(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 108780484 A
(43)申请公布日 2018.11.09

(21)申请号 201780018468.5

(22)申请日 2017.03.09

(30)优先权数据
62/314,928 2016.03.29 US
15/234,879 2016.08.11 US

(85)PCT国际申请进入国家阶段日
2018.09.19

(86)PCT国际申请的申请数据
PCT/US2017/021611 2017.03.09

(87)PCT国际申请的公布数据
WO2017/172322 EN 2017.10.05

(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 I•麦克莱恩 S•莫斯科维奇
B•坎贝尔 M•德拉吉斯维奇

(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 杨林勳

(51)Int.Cl.
G06F 21/54(2006.01)
G06F 21/76(2006.01)
G06F 21/57(2006.01)

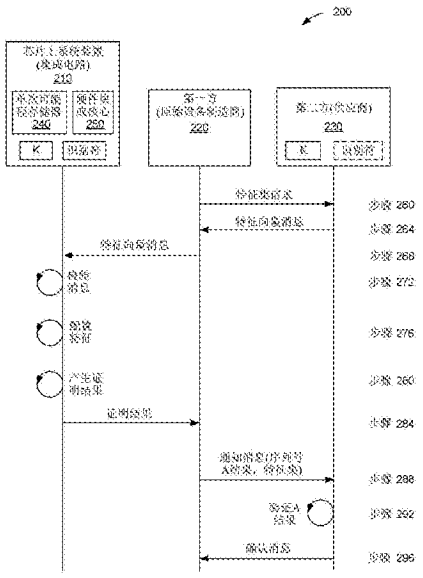
权利要求书2页 说明书8页 附图6页

(54)发明名称

用于以所请求的特征集来配置集成电路的方法和设备

(57)摘要

一种用于配置集成电路的特征的方法。在所述方法中,所述集成电路接收来自第一方的特征向量消息。所述特征向量消息包含于从所述第一方到第二方的对特征集请求的响应中。所述集成电路基于所述特征向量消息中的特征向量来配置所述集成电路的至少一个特征。所述集成电路基于所述集成电路的所述至少一个经配置特征,且使用安全地存储在所述集成电路中且所述第二方已知且所述第一方未知的密钥,来产生证明结果。所述集成电路将所述证明结果转发给所述第一方。



CN 108780484 A

1.一种用于配置集成电路的方法,其包括:

通过所述集成电路,接收来自第一方的特征向量消息,其中所述特征向量消息包含在从所述第一方到第二方的对特征集请求的响应中;

通过所述集成电路,基于所述特征向量消息中的特征向量来配置所述集成电路的至少一个特征;

通过所述集成电路,基于所述集成电路的所述至少一个经配置特征,且使用安全地存储在所述集成电路中且所述第二方已知且所述第一方未知的密钥来产生证明结果;以及

将所述证明结果转发给所述第一方。

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,其中所述第一方是原始设备制造商,且所述第二方是所述集成电路的供应商。

4.根据权利要求1所述的方法,所述特征向量消息由所述第二方签名,且所述方法进一步包括:

通过所述集成电路,使用所述特征向量消息的签名来验证所述特征向量消息。

5.根据权利要求1所述的方法,其中所述集成电路由唯一识别符识别,且所述密钥对于所述集成电路是唯一的。

6.根据权利要求1所述的方法,其中所述特征集请求的特征集对应于库存单位SKU。

7.根据权利要求1所述的方法,其进一步包括:

通过所述集成电路,将至少一个旗标设置在单次可编程OTP存储器中,其中每一设定旗标与所述集成电路的特征相关联。

8.根据权利要求7所述的方法,其中所述OTP存储器中的设定旗标对应于停用的特征。

9.根据权利要求7所述的方法,其中所述OTP存储器中的设定旗标对应于启用的特征。

10.一种集成电路,其包括:

用于接收来自第一方的特征向量消息的装置,其中所述特征向量消息包含在从所述第一方到第二方的对特征集请求的响应中;

用于基于所述特征向量消息中的特征向量来配置所述集成电路的至少一个特征的装置;

用于基于所述集成电路的所述至少一个经配置特征,且使用安全地存储在所述集成电路中且所述第二方已知且所述第一方未知的密钥来产生证明结果的装置;以及用于将所述证明结果转发给所述第一方的装置。

11.根据权利要求10所述的集成电路,其中所述集成电路是芯片上系统SOC装置。

12.根据权利要求10所述的集成电路,其中所述第一方是原始设备制造商,且所述第二方是所述集成电路的供应商。

13.根据权利要求10所述的集成电路,其中所述特征向量消息由所述第二方签名,且所述集成电路进一步包括:

用于使用所述特征向量消息的签名来验证所述特征向量消息的装置。

14.根据权利要求10所述的集成电路,其中所述集成电路由唯一识别符识别,且所述密钥对于所述集成电路是唯一的。

15.根据权利要求10所述的集成电路,其中所述特征集请求的特征集对应于库存单位

SKU。

16.根据权利要求10所述的集成电路，其进一步包括：

用于将至少一个旗标设置在单次可编程OTP存储器中的装置，其中每一设定旗标与所述集成电路的特征相关联。

17.根据权利要求16所述的集成电路，其中所述OTP存储器中的设定旗标对应于停用的特征。

18.根据权利要求16所述的集成电路，其中所述OTP存储器中的设定旗标对应于启用的特征。

19.一种站，其包括：

集成电路，其包含处理器，所述处理器经配置以：

接收来自第一方的特征向量消息，其中所述特征向量消息包含于从所述第一方到第二方的对特征集请求的响应中；

基于所述特征向量消息中的特征向量来配置所述集成电路的至少一个特征；

基于所述集成电路的所述至少一个经配置特征，且使用安全地存储在所述集成电路中且所述第二方已知且所述第一方未知的密钥来产生证明结果；以及

将所述证明结果转发给所述第一方。

20.根据权利要求19所述的站，其中所述集成电路是芯片上系统SOC装置。

21.根据权利要求19所述的站，其中所述第一方与原始设备制造商相关联，且所述第二方与所述集成电路的供应商相关联。

22.根据权利要求19所述的站，其中所述特征向量消息由所述第二方签名。

23.根据权利要求19所述的站，其中所述特征集对应于库存单位SKU。

24.根据权利要求19所述的站，其中所述密钥是由多于一个集成电路共享的全局密钥。

25.一种站，其包括：

处理器，其经配置以：

将对特征集的请求转发给另一站；

接收来自所述另一站的特征向量消息；

将所述特征向量消息转发给集成电路；

接收基于所述集成电路的至少一个经配置特征，且进一步基于安全地存储在所述集成电路中且所述另一站已知且所述站未知的密钥的证明结果；以及

将所述证明结果、所述特征集以及所述集成电路的唯一识别符转发给所述另一站。

26.根据权利要求25所述的站，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所述的站，其中所述站与原始设备制造商相关联，且所述另一站与所述集成电路的供应商相关联。

