例如订户信息的各种类型的信息的数据。如本文中所使用,订户信息可指代可标识及鉴别网络中的特定订户装置(例如,订户装置102)的信息。作为实例,订户信息可包含国际移动订户标识(IMSI)号码(例如,标识运营商网络中的订户装置的IMSI号码)、国际移动设备标识(IMEI)号码、个人标识码(PIN)(例如、订户装置用于存取标识装置的代码)、个人解锁码及/或个人解锁密钥(PUC/PUK)、鉴别密钥(K/Ki)及/或网络状态信息,例如,从位置区域标识(LAI)(例如,指示订户装置的位置的信息)接收。存储器资源218还可存储非订户信息,例如订户装置的多个文本消息(例如,短消息服务(SMS)消息)及/或联系信息。

[0039] 处理资源220可耦合到存储器资源218及收发器资源222,且经配置以经由收发器资源222从例如订户装置(例如,订户装置102)及/或网络(例如,网络308)的不同实体接收数据。

[0040] 各种无线通信技术可用于经由收发器资源222与不同实体(例如,订户装置302及/或网络308)进行通信。例如,不同代的宽带移动电信技术(例如,1G到5G)、装置到装置通信,包含蓝牙、Zigbee、1G到5G及/或LTE装置到装置通信技术及/或利用中间装置的其它无线通信(例如,利用接入点AP的WiFi)可用于与不同实体通信。

[0041] 在一些实施例中,标识装置204可验证订户装置,提供订户装置可用来对数据进行加密的特定密钥,且使用连同特定密钥一起生成的另一密钥来对从订户装置接收的数据进行解密。结合图3描述验证、提供及解密的更多细节。

[0042] 图3为根据本公开的实施例的能够与服务器306及网络308无线通信的实例计算系统310的框图。订户装置302及标识装置304可为例如先前分别结合图1及2所描述的订户装置102及标识装置204。在一个实例中,订户装置302可利用标识装置304来存取网络308。在另一实例中,标识装置304可为另一订户装置(例如,可穿戴装置,例如智能手表)的一部分,其SIM(例如,在标识装置304内实施)可由订户装置302激活。

[0043] 订户装置302可(例如,无线地)与服务器306通信。通过与服务器306通信,订户装置302可获得待存储在标识装置304中及/或用于存取网络308的数据。作为实例,可从服务器306获得的数据可包含订户信息,如结合图2所描述。

[0044] 可利用各种不同的技术来起始与服务器306的通信。例如,可向订户装置302的用户提供快速响应(QR)码(例如,来自网络运营商),其可将订户装置引导至服务器(例如,服务器306),使得通过通过订户装置扫描QR码,用户可从服务器获得数据。例如,可引导订户装置的用户登录到可提供订户信息的特定网站。例如,订户装置302可物理耦合到将订户信息发射到订户装置的特定装置。

[0045] 尽管服务器306被说明为与网络308分离,但服务器306可为网络308的部分。因此,

在一些实施例中,最初可向订户装置302提供对运营商网络的(例如,有限的)存取以存取服务器306。例如,订户装置302最初可被提供引导SIM并利用引导SIM来存取网络308的服务器306。

[0046] 订户装置302可进一步(例如,无线地)与标识装置304通信。例如,可根据订户装置302的请求修改标识装置304的内容(例如,存储在其中的数据)。如本文中所使用,其内容可被修改的标识装置(例如,SIM)可被称为嵌入式SIM(eSIM)。作为实例,eSIM可修改内容以添加另一网络运营商,切换到不同的网络运营商,及/或删除对应于特定网络运营商的现有订户信息,使得订户装置302不能再经由特定网络运营商存取网络308。因此,在一些实施例中,eSIM可包含对应于多个相应网络运营商的多个订户信息,使得订户装置302可在多个网络运营商中选择网络运营商来存取网络308。

[0047] 可以安全方式执行订户装置302与标识装置304之间的通信。在实施例中,订户装置302可接收(例如,从服务器306)待发送到标识装置304的数据,请求标识装置304验证订户装置302(例如,握手),使用从标识装置304接收(例如,在被标识装置304验证时)安全密钥对数据进行加密,及将加密数据提供给标识装置304。在实施例中,标识装置304可向订户装置302提供(例如,响应于验证订户装置302)特定密钥,接收用先前提供的特定密钥加密的数据,及使用另一密钥对数据进行解密,所述密钥与先前提供给订户装置302的特定密钥一起生成。在对从订户装置302接收的数据进行成功解密时,标识装置304可存储经解密数据,使得订户装置302可存取标识装置304以经由经解密数据存取网络308。下文描述在订户装置302与标识装置304之间交换密钥及数据的进一步细节。

[0048] 图4为根据本公开的实施例的包含订户装置402及标识装置404的实例系统的框图。订户装置402及标识装置404可分别为例如先前结合图1及2所描述的订户装置102及标识装置204。作为实例,标识装置404可为与订户装置402不同的可穿戴装置(例如,智能手表)的eSIM。在此实例中,订户装置402可经配置以无线激活可穿戴装置的eSIM,使得可穿戴装置可经由被激活的eSIM存取网络(例如,网络108)。

[0049] 计算装置可使用层分阶段启动,其中每一层鉴别并加载后续层,并在每一层处提供越来越复杂的运行时服务。层可由前一层提供服务并为后续层提供服务,因此创建建立在较低层上并为较高阶层提供服务的层的互连网络。在图5中所说明的实施例中,层0(“L_0”)451及层1(“L_1”)453在订户装置402内。层0 451可向层1 453提供固件派生秘密(FDS)密钥452。FDS密钥452可描述层1 453的代码及其它安全相关数据的标识。在实例中,特定协议(例如稳健物联网(RIOT)核心协议)可使用FDS 452来验证其加载的层1 546的代码。在实例中,特定协议可包含装置标识组合引擎(DICE)及/或RIOT核心协议。作为实例,FDS可包含层1固件图像本身、以加密方式标识经授权层1固件的清单、在安全启动实施方案的上下文中经签名固件的固件版本号,及/或装置的安全关键配置设置。

[0050] 装置秘密458可用于创建FDS 452并存储在订户装置402的存储器中。在一些实施例中,可从由特定网络运营商操作的服务器(例如,服务器106)接收装置秘密458。在实例操作中,订户装置402可读取装置秘密458,散列层1 453的标识,并执行计算,包含:

[0051] K_{L1}=KDF[Fs(s),Hash(“不可变信息”)]

[0052] 其中K_{L1}为公钥,KDF(例如,美国国家标准与技术研究所(NIST)特别出版物800-108中定义的KDF)为密钥派生函数(即,HMAC-SHA256),且Fs(s)为装置秘密458。FDS 452可通过

执行以下操作来确定：

[0053] FDS＝HMAC-SHA256[Fs(s),SHA256(“不可变信息”)]

[0054] 订户装置402可向标识装置404发射数据，如由箭头454所说明。作为实例，在订户装置402被标识装置404验证之前，所发射数据可包含公开的订户标识、证书(例如订户标识证书)及/或订户公钥。作为实例，在订户装置402被标识装置404验证之后，所发射数据可包含待存储在标识装置404中的数据，例如对应于订户信息的数据(例如，如结合图2所描述)、联系信息及/或订户装置402的文本消息。

[0055] 标识装置404的层2(“L_2”)455可接收所发射数据，并在操作系统(“OS”)457的操作中以及在第一应用程序459-1及第二应用程序459-2上执行数据。标识装置404还可向订户装置402发射数据，如由箭头456所说明。

[0056] 在一些实施例中，待存储在标识装置404中的数据(例如，订户信息、联系信息及/或文本消息)也可连同被接收用于验证订户装置402的订户公共标识、订户标识证书及/或订户公钥一起同时地被接收。在此实例中，可允许数据在订户装置402被验证时被存储在标识装置404中，而可在订户装置402没有被标识装置404验证时被丢弃。结合图6描述验证装置(例如，订户装置402及/或标识装置404)的进一步细节。

