



(12) 发明专利申请

(10) 申请公布号 CN 104541474 A

(43) 申请公布日 2015. 04. 22

(21) 申请号 201380042381. 3

(51) Int. Cl.

(22) 申请日 2013. 08. 09

H04L 9/14(2006. 01)

(30) 优先权数据

61/682, 001 2012. 08. 10 US

13/831, 545 2013. 03. 14 US

(85) PCT国际申请进入国家阶段日

2015. 02. 09

(86) PCT国际申请的申请数据

PCT/US2013/054306 2013. 08. 09

(87) PCT国际申请的公布数据

W02014/026095 EN 2014. 02. 13

(71) 申请人 密码研究公司

地址 美国加利福尼亚州

(72) 发明人 P · C · 科克 B · C-M · 琼

A · J · 莱瑟森

(74) 专利代理机构 北京市金杜律师事务所

11256

代理人 李辉 吕世磊

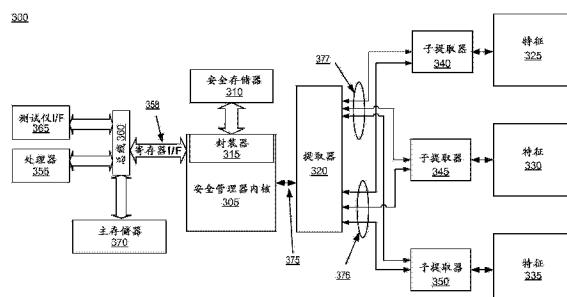
权利要求书3页 说明书34页 附图19页

(54) 发明名称

集成电路中的安全特征和密钥管理

(57) 摘要

描述了用于提供集成电路中的安全特征和密钥管理的机制。示例集成电路包括用于存储秘密密钥的安全存储器，以及被耦合至安全存储器以用于接收数字签名命令、利用秘密密钥来验证与命令相关联的签名并且利用命令来配置集成电路的操作的安全管理器内核。



1. 一种方法,包括 :

由集成电路的安全管理器接收经数字签名的命令 ;

由所述安全管理器从所述集成电路的安全存储器获取秘密密钥 ;

由所述安全管理器利用所述秘密密钥来验证与所述命令相关联的签名,以及

由所述安全管理器执行所述命令以配置所述集成电路的操作。

2. 根据权利要求 1 所述的方法,其中执行所述命令包括 :

更新所述集成电路的多个特征中的特征的状态,其中更新所述特征的所述状态引起以下项中的至少一项 :锁定所述特征、解锁所述特征或配置所述特征。

3. 根据权利要求 2 所述的方法,其中所述特征的所述状态的更新是永久性的或非永久性的。

4. 根据权利要求 1 所述的方法,其中执行所述命令包括 :

将一个或多个密钥传递至所述集成电路的一个或多个组件,其中所述密钥适合于以下项中的至少一项 :所述组件的加密操作、所述组件的数字权益管理操作、所述组件的口令管理操作或者所述组件的认证操作。

5. 根据权利要求 1 所述的方法,其中执行所述命令包括 :

标识一个或多个硬件常量并且将所述硬件常量存储在指定存储装置中,所述硬件常量包括以下项中的至少一项 :产品芯片标识符、一个或多个安全密钥、一个或多个基本密钥或者错误校正数据。

6. 根据权利要求 1 所述的方法,其中所述命令由根权限签名,并且所述秘密密钥是所述根权限的公钥。

7. 根据权利要求 1 所述的方法,其中所述命令由委托权限签名。

8. 根据权利要求 7 所述的方法,其中验证与所述命令相关联的所述签名包括 :

从由根权限签名的根签名块获取所述委托权限的委托许可和公钥 ;

利用所述委托权限的所述公钥来确定与所述命令相关联的所述签名有效 ;以及

利用所述委托许可来确定所述命令被许可。

9. 根据权利要求 1 所述的方法,其中所述命令与经加密的净荷相关联,所述方法进一步包括 :

利用所述安全管理器可访问的基本密钥导出混合密钥 ;

利用所述混合密钥导出传送密钥 ;

利用所述传送密钥将所述经加密的净荷解密 ;以及

将经解密的净荷传递至特征。

10. 一种集成电路,包括 :

安全存储器,用于存储秘密密钥 ;

安全管理器 (SM) 内核,被耦合至所述安全存储器,以用于 :

接收经数字签名的命令 ;

利用所述秘密密钥来验证与所述命令相关联的签名 ;以及

利用所述命令配置所述集成电路的操作。

11. 根据权利要求 10 所述的集成电路,进一步包括 :

可由所述 SM 内核配置的多个特征。

12. 根据权利要求 11 所述的集成电路, 进一步包括 :

被耦合至所述 SM 内核的提取器 ; 以及

被耦合至所述提取器的多个子提取器, 其中所述多个子提取器中的每一个子提取器还被耦合至所述多个特征中的一个特征。

13. 根据权利要求 11 所述的集成电路, 其中所述 SM 内核包括 :

密码机模块, 用于验证所述命令的所述签名 ;

执行引擎模块, 用于执行所述命令 ;

通信模块, 用于促进所述 SM 内核与所述集成电路的组件之间的通信 ; 以及

数据存储模块, 用于管理所述 SM 内核的内部存储并且与所述安全存储器通过接口接合。

14. 一种方法, 包括 :

由根权限系统接收标识影响集成电路的操作的命令的数据 ;

由所述根权限系统利用根权限密钥来对所述命令进行签名以创建根签名块 (RSB) ; 以及

将所述 RSB 提供至所述集成电路的安全管理器。

15. 根据权利要求 14 所述的方法, 其中所述 RSB 经由所述集成电路的测试仪接口被提供至所述安全管理器。

16. 根据权利要求 14 所述的方法, 其中所述命令指示所述安全管理器更新所述集成电路的特征, 其中所述特征的更新是永久性的或非永久性的。

17. 根据权利要求 14 所述的方法, 其中所述命令是将一个或多个密钥传递至所述集成电路的组件, 其中所述密钥适合于以下项中的至少一项 : 所述组件的加密操作、所述组件的数字权益管理操作、所述组件的口令管理操作或者所述组件的认证操作。

18. 根据权利要求 14 所述的方法, 其中所述命令是将一个或多个硬件常量存储在所述集成电路内, 所述硬件常量包括以下项中的至少一项 : 产品芯片标识符、一个或多个安全密钥、一个或多个基本密钥或者错误校正数据。

19. 一种方法, 包括 :

由根权限系统接收表明影响集成电路的操作的命令的输入参数 ;

由所述根权限系统创建包括所述命令和与委托权限系统相关联的委托许可的根签名块 (RSB), 所述 RSB 由所述根权限系统签名 ; 以及

将所述 RSB 提供至所述集成电路的安全管理器。

20. 根据权利要求 19 所述的方法, 其中所述委托许可限定所述委托权限系统对于所述安全管理器的管理能力。

21. 根据权利要求 19 所述的方法, 其中所述 RSB 进一步包括与所述委托权限系统相关联的公钥。

22. 根据权利要求 19 所述的方法, 其中所述 RSB 进一步包括与所述命令相关联的命令模版。

23. 根据权利要求 19 所述的方法, 其中所述 RSB 进一步包括用于委托权限签名的一个或多个要求。

24. 根据权利要求 19 所述的方法, 进一步包括将所述 RSB 传递至所述委托权限系统。

25. 一种方法,包括 :

由委托权限系统接收包括影响集成电路的操作的命令的输入参数;

由所述委托权限系统对所述委托输入参数进行签名以创建委托签名块 (DSB) ;以及将所述 DSB 提供至所述集成电路的安全管理器。

26. 根据权利要求 25 所述的方法,其中所述输入参数被接收作为由根权限系统提供的根签名块 (RSB) 的一部分。

27. 根据权利要求 26 所述的方法,其中所述 DSB 与所述 RSB 相关联,所述 RSB 被提供至所述安全管理器。

28. 根据权利要求 26 所述的方法,其中所述 RSB 包括以下项中的一项或多项:与所述委托权限系统相关联的委托许可、与所述委托权限系统相关联的公钥、与所述命令相关联的命令模版或者用于委托权限签名的要求。