28.根据权利要求25所述的站，其中所述特征向量消息由所述另一站签名。

29.根据权利要求25所述的站，其中所述特征集对应于库存单位SKU。

30.根据权利要求25所述的站，其中所述密钥是由多于一个集成电路共享的全局密钥。

用于以所请求的特征集来配置集成电路的方法和设备

[0001] 相关申请案的交叉参考

[0002] 本申请案主张2016年3月29日在美国专利与商标局申请的第62/314,928号临时申请案以及2016年8月11日在美国专利与商标局申请的第15/234,879号非临时申请案的优先权和权益,这两个申请案的完整内容以引用的方式并入本文中。

技术领域

[0003] 本发明大体上涉及以原始设备制造商(OEM)所请求的特征集来配置集成电路。

背景技术

[0004] 现代芯片上系统(SoC)设计可含有数百或甚至数千个不同的硬件和软件特征。这些特征既定满足不同的市场、标准、产品层次和使用情况。某一特征是不需要的或甚至在一些产品中是不合意的,且客户并不想要为不使用的特征付费。因此,芯片供应商可创建许多不同版本,各自支持不同的特征子集。然而,对于芯片供应商来说,创建物理上不同的SoC版本,其中每一版本物理上添加或去除特定的硬件逻辑可能是不切实际的。

[0005] 实情为,供应商可制作物理上不同的SoC版本,其中每一版本既定以总体市场的广泛层次为目标。这些版本中的每一者可进一步定制,其中供应商在芯片制造期间启用或停用某些特征。因此,物理上相同的SoC可支持不同的特征集,且可相应地定价。

[0006] 这对于芯片供应商和原始设备制造商(OEM)两者造成若干显著问题。这些问题包含针对供应商和OEM两者的存量管理问题。在完成订单之前,供应商必须确切地决定要制造多少给定版本。OEM必须确切地决定他们打算制造多少给定模型。双方的此预测必须在任何硬销售图可用之前数月完成。如果OEM订购的零件太少,那么他们在完成后续订单时将面临可能的制造延迟。如果OEM订购太多,那么他们必须承担未用零件的成本。如果供应商制造太多的给定版本,那么这些芯片可能以无法出售的芯片“骨堆”收场。另外,这些许多版本中的每一者可为制造、测试、物理标记、储存、跟踪和发货引入专用“通道”。一个通道中的芯片不能与另一通道中的那些芯片混合。

[0007] 因此需要一种用于以对OEM和芯片供应商有利的方式来以若干特征配置集成电路的技术。

发明内容

[0008] 本发明的方面可存在于一种用于配置集成电路的方法中。在所述方法中,所述集成电路接收来自第一方的特征向量消息。所述特征向量消息包含于从第一方到第二方的对特征集请求的响应中。所述集成电路基于所述特征向量消息中的特征向量来配置所述集成电路的至少一个特征。所述集成电路基于所述集成电路的所述至少一个经配置特征,且使用安全地存储在所述集成电路中且第二方已知且第一方未知的密钥,来产生证明结果。所述集成电路可将所述证明结果转发给所述第一方。

[0009] 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,所述第一方

可为原始设备制造商(OEM),和/或所述第二方可为集成电路的供应商。所述集成电路可由唯一识别符识别,且所述密钥对于所述集成电路可为唯一的。并且,所述特征集可对应于库存单位(SKU)。

[0010] 在本发明的其它更详细方面中,特征向量消息可由第二方签名,且所述方法可进一步包括:通过集成电路,使用特征向量消息的签名来验证所述特征向量消息。另外,所述方法可进一步包括:通过所述集成电路,将至少一个旗标设置在单次可编程(OTP)存储器中,其中每一设定旗标与集成电路的一特征相关联。OTP存储器中的设定旗标可对应于停用的特征或启用的特征。

[0011] 本发明的另一方面可存在于集成电路中,其包括:用于接收来自第一方的特征向量消息的装置,其中所述特征向量消息包含于从第一方到第二方的对特征集请求的响应中;用于基于特征向量消息中的特征向量来配置集成电路的至少一个特征的装置;用于基于集成电路的至少一个经配置特征且使用安全地存储在集成电路中且第二方已知且第一方未知的密钥来产生证明结果的装置;以及用于将证明结果转发给第一方的装置。

[0012] 本发明的另一方面可存在于一种集成电路中,其包括:处理器,其经配置以:接收来自第一方的特征向量消息,其中所述特征向量消息包含于从第一方到第二方的对特征集请求的响应中;基于所述特征向量消息中的特征向量来配置集成电路的至少一个特征;基于集成电路的至少一个经配置特征,且使用安全地存储在集成电路中且第二方已知且第一方未知的密钥来产生证明结果;以及将所述证明结果转发给第一方。

[0013] 本发明的另一方面可存在于一种用于配置集成电路的方法中。在所述方法中,第一方将对特征集的请求转发给第二方。作为响应,第一方接收来自第二方的特征向量消息。第一方将特征向量消息转发到集成电路。第一方接收基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且第二方已知且第一方未知的密钥的证明结果。第一方将证明结果、特征集以及集成电路的唯一识别符转发给第二方。

[0014] 本发明的另一方面可存在于一种站中,其包括:用于将对特征集的请求转发给另一站的装置;用于接收来自所述另一站的特征向量消息的装置;用于将特征向量消息转发给集成电路的装置;用于接收基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且另一站已知且所述站未知的密钥的证明结果的装置;以及用于将证明结果、特征集以及集成电路的唯一识别符转发给另一站的装置。

[0015] 本发明的另一方面可存在于一种站中,其包括:处理器,其经配置以:将对特征集的请求转发到另一站;接收来自另一站的特征向量消息;将所述特征向量消息转发到集成电路;接收基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且另一站已知且所述站未知的密钥的证明结果;以及将证明结果、特征集以及集成电路的唯一识别符转发到另一站。

[0016] 本发明的另一方面可存在于一种计算机可读媒体中,其包括:用于致使计算机将对特征集的请求转发给另一计算机的代码;用于致使计算机接收来自另一计算机的特征向量消息的代码;用于致使计算机将所述特征向量消息转发给集成电路的代码;用于致使计算机接收基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且另一计算机已知且所述计算机未知的密钥的证明结果的代码;以及用于致使计算机将证明结果、特征集以及集成电路的唯一识别符转发到给另一站的代码。

[0017] 本发明的另一方面可存在于用于验证集成电路的特征的方法中。在所述方法中，第二方接收来自第一方的对特征集的请求。第二方将特征向量消息转发给第一方。第二方从第一方接收证明结果、特征集以及集成电路的唯一识别符。所述证明结果是基于集成电路的至少一个经配置特征，且进一步基于安全地存储在集成电路中且第二方已知且第一方未知的密钥。第二方使用所述密钥来验证证明结果。