[0057] 图5为根据本公开的实施例的用于确定多个参数的实例过程的框图。图5为确定参数的实例，所述参数包含公共标识(例如，565)、证书(例如，581)及公钥(例如，583)，然后由箭头554所指示将所述参数发送到标识装置(例如，图4中的404)的层2(例如，层2 455)。如本文中所使用，从订户装置402生成的公共标识、证书及公钥可分别称为订户公共标识、订户证书及订户公钥。图5中的层0(“L_0”)551对应于图4中的层0 451，且同样FDS 552对应于FDS 452，层1 553对应于层1 453，且箭头554及556分别对应于箭头454及456。

[0058] 来自层0 551的FDS 552被发送到层1 553，且由非对称ID生成器561使用以生成公共标识(“$ID_{lk\ public}$”)565及私有标识567。在缩写“$ID_{lk\ public}$”中，“lk”指示层k(在此实例中，层1)，且“public”指示标识是公开共享的。公共标识565被说明为由延伸到订户装置(例如，订户装置402)的层1 553的右侧及外部的箭头共享。生成的私有标识567用作输入到加密器573的密钥。加密器573可为用于对数据进行加密的任何处理器、计算装置等。

[0059] 订户装置的层1 553可包含非对称密钥生成器563。在至少一个实例中，随机数生成器(RND)536可任选地将随机数输入到非对称密钥生成器563中。非对称密钥生成器563可生成与例如图4中的订户装置402的订户装置相关联的订户公钥(“$K_{Lk\ public}$”)583及订户私钥(“$K_{LK\ private}$”)571。订户公钥583可为到加密器573的输入(作为“数据”)。加密器573可使用订户私有标识567及订户公钥583的输入来生成结果K’575。订户私钥571及结果K’575可被输入到额外加密器577中，从而产生输出K”579。输出K”579是发射到层2(图4的455)的证书(“ID_{L1}证书”)581。订户证书581可提供验证及/或鉴别从装置发送的数据的来源的能力。作为实例，从订户装置发送的数据可通过验证证书与订户装置的标识相关联，如将结合图6进一步描述。此外，订户公钥(“$K_{L1\ public\ key}$”)583可发射到层2。因此，订户装置的公共标识565、证书581及公钥583可被发射到标识装置的层2。

[0060] 图6为根据本公开的实施例的验证证书的实例过程的框图。在图6的所说明实例中，从订户装置(例如，从图4中的订户装置402的层1 453)提供公钥683、证书681及公共标识665。证书681及公钥683的数据可用作到解密器685的输入。解密器685可为用于对数据进

行解密的任何处理器、计算装置等。证书681及公钥683的解密的结果可连同公共标识一起用作到辅助解密器687的输入，从而产生输出。公钥683及来自解密器687的输出可指示，如在689处所说明，是否验证证书681，从而产生是或否691作为输出。

[0061] 响应于证书681被验证，可在订户装置与标识装置之间进一步交换数据。在一个实例中，响应于订户装置被验证，可将在标识装置处生成的公钥、证书及公共标识提供回到订户装置。在另一实例中，响应于订户装置被验证，订户装置可进一步提供待存储在标识装置中的数据且可接受、解密及处理所述数据。然而，响应于证书未被验证，从被验证的装置接收的数据可被丢弃、移除及/或忽略及/或在两者之间进一步交换数据可被禁止。以此方式，可检测并避免发送恶意数据的恶意装置。作为实例，可标识发送待处理数据的黑客，而不处理黑客数据。结合图7描述验证之后的数据交换的更多细节。

[0062] 图7为根据本公开的实施例的用于确定多个参数的实例过程的框图。图7说明生成标识(“ID_{L2}公共”)766、证书(“ID_{L2}证书”)782及公钥(“$K_{L2\ public\ key}$”)784的标识装置(例如，图4中的标识装置404)的层2 755。如本文中所使用，在标识装置(例如，标识装置404)处生成的公共标识、证书及公钥可分别被称为标识公共标识、标识证书及标识公钥。

[0063] 从订户装置的层1发射到标识装置的层2 755的订户公钥(“$K_{L1\ public\ key}$”)783，如在图5中所描述，由标识装置的非对称ID生成器762使用来生成标识装置的公共标识(“$ID_{lk\ public}$”)766及私有标识768。在缩写“$ID_{lk\ public}$”中，“lk”指示层k(在此实例例中为层2)，且“public”指示标识是公开共享的。公共标识766被说明为由延伸到右侧及外部2 755的箭头共享。所生成的私有标识768用作输入到加密器774中的密钥。

[0064] 标识装置的层2 755可包含非对称密钥生成器764。在至少一个实例中，随机数生成器(RND)738可任选地将随机数输入到非对称密钥生成器764中。非对称密钥生成器764可生成与例如图4中的标识装置406的标识装置相关联的公钥(“$K_{Lk\ public}$”)770及私钥(“$K_{LK\ private}$”)772。标识公钥770可为到加密器774中的输入(作为“数据”)。加密器774可使用标识私有标识768及标识公钥770的输入生成结果K’776。标识私钥772及结果K’776可被输入到额外加密器778中，从而产生输出K”780。输出K”780是发射回到层1(图4的453)的标识证书(“ID_{L2}证书”)782。标识证书782可提供验证及/或鉴别从装置发送的数据来源的能力。作为实例，从标识装置发送的数据可通过验证证书与标识装置的标识相关联，如将结合图7进一步描述。此外，标识公钥(“$K_{L2\ public\ key}$”)784可被发射到层1。因此，标识装置的公共标识766、证书782及公钥784可被发射到订户装置的层1。

[0065] 在实例中，响应于订户装置从标识装置接收公钥，订户装置可使用标识公钥来对待发送到标识装置的数据进行加密。反之亦然，标识装置可使用订户公钥对待发送到订户装置的数据进行加密。响应于标识装置接收到使用标识公钥加密的数据，标识装置可使用其特有私钥(例如，标识私钥)对数据进行解密。同样地，响应于订户装置接收到使用订户公钥加密的数据，订户装置可使用其特有私钥(例如，订户私钥)对数据进行解密。由于标识私钥不与标识装置外部的另一装置共享，且订户私钥不与订户装置外部的另一装置共享，因此发送到标识装置及订户装置的数据保持安全。

[0066] 在实施例中，最初请求与第二实体握手的第一实体可基于其特有的装置秘密生成第一公钥、第一公共标识及第一证书。另一方面，接收到握手请求的第二实体可基于由第一实体提供的第一公钥生成第二公钥、第二公共标识及第二证书。例如，图4、5及7中所说明的

实施例将订户装置(例如,订户装置402)说明为最初请求与标识装置(例如,标识装置404)握手的实体。在此实施例中,订户装置基于订户装置的装置秘密(例如,从网络运营商提供)生成公钥(例如,公钥583)、公共标识(例如,公共标识565)及证书(例如,证书581),且标识装置基于从订户装置提供的公钥生成那些。然而,实施例并不限于此。例如,标识装置最初可请求与订户装置握手,使得标识装置使用其特有装置秘密生成公钥、公共标识及证书,而订户装置基于从标识装置提供的公钥生成那些。

[0067] 图8为根据本公开的实施例的验证签名的实例过程的框图。在装置正发送可被验证以便避免后续否认的数据的情况下,可生成签名并将其与数据一起发送。作为实例,第一装置可向第二装置发出请求,且一旦第二装置执行所述请求,第一装置可指示第一装置从未发出此类请求。反否认方法,例如使用签名,可避免第一装置的否认,并确保第二装置可随后毫无困难地执行所请求的任务。

[0068] 订户装置802(例如图1中的订户装置102)可向标识装置804(例如图2中的标识装置204)发送数据890。订户装置802可在894处使用装置私钥871生成签名896。签名896可被发射到标识装置804。在898处,标识装置804可使用先前接收的数据892及订户公钥883来验证签名。以此方式,签名是使用私钥生成的,并使用公钥进行验证。以此方式,每一装置的唯一签名可对发送签名的装置保持私有,同时允许接收装置能够对签名进行解密以进行验证。此与数据的加密/解密形成对比,所述数据由发送装置使用接收装置的公钥进行加密并由接收装置使用接收器的私钥进行解密。在至少一个实例中,装置可通过使用内部密码术过程(例如,椭圆曲线数字签名(ECDSA)或类似过程)来验证数字签名。

