(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106133737 A
(43)申请公布日 2016.11.16

(21)申请号 201580016669.2

(22)申请日 2015.03.31

(30)优先权数据
14/245,661 2014.04.04 US

(85)PCT国际申请进入国家阶段日
2016.09.27

(86)PCT国际申请的申请数据
PCT/US2015/023518 2015.03.31

(87)PCT国际申请的公布数据
WO2015/153562 EN 2015.10.08

(71)申请人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 伊万·休·麦克莱恩

(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.
G06F 21/33(2013.01)
H04L 29/06(2006.01)
G01R 31/317(2006.01)

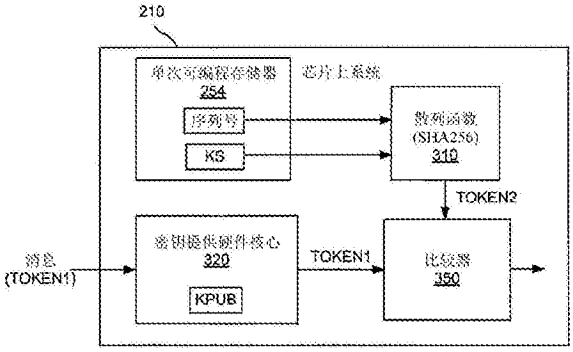
权利要求书3页 说明书5页 附图3页

(54)发明名称

用于在芯片上系统装置中重新启用被停用的除错能力的远程站和方法

(57)摘要

可在例如芯片上系统SoC装置等集成电路中安全地重新启用被停用的除错能力。在方法中，所述集成电路接收除错重新启用消息。所述除错重新启用消息包含通过私用密钥签署的除错重新启用令牌。所述除错重新启用令牌是基于所述集成电路的序列号和对称密钥的第一副本。使用对应于所述私用密钥的公共密钥证实所述除错重新启用令牌。使用所述集成电路的所述序列号且使用存储在所述集成电路的单次可编程OTP存储器中的所述对称密钥的第二副本产生比较令牌。所述集成电路将所述除错重新启用令牌和所述比较令牌进行比较。在所述除错重新启用令牌匹配于所述比较令牌的情况下在所述集成电路中重新启用所述被停用的除错能力。



CN 106133737 A

1.一种用于在集成电路中重新启用被停用的除错能力的方法,其包括:

由所述集成电路接收除错重新启用消息,其中:

所述除错重新启用消息包含通过私用密钥签署的除错重新启用令牌,且

所述除错重新启用令牌是基于所述集成电路的唯一识别符和对称密钥的第一副本;

使用对应于所述私用密钥的公共密钥证实所述除错重新启用令牌;

使用所述唯一识别符且使用安全地存储在所述集成电路中的所述对称密钥的第二副本产生比较令牌;

将所述除错重新启用令牌与所述比较令牌进行比较;以及

在所述除错重新启用令牌匹配于所述比较令牌的情况下在所述集成电路中重新启用所述被停用的除错能力。

2.根据权利要求1所述的方法,其中所述集成电路是芯片上系统SoC装置。

3.根据权利要求1所述的方法,其中所述除错重新启用消息是从第一方接收,且所述私用密钥是所述第一方的私用密钥。

4.根据权利要求3所述的方法,其中所述对称密钥的所述第一副本存储在第二方处。

5.根据权利要求4所述的方法,其中所述第一方的所述私用密钥不可用于所述第二方,且所述对称密钥不可用于所述第一方。

6.根据权利要求1所述的方法,其中所述唯一识别符是所述集成电路的序列号。

7.根据权利要求6所述的方法,其中使用所述序列号和所述对称密钥的所述第二副本作为输入,基于单向加密函数产生所述比较令牌。

8.根据权利要求1所述的方法,其中所述对称密钥安全地存储在所述集成电路的单次可编程OTP存储器中。

9.一种远程站,其包括:

用于接收除错重新启用消息的装置,其中所述除错重新启用消息包含通过私用密钥签署的除错重新启用令牌,且所述除错重新启用令牌是基于集成电路的唯一识别符和对称密钥的第一副本;

用于使用对应于所述私用密钥的公共密钥证实所述除错重新启用令牌的装置;

用于使用所述唯一识别符且使用安全地存储在所述集成电路中的所述对称密钥的第二副本产生比较令牌的装置;