29. 根据权利要求 28 所述的方法,其中所述委托许可限定所述委托权限系统对于所述安全管理器的管理能力。

## 集成电路中的安全特征和密钥管理

### 背景技术

[0001] 目前，片上系统的供应商可能销售很多不同品种的相同芯片，其中各品种被配置用于特定应用。芯片配置经常通过使一个或多个熔断器烧断或以其他方式对芯片上的一次性可编程存储器进行编程而发生。该类型的芯片配置通常是单向过程并且不能撤销。规避配置过程的永久性的一个方法是在一次性可编程存储器内添加能够被组合以修改先前的设定（例如，通过将多个位一起异或以产生最终的配置设定）的冗余或备用的位。然而，该类型的冗余具有受限的灵活性，并且要求在芯片上占据附加基板面（real estate）的附加熔断器。另外，在设定之后具有多个熔断器不能消除进行多个编程步骤以配置芯片的需要并且增加了成本。同样，如今配置继续由芯片供应商（或他们的承包商）进行，他们接着维持具有多个熔断器配置的芯片的库存。

[0002] 不同品种的相同芯片的储备经常是效率低的。例如，如果配置用于特定应用的所储备的芯片被过度生产，或者如果客户的芯片配置需要改变，则潜在地浪费了所储备的芯片。另外，在一些情况下，如果配置的芯片的库存不足以满足需求，则可能延误订单履行。此外，由芯片供应商配置的本模式可能限制商业关系的范围和芯片供应商与下游客户之间实际的收益流。例如，本模式可能限制在初始销售之后从芯片的重新配置生成未来收益的能力。如果下游客户希望获取超出所配置的特征集的特征，则当前的芯片典型地缺乏用于解锁该功能性的手段，并且因此没有机会使用下游特征实现作为收益流。

[0003] 此外，对于安全系统和应用的需要正在增长。目前，据称安全芯片经常在工厂车间用安全密钥编程。安全密钥可以以多种途径使用，诸如例如为了保护所存储的数据、控制对数字内容的访问或者加密 / 认证交易中使用的数据等。如今，这些密钥可以存储在一次性可编程存储器中，该存储器可以直接保持密钥，或者保持与密码功能一起使用的基本密钥，该密码功能为各种功能导出密钥。典型地，安全性通过在确保安全的设施中进行密钥加载过程来提供。

### 附图说明

- [0004] 现在将参照行出了本申请的示例实施例的附图，并且其中：
- [0005] 图 1A 是描绘了示例性生态系统的框图。
- [0006] 图 1B 是示出生态系统内的安全管理器被启用的装置的示例性生命周期的流程图。
- [0007] 图 2A 以框图形式描绘了用于配置和管理具有安全管理器被启用的芯片的一个或多个装置的示例性操作系统。
- [0008] 图 2B 是与安全管理器被启用的 IC 相关联的特征空间的示例性实施例的框图。
- [0009] 图 3 是用于进行在本文中描述的方法的包括了安全管理器被启用的 IC 的系统的示例性实施例的框图。
- [0010] 图 4 是安全管理器内核的示例性实施例的框图。
- [0011] 图 5 是用于针对由根权限系统签名的命令生成根签名块的示例性方法的流程图。

- [0012] 图 6 是用于通过安全管理器内核来处理图 5 中生成的根签名块示例性方法的流程图。
- [0013] 图 7 是用于生成能够与委托签名块相关联的根签名块的示例性方法的流程图。
- [0014] 图 8 是用于生成委托签名块的示例性方法的流程图。
- [0015] 图 9A 是用于通过安全管理器内核来处理图 8 中生成的委托签名块以及相关联的根签名块的示例性方法的流程图。
- [0016] 图 9B 是用于通过安全管理器内核来处理从根签名块检索的命令的示例性方法的流程图。
- [0017] 图 10 是用于安全管理器被启用的 IC 内的特征管理的示例性方法的流程图。
- [0018] 图 11 是用于生成用于传送净荷密钥的委托签名块的示例性方法的流程图。
- [0019] 图 12 是用于通过安全管理器内核来处理包括净荷的一个或多个签名块的示例性方法的流程图。
- [0020] 图 13A 是用于在安全管理器被启用的 IC 的设计过程期间利用配置器系统的示例性方法的流程图。
- [0021] 图 13B 是用于在芯片开发之后利用配置器系统的示例性方法的流程图。
- [0022] 图 14 是用于初始化安全管理器被启用的 IC 的示例性方法的流程图。
- [0023] 图 15 以框图形式图示了示例性个性化处理。
- [0024] 图 16 是通过委托权限系统进行的用于对针对安全管理器被启用的 IC 进行特征更新的请求进行授权的示例性方法的流程图。
- [0025] 图 17 是通过根权限系统进行的用于对针对安全管理器被启用的 IC 进行特征更新的请求进行授权的示例性方法的流程图。

## 具体实施方式

- [0026] 现在将详细地参照附图中图示的本示例性实施例。
- [0027] 1. 概念
- [0028] 1.1 生态系统概要
- [0029] 现在将参照以框图形式示出了示例性生态系统 100 的图 1A。如图 1A 所示, 系统 100 可以包括集成电路 (“IC”) 提供商 105、第三方 IP 提供商 107、IC 制造商 110、IP 和 / 或安全密钥提供商 115、安全服务 120、计费和报告服务 122、产品供应商 125、装置管理员 127 以及最终用户 130。为简单起见, 在该示例性生态系统中, 每个实体仅示出了一个。在实践中, 与在本文中描述的原理一致的生态系统可以具有一个或多个的各实体 (即, 供应同样的 IC 的多个 IC 制造商、提供利用相同 IC 设计的产品的多个产品供应商、以及多个客户)。图 1A 中示出的一些步骤还可以牵涉到数个公司 (例如, IC 制作可以牵涉到不同公司和 / 或阶段来制造晶片、进行初始测试、切割晶片、封装芯片等等)。另外, 在一些场合中, 一些实体以及他们的功能可以被包含在单个实体内。例如, 一些公司不仅设计而且制造 IC, 在该情况下, IC 制造商 110 和 IC 提供商 105 可以是相同的实体。
- [0030] IC 提供商 105 是将芯片设计提供给用于芯片生产的 IC 制造商 110 的实体。具体地, IC 提供商 105 提供用于可配置的 IC 的芯片设计, 使得芯片的一些方面可以在制造之后被配置 (例如, 用于特定应用或者启用 / 禁用特定特征)。例如, IC 提供商 105 可以在设计

中包括安全管理器（“SM”）内核，或者能够指定制造出的 IC 包括 SM 内核。包括了 SM 内核的 IC 称作 SM 被启用的 IC。除其他事项外，SM 内核允许 IC 的一个或多个可配置的特征（“特征”）取决于期望的配置和安全需要而被锁定或解除锁定（或者以其他方式配置，例如，诸如调谐 PLL 以调节 CPU 的特性或者传递供特征使用的秘密密钥等）。SM 被启用的 IC 例如包括一个（或者许多个）SM 内核以及一个（或多个）安全的永久性存储器。并且如下面所详细讨论的，SM 被启用的 IC 可选地可以包括一些其他元素（例如，一个或多个提取器、一个或多个特征，等等），或者它们的一些组合。IC 提供商 105 可以包括根公钥作为提供给 IC 制造商 110 的掩码的一部分。IC 提供商 105 可以从可用作根权限（root authority）的安全服务 120 获取根公钥。

[0031] 根权限是与管理 SM 编程能力的根权限系统相关联的实体，并且能够将能力的子集分配至与一个或多个委托权限（delegate-authority）相关联的一个或多个委托权限系统。如下面所更加详细讨论的，根权限系统可以控制 SM 被启用的 IC 的配置。SM 被启用的 IC 的配置可以包括例如进行 SM 被启用的 IC 的特征管理、进行 SM 被启用的 IC 的密钥管理或者它们的组合。根权限系统可以控制由系统 100 中的其他实体拥有的 SM 被启用的 IC 的特征管理。例如，根权限系统可以直接创建能够以密码的方式验证的（例如，数字签名的）命令来锁定、解除锁定或者配置与 SM 被启用的 IC 相关联的特征。另外，根权限系统可以创建受限的授权，该受限的授权允许由 IC 制造商 110、产品供应商 125、装置管理员 127、最终用户 130、其他实体或者它们的一些组合创建对于 SM 被启用的 IC 的配置改变。