[0069] 图9说明流程图,所述流程图说明根据本公开的实施例的用于存取网络的实例方法992的流程图。在框993处,方法992可包含至少基于订户公钥来验证(例如,通过标识装置)订户装置的标识。当标识装置接收到(例如,从订户装置)修改标识装置的内容的请求时,可验证订户装置。连同请求,还可从订户装置接收订户公钥。订户装置及标识装置可为例如订户装置302及标识装置304,如先前结合图3所描述。

[0070] 在块995处,方法992可包含生成(例如,通过标识装置)标识公钥及标识私钥。标识公钥及标识私钥可在标识装置验证订户装置时生成。否则,标识装置可不生成那些,且禁止从订户装置接收数据及/或丢弃从订户装置接收的数据。标识公钥可被提供给订户装置,使得订户装置可使用标识公钥对待发送到标识装置的数据进行加密。

[0071] 在块997处,方法992可包含接收(例如,在标识装置处)与使用标识公钥进行加密的订户信息对应的数据。经加密数据可在标识装置处进一步解密,例如,使用连同先前提供给订户装置的标识公钥一起生成的标识私钥。可使用DICE-RIOT协议执行对数据的加密及解密。

[0072] 在块999处,方法992可包含基于经解密订户信息修改标识装置的内容。如本文中所描述,经解密订户信息可由订户装置存取进一步存取由特定运营商运营的网络。

[0073] 图10为根据本公开的实施例的包含主机1005及呈存储器装置1003形式的设备的计算系统1034的框图。在实例中,主机1005及存储器装置1003可为订户装置102及标识装置204,如先前分别结合图1及2所描述。如本文中所使用,“设备”可指但不限于各种结构或结构组合中的任一个,例如,电路或电路系统、一或多个裸片、一或多个模块、一或多个装置或一或多个系统。此外,在实施例中,计算系统1034可包含与存储器装置1003类似的多个存储

器装置。

[0074] 在图10中所说明的实施例中,存储器装置1003可包含具有存储器阵列1001的存储器1030。存储器阵列1001可类似于先前分别结合图1及2所描述的存储器资源112及/或218。此外,如本文中将进一步描述,存储器阵列1001可为安全阵列。尽管图10中说明一个存储器阵列1001,但存储器1030可包含任何数目个类似于存储器阵列1001的存储器阵列。

[0075] 如在图10中所说明,主机1005可经由接口1024耦合到存储器装置1003。主机1005及存储器装置1003可在接口1024上进行通信(例如,发送命令及/或数据)。主机1005及/或存储器装置1003可为膝上型计算机、个人计算机、数码相机、数字记录及播放装置、移动电话、PDA、存储卡读取器、接口集线器或具有物联网(IoT)能力的装置,例如汽车(例如,车辆及/或运输基础设施)具有IoT能力装置或医疗(例如,可植入及/或运行状况监测)具有IoT能力的装置,以及其它主机系统,或为其一部分,且可包含存储器存取装置(例如,处理器)。所属领域的普通技术人员将了解,"处理器"可意指一或多个处理器,例如并行处理系统,多个协处理器等。

[0076] 在一些实施例中,接口1024可呈标准化物理接口的形式。例如,当存储器装置1003用于计算系统1034中的信息存储时,接口1024可为串行先进技术总线附属(SATA)物理接口、快速外围组件互连(PCIe)物理接口、通用串行总线(USB)物理接口、或小型计算机系统接口(SCSI)以及其它物理连接器及/或接口。然而,一般来说,接口1024可提供用于在存储器装置1003与主机(例如,主机1005)之间传递控制、地址、信息(例如,数据)及其它信号的接口,所述主机具有用于接口1024的兼容接纳器。

[0077] 在一些实施例中,接口1024可用于无线通信技术,例如不同代的宽带移动电信技术(例如,1G到5G)、装置到装置通信,包含蓝牙、Zigbee、1G到5G及/或长期演进(LTE)装置到装置通信技术及/或利用中间装置的其它无线通信(例如,利用接入点AP的WiFi)可用于与不同实体通信,如结合图1及2所描述。

[0078] 存储器装置1003包含控制器1009以与主机1005及存储器1030(例如,存储器阵列1001)通信。例如,控制器1009可发送命令以对存储器阵列1001执行操作,包含感测(例如,读取)、编程(例如,写入)、移动及/或擦除数据的操作,以及其它操作。

[0079] 控制器1009可被包含在与存储器1030相同的物理装置(例如,相同裸片)上。替代地,控制器1009可被包含在单独物理装置上,所述物理装置通信地耦合到包含存储器1030的物理装置。在实施例中,控制器1009的组件可作为分布式控制器横跨多个物理装置(例如,与存储器在同一裸片上的一些组件,以及在不同裸片、模块或板上的一些组件)扩散。

[0080] 主机1005可包含主机控制器(图10中未展示)以与存储器装置1003通信。主机控制器可经由接口1024向存储器装置1003发送命令。主机控制器可与存储器装置1003及/或存储器装置1003上的控制器1009通信以读取、写入及/或擦除数据以及其它操作。此外,在实施例中,主机1005可为具有IoT能力的装置,如本文中先前所描述,具有IoT通信能力。

[0081] 存储器装置1003上的控制器1009及/或主机1005上的主机控制器可包含控制电路系统及/或逻辑(例如,硬件及固件)。在实施例中,存储器装置1003上的控制器1009及/或主机1005上的主机控制器可为耦合到包含物理接口的印刷电路板的专用集成电路(ASIC)。此外,存储器装置1003及/或主机1005可包含易失性及/或非易失性存储器的缓冲器及多个寄存器。

[0082] 例如,如在图10中所展示,存储器装置可包含电路系统1026。在图10中所说明的实施例中,电路系统1026被包含在控制器1009中。然而,本公开的实施例不限于此。例如,在实施例中,电路系统1026可被包含在(例如,在同一裸片上)存储器1030中(例如,而不是在控制器1009中)。电路系统1026可包括例如硬件、固件及/或软件。

[0083] 电路系统1026可在块链中生成块1032,用于验证(例如,鉴别及/或证明)存储在存储器1030中(例如,在存储器阵列1001中)的数据。块1032可包含块链中前一个块(例如,到其链接)的密码散列,及(例如,标识)存储在存储器阵列1001中的数据的密码散列。块1032还可包含具有指示块何时生成的时间戳的标头。此外,块1032可具有与其相关联的数字签名,其指示所述块被包含在块链中。

[0084] 存储在存储器阵列1001中的数据的密码散列及/或块链中前一个块的密码散列可包括例如SHA-256密码散列。此外,存储在存储器阵列1001中的数据的密码散列及区块链中前一个区块的密码散列可分别各自包括256字节的数据。

[0085] 存储在存储器阵列1001中的数据的密码散列可例如由电路系统1026生成(例如,计算)。在此类实例中,所存储数据的密码散列可由存储器装置1003内部生成,而无需外部数据在接口1024上移动。作为额外实例,可从外部实体传达数据的密码散列。例如,主机1005可生成存储在存储器阵列1001中的数据的密码散列,且将生成的密码散列发送到存储器装置1003(例如,电路系统1026可从主机1005接收存储在存储器阵列1001中的数据的密码散列)。

[0086] 与块1032相关联的数字签名可例如由电路系统1026基于(例如,响应于)外部命令,例如从主机1005接收的命令来生成(例如,计算)。例如,可使用对称或非对称密码术生成数字签名。作为额外实例,主机1005可生成数字签名,且将生成的数字签名发送(例如提供)到存储器装置1003(例如,电路系统1026可从主机1005接收数字签名)。