用于将所述除错重新启用令牌与所述比较令牌进行比较的装置;以及

用于在所述除错重新启用令牌匹配于所述比较令牌的情况下在所述集成电路中重新启用被停用的除错能力的装置。

10.根据权利要求9所述的远程站,其中所述集成电路是芯片上系统SoC装置。

11.根据权利要求9所述的远程站,其中所述除错重新启用消息是从第一方接收,且所述私用密钥是所述第一方的私用密钥。

12.根据权利要求11所述的远程站,其中所述对称密钥的所述第一副本存储在第二方处。

13.根据权利要求12所述的远程站,其中所述第一方的所述私用密钥不可用于所述第二方,且所述对称密钥不可用于所述第一方。

14.根据权利要求9所述的远程站,其中所述唯一识别符是所述集成电路的序列号。

15.根据权利要求14所述的远程站，其中使用所述序列号和所述对称密钥的所述第二副本作为输入，基于单向加密函数产生所述比较令牌。

16.根据权利要求9所述的远程站，其中所述对称密钥安全地存储在所述集成电路的单次可编程OTP存储器中。

17.一种远程站，其包括：

处理器，其经配置以：

接收除错重新启用消息，其中所述除错重新启用消息包含通过私用密钥签署的除错重新启用令牌，且所述除错重新启用令牌是基于集成电路的唯一识别符和对称密钥的第一副本；

使用对应于所述私用密钥的公共密钥证实所述除错重新启用令牌；

使用所述唯一识别符且使用安全地存储在所述集成电路中的所述对称密钥的第二副本产生比较令牌；

将所述除错重新启用令牌与所述比较令牌进行比较；以及

在所述除错重新启用令牌匹配于所述比较令牌的情况下在所述集成电路中重新启用被停用的除错能力。

18.根据权利要求17所述的远程站，其中所述集成电路是芯片上系统SoC装置。

19.根据权利要求17所述的远程站，其中所述除错重新启用消息是从第一方接收，且所述私用密钥是所述第一方的私用密钥。

20.根据权利要求19所述的远程站，其中所述对称密钥的所述第一副本存储在第二方处。

21.根据权利要求20所述的远程站，其中所述第一方的所述私用密钥不可用于所述第二方，且所述对称密钥不可用于所述第一方。

22.根据权利要求17所述的远程站，其中所述唯一识别符是所述集成电路的序列号。

23.根据权利要求22所述的远程站，其中使用所述序列号和所述对称密钥的所述第二副本作为输入，基于单向加密函数产生所述比较令牌。

24.根据权利要求18所述的远程站，其中所述对称密钥安全地存储在所述集成电路的单次可编程OTP存储器中。

25.一种集成电路，其包括：

用于接收除错重新启用消息的装置，其中所述除错重新启用消息包含通过私用密钥签署的除错重新启用令牌，且所述除错重新启用令牌是基于所述集成电路的唯一识别符和对称密钥的第一副本；

用于使用对应于所述私用密钥的公共密钥证实所述除错重新启用令牌的装置；

用于使用所述唯一识别符且使用安全地存储在所述集成电路中的所述对称密钥的第二副本产生比较令牌的装置；

用于将所述除错重新启用令牌与所述比较令牌进行比较的装置；以及

用于在所述除错重新启用令牌匹配于所述比较令牌的情况下在所述集成电路中重新启用被停用的除错能力的装置。

26.根据权利要求25所述的集成电路，其中所述集成电路是芯片上系统SoC装置。

27.根据权利要求25所述的集成电路，其中所述除错重新启用消息是从第一方接收，

所述私用密钥是所述第一方的私用密钥，且所述对称密钥的所述第一副本存储在第二方处。

28.根据权利要求25所述的集成电路，其中所述唯一识别符是所述集成电路的序列号。

29.根据权利要求28所述的集成电路，其中使用所述序列号和所述对称密钥的所述第二副本作为输入，基于单向加密函数产生所述比较令牌。

30.根据权利要求25所述的集成电路，其中所述对称密钥安全地存储在所述集成电路的单次可编程OTP存储器中。

用于在芯片上系统装置中重新启用被停用的除错能力的远程站和方法

[0001] 相关申请案的交叉参考

[0002] 本申请案主张2014年4月4日在美国专利商标局申请的美国非临时专利申请案第14/245,661号的优先权及权益，所述非临时专利申请案的整个内容以引用的方式并入本文中。

技术领域

[0003] 本发明大体上涉及在芯片上系统(SoC)装置中重新启用被停用的除错能力。

背景技术

[0004] 芯片上系统(SoC)装置中的除错重新启用带来安全敏感性。将SoC装置并入到其产品中的原始设备制造商(OEM)不希望其安全性方案受到危及，且必须允许SoC装置的制造商/供应商对基于可能的制造或其它缺陷而返回的装置进行除错。一些OEM可能不关心安全性且可能仅希望事情顺利，而不要求其自身的额外安全性努力。