[0032] 根权限系统还可以控制针对 SM 被启用的 IC 的密钥管理。例如，根权限系统可以授权 SM 内核将净荷（例如，秘密密钥，或者其他值）安全地传递至 SM 被启用的 IC 的其他部分（包括在 SM 被启用的 IC 上执行的软件）。根权限系统可以授权一个或多个委托权限系统来安全地传递净荷。

[0033] 如上面所提到的，根权限是与根权限系统相关联的实体。于是，虽然在本文中描述的实施例可能是指作为根权限的安全服务 120，但可以设想其他实体可以用作根权限。例如，IC 提供商 105、产品供应商 125 或者一些其他实体。

[0034] 先前的段落描述了授予另一实体许可的根权限。这些许可的接收方被称作委托权限。在一些场合中，委托权限与已经被赋予根权限系统的 SM 编程能力的子集的委托权限系统相关联。SM 编程能力的子集可以在委托权限系统之间不同。委托权限可以是产品供应商 125、IC 制造商 110、装置管理员 127、一些其他实体或者它们的一些组合。

[0035] 如下面所详细讨论的，根权限系统、一个或多个委托权限系统或者它们的一些组合可以具有对于控制系统 100 中的 SM 被启用的 IC 的修改（例如，特征和密钥管理操作）的一些（或完全）控制。

[0036] IC 制造商 110 是制造 IC 的实体。如上面所讨论的，一些 IC 是可配置的，使得芯片可以在制造之后被配置用于特定应用。片上系统（“SOC”）、专用集成电路（ASIC）、FPGA、移动无线电芯片以及处理器（例如 CPU）是适用于与在本文中描述的实施例一起使用的 IC 的示例。通常，特征管理最特别地适合于集成了能够独立使用的多个功能的芯片、或者具有可配置的功能或具有应该在芯片生命周期中的不同阶段（例如，诸如调试 / 测试模式等）被启用 / 禁用的能力的芯片。并且对于密钥管理应用，利用了密码密钥或类似秘密的任何芯片都可以是良好的候选。IC 制造商 110 可以制造包括了 SM 内核的 IC。IC 制造商 110 可

以将一个或多个安全密钥、装置 ID、初始特征配置设定或者它们的一些组合嵌入到 SM 内核中，作为其制造过程、测试过程或两者的一部分。为了做到这一点，IC 制造商 110 配备成提供在下面详细讨论的定制的第一阶段。具体地，IC 制造商 110 可以是使得能够对 SM 被启用的 IC 做出特定配置改变的委托权限。例如，在包含多个处理器的 IC 中，IC 制造商 110 可以被允许设定能够用在 SM 被启用的 IC 中的处理器的数量，而不是用于各处理器的时钟速率。在未示出的一些实施例中，IC 制造商 110 和 IC 提供商 105 是相同的实体。

[0037] 另外，IC 制造商 110 可以在制造出的 IC 上进行测试以确保他们在设计规范内操作。在一些情况下，诸如晶片分类等的测试过程可以在与 IC 制作不同的设施处和 / 或通过不同公司来进行，在该情况下，标签“IC 制造商 110”代表这些角色 / 步骤的组合。IC 制造商 110 将 SM 被启用的 IC 提供给产品供应商 125。

[0038] 产品供应商 125 将 SM 被启用的 IC 并入到被接着做成对于最终用户 130 可用的一个或多个产品（例如，SM 被启用的装置）内。在一些实施例中，产品供应商 125 是装置或服务零售商并且使 SM 被启用的装置对于最终用户 130 直接可用。在其他实施例中，产品供应商 125 将 SM 被启用的装置分发至用于分发给最终用户 130 的一个或多个第三方装置或服务零售商（未示出）。

[0039] 产品供应商 125 可以添加 SM 被启用的 IC 的附加定制。为了做到这一点，产品供应商 125 可以是使得能够对 SM 被启用的 IC 做出某些特定配置改变的委托权限。例如，作为委托权限，产品供应商 125 的委托权限系统可以通过根权限系统被允许某些能力。

[0040] 甚至在产品被销售给最终用户 130 之后，也能够进一步配置或启用 SM 被启用的 IC 中的特征。例如，最终用户 130 和 / 或产品可以与产品供应商 125、装置管理员 127、安全服务 120、委托权限、根权限或者它们的一些组合协作以启用 SM 被启用的 IC 中的特征。例如，该处理可以牵涉到在网络之上传输请求（例如，通过利用产品中的无线电来经由蜂窝数据网络传输请求报文）和接收（例如，通过利用产品中的无线电来接收来自蜂窝数据网络的报文）授权被请求的配置改变的芯片特定的报文。

[0041] 在一些场合中，产品供应商 125 也可以用作用于安装在 SM 被启用的装置上的一个或多个应用的应用作者。另外，产品供应商 125 可以用作管理与应用相关联的功能性的应用操作者。类似地，产品供应商 125 也可以用作分发与 SM 被启用的装置兼容的操作系统的操作系统供应商。产品供应商 125 也可以用作服务操作者（诸如移动网络操作者），例如管理可以对于 SM 被启用的装置可用的一个或多个服务或能力。

[0042] 在其他实施例中，其他实体、一个或多个第三方（未示出）或者它们的一些组合可以是应用作者、操作系统供应商、应用操作者或者它们的一些组合。

[0043] IP 和 / 或安全密钥提供商 115 管理用于与 SM 被启用的 IC 一起使用的安全密钥。包括了公钥和秘密密钥的安全密钥值可以被提供至 IC 制造商 110、安全服务 120、产品供应商 125、装置管理员 127 或者它们的一些组合。在未示出的一些实施例中，IP 和 / 或安全密钥提供商 115 也可以将安全密钥提供至第三方 IP 提供商 107、IC 提供至 105 或者它们的一些组合。

[0044] 安全服务 120 可以用作用于可被生态系统中的实体使用的安全密钥的中央分发器。例如，安全服务 120 可以从 IP 和 / 或安全密钥提供商 115（或者从多个安全密钥提供商）获取安全密钥并且将他们分发至系统 100 中的其他实体。例如，SM 被启用的移动电话

应用处理器可以使用来自多个 IP 和 / 或安全密钥提供商 115 的密钥编程，包括独立地操作和 / 或未束缚于特定 IC 提供商 105 的很多。这样的 IP 和 / 或安全密钥提供商 115 的示例包括但不限于电子支付系统、DRM/ 反盗版系统、身份系统，等等。在一些实施例中，安全服务 120 可以包括根权限系统并且用作用于 SM 被启用的 IC 的根权限。在其他实施例中，聚集和根权限角色可以是分开的。作为根权限，安全服务 120 可以授权待作为委托权限的系统 100 中的一个或多个其他实体以例如锁定或解除锁定与 SM 被启用的 IC 相关联的某些特征、将密钥安全地传递至 SM 被启用的 IC（或者至在 SM 被启用的 IC 上执行的软件）的一部分，等等。如下面所详细讨论的，依照由根权限以密码图形方式授予的特权，委托权限被授权对 SM 被启用的 IC 做出某些配置改变。

[0045] 计费和报告服务 122 可以耦合至系统 100 内的其他实体中的一些实体或所有实体。在一些情况下，系统 100 中的一个或多个实体可能希望对于 SM 被启用的 IC 的某些配置设定（例如，以启用增值特征）的收取费用。计费和报告服务 122 通过生态系统中的各种实体来追踪与各种交易类型相关联的费用。例如，实体可以被要求支付以启用或禁用与 SM 被启用的 IC 相关联的特征或将密钥传递至 SM 被启用的 IC。计费和报告系统 122 例如通过从委托权限系统接收电子交易或审核记录来收集关于由委托进行的交易的数量的信息。基于收集到的记录，计费和报告服务 122 可以将横跨多个芯片类型和交易类型（例如，所启用的特征的种类）的计费金额聚集起来，并且最终计算出由启用特征或进行其他交易的实体所欠的金额。同样，如下所述，计费和报告服务 122 能够帮助计算出欠诸如第三方 IP 提供商 107 等的第三方的金额。去往由计费和报告服务 122 进行的计费计算的输入可以包括但不限于进行的交易的数量、启用了什么特征、启用了该特征的时间的长度等等。在一些实施例中，根权限或委托权限可以在 SM 被启用的 IC 上强加在启用或配置特征之前接收支付的政策，但是在其他情况下，可以在启用之后进行计费和支付。在两种情况下，安全服务 120 都能够经由其与根权限系统以及一个或多个委托权限系统的通信而动态地调节所进行的交易的数量上的限制。在一些实施例中，计费和报告服务 122 是安全服务 120 的一部分。在其他实施例中，计费和报告服务 122 可以仅进行交易追踪，并且计费和财务处理可以分开地（或甚至手动地）进行。