[0087] 如在图10中所展示,块1032以及与块1032相关联的数字签名可存储在存储器阵列1001中。例如,块1032可被存储在存储器装置1003的用户及/或主机1005不可存取的存储器阵列1001的一部分中(例如,在存储器阵列1001的“隐藏”区域中)。将块1032存储在存储器阵列1001中可通过例如消除对块的软件存储管理的需求来简化块的存储。

[0088] 在实施例中,存储器阵列1001(例如,阵列1001的子集,或整个阵列1001)可为安全阵列(例如,待保持在控制之下的存储器1030的区域)。例如,存储在存储器阵列1001中的数据可包含敏感(例如,非用户)数据,例如主机固件及/或待为敏感应用程序执行的代码。在此类实施例中,可使用一对非易失性寄存器来定义安全阵列。例如,在图10中所说明的实施例中,电路系统1026包含可用于定义安全阵列的寄存器1028-1及1028-2。例如,寄存器1028-1可定义安全阵列的地址(例如,数据的起始LBA),且寄存器1028-2可定义安全阵列的大小(例如,数据的结束LBA)。一旦已定义安全阵列,电路系统1026就可生成(例如,计算)与安全阵列相关联的密码散列,密码散列在本文中被称为黄金散列,使用经鉴别及防重放保护命令(例如,以使得只有存储器装置1003知晓黄金散列,且只有存储器装置1003能够生成及更新所述黄金散列)。黄金散列可存储在存储器阵列1001的不可存取部分(例如,其中存储块1032的相同不可存取部分)中,且可在验证安全阵列的数据的过程期间使用。

[0089] 存储器装置1003(例如,电路系统1026)可经由接口1024将块1032连同与块1032相关联的数字签名一起发送到主机1005,用于验证存储在存储器阵列1001中的数据。例如,电

路系统1026可感测(例如,读取)存储在存储器阵列1001中的块1032,且响应于通电(例如,通电及/或加电)存储器装置1003将所感测块发送到主机1005以验证存储在阵列1001中的数据。如此,存储在存储器阵列1001中的数据的验证可在存储器装置1003通电时(例如,自动地)起始。

[0090] 作为额外实例,电路系统1026可在外部实体(例如主机1005)起始对存储在存储器阵列1001中的数据的验证时将块1032连同与块1032相关联的数字签名一起发送到主机1005。例如,主机1005可向存储器装置1003(例如,电路系统1026)发送命令以感测块1032,且电路系统1026可执行用以感测块1032的命令,且响应于接收到命令将所感测块发送到主机1005用于验证存储在阵列1001中的数据。

[0091] 在接收到块1032时,主机1005可使用所接收到的块来验证(例如,确定是否验证)存储在存储器阵列1001中的数据。例如,主机1005可使用块链中的前一个区块的密码散列及存储在存储器阵列1001中的数据的密码散列来验证数据。此外,主机1005可验证与块1032相关联的数字签名以确定块被包含(例如,有资格被包含)在块链中。如本文中所使用,验证存储在存储器阵列1001中的数据可包含及/或指代鉴别及/或证明数据是真实的(例如,与最初编程的相同)且未被黑客活动变更或其它未经授权的改变。

[0092] 在其中存储器阵列1001是安全阵列的实施例中,本文中先前描述的黄金散列也可用于验证存储在存储器阵列1001中的数据。例如,可生成(例如,计算)运行时密码散列,并与黄金散列进行比较。如果比较指示运行时与黄金散列匹配,如果可确定安全阵列尚未变更,且因此存储在其中的数据是有效的。然而,如果比较指示运行时及黄金散列不匹配,那么此可指示存储在安全阵列中的数据已改变(例如,由于黑客或存储器中的故障),且此可报告给主机1005。

[0093] 在对存储在存储器阵列1001中的数据进行验证之后,电路系统1026可以类似于生成块1032的方式生成块链中的额外(例如,下一个)块以验证存储在存储器阵列1001中的数据。例如,此额外块可包含块1032(其现在已成为块链中前一个块)的密码散列,及存储在存储器阵列1001中的数据的新密码散列。此外,此额外块可包含具有指示此块何时生成的时间戳的标头,且可具有与其相关联的指示此块被包含在块链中的数字签名。此外,在存储器阵列1001是安全阵列的实施例中,可生成额外(例如,新的)黄金散列。

[0094] 额外块以及与额外块相关联的数字签名及额外黄金散列可存储在存储器阵列1001中。例如,额外块可替换存储器阵列1001中的块1032(例如,前一个块)。然后以类似于本文中先前针对块1032所描述的方式,主机1005可使用额外块、数字签名及额外黄金散列来验证存储在存储器阵列1001中的数据。块链中的额外块可继续由电路系统1026生成,并由主机1005使用以在存储器装置1003的整个生命周期中以此类方式验证存储在存储器阵列1001中的数据。

[0095] 图10中所图解说明的实施例可包含未说明以便不使本公开的实施例模糊的额外电路系统、逻辑及/或组件。例如,存储器装置1003可包含地址电路系统以锁存通过I/O电路系统经由I/O连接器提供的地址信号。地址信号可由行解码器及列解码器接收及解码以存取存储器阵列1001。此外,存储器装置1003可包含与存储器阵列1001分离及/或除存储器阵列1001之外的主存储器,例如DRAM或SDRAM。本文中(例如,结合图11)将进一步描述进一步说明存储器装置1003的额外电路系统、逻辑及/或组件的实例。

[0096] 图11为根据本公开的实施例的实例存储器装置1103的框图。例如,存储器装置1103可为分别结合图1及2所描述的订户装置102或标识装置206。

[0097] 如在图11中所展示,存储器装置1103可包含多个存储器阵列1101-1到1101-7。此外,在图11中所说明的实例中,存储器阵列1101-3是安全阵列,存储器阵列1101-6的子集1111包括安全阵列,且存储器阵列1101-7的子集1113及1115包括安全阵列。子集1111、1113及1115可各自包含例如4千字节的数据。然而,本公开的实施例不限于特定数数目或布置的存储器阵列或安全阵列。

[0098] 如在图11中所展示,存储器装置1103可包含修复(例如,恢复)块1117。修复块1117可用作在存储器装置1103的操作期间可能发生的错误(例如,失配)的状况下的数据源。修复块1117可在可由主机寻址的存储器装置1103的区域之外。

[0099] 如在图11中所展示,存储器装置1103可包含串行外围接口(SPI)1107及控制器1109。存储器装置1103可使用SPI 1107及控制器1109来与主机及存储器阵列1101-1到1101-7通信。

[0100] 如在图11中所展示,存储器装置1103可包含用于管理存储器装置1103的安全性的安全寄存器1119。例如,安全寄存器1119可配置应用控制器并在外部与应用程序控制器通信。此外,安全寄存器1119可由鉴别命令修改。

[0101] 如在图11中所展示,存储器装置1103可包含密钥1121。例如,存储器装置1103可包含八个不同的槽来存储例如根密钥、DICE-RIOT密钥及/或其它外部会话密钥的密钥。

[0102] 如在图11中所展示,存储器装置1103可包含电子可擦除可编程只读存储器(EEPROM)1123。EEPROM 1123可为主机提供安全的非易失性区域,其中可擦除及编程个别字节的数据。

[0103] 如在图11中所展示,存储器装置1103可包含计数器(例如,单调计数器)1125。例如,存储器装置1103可包含六个不同的单调计数器,其中两个可由存储器装置1103用于经鉴别命令,且其中四个可由主机使用。

[0104] 如在图11中所展示,存储器装置1103可包含SHA-256密码散列函数1127及/或HMAC-SHA256密码散列函数1129。SHA-256及/或HMAC-SHA256密码散列函数1127及1129可由存储器装置1103使用以生成密码散列,例如,如先前本文中所描述的命令的密码散列,及/或用于验证存储在存储器阵列1101-1到1101-7中的数据黄金散列。此外,存储器装置1103可支持DICE-RIOT 1131的L0及L1。

[0105] 在先前详细说明中,参考形成本文的一部分且其中以说明的方式展示特定实例的附图。在图式中,相同编号遍及数个视图描述基本上类似组件。可利用其它实例,且可在不背离本公开的范围的情况下做出结构、逻辑及/或电改变。