[0005] 因此需要用于以有效方式在SoC装置中重新启用被停用的除错能力的技术。

发明内容

[0006] 本发明的方面可在于用于在集成电路中重新启用被停用的除错能力的方法。在所述方法中，所述集成电路接收除错重新启用消息。所述除错重新启用消息包含通过私用密钥签署的除错重新启用令牌。所述除错重新启用令牌是使用所述集成电路的唯一识别符和对称密钥的第一副本产生。使用对应于所述私用密钥的公共密钥证实所述除错重新启用令牌。使用所述唯一识别符且使用安全地存储在所述集成电路中的所述对称密钥的第二副本产生比较令牌。所述集成电路将所述除错重新启用令牌和所述比较令牌进行比较。在所述除错重新启用令牌匹配于所述比较令牌的情况下在所述集成电路中重新启用所述被停用的除错能力。

[0007] 在本发明的更详细方面中，所述集成电路可为芯片上系统(SoC)装置。所述除错重新启用消息可从第一方接收，且所述私用密钥可为所述第一方的私用密钥。所述对称密钥的第一副本可存储在第二方处。所述第一方的私用密钥不可用于所述第二方，且所述对称密钥不可用于所述第一方。所述唯一识别符可为所述集成电路的序列号。可使用所述序列号和所述对称密钥的第二副本作为输入，基于单向加密函数产生所述比较令牌。所述对称密钥可安全地存储在所述集成电路的单次可编程(OTP)存储器中。

[0008] 本发明的另一方面可在于远程站，其包括：用于接收除错重新启用消息的装置，其中所述消息包含通过私用密钥签署的除错重新启用令牌，且所述除错重新启用令牌是基于集成电路的唯一识别符和对称密钥的第一副本；用于使用对应于私用密钥的公共密钥证实除错重新启用令牌的装置；用于使用所述唯一识别符且使用安全地存储在集成电路中的对称密钥的第二副本产生比较令牌的装置；用于将除错重新启用令牌与比较令牌进行比较的

装置;以及用于在除错重新启用令牌匹配于比较令牌的情况下在集成电路中重新启用被停用的除错能力的装置。

[0009] 本发明的另一方面可在于远程站,其包括处理器,所述处理器经配置以:接收除错重新启用消息,其中所述消息包含通过私用密钥签署的除错重新启用令牌,且所述除错重新启用令牌是基于集成电路的唯一识别符和对称密钥的第一副本;使用对应于私用密钥的公共密钥证实除错重新启用令牌;使用所述唯一识别符且使用安全地存储在集成电路中的对称密钥的第二副本产生比较令牌;将除错重新启用令牌与比较令牌进行比较;以及在除错重新启用令牌匹配于比较令牌的情况下在集成电路中重新启用被停用的除错能力。

[0010] 本发明的另一方面可在于集成电路,其包括:用于接收除错重新启用消息的装置,其中所述消息包含通过私用密钥签署的除错重新启用令牌,且所述除错重新启用令牌是基于集成电路的唯一识别符和对称密钥的第一副本;用于使用对应于私用密钥的公共密钥证实除错重新启用令牌的装置;用于使用所述唯一识别符且使用安全地存储在集成电路中的对称密钥的第二副本产生比较令牌的装置;用于将除错重新启用令牌与比较令牌进行比较的装置;以及用于在除错重新启用令牌匹配于比较令牌的情况下在集成电路中重新启用被停用的除错能力的装置。

附图说明

[0011] 图1是无线通信系统的实例的框图。

[0012] 图2是根据本发明的用于在例如芯片上系统(SoC)装置等集成电路中重新启用被停用的除错能力的方法的框图。

[0013] 图3是SoC装置的框图。

[0014] 图4是包含处理器以及存储器的计算机的框图。

[0015] 图5是用于使用私用密钥产生令牌的签名的方法的框图。

具体实施方式

[0016] 词语“示范性”在本文中用于意指“充当实例、例子或说明”。本文中被描述为“示范性的”任何实施例不必须被理解为比其它实施例优选或有利。

[0017] 参考图2和3,本发明的方面可在于用于在例如芯片上系统(SoC)装置210等集成电路中重新启用被停用的除错能力的方法200。在所述方法中,所述集成电路接收除错重新启用消息MSG(步骤230)。所述除错重新启用消息包含通过私用密钥KPRI签署的除错重新启用令牌TOKEN1。所述除错重新启用令牌可基于集成电路的唯一识别符和对称密钥KS的第一副本。使用对应于私用密钥的公共密钥KPUB来证实所述除错重新启用令牌(步骤250)。使用所述唯一识别符且使用安全地存储在所述集成电路中的对称密钥的第二副本来产生比较令牌TOKEN2(步骤260)。所述集成电路将除错重新启用令牌与比较令牌进行比较(步骤270)。如果除错重新启用令牌匹配于比较令牌,那么在集成电路中重新启用被停用的除错能力(步骤280)。