[0046] 系统 100 可以包括第三方 IP 提供商 107（或，如先前所提到的，数个第三方 IP 提供商 107）。第三方 IP 提供商 107 可以将一个或多个特征或者特征的一部分提供至 IC 提供商 105，用于集成到 SM 被启用的 IC 内。或者在一些场合中，第三方 IP 提供商 107 可以简单地给 IC 提供商 105 发放许可证以使用一个或多个现有的特征或特征的一部分。集成的特征可以通过根权限或在其被委托能力内操作的委托权限被启用。在一些实施例中，特征未被启用（例如，被解除锁定）直到第三方 IP 提供商 107 被补偿用于 IP 区块的使用为止。例如，如在计费和报告服务 122 的上下文中所讨论的，委托权限系统可以未提供有授权特征激活的能力或授权，直到由计费和报告服务 122 和 / 或由第三方 IP 提供商 107 接收到支付为止。

[0047] 最终用户 130 是使用产品（例如，包含了 SM 被启用的 IC 的装置）的实体。最终用户 130 可以例如从 IC 制造商 110、产品供应商 125、装置管理员 127 或者一些第三方装置或服务零售商购买 SM 被启用的装置。

[0048] 在一些实施例中，系统 100 包括装置管理员 127。装置管理员 127 可以是使其能

够对 SM 被启用的 IC 做出特定配置改变的委托权限。最终用户 130 可以接着与装置管理员 127 (或安全服务 120, 等等) 协作以启用 SM 被启用的 IC 中的特征。该处理可以包括用户和 / 或装置在网络之上传输请求、接收授权响应并且将响应报文的至少一部分 (该部分可以例如包括来自授权委托权限的安全服务 120 中的根权限系统的数字签名以及来自用作委托权限的装置管理员 127 的数字签名两者) 提供至 SM 被启用的 IC 以实际上启用所请求的特征。请求可以包括支付、已经做出支付的确认或者对未来支付的承诺。另外, 在一些实施例中, 装置管理员 127 可以是具有控制系统 100 中的 SM 被启用的 IC 的修改 (例如, 特征和密钥管理操作) 的一些直接或间接控制的装置或服务零售商。

[0049] 另外, 在未示出的一些实施例中, 系统 100 可以包括装置特征管理员或装置密钥管理员。装置特征管理员可以是具有授权牵涉到 SM 被启用的 IC 的配置改变 (例如, 经由密钥管理操作、特征管理操作或者它们的一些组合) 的某些有限能力的委托权限。

[0050] 另外, 在一些实施例中, 根权限可以安全地允许系统 100 中的其他实体启用或部分地启用用于测试的 SM 被启用的 IC 或 SM 被启用的装置的一个或多个特征。例如, 根权限经由根权限系统可以在设定时间段或若干电力不间断电源内启用 (或部分地启用) SM 被启用的 IC 内的特征 (例如, 使得特征仅被启用直到下一次 SM 被启用的 IC 被上电或复位为止)。类似地, 在一些实施例中, 经由委托权限系统的当被根权限许可时的委托也可以被允许启用或部分地启用用于测试的 SM 被启用的 IC 或装置的特征。

[0051] 上面实体中的一个或多个可以经由通过一个或多个通信网络操作者操作的一个或多个网络彼此耦合。这些网络中的一些可以由一个或多个网络管理员维持。

[0052] 现在参照示出了用于生态系统 (例如, 系统 100) 内的 SM 被启用的装置的示例性生命周期 140 的图 1B。虽然生命周期以特定顺序公开了下面的步骤, 但应该理解的是步骤中的至少一些可以被移动、修改或者在适当情况下被删除。

[0053] 在步骤 142 中, 设计 SM 被启用的 IC。如下面所详细讨论的, 设计过程可以利用例如配置器、从 SM 供应商接收到的网表以及用于生成硬件配置密钥和常量的部件。例如, 该生成过程可以牵涉到根权限系统, 例如在一些实施例中, 根权限系统可以生成用于公钥密码系统的密钥对, 其中公钥被输出作为硬件配置密钥, 并且私钥被保留在根权限系统中 (例如, 用于授权委托)。SM 被启用的 IC 设计可以包括可被硬接线至制造出的 SM 被启用的 IC 中的一个或多个安全密钥。SM 被启用的 IC 设计可以被配置成允许用于可被编程到制造出的 SM 被启用的 IC 内的一个或多个安全密钥的存储 (例如, 在步骤 150 中、步骤 155 中或者在两者中)。

[0054] 在步骤 145 中, 基于 SM 被启用的 IC 设计来制造和测试 SM 被启用的 IC。各 SM 被启用的 IC 可以具有一个或多个 SM 内核, 其中各 SM 内核可以控制一个或多个特征。如下面所详细讨论的, 特征可以根据被一个或多个安全密钥授权、经由一个或多个 SM 命令或者它们的一些组合而被更改、启用、禁用或者它们的一些组合。另外, 在一些实施例中, 来自第三方提供商 (例如, 第三方提供商 107) 的特征或特征的一部分可以被并入到 SM 被启用的 IC 内。例如, 第三方提供商可以提供用于以高速度呈现大图像文件的特征, 但是初始时未被启用。测试可以被进行用以确认 SM 被启用的 IC 的特征是否被正确地操作。例如, 当被根权限许可时的委托权限 (或者根权限自身) 可以临时地 (例如, 在固定时间内和 / 或直到芯片被复位为止) 启用一个或多个特征以便于测试。取决于实施例, 步骤 145 可以由 IC 制造

商 110、IC 提供商 105、一些其他实体（例如，专门的测试设施）或者它们的一些组合来进行。

[0055] 在步骤 150 中，定制的第一阶段发生。在该步骤中，SM 被启用的 IC 可以被分配装置标识符（“ID”）并且被配置有来自根权限系统、委托权限系统、一个或多个密钥拆分（keysplit）或基本密钥的一个或多个密钥。

[0056] 密钥拆分是密钥的当与不同密钥拆分组合时形成完整密钥（例如，基本密钥）的部分。密钥拆分可以用于例如通过使 SM 被启用的 IC 中的 SM 内核通过不同方被编程有不同密钥拆分而增加基本密钥的安全，所述不同方中没有一个具有所有不同密钥拆分的知识。在 SM 内核内发生密钥拆分的经由组合功能的组合以提供基本密钥。因为编程方中没有一个知道所有密钥拆分，所以单个设施的损害并不一定损害基本密钥。

[0057] 下面更加详细地讨论示例性配置过程。其他参数也可以在定制的第一阶段期间设定。例如，如果 SM 被启用的 IC 包含多个处理器，则定制的第一阶段可以设定可以在初始时由产品供应商 125 使用的处理器的数量。或者，例如，定制的第一阶段可以设定用于各处理器的最大时钟速率以抑制欠载的过热或者以匹配在测试 145 期间确定的最大速率。例如，安全地存储这样的限制能够防止不诚实的分发商欺骗性地将较低速度的部件备注为较高速度等级。在未示出的可选实施例中，没有步骤 150，并且而是将定制的第一阶段作为步骤 155 的一部分来进行。

[0058] 在步骤 155 中，定制的第二阶段发生。例如，相同系列的 SM 被启用的 IC 可以被进一步配置成满足用于不同产品供应商的要求。在很多场合中，一些产品供应商可能想要专门配置的 SM 被启用的 IC。在定制的该阶段期间，SM 内核的特征状态可以被更新以定制 SM 被启用的 IC 来满足各产品供应商的需要。更新特征状态可以包括禁用、启用或更改与 SM 被启用的 IC 相关联的一个或多个特征、以及加载附加的密钥或者它们的一些组合。定制的该第二阶段可以例如由 IC 制造商 110、IC 提供商 105、产品供应商 125、一些其他实体或者它们的一些组合来进行。尽管成本因素典型地希望维持定制步骤的数量尽可能地小，但是些应用也可以采用多于或少于两阶段的定制。注意，定制的两个阶段（150 和 160）可以例如分别在 IC 的晶片级别测试和封装级别测试处进行。