[0106] 本文中的图遵循其中第一个数字或前几个数字对应于图式的图编号且剩余数字标识图式中的元件或组件的编号惯例。可通过使用类似的数字来标识不同图之间的类似元件或组件。如将了解,可添加、交换及/或消除本文中的各种实施例中所展示的元件以便提供本公开的多个额外实施例。另外,如将了解,各图中所提供的元件的比例及相对尺度打算说明本公开的实施例且不应视为具限制意义。

[0107] 如本文中所使用,“一”、“一”或“一定数目个”某物可指此类事物中的一或多个。“多个”某物意指两个或多于两个。如本文中所使用,术语“耦合”可包含不与中间元件电耦

合、直接耦合及/或直接连接(例如,通过直接物理接触)或与中间元件间接耦合及/或连接。术语耦合可进一步包含彼此协作或相互作用的两个或多于两个元件(例如,如呈因果关系)。

[0108] 虽然本文中已说明及描述特定实例,但所属领域普通技术人员将了解,旨在实现相同结果的布置可替代所展示的特定实施例。本公开意欲涵盖本公开的一或多个实施例的变更或变化形式。应理解,已以说明性方式而非限定性方式做出以上说明。本公开的一或多个实例的范围应参考所附权利要求书连同此权利要求书授权的等效物的整个范围来确定。

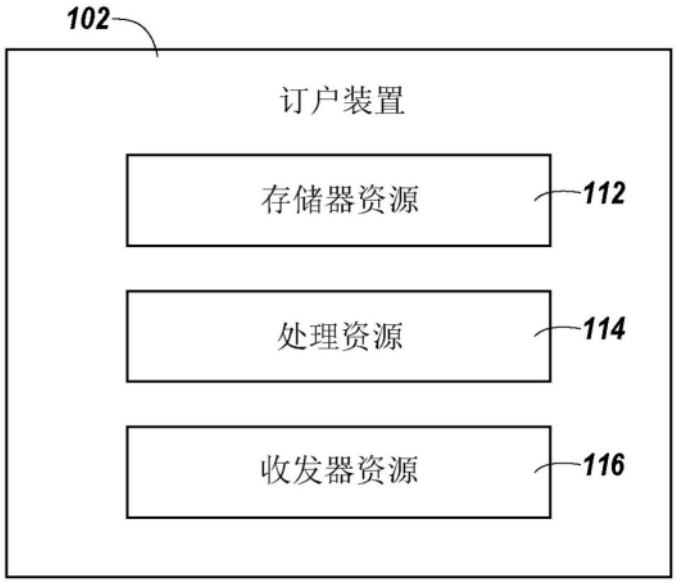

102
订户装置
存储器资源
112
处理资源
114
收发器资源
116

图1

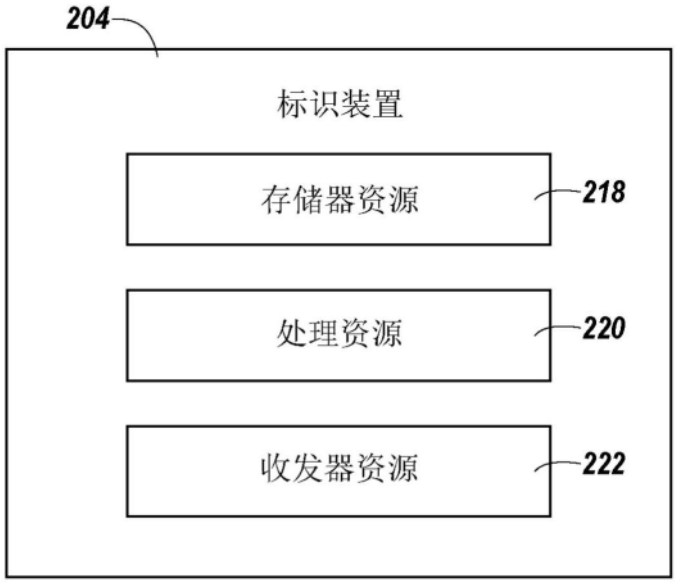

204
标识装置
存储器资源
218
处理资源
220
收发器资源
222

图2

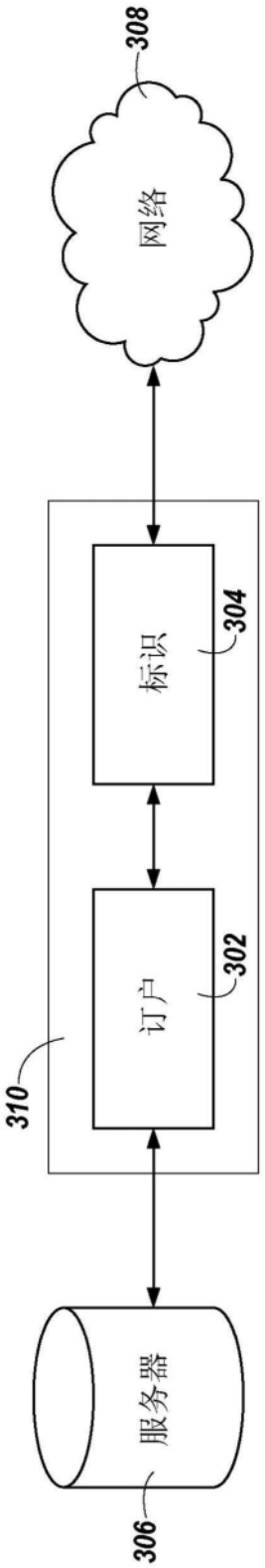


图3

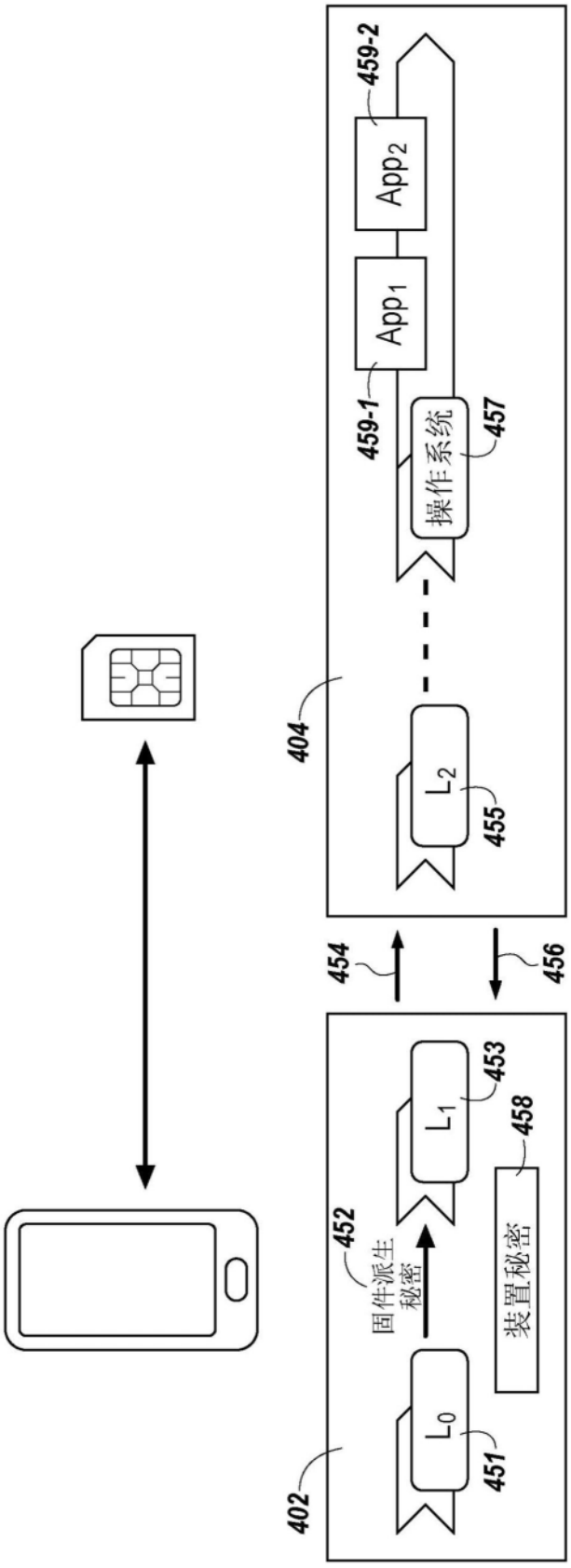

459-2
App2
App1
459-1
操作系统
457
404
L2
455
454
456
453
L1
458
452
固件派生秘密
装置秘密
L0
451
402