[0018] 在本发明的更详细方面中,除错重新启用消息可从第一方220接收,且私用密钥可为所述第一方的私用密钥。对称密钥的第一副本可存储在第二方240处。第一方的私用密钥KPRI不可用于第二方,且对称密钥KS不可用于第一方。所述唯一识别符可为SoC装置的序列

号。可使用所述序列号和对称密钥的第二副本作为输入，基于例如SHA256散列函数310等单向加密函数来产生比较令牌TOKEN2。对称密钥可安全地存储在SoC装置的单次可编程(OTP)存储器254中。

[0019] 在本发明的更详细方面中，第一方220可为SoC装置210的供应商和/或制造商，且第二方240可为原始设备制造商(OEM)。

[0020] SoC装置210的供应商(制造商)220保持用于签署消息的私用密钥KPRI，且不与外部方共享此私用密钥。想要阻止供应商解锁/重新启用其SoC装置中的除错能力的OEM 240可将对称(或OEM)密钥KS提供到SoC装置中的OTP存储器(即，eFuse、QFPROM等)中。对称密钥可对于每一装置是唯一的，或可跨越装置全局地共享。因此，供应商可如下继续在SoC装置210中重新启用除错。

[0021] 供应商220将指定芯片序列号的正式请求转发到OEM 240(步骤222)。这是存储在OTP存储器254中的唯一序列号。替代地，OEM首先将具有所述唯一序列号的返回材料授权(RMA)发送到供应商。

[0022] OEM 240通过对所述序列号和OEM密钥KS进行散列而产生每装置256位除错解锁/重新启用令牌TOKEN1(步骤224)。OEM为供应商220提供此令牌(步骤226)。

[0023] 供应商220产生通过仅对供应商已知的私用密钥KPRI签署的除错重新启用消息。所述经签署的消息包含OEM提供的令牌TOKEN1。

[0024] SoC装置210内的密钥提供硬件核心320证实所述消息上的签名，且解开并输出除错重新启用令牌TOKEN1到比较器350。SoC硬件(HW)还通过执行序列号与存储在OTP存储器254中的OEM密钥KS的散列而产生256位令牌TOKEN2。如果所接收的除错重新启用令牌TOKEN1匹配于SoC HW产生的比较令牌TOKEN2，那么允许操作(例如，除错重新启用)。

[0025] 本发明的技术简单到足以在硬件中实施，且允许SoC装置制造商保持最终的RMA除错控制，同时允许OEM阻止他们未授权的操作。

[0026] 进一步参看图1和4，远程站102可包括计算机400，其包含处理器410(例如SoC装置210)、存储媒体420(例如存储器和/或磁盘驱动器)、显示器430、以及例如小键盘440等输入、以及无线连接450(例如Wi-Fi连接和/或蜂窝式连接)。

[0027] 本发明的另一方面可在于远程站102，其包括：用于接收除错重新启用消息的装置410，其中所述消息包含通过私用密钥KPRI签署的除错重新启用令牌TOKEN1，且所述除错重新启用令牌是基于集成电路的唯一识别符和对称密钥KS的第一副本；用于使用对应于私用密钥的公共密钥KPUB证实除错重新启用令牌的装置410；用于使用所述唯一识别符且使用安全地存储在集成电路中的对称密钥的第二副本产生比较令牌TOKEN2的装置410；用于将除错重新启用令牌与比较令牌进行比较的装置410；以及用于在除错重新启用令牌匹配于比较令牌的情况下在集成电路中重新启用被停用的除错能力的装置410。

[0028] 本发明的另一方面可在于远程站102，其包括处理器410，所述处理器经配置以：接收除错重新启用消息，其中所述消息包含通过私用密钥KPRI签署的除错重新启用令牌TOKEN1，且所述除错重新启用令牌是基于芯片上系统(SoC)装置的唯一识别符和对称密钥KS的第一副本；使用对应于私用密钥的公共密钥KPUB证实除错重新启用令牌；使用所述唯一识别符且使用安全地存储在集成电路中的对称密钥的第二副本产生比较令牌TOKEN2；将除错重新启用令牌与比较令牌进行比较；以及在除错重新启用令牌匹配于比较令牌的情况