[0018] 本发明的另一方面可存在于一种站中，其包括：用于接收来自另一站的对特征集的请求的装置；用于将特征向量消息转发给另一站的装置；用于从另一站接收证明结果、特征集以及集成电路的唯一识别符的装置，其中所述证明结果是基于集成电路的至少一个经配置特征，且进一步基于安全地存储在集成电路中，且所述站已知且另一站未知的密钥；以及用于使用所述密钥来验证证明结果的装置。

[0019] 本发明的另一方面可存在于一种站中，其包括：处理器，其经配置以：接收来自另一站的对特征集的请求；将特征向量消息转发给另一站；从另一站接收证明结果、特征集，以及集成电路的唯一识别符，其中所述证明结果是基于集成电路的至少一个经配置特征，且进一步基于安全地存储在集成电路中，且所述站已知且另一站未知的密钥；以及使用所述密钥来验证所述证明结果。

[0020] 本发明的另一方面可存在于一种计算机可读媒体中，其包括：用于致使计算机接收来自另一计算机的对特征集的请求的代码；用于致使计算机将特征向量消息转发给另一计算机的代码；用于致使计算机从另一计算机接收证明结果、特征集以及集成电路的唯一识别符的代码，其中所述证明结果是基于集成电路的至少一个经配置特征，且进一步基于安全地存储在集成电路中，且所述计算机已知且另一计算机未知的密钥；用于致使计算机使用所述密钥来检验证明结果的代码。

附图说明

[0021] 图1是无线通信系统的实例的框图。

[0022] 图2是根据本发明的用于以所请求的特征集来配置集成电路的方法的流程图。

[0023] 图3是根据本发明的用于以特征集来配置集成电路的方法的流程图。

[0024] 图4是用于为特征向量消息产生签名的方法的流程图。

[0025] 图5是用于产生证明结果的方法的流程图。

[0026] 图6是包含处理器和存储器的计算机的框图。

[0027] 图7是根据本发明的用于以特征集来配置集成电路的另一方法的流程图。

[0028] 图8是根据本发明的用于验证集成电路的特征的方法的流程图。

具体实施方式

[0029] 词语“示范性”在本文中用于表示“充当实例、例子或说明”。在本文中被描述为“示范性”的任何实施例未必被理解为比其它实施例优选或有利。

[0030] 参看图2和3，本发明的方面可存在于用于配置集成电路(IC)210的方法300中。在所述方法中，集成电路接收来自第一方220的特征向量消息(步骤310)。所述特征向量消息包含于从第一方到第二方230的对特征集请求的响应中。集成电路基于特征向量消息中的特征向量来配置集成电路的至少一个特征(步骤320)。集成电路基于集成电路的至少一个

经配置特征，且使用安全地存储在集成电路中且第二方已知且第一方未知的密钥K来产生证明结果(步骤330)。集成电路可将证明结果转发给第一方(步骤340)。

[0031] 在本发明的更详细方面中，集成电路210可为芯片上系统(SOC)装置，第一方220可为原始设备制造商，和/或第二方230可为集成电路的供应商。集成电路可由唯一识别符(ID#)识别，且密钥对于集成电路可为唯一的。并且，所述特征集可对应于库存单位(SKU)。

[0032] 在本发明的其它更详细方面中，特征向量消息可由第二方230签名，且所述方法可进一步包括：通过集成电路210，使用特征向量消息的签名来验证特征向量消息。另外，所述方法可进一步包括：通过集成电路，将至少一个旗标设置在单次可编程(OTP)存储器240中，其中每一设定旗标与集成电路的一特征相关联。OTP存储器中的设定旗标可对应于停用的特征或启用的特征。

[0033] 集成电路(IC)210可包含安全硬件块或核心(HWC)250。合适的HWC可由加利福尼亚州旧金山的密码研究公司(Cryptographic Research，Incorporated，CRI)供应。HWC保持或具有对密钥K的排它性存取。所述密钥可为对称密钥(例如AES密钥)或私钥(例如RSA或ECC私钥)。所述密钥可对于集成电路是唯一的，或其可跨集成电路共享。存储在OTP 240中的每装置密钥提供极好的安全性，但供应商/销售商230的后端检验涉及增加的操作复杂性，需要每装置密钥的大数据库的管理/查找。相反，全局共享的密钥较不安全，因为密钥的曝光破坏系统的安全性。然而，全局共享的密钥有助于简单的多的后端管理。所述密钥无法从集成电路提取，且另外其仅为供应商230已知(例如全局密钥或每装置/IC密钥K)。具体地说，所述密钥不得为OEM 220可存取的。HWC具有对OTP存储器240的排它性读取和写入存取权，所述OTP存储器持久地存储集成电路的配置状态。HWC必须具有对唯一IC识别符的存取权。所述识别符不必为机密的，但必须确保其真实性。HWC能够经由OTP存储器所保持的值来创建签名或HMAC。

[0034] 更具体参看图2中示出的方法，OEM 220向IC供应商/销售商(即，制造商)230做出正式请求，陈述他们希望制造/配置某一特征集(SKU)或特征集群组(SKU)的IC 210(步骤260)。此时，OEM不需要指示他们打算生产给定特征集的多少IC，且在实际配置IC的时间之前，他们可随意放弃配置决策。OEM从供应商订购若干IC。所有这些IC具有相同的初始“默认”配置。通常，这些IC将默认使所有特征启用，且OEM将为每一IC支付溢价。然而，取决于供应商与OEM之间的商业关系，此方法的变化是可能的。举例来说，“默认”配置可默认使大多数或所有优质特征停用，在此情况下，OEM仅最初为“基础”配置付费。

[0035] IC供应商230创建特征向量消息，其将由IC 210的HWC 250解译。所述消息含有对应于OEM所请求的特征集的特定特征向量。参看图4，所述消息可经数字签名(但并不是必须这样)。可使用例如RSA算法等带密钥函数440，经由消息产生所述签名。私钥可具有对应的公钥，且可不与用以产生证明结果的密钥K有关。在HWC处理消息签名之前，HWC可检验所述消息签名。所述消息并不需要加密，但应确保其真实性。供应商将特征向量消息转发给OEM(步骤264)。

[0036] 有时，在装置制造工艺期间，OEM 220将消息馈送到IC 210的HWC 250中(步骤268)。可将相同的全局消息馈送到根据指定特征集(SKU)配置的每一IC。用于加载所述消息的机制由OEM决定。举例来说，可将消息存储在IC上的文件中，或建构到SW图像中，或从外部测试仪馈送到IC中。