图4

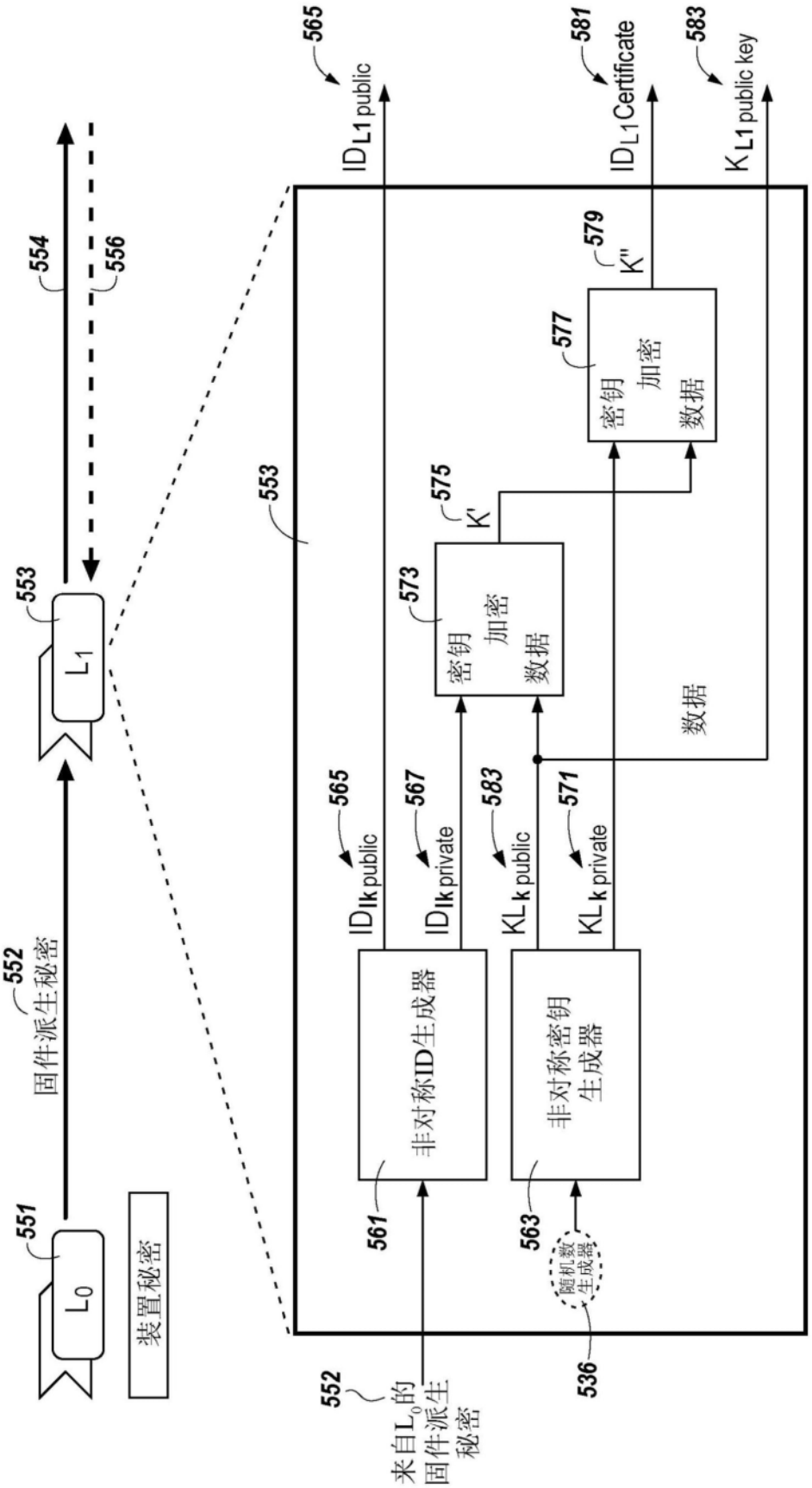

565
581
583
ID_{L1} public
ID_{L1} Certificate
K_{L1} public key
554
556
579
K''
577
密钥 加密 数据
553
575
K'
573
密钥 加密 数据
553
数据
565
567
583
571
ID_{Ik} public
ID_{Ik} private
KL_k public
KL_k private
552
固件派生秘密
非对称ID生成器
非对称密钥 生成器
561
563
随机数 生成器
536
551
L_0
装置秘密
552
来自L_0的 固件派生 秘密
553
L_1