下在集成电路中重新启用被停用的除错能力。

[0029] 本发明的另一方面可在于集成电路410，其包括：用于接收除错重新启用消息的装置，其中所述消息包含通过私用密钥KPRI签署的除错重新启用令牌TOKEN1，且所述除错重新启用令牌是基于集成电路的唯一识别符和对称密钥KS的第一副本；用于使用对应于私用密钥的公共密钥KPUB证实除错重新启用令牌的装置；用于使用所述唯一识别符且使用安全地存储在集成电路中的对称密钥的第二副本产生比较令牌TOKEN2的装置；用于将除错重新启用令牌与比较令牌进行比较的装置；以及用于在除错重新启用令牌匹配于比较令牌的情况下在集成电路中重新启用被停用的除错能力的装置。

[0030] 图5中展示用于产生载运除错重新启用令牌TOKEN1的消息MSG的签名的方法500。所述消息中的信息输入到散列函数520(例如，SHA2或SHA3)以产生摘要530。所述摘要输入到算法540中以使用第一方220的私用密钥KPRI产生消息签名值550。

[0031] 参考图1，无线远程站(RS)102可与无线通信系统100的一或多个基站(BS)104通信。所述RS可为移动台。无线通信系统100可进一步包含一或多个基站控制器(BSC)106及核心网络108。核心网络可经由适合回程连接至因特网110及公共交换电话网络(PSTN)112。典型的无线移动站可以包含手持式电话、或膝上型计算机。无线通信系统100可使用数种多址技术中的任一者或所属领域中已知的其它调制技术，所述多址技术例如码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)、空分多址(SDMA)、极化分多址(PDMA)。

[0032] 所属领域的技术人员将理解，可以使用多种不同技术和技艺中的任一者来表示信息和信号。举例来说，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在整个上文描述中可能参考的数据、指令、命令、信息、信号、位、符号和码片。

[0033] 所属领域的技术人员将进一步了解，结合本文所揭示的实施例描述的各种说明性逻辑块、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，以上已大体就其功能性来描述了各种说明性组件、块、模块、电路和步骤。此功能性是实施为硬件还是软件取决于特定应用及施加于整个系统的设计约束。熟练的技术人员可针对每一特定应用以不同方式来实施所描述的功能性，但这样的实施方案决策不应被解释为会引起脱离本发明的范围。

[0034] 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(FPGA)或经设计以执行本文所描述的功能的其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或其任何组合来实施或执行结合本文中所揭示的实施例而描述的各种说明性逻辑块、模块和电路。通用处理器可为微处理器，但在替代方案中，处理器可以为任何常规处理器、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、一或多个微处理器结合DSP核心，或任何其它此类配置。

[0035] 结合本文所揭示的实施例而描述的方法或算法的步骤可直接体现在硬件、由处理器执行的软件模块或所述两者的组合中。软件模块可驻留在RAM存储器、快闪存储器、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可装卸磁盘、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和将信息写入到存储媒体。在替代方案中，存储媒体可集成到处理器。处理器和存储媒体可驻留于ASIC中。ASIC可以驻留于用户终端中。在替代例中，处理器及存储媒体可作为离散组件驻留于用户终端中。

[0036] 在一或多个示范性实施例中，所述功能可以在硬件、软件、固件或其任何组合中实施。如果以软件实施为计算机程序产品，那么可将功能作为一或多个指令或代码存储于计算机可读媒体上或经由计算机可读媒体予以传输。计算机可读媒体包含非暂时性计算机存储媒体以及包含促进将计算机程序从一处传递到另一处的任何媒体的通信媒体两者。存储媒体可以是可由计算机存取的任何可用媒体。举例来说且非限制，此类非暂时性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，或可用于携载或存储呈指令或数据结构的形式的所要程序代码且可由计算机存取的任何其它媒体。并且，任何连接被恰当地称作计算机可读媒体。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、无线电及微波等无线技术从网站、服务器或其它远程源发射软件，则同轴电缆、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，磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软性磁盘和蓝光光盘，其中磁盘通常以磁性方式再现数据，而光盘利用激光以光学方式再现数据。以上各项的组合也应包含在计算机可读媒体的范围内。