[0059] 在步骤 160 中，SM 被启用的 IC 被并入到装置内以在产品制造过程期间创建 SM 被启用的装置。SM 被启用的 IC 的特征状态在该点上也可以更新。例如，产品供应商可以启用特征的组合以创建 SM 被启用的装置的不同产品线。该编程过程能够利用从安全服务 120 发布的硬件安全模块而被保证安全（例如，以确保精确的记录被最终提供至计费和报告服务 122）。以该方式，产品供应商 125 可以仅需要在其库存中取得并保持来自 IC 提供商 105 的单个类型的芯片，接着该芯片可以被用在具有在产品组装期间设定的不同配置的多个产品中。计费和报告服务 122 用于确保正在启用的能力被支付（例如，使得 IC 提供商 105 能够收集取决于芯片配置的用于各芯片的适当金额）。密钥也可以作为步骤 160 的一部分被编程到 SM 内核内。例如，产品供应商可以在各 SM 被启用的 IC 中编程唯一的密钥（诸如产品供应商 125 知道但 IC 提供商 105 不知道的密钥）。

[0060] 在步骤 165 中，分发 SM 被启用的装置。SM 被启用的装置可以例如被分发至另一产品供应商、中间商、最终用户 130、装置管理员 127 或者生态系统中的其他实体。

[0061] 在步骤 170 中，能够完成 SM 被启用的装置的内场管理。（已经离开产品供应商的

SM 被启用的装置被说成在内场。注意，这不一定与在最终用户的手中同义，例如，移动电话运营商操作者可以在将其传递至最终用户 130 之前进行电话的定制或规定）。内场管理可以包括被接收以更新 SM 被启用的装置的特征状态的请求。例如，请求可以被接收以启用 SM 被启用的 IC 的特殊的音频组件。这样的请求可以例如由最终用户 130 或装置自身向根权限或适当地被授权的委托权限发送请求来引发。内场管理接着牵涉到一个或多个授权和 / 或安全密钥的至 SM 被启用的装置的传输。如下面所详细讨论的，安全密钥传递和特征管理可以经由与 SM 被启用的装置通信的根权限系统由根权限进行，或者经由在其委托的 SM 编程能力内起作用并且与 SM 被启用的装置通信的委托权限系统由委托权限进行。一旦收到响应，SM 被启用的装置中的软件就将响应的一部分（包括来自根权限和 / 或委托权限的密码授权）提供至 SM 内核，该 SM 内核验证授权是否在进行被请求的操作（例如，特征配置，键入密钥，等等）之前对于特定装置有效。

[0062] 或者单独地或者与其他实体结合地起作用的先前所述实体中的所有都可以请求、生产、缓存、传输或者修改前述更新、管理以及审核报文以控制 SM 被启用的装置的密钥和特征。在装置生命周期的各种点处具有角色的这些实体中的每一个都可以独立地操作，并且可以具有 SM 被启用的装置或者与装置交互操作的基础结构的不同程度的所有权。某些密钥或特征的部署可以牵涉到支付、审核或者其中 SM 内核活动的便利、进行某些动作的请求、制定或演绎 SM 内核报文、通信或存储所述报文、授权动作的过程可以通过前述实体中的一个或多个来进行所在的其他商业布置。

## [0063] 2. 安全管理器系统架构

[0064] 现在参照以框图形式示出了用于配置和管理一个或多个 SM 被启用的装置的示例性操作系统 200 的图 2A。系统 200 可以包括由网络 205 可操作性地连接的公共陆地移动网络 (PLMN) 210、根权限 215、根权限系统 217、委托权限 220、委托权限系统 222、IC 提供商 105、SM 被启用的装置 240、245、250、255 和 260、SM 被启用的 IC 265、无线访问点 275、配置器系统 280 以及附加的实体 287 中的一些或所有。

[0065] 网络 205 可以例如是互联网、内联网、局域网、广域网、校园区域网、城域网、外联网、私有外联网、两个或多个耦合的电子装置中的任何集合或者这些或其他适当的网络中的任何的组合。网络 205 还可以与也称作无线广域网 (WWAN) 或者在一些情况下称作蜂窝网络的 PLMN 210 通信。为简单起见，网络 205 示出为单个实体，但能够可以存在多个网络。例如，私有外联网可以将 IC 提供商 105 与根权限 215 连接，即使图 2A 中的其他实体由互联网连接。

[0066] 根权限 215 是管理 SM 编程能力并且能够将能力的子集分配至一个或多个委托权限 220 的实体（例如，安全服务 120）。根权限 215 与包含（或以其他方式有权访问）管理 SM 被启用的 IC 265 和 SM 被启用的装置 240、245、250、255 和 260 的密码密钥的根权限系统 217 相关联。根权限系统 217 被配置成生成一个或多个根签名块（“RSB”）。如下面所详细讨论的，RSB 可以包括一个或多个 SM 命令、命令模板、一个或多个委托许可、一个或多个密钥（例如，委托公钥）或者它们的一些组合。RSB 包含由根权限系统 217 利用对应于 SM 内核中的公钥的根私钥（例如，RSA 私钥）签名的至少一个数字证书。根权限系统 217 可以被配置成将一个或多个 RSB 或其他数据提供至配置器系统 280、SM 被启用的 IC 265、委托权限系统 222、SM 被启用的装置（例如，240、245、250、255 或 260）、一个或多个其他实体

287、电子存储介质（未示出）或者它们的一些组合。另外，根权限系统 217 可以被配置成当由根权限系统 217 的用户指示时提供 RSB。根权限系统 217 可以在单个计算机上实现，或者在一些场合中可以横跨可在地理上分散多个计算机（例如，其包含用于门限签名系统的密钥共享，其中，需要来自多个密钥共享的协作来计算数字签名）分布。

[0067] 如下面所详细讨论的，根权限系统 217 可以被配置成把特权委托给一个或多个委托权限系统 222。根权限系统 217 还可以配置成生成用于一个或多个配置器系统 280 的系统和网表密钥常量。另外，根权限系统 217 可以被配置成管理在定制处理（下面讨论）期间使用的万能密钥。根权限系统 217 也可以被配置成创建测试矢量以及辅助 SM 内核集成和 ASIC 制造的其他值。

[0068] 在一些实施例中，根权限系统 217 可以被配置成委托用于创建附加委托的能力。在该实施例中，第一委托权限系统可以被配置成创建各具有第一委托权限系统的 SM 编程能力的子集的一个或多个第二委托权限系统。委托级别的最大数量（如果有限制的话）可以是可配置的选项。简化的实施例可以对于委托权限省略 SM 内核中的支持，并且而是针对所有任务使用根秘密密钥（例如，其中用作委托权限的实体具有包含根签名密钥的签名装置并且 / 或者利用这样的装置在网络之上交互）。

[0069] 根权限系统 217 可以包括防篡改签名模块（未示出）以提供增加的安全和 / 或特性。委托权限系统 222 典型地通过根权限系统 217 被授予授权以仅行使根权限系统 217 的权限的子集。根和委托权限系统 217 和 222 的特权阶段可以例如通过密码密钥、由签名软件强加的约束、操作者策略以及在防篡改签名模块内的策略来调整。

[0070] 系统 200 可以包括多个委托权限 220。委托权限 220 是与委托权限系统 222 相关联的实体。委托权限系统 222 已经被根权限系统 217 赋予了 SM 编程能力的子集。委托权限 220 的示例可以例如包括产品供应商 125、IC 制造商 110、装置管理员 127、服务操作者、零售商、一些其他实体（例如，如参照图 1A 讨论的）或者它们的一些组合。