[0037] HWC 250可检验特征向量消息(其可检查签名)(步骤272)。HWC接着检查预定义的非易失性“寿命周期位”未设定。如果设定,那么HWC终止操作。如果未设定,那么HWC从消息有效负载检索特征向量,并将此特征向量写入到OTP存储器240(例如熔固适当的融合位)(步骤276)。图5中示出特征旗标(FF)或位。所述旗标可对应于某些特征,例如激活或去活调制解调器能力(例如CDMA或UMTS),设置最大调制解调器数据带宽(例如经由载波聚合),接通或断开处理器(CPU),设置最大显示器分辨率,设置最大相机分辨率,或激活或去活软件特征。HWC接着设定预定义的寿命周期位。

[0038] 寿命周期位的作用是确保任何/所有特征向量消息可仅由HWC 250消耗一次。这通过OEM 220使用具有相同IC 210的多个特征向量消息,但仅报告最低特征化结果,来防止某些攻击。HWC接着从OTP读取唯一芯片ID,并经由所述芯片ID和特征向量值来标记或HMAC(步骤280)。还见图5。HMAC可使用AES-256算法,且签名可使用RSA算法。所得的签名/带密钥的摘录(证明结果)由HWC导出。OEM读取和记录此HWC证明的结果(步骤284)。

[0039] 对于每一IC 210,OEM 220向供应商230呈现<芯片ID,证明的结果,所请求的特征集>三元组(步骤288)。芯片供应商接着对照OEM供应的针对指定芯片ID和特征集的结果来检验预期结果(步骤292)。如果值匹配,那么供应商将确认消息转发到OEM(步骤296)。

[0040] 举例来说,供应商230可向OEM 220发布针对所有未用特征的折扣。然而,如果所述值并不与预期结果匹配,那么这可指示违禁配置尝试,且供应商可采取适当的行动。

[0041] 图2中所示的技术允许OEM 220在制造期间的“准时制”IC配置。IC/SoC 210的HWC 250接收静态特征向量消息,并返回证明结果。支持此能力,而不需要部署和操作安全基础设施,且不需要到供应商的“实况”连接。仅端点(即,HWC 250和供应商230)需要为安全的。与OEM 220的通信连接并不需要为安全或实况的。另外,所述技术最小化OEM的复杂性和测试时间开销。每一IC/SoC 210是使用单个往返协议来配置的,且所述协议可由任何芯片外或芯片上实体执行。所述协议可在制造工艺期间的任何时间触发,在与OEM的现有流最佳配合的时间触发。

[0042] 本发明的另一方面可存在于集成电路210中,其包括:用于接收来自第一方220的特征向量消息的装置(例如HWC 250),其中所述特征向量消息包含于从第一方到第二方230的对特征集请求的响应中;用于基于特征向量消息中的特征向量来配置集成电路的至少一个特征的装置(例如HWC 250);用于基于集成电路的至少一个经配置特征且使用安全地存储在集成电路中且第二方已知且第一方未知的密钥来产生证明结果的装置(例如HWC 250);以及用于将证明结果转发给第一方的装置(例如HWC 250)。

[0043] 本发明的另一方面可存在于一种集成电路中,其包括:处理器(例如HWC 250),其经配置以:接收来自第一方的特征向量消息,其中所述特征向量消息包含于从第一方到第二方的对特征集请求的响应中;基于所述特征向量消息中的特征向量来配置集成电路的至少一个特征;基于集成电路的至少一个经配置特征,且使用安全地存储在集成电路中且第二方已知且第一方未知的密钥来产生证明结果;以及将所述证明结果转发给第一方。

[0044] 远程站102(图1)可包括计算机600,其包含处理器610、存储媒体620(例如存储器和/或磁盘驱动器)、显示器630,以及例如小键盘640的输入,以及无线连接650。

[0045] 参看图2和7,本发明的另一方面可存在于用于配置集成电路210的方法700中。在所述方法中,第一方220将对特征集的请求转发给第二方230(步骤710)。作为响应,第一方

接收来自第二方的特征向量消息(步骤720)。第一方将特征向量消息转发给集成电路(步骤730)。第一方接收基于集成电路的至少一个经配置特征且进一步基于安全地存储在集成电路中且第二方已知且第一方未知的密钥的证明结果(步骤740)。第一方将证明结果、特征集,以及集成电路的唯一识别符转发给第二方(步骤750)。

[0046] 本发明的另一方面可存在于第一方220的站(例如计算机600)中,其包括:用于将对特征集的请求转发给第二方230的另一站的装置(例如处理器610);用于接收来自另一站的特征向量消息的装置(例如处理器610);用于将特征向量消息转发给集成电路210的装置(例如处理器610);用于用于接收基于集成电路的至少一个经配置特征且进一步基于安全地存储在集成电路中且另一站已知且所述站未知的密钥的证明结果的装置(例如处理器610);以及用于将证明结果、特征集,以及集成电路的唯一识别符转发给另一站的装置(例如处理器610)。

[0047] 本发明的另一方面可存在于第一方220的站(例如计算机600)中,其包括:处理器(例如处理器610),其经配置以:将对特征集的请求转发给第二方230的另一站;接收来自所述另一站的特征向量消息;将所述特征向量消息转发给集成电路210;接收基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且另一站已知且所述站未知的密钥的证明结果;以及将证明结果、特征集,以及集成电路的唯一识别符转发给所述另一站。

[0048] 本发明的另一方面可存在于一种计算机可读媒体(例如存储媒体620)中,其包括:用于致使第一方220的计算机(例如600)将对特征集的请求转发给第二方230的另一计算机的代码;用于致使所述计算机接收来自另一计算机的特征向量消息的代码;用于致使所述计算机将特征向量消息转发给集成电路210的代码;用于致使计算机接收基于集成电路的至少一个经配置特征且进一步基于安全地存储在集成电路中且另一计算机已知且所述计算机未知的密钥的证明结果的代码;以及用于致使所述计算机将证明结果、特征集,以及集成电路的唯一识别符转发给另一站的代码。

[0049] 参看图2和8,本发明的另一方面可存在于用于验证集成电路210的特征的方法800中。在所述方法中,第二方接收来自第一方的对特征集的请求(步骤810)。第二方将特征向量消息转发给第一方(步骤820)。第二方接收来自第一方的证明结果、特征集,以及集成电路的唯一识别符(步骤830)。所述证明结果是基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且第二方已知且第一方未知的密钥。第二方使用所述密钥来验证所述证明结果(步骤840)。

[0050] 本发明的另一方面可存在于第二方230的站(例如另一计算机,例如计算机600)中,其包括:用于接收来自第一方220的另一站的对特征集的请求的装置(例如处理器610);用于将特征向量消息转发给所述另一站的装置(例如处理器610);用于从另一站接收证明结果、特征集,以及集成电路210的唯一识别符的装置(例如处理器610),其中所述证明结果是基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且所述站已知且另一站未知的密钥;以及用于使用所述密钥来验证所述证明结果的装置(例如处理器610)。