[0037] 提供所揭示实施例的先前描述以使得所属领域的任何技术人员能够制作或使用本发明。所属领域的技术人员将容易地了解对这些实施例的各种修改，并且可以在不脱离本发明的精神或范围的情况下将本文所定义的一般原理应用到其它实施例中。因此，本发明并不既定限于本文中所展示的实施例，而应被赋予与本文中所揭示的原理和新颖特征相一致的最广泛范围。

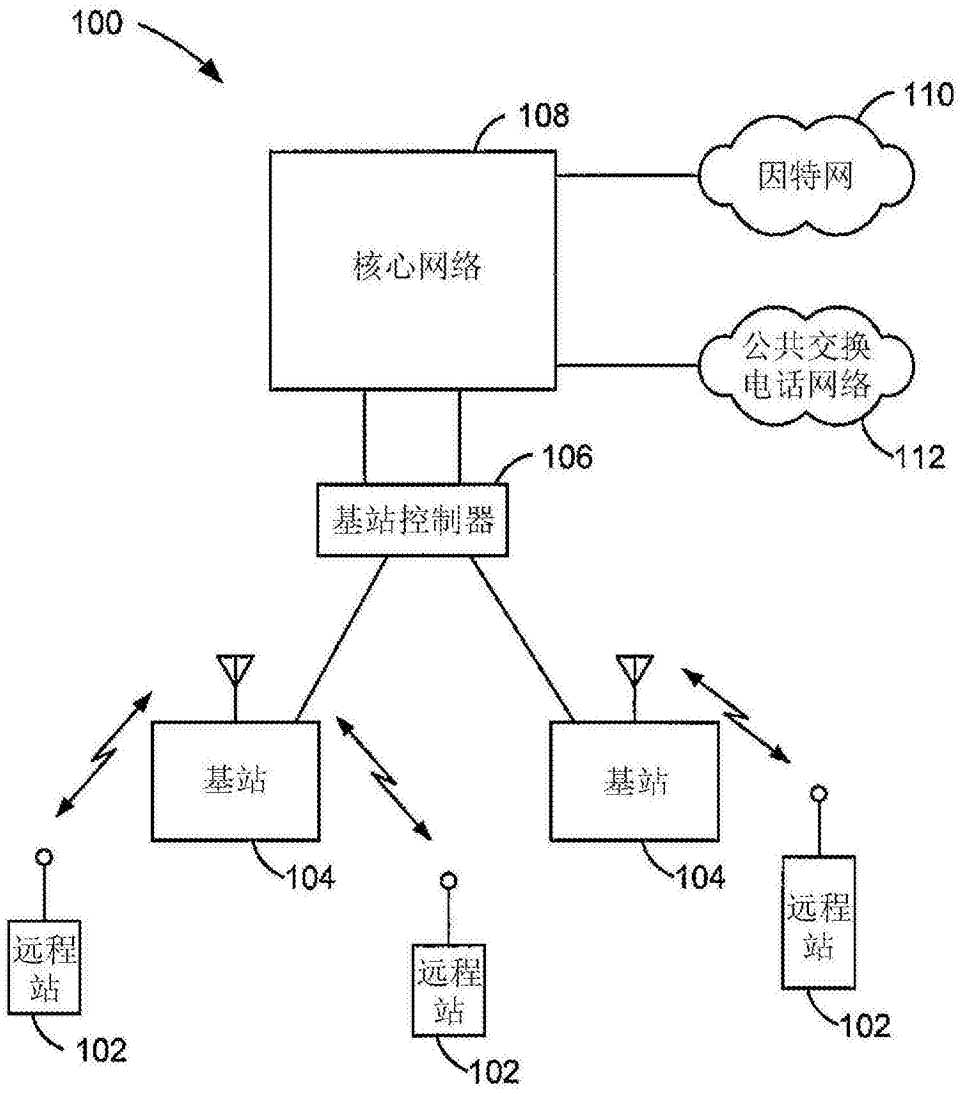

100
108
110
因特网
核心网络
公共交换
电话网络
112
106
基站控制器
基站
基站
104
104
远程
站
远程
站
远程
站
102
102
102