图5

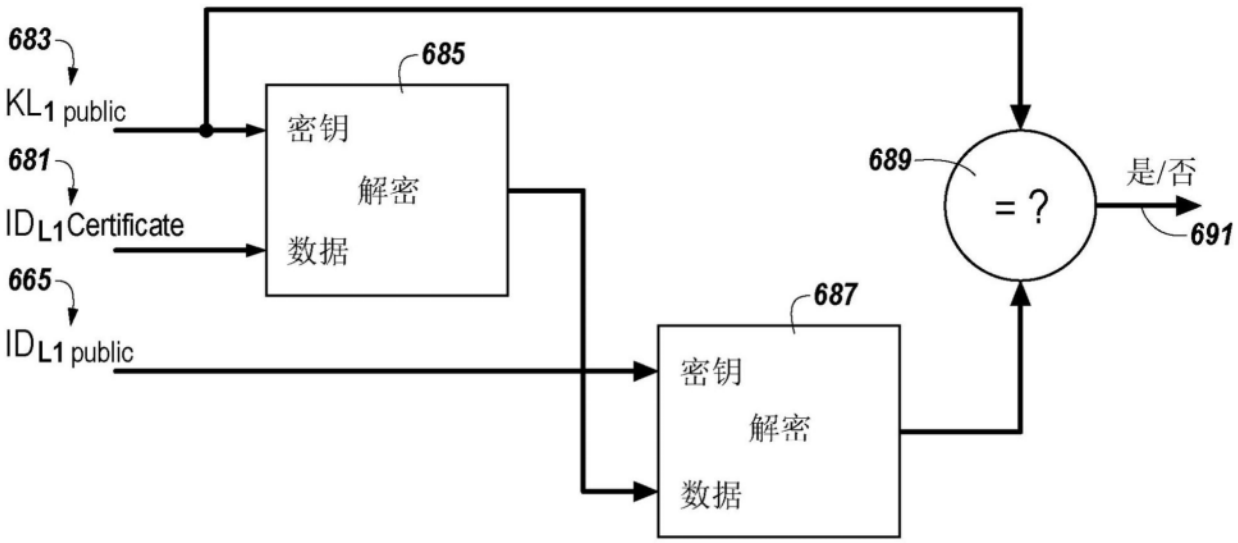

683
KL1 public
681
ID L1 Certificate
665
ID L1 public
685
密钥
解密
数据
687
密钥
解密
数据
689
= ?
是/否
691

图6

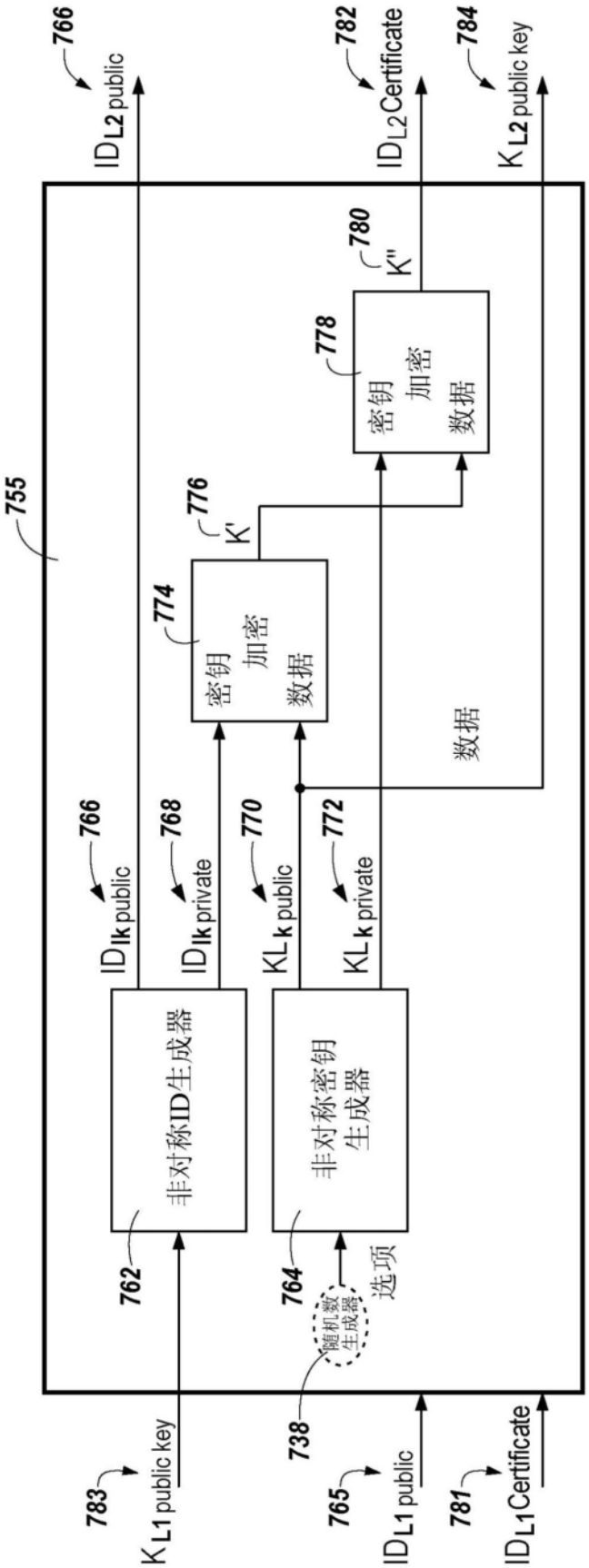

766
ID L2 public
782
ID L2 Certificate
784
K L2 public key
780
K''
778
密钥 加密 数据
755
776
K'
774
密钥 加密 数据
数据
766
ID lk public
768
ID lk private
770
KL k public
772
KL k private
非对称ID生成器
非对称密钥 生成器
762
764
随机数 生成器
选项
738
783
K L1 public key
765
ID L1 public
781
ID L1 Certificate

图7

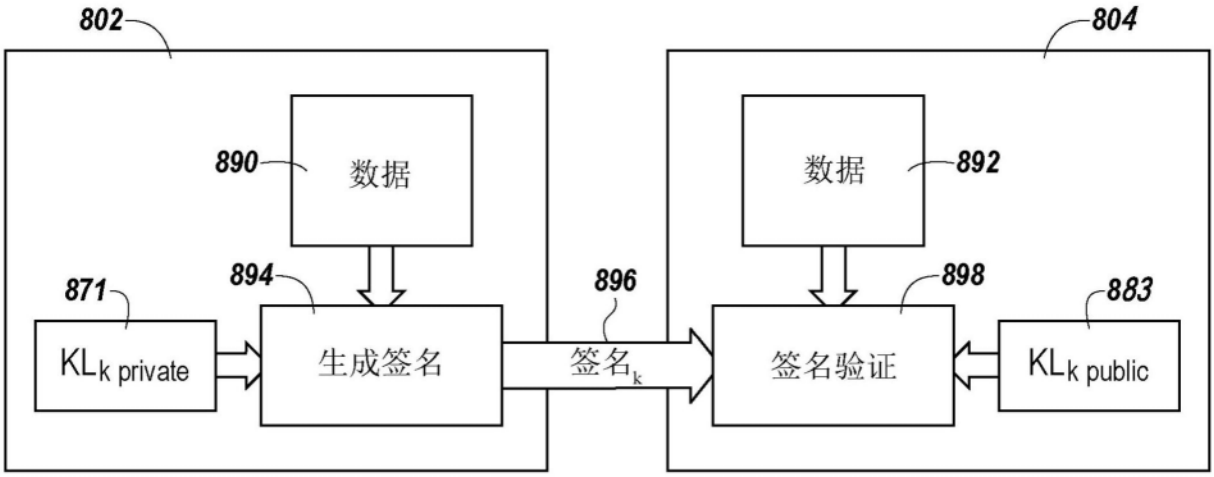

802
804
890
数据
892
数据
871
894
896
898
883
KLk private
生成签名
签名k
签名验证
KLk public

图8

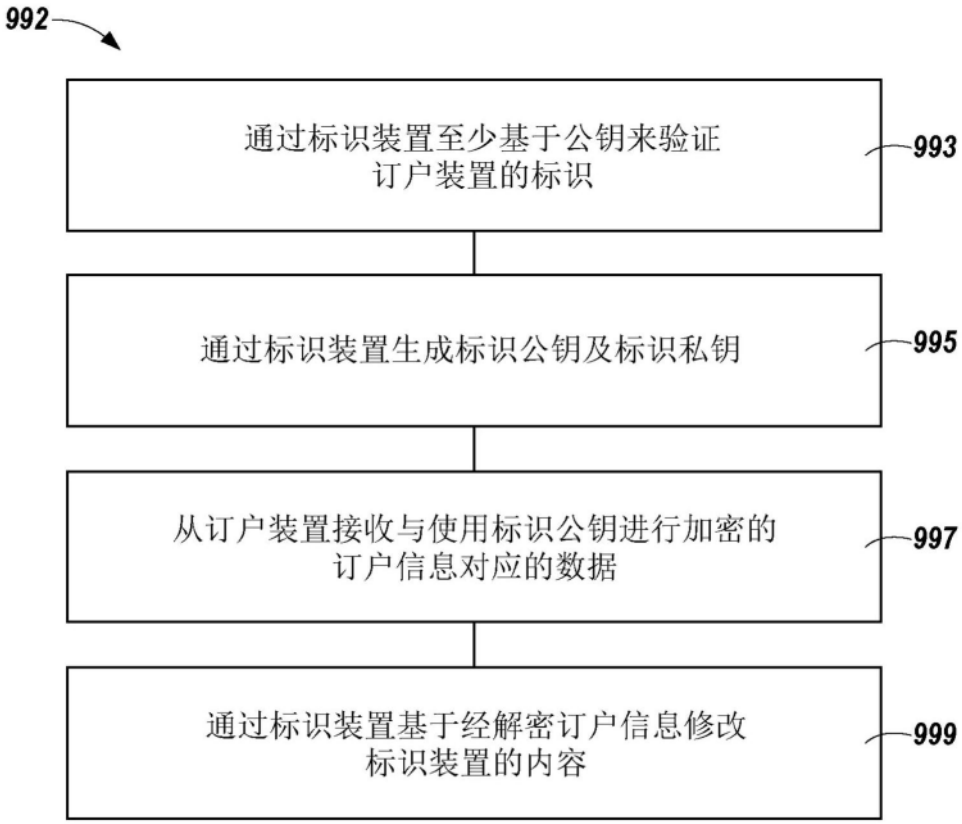

992
通过标识装置至少基于公钥来验证
订户装置的标识
993
通过标识装置生成标识公钥及标识私钥
995
从订户装置接收与使用标识公钥进行加密的
订户信息对应的数据
997
通过标识装置基于经解密订户信息修改
标识装置的内容
999