[0071] 委托权限系统 222 可以具有从根权限系统 217 委托给它的某些能力（例如，密钥管理操作、特征管理操作或两者的一部分）。这些能力可以被输送作为正向授权的集合或作为约束的集合。例如，特权可以通过控制由权限系统提供什么签名报文（例如，签名块）、由权限系统使用的签名密钥的调整、可以由权限系统中的一个签名的净荷的特定类型的调整、通信信道 / 目的地的调整以及可被输送至 SM 内核的报文的类型或者它们的一些组合而由根权限系统 217、委托权限系统 222 输送和限制。可以被委托的示例性特权包括：能够启用或禁用某些硬件能力、调节特性设定或其他值、允许某些外部接口的使用、允许操作的某些模式的使用、启用或禁用测试模式（例如，控制诊断和调试模式）、控制什么时候特定模式或特征被激活（例如，仅在制造过程期间被激活）、能够调节 SM 被启用的 IC 的特征的某些配置设定的值、导出和 / 或使用一个或多个密钥加密密钥、将以供某些 SM 被启用的 IC 使用的密钥加密、将密钥供应至 IC 子组件、调节 SM 被启用的 IC 的通常配置、审核可由 SM 内核访问的状态信息、为密钥 / 密钥拆分编程、在内场 SM 被启用的 IC 上进行诊断活动、校准或调谐模拟电路以补偿处理变化、配置用于特定产品中的输入时钟和期望的操作频率的 PLL、调节无线电的功率和频率、配置由内部热失效安全强加的限制（热限制可以基于不同产品中使用的封装和冷却溶液而变化）、配置电池充电电路，等等。

[0072] 根权限系统 217 的对委托权限系统 222 的授权也可以包括在委托权限系统 222 的

授权上的约束,包括但不限于委托权限系统 222 是能够永久地(例如,通过引导 SM 内核将特征配置数据保存在非易失性 / 一次性可编程存储器中)还是短暂地配置特征、授权是必须被绑定至单个 IC 还是至特定类或组的 IC、授权是否必须被绑定成随机数量发生器状态(以防止授权被复用)。

[0073] 如先前所提到的,特征设定不限于简单二进制开 / 关设定。例如,可以有使得期望使用委托权限系统 222 或根权限系统 217 以要求用于配置上的改变的授权的关注(例如,安全性、可靠性、责任,等等)。例如,错误配置 PLL 或者使用不正确的模拟校准可以引起 SM 被启用的 IC 误动作,所以 PLL 设定可以通过 SM 内核来保证安全。

[0074] 如下面所详细讨论的,委托权限系统 222 被配置成生成一个或多个委托 - 签名块(“DSB”)。委托权限系统 222 可以被配置成将 DSB 提供至 : 配置器系统 280、SM 被启用的 IC 265、根权限系统 217、IC 提供商 105、SM 被启用的装置(例如,240、245、250、255 或 260)、电子存储介质(未示出)、一个或多个实体 287 或者它们的一些组合。另外,委托权限系统 222 可以被配置成在由委托权限系统 222 的用户指示时提供 DSB。一个或多个实体 287 是其既不是委托权限也不是根权限的实体,但是仍然可以接收 RSB、委托 - 签名块(“DSB”)或它们的一些组合。例如,在一些实施例中,装置管理员 127、IP 和 / 或安全密钥提供商 115、托管服务提供商等等可以不是委托权限,但是仍然可以接收 RSB、DSB 或它们的一些组合。

[0075] 委托权限系统 222 可以包括被配置成存储一个或多个安全密钥(例如,委托私钥、AES 密钥或两者)的防篡改签名模块(未示出)。例如,防篡改签名模块可以是智能卡或硬件安全模块(“HSM”)。

[0076] 在一些实施例中,委托权限系统 222 具有创建附加委托的能力。在这样的实施例中,提供 SM 编程能力的系统能够被禁止委托比当前拥有的更多的 SM 编程能力。例如,如果根权限系统 217 伴随着将 SM 编程能力分配至附加的委托权限系统(未示出)的能力将仅 SM 编程能力 A、B 和 C 提供至委托权限系统 222,则委托权限系统 222 将不能进一步提供 SM 编程能力 D,但能够在没有许可 C 的情况下委托 A 和 B。委托权限系统 222 可以在单个计算机上实现,或者在一些场合中被横跨多个计算机分布。分布的委托可以如先前所述使用门限签名。委托权限系统 222 还可以包括用于可靠性和特性的多个冗余的和 / 或群聚的组件。

[0077] 另外,在一些实施例中,根权限系统 215、委托权限系统 222 或两者可以被配置成在一个或多个电子存储介质(未示出)中存储签名块(例如,RSB、DSB)。电子存储介质可以例如是易失性的(例如,SRAM、DRAM 或者其他半导体存储器)或非易失性的(例如,硬盘、R/W 光盘、闪存驱动器)或者它们的一些组合。RSB 和 / 或 DSB 也可以被存储在 SM 装置内(例如,如果 RSB/DSB 对仅配置特征直到装置被复位为止,则配置可能需要在每次产品复位时被加载)。

[0078] 系统 200 可以包括若干 SM 被启用的装置,例如,SM 被启用的装置 240、245、250、255 和 260。SM 被启用的装置 240、245、250、255 和 260 可以是例如智能电话、平板电脑、上网本、台式计算机、机顶盒、移动装置、膝上型计算机、数字视频记录仪、付费 TV 机顶盒、汽车、制造设备、数字和视频照相机、电池、认证外围的装置、视频游戏用户接口以及其他用户接口,等等。尽管用多个 SM 装置示出了图 2A 的示例性系统,但是系统可以用一个或任何数量的 SM 被启用的装置实现。SM 被启用的装置 240、245、250、255 和 260 对来自进而能够授权的根权限系统 217、委托权限系统 222 的签名或其他授权进行验证。另外,SM 被启用的装

置（例如，SM 被启用的装置 240、245、250、255 和 260）与根权限系统 217、与委托权限系统 222 或者与两者之间的耦合可以是临时的。例如，耦合可以存在于用以修改 SM 被启用的 IC 的操作所需要的时间。用于 SM 被启用的装置 260 和 SM 被启用的 IC 265 的授权可以由根权限系统 217 或委托权限系统 222 创建，并且经由一个或多个装置测试仪（未示出）、编程器具（未示出）或其他中间体（未示出）传递。

[0079] 装置测试仪通常被配置成测试 IC 的功能性。特别地对于 SM 被启用的 IC，装置测试仪可以附加地被配置成将信息（例如，密钥、装置 IC 等等）编程到 SM 被启用的 IC 内（例如，通过将编程命令供应至 SM 内核）。装置测试仪或编程器具也可以在数据库中记录关于装置及其 SM 内核的信息，包括装置身份信息和配置信息。各装置测试仪可以被配置成将一个或多个 SM 被启用的装置耦合至根权限系统、委托权限系统或两者。可能具有一套特征或能力的系统或装置理想地适合 SM 被启用的 IC 的使用。

[0080] SM 被启用的装置可以包括一个或多个 SM 被启用的 IC（例如，265）。同样，SM 被启用的 IC 265 可以包括例如一个或多个 SM 内核，以及一个或多个安全存储器。并且如下面所详细讨论的，SM 被启用的 IC 可以可选地包括一些其他元素（例如，一个或多个提取器、控制一个或多个特征的输出，等等）、或者它们的一些组合。如下面所讨论的，可以经由密钥管理或特征管理操作对 SM 被启用的 IC 265 进行某些修改。

[0081] SM 被启用的装置 240、245、250、255 和 260 可以被配备用于通过 PLMN 210 的蜂窝通信、被配备用于利用无线访问点 275 的 Wi-Fi 通信、或能够进行利用网络 210 的蜂窝以及 Wi-Fi 通信两者或者他们中的任何组合。无线访问点 275 可以被配置成根据 IEEE 802.11 规范中的一个进行操作的 WLAN。例如，SM 被启用的装置 250 利用无线访问点 275 无线地耦合至网络 205，并且 SM 被启用的装置 240 经由 PLMN 210 耦合至网络 205。SM 被启用的装置 240、245、250、255 和 260 能够支持的其他通信接口的示例包括以太网、JTAG、串口 /USB、I2C，等等。