图1

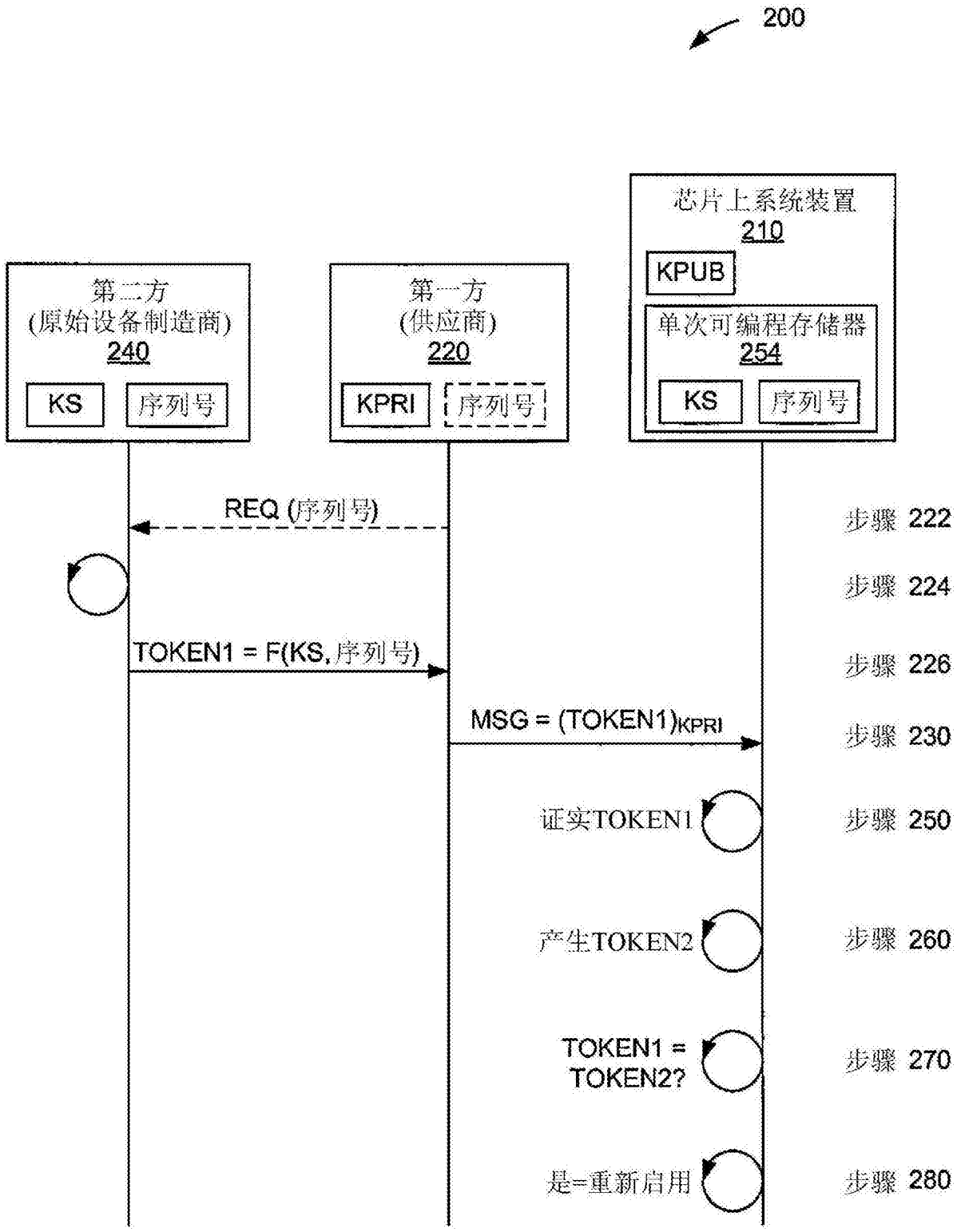

200
芯片上系统装置
210
KPUB
单次可编程存储器
254
KS
序列号
第二方
(原始设备制造商)
240
KS
序列号
第一方
(供应商)
220
KPRI
序列号
REQ (序列号)
步骤 222
步骤 224
TOKEN1 = F(KS, 序列号)
步骤 226
MSG = (TOKEN1)KPRI
步骤 230
证实TOKEN1
步骤 250
产生TOKEN2
步骤 260
TOKEN1 = TOKEN2?
步骤 270
是=重新启用
步骤 280