图9

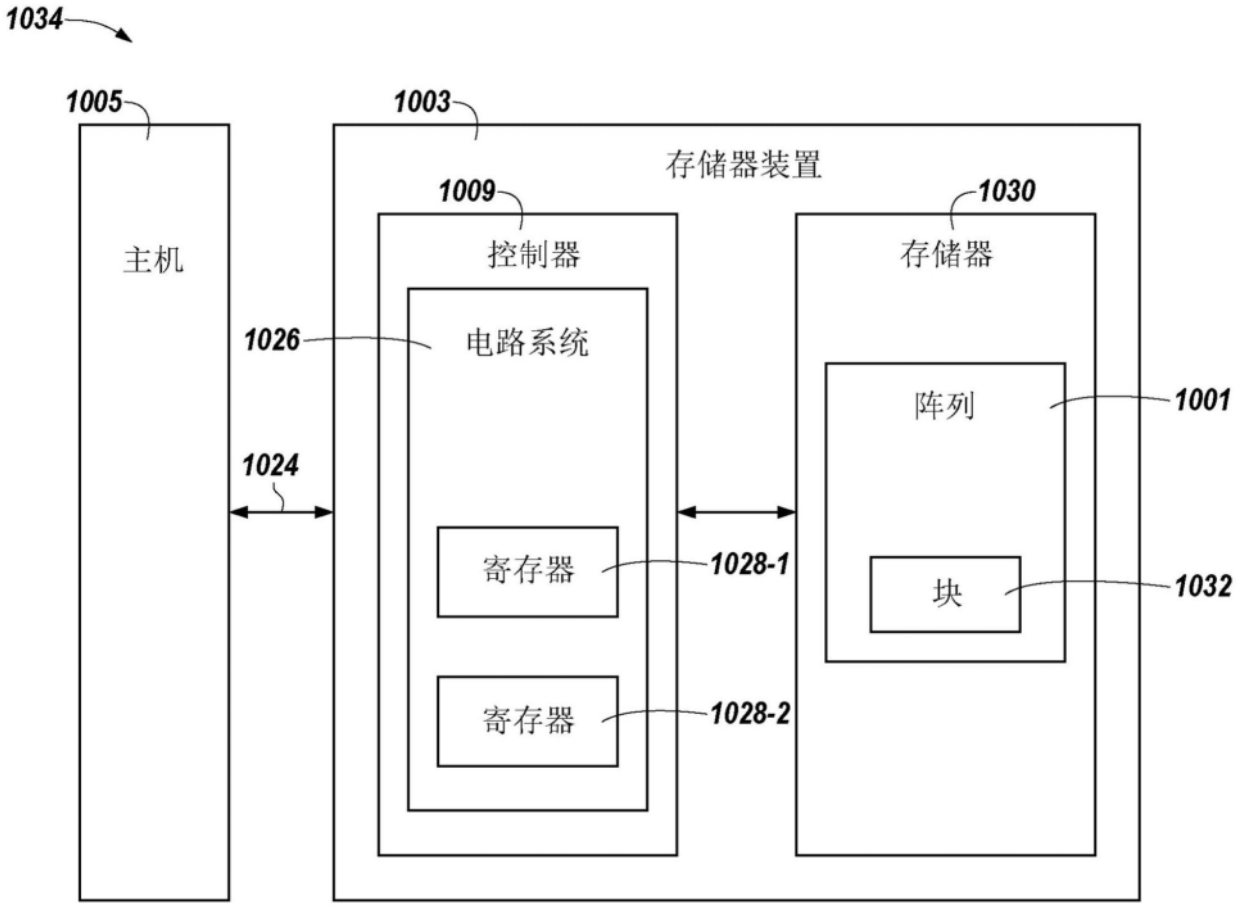

1034
1005
主机
1003
存储器装置
1009
控制器
1030
存储器
1026
电路系统
1024
阵列
1001
寄存器
1028-1
块
1032
寄存器
1028-2

图10

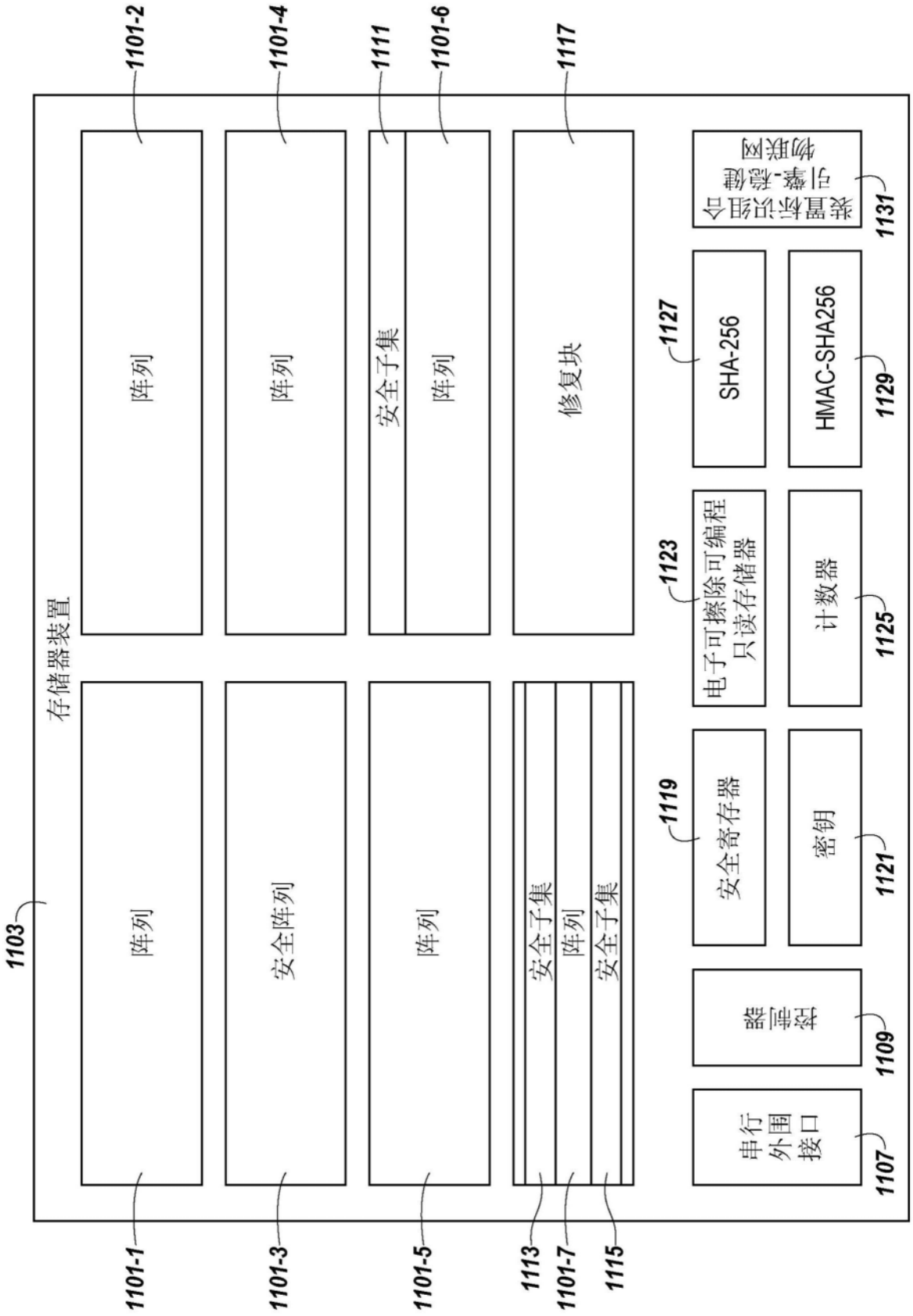

1103
存储器装置
阵列
1101-1
安全阵列
1101-3
阵列
1101-5
安全子集
阵列
安全子集
1113
1101-7
1115
阵列
1101-2
安全子集
阵列
1101-4
1111
阵列
1101-6
修复块
1117
串行外围接口
1107
控制器
1109
安全寄存器
1119
密钥
1121
电子可擦除可编程只读存储器
1123
计数器
1125
SHA-256
1127
HMAC-SHA256
1129
装置标识组合引擎-稳健物联网
1131

图11