[0051] 本发明的另一方面可存在于第二方230的站(例如另一计算机,例如计算机600)中,其包括:处理器(例如处理器610),其经配置以:接收来自第一方220的另一站的对特征

集的请求;将特征向量消息转发给另一站;从另一站接收证明结果、特征集,以及集成电路210的唯一识别符,其中所述证明结果是基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且所述台已知且所述另一站未知的密钥;以及使用所述密钥来验证所述证明结果。

[0052] 本发明的另一方面可存在于一种计算机可读媒体(例如存储媒体620)中,其包括:用于致使第二方230的计算机(例如600)接收来自第一方220的另一计算机的对特征集的请求的代码;用于致使计算机将特征向量消息转发给另一计算机的代码;用于致使计算机从另一计算机接收证明结果、特征集,以及集成电路210的唯一识别符的代码,其中所述证明结果是基于集成电路的至少一个经配置特征,且进一步基于安全地存储在集成电路中且所述计算机已知且所述另一计算机未知的密钥;用于致使计算机使用所述密钥来验证所述证明结果的代码。

[0053] 参看图1,无线远程站(RS)102(例如移动台MS)可与无线通信系统100的一或多个基站(BS)104通信。移动台可包含SoC 210。无线通信系统100可进一步包含一或多个基站控制器(BSC)106,以及核心网络108。核心网络可经由合适的回程连接到因特网110和公共交换电话网络(PSTN)112。典型的无线移动站可包含手持式电话或膝上型计算机。无线通信系统100可使用若干多址技术中的任一者,所述多址技术例如为码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)、空分多址(SDMA)、极分多址(PDMA)或此项技术中已知的其它调制技术。

[0054] 本领域技术人员将理解,可使用多种不同技术和技法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。

[0055] 所属领域的技术人员将进一步了解,结合本文中所揭示的实施例描述的各种说明性逻辑块、模块、电路和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这种可互换性,上文已大体就各种说明性组件、块、模块、电路和步骤的功能性加以描述。此类功能性是实施为硬件还是软件取决于特定应用以及强加于整个系统的设计约束。本领域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,但这样的实施决策不应被解释为会引起脱离本发明的范围。

[0056] 可使用经设计以执行本文所描述的功能的通用处理器、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公开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、多个微处理器的组合、一或多个微处理器与DSP核心结合,或任何其它此类配置。

[0057] 结合本文中所公开的实施例描述的方法或算法的步骤可直接体现于硬件、由处理器执行的软件模块中或两者的组合中。软件模块可存在于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、可移动磁盘、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以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成一体式。处理器

和存储媒体可存在于ASIC中。ASIC可存在于用户终端中。在替代方案中，处理器和存储媒体可作为离散组件存在于用户终端中。

[0058] 在一或多个示范性实施例中，所描述的功能可实施在硬件、软件、固件或其任何组合中。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在计算机可读媒体上或经由计算机可读媒体传输。计算机可读媒体包含非暂时性计算机可读存储媒体和通信媒体两者，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。存储媒体可为可由计算机存取的任何可用媒体。作为实例而非限制，此类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，适当地将任何连接称作计算机可读媒体。举例来说，如果使用同轴缆线、光纤缆线、双绞线、数字订户线(DSL)或红外线、无线电和微波等无线技术从网站、服务器或其它远程源传输软件，那么所述同轴缆线、光纤缆线、双绞线、DSL或红外线、无线电和微波等无线技术包含在媒体的定义中。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。

[0059] 提供对所公开的实施例的先前描述是为了使所属领域的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明白对这些实施例的各种修改，且在不脱离本发明的精神或范围的情况下，本文所定义的一般原理可应用于其它实施例。因此，本发明无意限于本文中所示的实施例，而是将被赋予与本文中所公开的原理和新颖特征相一致的最宽范围。

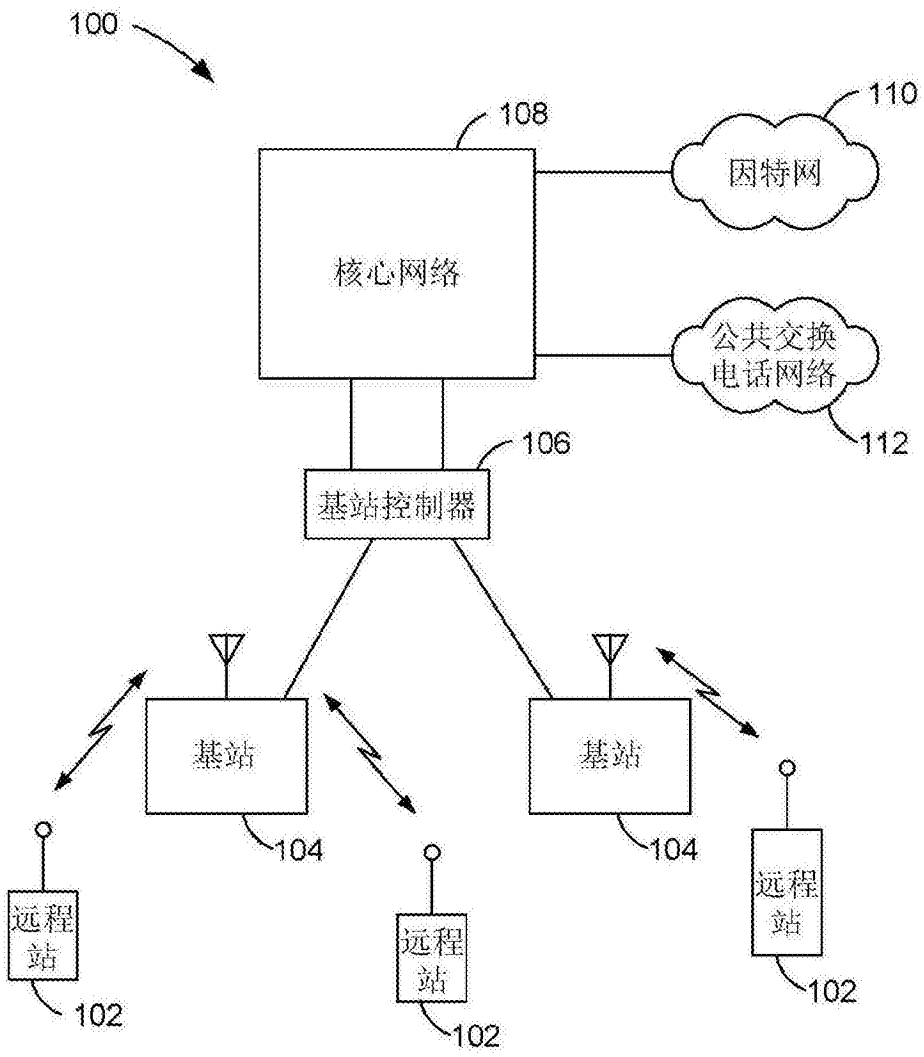

100
108
110
因特网
核心网络
公共交换
电话网络
112
106
基站控制器
基站
基站
104
104
远程
站
远程
站
远程
站
102
102
102