[0082] 即使包括了在编程之前同样的 IC，SM 被启用的装置 240、245、250、255 和 260 也可以不同地配置。在消费电子产品中，可以在宽范围的产品（例如，高端和低端产品两者）中使用类似的硅或 IC（例如，由相同掩模集制作），其中特性上的差异至少部分由配置控制。特征丰富的产品可能具有例如先进的音频能力（例如，环绕立体声）、多个 HD 视频流、大量且多样的输入和输出、包括了有线的或卫星的或无线的特定调制解调器和转码器、各种调谐器等等的用于多个有线电视提供商的支持、诸如画中画等的观看特征、Wi-Fi 支持，等等。同样，预期用于在智能电话中使用的 SM 被启用的 IC 可以包括用于诸如 GPS 等的能力的特征管理支持、各种无线网络无线电协议、Wi-Fi、基于近场通信的财务交易、蓝牙或其他外围接口、空中视频服务、HD 视频支持、无线视频接口、附加的外部视频接口、许多且各种分辨率的照相机和传感器、用于各种屏幕大小和分辨率的支持、用于触觉的、图形的和视频的增强与加速的处理。SM 被启用的 IC 中的 SM 内核可以用于管理诸如例如可用的或可使用的存储器等的系统资源的大小和特性，或者可用的处理器的速度和数量。在未示出的一些实施例中，SM 被启用的装置（例如，240、245、250、255 和 260）也可以被可操作性地耦合至配置器系统 280。特定特征为什么应该在特定芯片上被禁用的原因有很多，包括降低用于未用的特征的 IP 许可证发放成本、禁用非工作的或未经测试的硅面积、避免较高端部件的拆用销售、禁用可能造成安全风险的模式 / 设定，等等。

[0083] 委托权限 220(例如, IC 提供商 105 或 IC 制造商 110) 可以接收来自配置器系统 280 的配置数据。由配置系统 280 生成的数据可以通知委托权限 220 如何寻址特定特征或密钥。

[0084] 在示例性实施例中, SM 内核特征空间是存储在存储器中的包括了控制 SM 被启用的 IC 的特定功能性或配置方面的值的地址空间。图 2B 是与 SM 被启用的 IC 相关联的特征空间 285 的示例性实施例的框图。特征空间 285 包括一个或多个值 295, 其中每一个都具有相关的地址 290。例如, 值“GPS 无线电启用的”可能被分配至特征空间中的地址 0。诸如多位 PLL 配置值等的特征空间中的其他值可以跨距多个位 (和相应的地址)。

[0085] 在一些实施例中, 除了 SM 被启用的 IC 的其他特征以外, 特征空间 285 内的值中的一个或多个可以涉及 SM 内核自身。这样的特征空间值称为内部特征。例如, 内部特征可能控制某些基本密钥是否可用以供使用、携带关于装置的信息 (诸如, 产品制造商的身份、产品售出所在的地理区域), 等等。这些内部特征可以用于控制授权 (例如, 使得预期用于一个地理区域内的装置的授权将不能在另一区域中的装置上工作)。

[0086] 内部特征是可寻址的并且被以与用于控制装置元素的特征类似的方式控制。内部特征可以用于代表接着被映射到引导设备的元素的更加具体的 SM 内核输出的较高级别的特权或特征条件。例如, 内部特征可以代表从 1 到 7 的数值的速度等级, 而 SM 内核输出包括用于设定映射到速度等级的较大量 PLL 时钟控制设定的信号。以该方式, 如将在后面描述的, 数值的速度等级设定可以用作用于形成其操作被限于特定速度等级的 SM 内核命令的条件。在另一示例中, 内部特征可以在 SM 内核内使用以追踪已发布组标识符、装置标识符或者装置已经通过一定身份被封装、制造或者售出的事实。在该示例中, 制造实体可能是具有将其制造商 ID 编程到内部特征内的许可的委托权限 220。SM 内核命令可以演绎内部特征并使用结果来控制 SM 内核如何管理其他特征或密钥。例如, SM 内核可以对于由特定网络操作者操作的装置或仅对于处于预零售状态的装置仅输出某些密钥或者某些调试设定许可。

[0087] 返回参见图 2A, 配置器系统 280 也可以配置成将装置特定密钥映射到 SM 内核密钥接口。配置器系统 280 可以在芯片开发期间也可以在之后被利用来管理这些设定和配置。

[0088] 配置器系统 280 可以被配置成接收一个或多个配置器输入文件、硬件 (“HW”) 常量或者他们的组合, 并且将他们进行处理以生成一个或多个提取器硬件限定、一个或多个子提取器硬件限定以及 IC 配置映射。生成的限定例如是描述 SM 被启用的 IC 的组件的 Verilog 模块。一个或多个配置器输入文件可以限定用于 SM 被启用的 IC 的特定配置、列出一个或多个安全密钥及其相关的在 SM 被启用的 IC 上的目的地、由 SM 内核管理的特征的名字和地址、等等。例如, 一个或多个配置器输入文件可以被配置成指定这样的事物作为已命名的特征信号、配置位、配置位的分组、安全密钥总线输出、安全密钥总线属性、安全存储器映射属性或者他们的组合。可以由配置器系统 280 配置并且被嵌在硬件内 (例如, 被固定在硅内并且对于用相同掩模做出的所有芯片共用) 的硬件常量的示例包括例如芯片产品 ID、来自根权限 (例如, 根权限系统公钥) 的一个或多个密钥、来自委托权限的一个或多个密钥、一个或多个基本密钥、一个或多个附加的安全密钥、错误校正数据、用于特征控制的默认值, 等等。

[0089] 生成的提取器硬件限定被用在 IC 设计中以将总线输出从 SM 内核布线到各种子提

取器。如在一个或多个配置器输入文件中指定的，子提取器硬件限定被用在 IC 设计中以将特征空间位从提取器映射到已命名的特征和密钥。提取器硬件限定和任何子提取器硬件限定被用于产生包含提取器和子提取器的 SM 被启用的 IC 设计。

[0090] 配置器系统 280 也可以被配置成利用追踪配置上的改变的状态缓存，并且该状态缓存可以用于使现有的电路设计布局的修改最小化。状态缓存例如可以是映射文件、IC 配置映射，等等。在一些实施例中，代替利用映射文件来更新状态缓存，配置器 280 被配置成重新读取之前的输出以实现状态缓存。

[0091] 在一些实施例中，配置器系统 280 可以被配置成附加地生成一个或多个命令映射文件、一个或多个固件映射文件和一个或多个文档文件。命令映射文件例如是用于将命令映射成为可由 SM 被启用的 IC 理解的形式的文件。固件映射文件是包含用于软件开发所需要的限定和结构的文件（例如，标头和源文件，等等）。文档文件提供了 SM 被启用的 IC 设计的概要。另外，文档文件可以包括软件组件的设计中使用的环境和构造原理。文档文件可以是以下格式中的一个或多个：XML、HTML、text、PDF、MICROSOFT WORD，等等。

[0092] 配置器系统 280 可以用在一个或多个 SM 被启用的 IC 265 的生产中。在未示出的一些实施例中，配置器系统 280 可以用在 SM 被启用的装置 240、245、250、255 和 260 中的一个或多个的生产中。配置器系统 280 可以包括一个或多个处理器（未示出）、存储器（未示出）以及数据接口（未示出）。配置器系统 280 可以在单个计算机上实现，或者在一些场合中横跨多个计算机分布。

[0093] 图 3 是用于进行在本文中描述的方法的包括了 SM 内核的系统 300 的示例性实施例的框图。系统 300 可以包括 SM 内核 305、安全存储器 310、提取器 320、总线 360、处理器 355、提取器接口 375、密钥接口 376、配置值接口 377、主存储器 370、特征 325、330 和 335、子提取器 340、345 和 350、寄存器接口 358、测试仪接口 365 或者它们的一些组合。SM 被启用的 IC 包括 SM 内核 305 和安全存储器 310，并且可选地可以包括 SM 系统 300 的示出来的其他元素中的一些（或所有）（例如，提取器 320、总线 360、处理器 355、提取器接口 375、子提取器 340、345 和 350、密钥接口 376、配置值接口 377、主存储器 370、特征 325、330 和 335，等等）。尽管图 3 中每个组件仅示出了一个，但是应该理解的是，系统 300 可以包括超过一个的任意已命名组件。例如，系统 300 可以具有多个处理器 355。类似地，尽管用单个 SM 内核 305 示出了图 3 的示例性系统，但是 SM 被启用的 IC 可以包含多个 SM 内核 305。此外，在一些实施例中，系统 300 可以包括可以被可操作性地耦合（诸如利用光、电或无线传输被可通信地耦合）至测试仪的测试仪接口（“I/F”）365。在未示出的一些实施例中，一个或多个子提取器 340、345 和 350 可以与提取器 320 组合。