图2

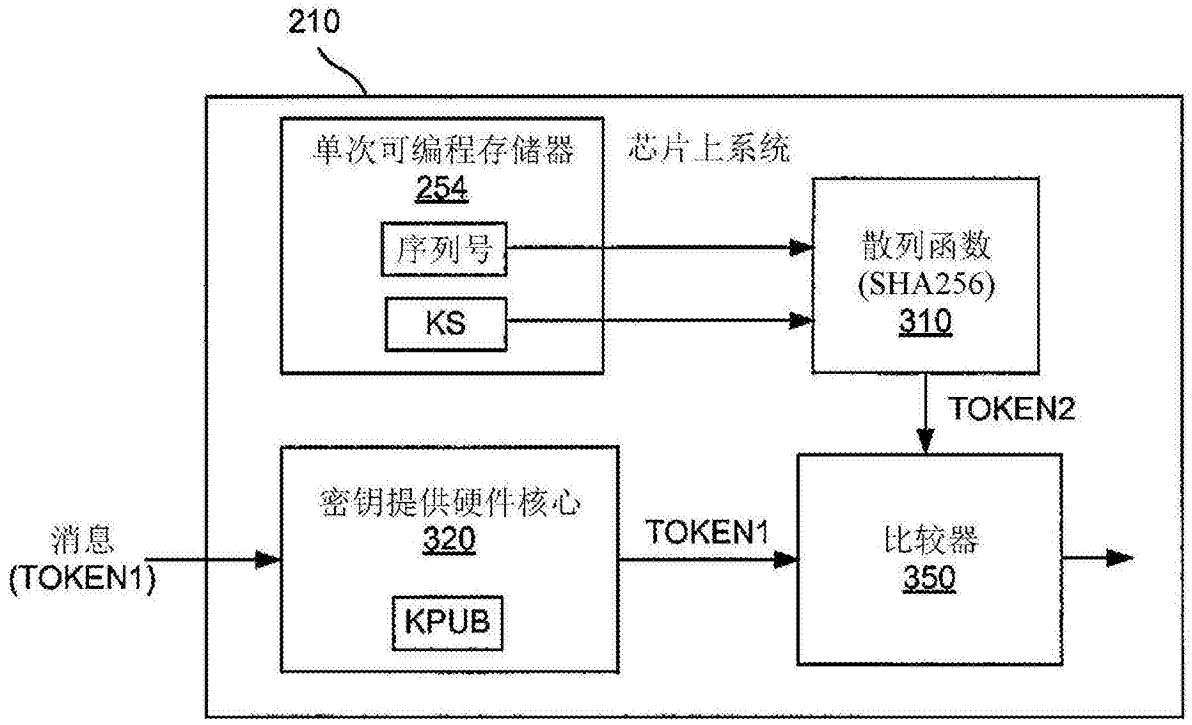

210
单次可编程存储器
254
芯片上系统
序列号
KS
散列函数
(SHA256)
310
TOKEN2
密钥提供硬件核心
320
KPUB
TOKEN1
比较器
350
消息
(TOKEN1)

图3

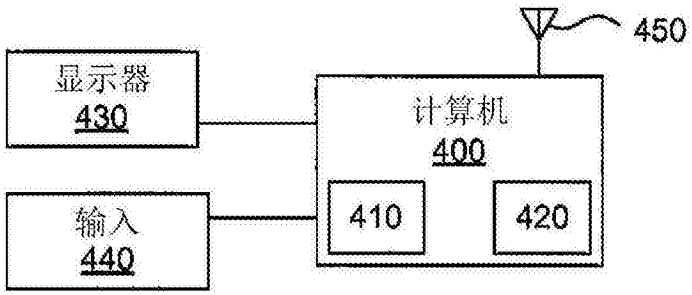

450
显示器
430
计算机
400
410
420
输入
440

图4

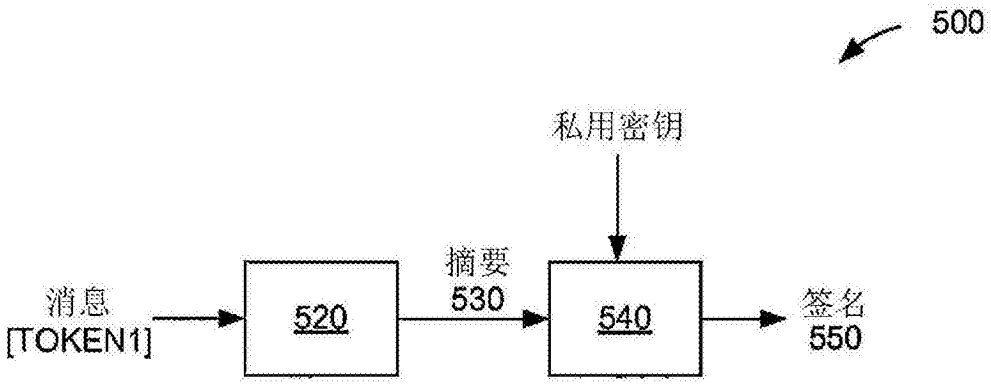

500
私用密钥
摘要
530
消息
[TOKEN1]
520
540
签名
550

图5