图1

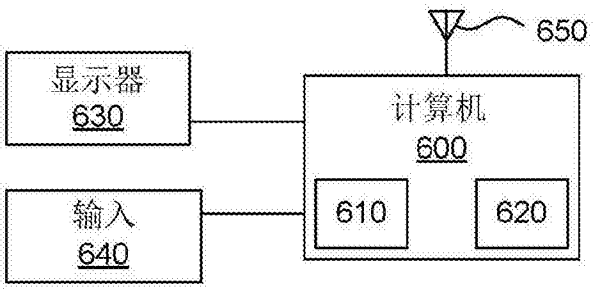

650
显示器
630
计算机
600
610
620
输入
640

图6

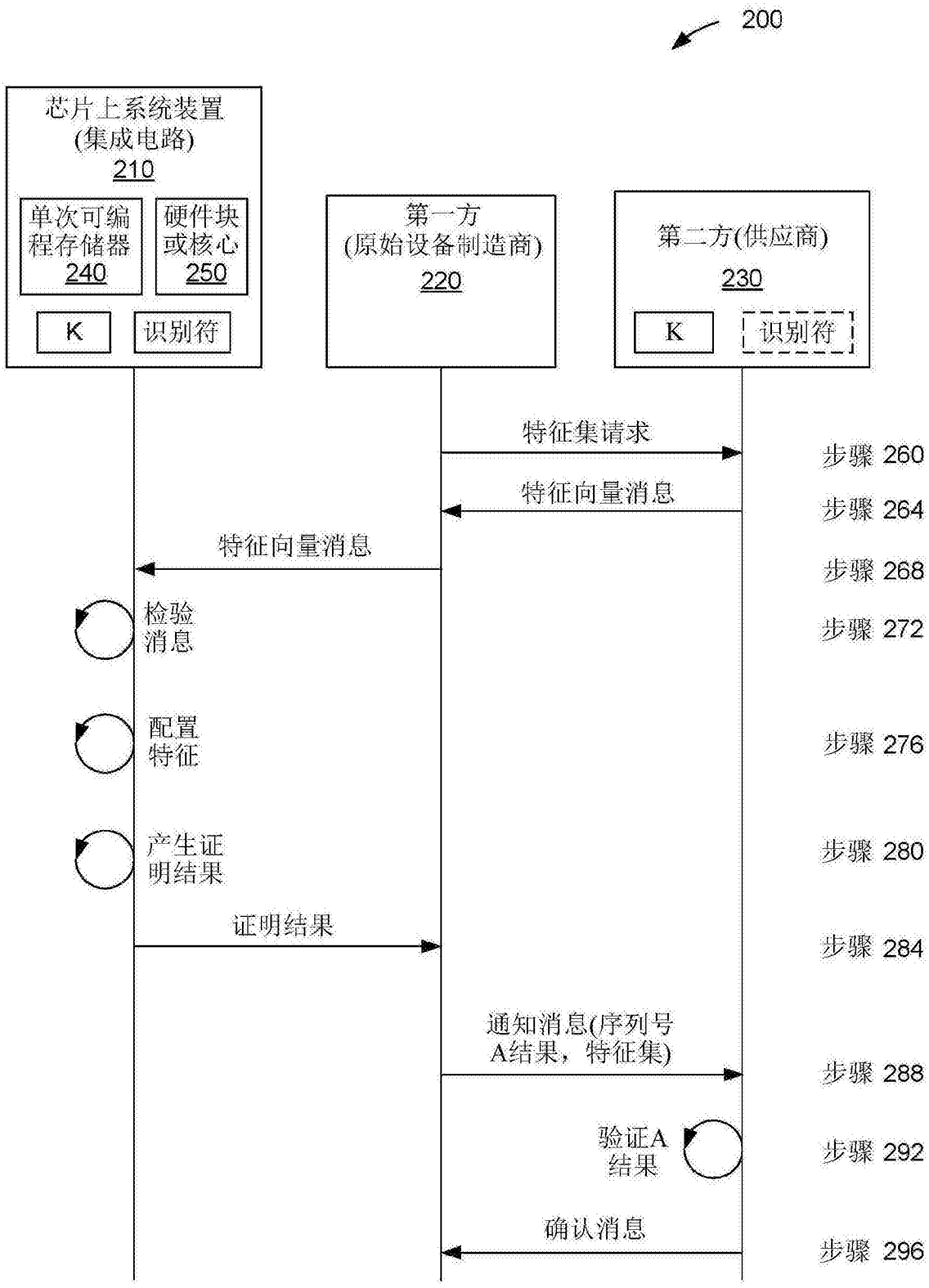

200
芯片上系统装置
(集成电路)
210
单次可编程存储器
240
硬件块或核心
250
K
识别符
第一方
(原始设备制造商)
220
第二方(供应商)
230
K
识别符
特征集请求
步骤 260
特征向量消息
步骤 264
特征向量消息
步骤 268
检验消息
步骤 272
配置特征
步骤 276
产生证明结果
步骤 280
证明结果
步骤 284
通知消息(序列号A结果，特征集)
步骤 288
验证A结果
步骤 292
确认消息
步骤 296

图2

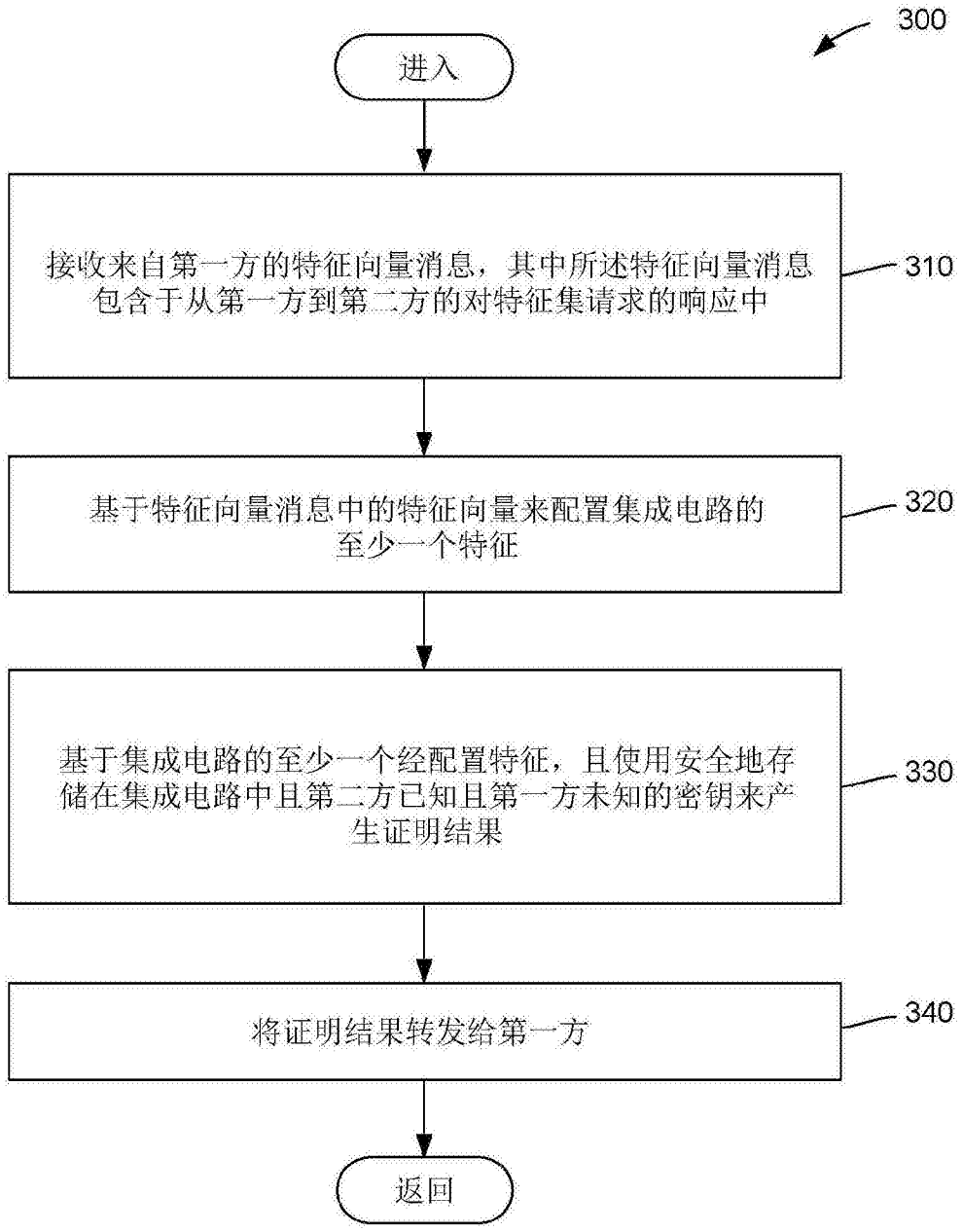

300
进入
接收来自第一方的特征向量消息，其中所述特征向量消息包含于从第一方到第二方的对特征集请求的响应中
310
基于特征向量消息中的特征向量来配置集成电路的至少一个特征
320
基于集成电路的至少一个经配置特征，且使用安全地存储在集成电路中且第二方已知且第一方未知的密钥来产生证明结果
330
将证明结果转发给第一方
340
返回

图3

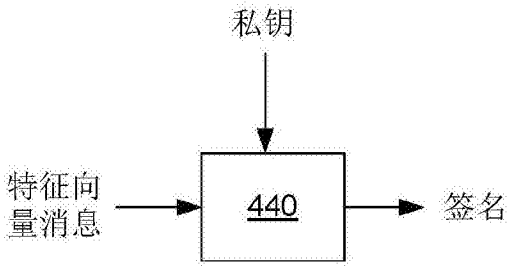

私钥
特征向量消息
440
签名

图4

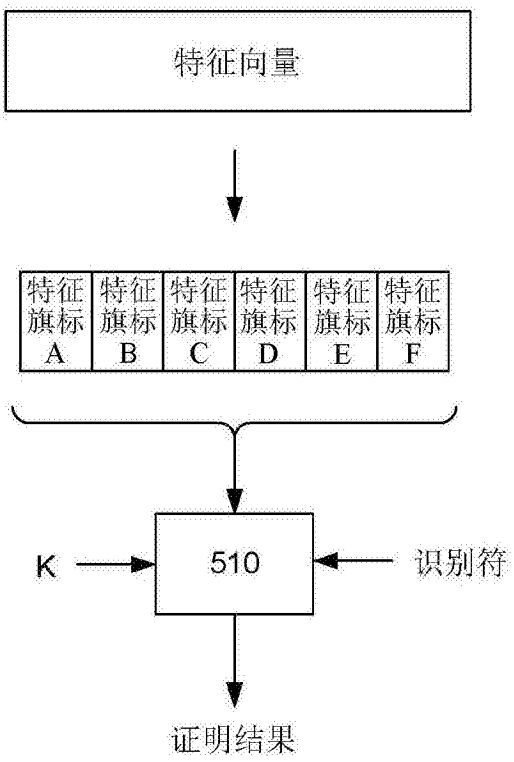


图5

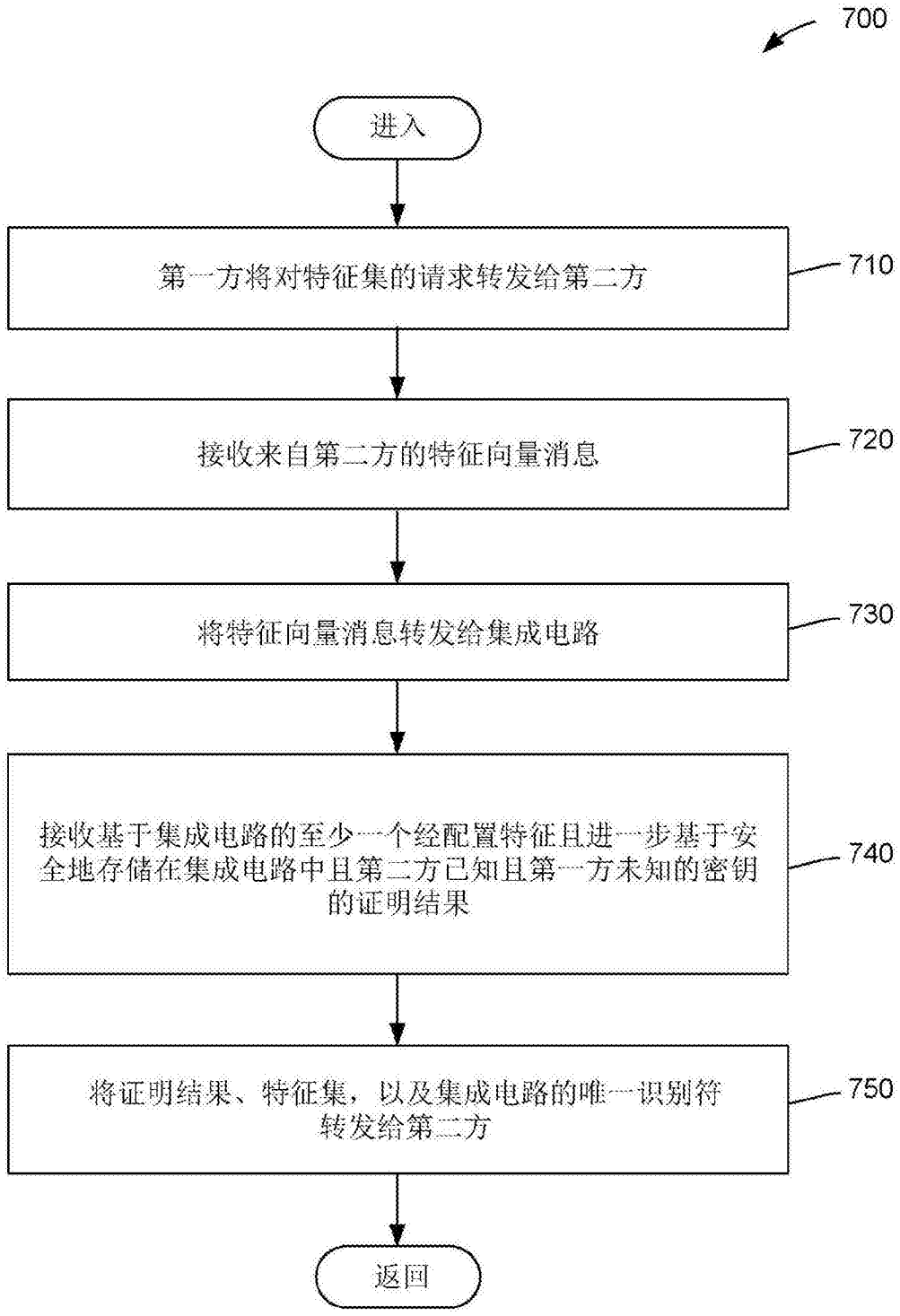

700
进入
第一方将对特征集的请求转发给第二方
710
接收来自第二方的特征向量消息
720
将特征向量消息转发给集成电路
730
接收基于集成电路的至少一个经配置特征且进一步基于安全地存储在集成电路中且第二方已知且第一方未知的密钥的证明结果
740
将证明结果、特征集，以及集成电路的唯一识别符转发给第二方
750
返回

图7

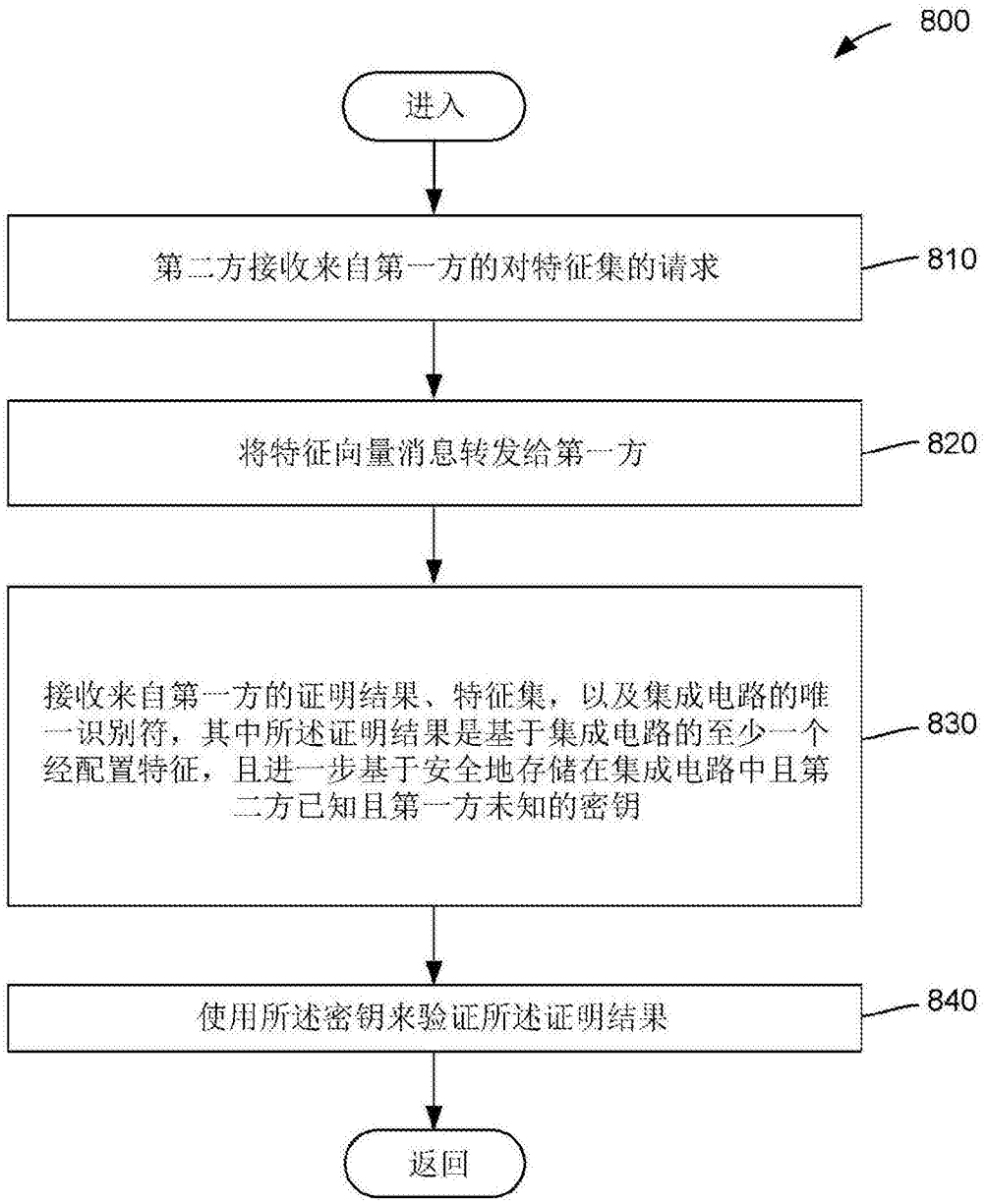

800
进入
第二方接收来自第一方的对特征集的请求
810
将特征向量消息转发给第一方
820
接收来自第一方的证明结果、特征集，以及集成电路的唯一识别符，其中所述证明结果是基于集成电路的至少一个经配置特征，且进一步基于安全地存储在集成电路中且第二方已知且第一方未知的密钥
830
使用所述密钥来验证所述证明结果
840
返回

图8