[0094] 另外，在一些实施例（未示出）中，SM 内核 305 可以与一个或多个特征（未示出）直接连接，并且如果所有这样的连接都被直接地处理，则可以不需要提取器 320 和子提取器。并且在一些实施例中，特征 325、330 和 335 可以继续利用提取器 320、一个或多个子提取器（例如，340、345 和 350）和接口（375、376、377）连接。

[0095] 另外，SM 内核 305 可以直接读取和写入信号至系统 300 的其他组件。在一些实施例中，SM 内核 305 可以经由例如专用接口（未示出）或者经由总线 360 采样系统状态、读取数据参数，等等。例如，SM 内核 305 可以在总线 360 之上发布读取操作以获取期望的信息。

[0096] 系统 300 包括安全存储器 310。安全存储器 310 可以是单个安全存储器和 / 或多

个同类或异类的安全存储器。安全存储器 310 可以是其中每个位的设定可以以非易失性形式固定的数字存储器的形式。安全存储器 310 可以包括例如熔丝存储器、反熔丝存储器、一次性可编程（“OTP”）存储器、可擦除可编程只读存储器（“EPROM”）、电可擦除可编程只读存储器（“EEPROM”）、RAM（包括电池供电的 RAM）或者它们的一些组合。在一些实施例中，其中安全存储器 310 是熔丝或反熔丝存储器，安全存储器 310 可以包括提供修订先前存储在安全存储器 310 内的信息（例如，通过重写或重新映射先前写入的数据）的能力的冗余通路。取决于目前的技术和安全特征，安全存储器 310 的内容可以被加密和 / 或认证、可以被保护不被除了 SM 内核 305 以外的区块读取、可以被配置成一次性可编程的。还有，安全存储器 310 可以是孤立的，使得仅 SM 内核 305 被连接至安全存储器 310，或者使得 SM 被启用的 IC 的其他组件可以从安全存储器 310 读取但是仅 SM 内核 305 可以写入安全存储器 310。安全存储器 310 也可以被划分成可以由 SM 被启用的 IC 中的除 SM 内核 305 以外的组件读取的一个或多个部分以及可以仅由 SM 内核 305 读取的一个或多个部分。SM 内核 305 可以直接负责进行所有制造测试和用于安全存储器 310 的编程操作。另外，在一些实施例中，安全存储器 310 被设计成抵抗例如通过从 IC 上去除某些层、捕捉 IC 的显微照片或者在操作期间电探测 IC 来获悉其内容的努力。另外，在一些实施例中，SM 内核 305 包括封装器 315。封装器 315 将来自 SM 内核 305 的请求翻译成由安全存储器 310 理解的请求，并且反之亦然。在一些实施例，安全存储器 310 可以被集成至 SM 内核 305。

[0097] 系统 300 包括一个或多个特征 325、330 和 335。经由子提取器 340、345、350 传递至特征 325、330 和 335 的输入通常是可配置的，由此提供了与特征 325、330 和 335 相关联的功能性的可配置性（例如，经由密钥管理和特征管理操作）。这样的配置改变可以通过经由寄存器接口 358 传递至 SM 内核 305 的 SM 命令（下面描述）来进行。

[0098] 特征 325、330 和 335 可以包括硬件、软件和他们的组合。例如，特征 325、330 和 335 可以是全球定位服务、一个或多个处理器（例如，CPU、图形处理器、密码内核，等等）、附加的存储器、USB 端口、视频输入或输出端口、音频输入或输出端口、提供先进的图形能力（例如，画中画，多个 HD 视频流、图形加速，等等）的电路、用于访问一个或多个网络（例如，Wi-Fi、近场、蓝牙，等等）的网络收发器、照相机，等等。上面的特征列表不应该被考虑为限制的，因为特征可以包括经由密钥管理或特征管理操作而可配置的任何组件或能力。上面参照例如图 2A 讨论了特征能力，并且在下面讨论例如特征管理部。在一些实施例中，特征或特征的一部分由第三方 IP 提供商提供。特征 325、330 和 335 分别与子提取器 340、345 和 350 相关联。在未示出的一些实施例中，多个特征可以共享单个子提取器。子提取器 340、345 和 350 便于 SM 内核输出（诸如配置值和密钥）的横跨 SM 被启用的 IC 设计的传递。另外，如上面所讨论的，子提取器 340、345 和 350 是选择性的，并且通常用于包括多个特征的大型或复杂的 SM 被启用的 IC（包括其中顶级 ASIC 布图规划和 / 或布线是具有挑战性的）。提取器 320 被配置成将来自 SM 内核 305 的输出传递至子提取器 340、345 和 350，子提取器 340、345 和 350 进而将信号分别传递至特征 325、330 和 335。

[0099] 示例性系统 300 包括提取器 320。提取器 320 是配置成以适于预期的目的地特征的形式对从 SM 内核 305 到与该特征相关联的适当的子提取器的信息（例如，密钥和特征状态）进行接收和布线的硬件组件。特征状态是指已经被 SM 内核 305 以及可能的提取器 320 处理过使得其呈可以由目的地特征理解的形式的信息。特征状态可以在特征空间中具有一

个或多个相关联的地址。通过示例的方式,特征状态可以包括使能信号、元数据、配置或校准信息或者对于特征有用的其他数据。

[0100] 提取器 320 被可操作性地耦合至 SM 内核 305, 并且被可操作性地耦合至一个或多个特征(例如, 特征 325、特征 330 和特征 335)。在一些实施例中, 提取器 320 经由提取器接口 375 耦合至 SM 内核 305。提取器接口 375 提供从 SM 内核 305 到提取器 320 的信息(诸如, 特征数据、安全密钥等类似物)的通信。特征数据可以是秘密的或非秘密的, 并且是用于配置特征的总体数据。提取器接口 375 可以包括将 SM 内核 305 耦合至提取器 320 的导线。提取器 320 接着经由密钥接口 376、配置值接口 377 或者它们的组合将信息转送至与各目的地特征相关联的子提取器。密钥接口 376 是配置成使秘密信息(例如密码密钥, 如针对诸如 RSA 和 EC-DSA 等公钥系统的私钥、诸如 AES 或三重 DES 等的针对密码系统的对称密钥以及用于诸如 HDCP 或 EMV 等的协议的密钥)通过的通信路径。例如, 提取器 320 可以经由密钥接口 376 将 128 位密钥和目标密钥地址通信至一个或多个特征(例如, 325、330 和/或 350)。提取器 320 可以被配置成将目标地址解码以便标识与目的地特征相关联的特定子提取器。例如, 子提取器 340、子提取器 345 和子提取器 350 分别与特征 325、330 和 335 相关联。配置值接口 377 是配置成使与特征管理操作相关联的特征数据通过的通信路径。例如, 如果一个或多个特征(例如, 325、330、335 或它们的一些组合)正被配置或启用, 则提取器 320 经由配置值接口 377 使特征数据传到适当的子提取器。同样, 如果特定特征不需要(并且/或者为了安全原因可能不被许可接收)与给定的地址相关联的值, 则提取器和/或子提取器能够保留这些来自目的地的值。保留不必要的值能够通过避免值的到不需要了的子提取器或特征的不必要布线和传递来提高 ASIC 上的效率。在一些实施例中, 提取器接口 375 提供报文的从 SM 内核 375 到提取器 320 的双向通信。在其他实施例中, 提取器接口 375 提供报文的从 SM 内核 305 到提取器 320 的单向通信。密钥接口 376 和配置值接口 377 可以包括将 SM 提取器 320 耦合至一个或多个子提取器 240、234 和 350 的导线。

[0101] 提取器接口 375、密钥接口 376 和配置值接口 377 或者它们的一些组合将 SM 内核 305 耦合至提取器 320 和子提取器 340、345、350。接口的组合可以例如通过连续地发送数据值、发送当发生值改变事件(例如, 使能特征)或接收到请求(例如, 因为特征上电)时的数据或者它们的一些组合而将来自 SM 内核 305 的数据传输至特定特征。

[0102] 特征空间的各元素的与 SM 内核相关联的当前值可以被存储在例如安全存储器 310 或 SM 私有存储器(下面讨论)中。在一些实施例中, 给定的操作(例如, 下面讨论的 RSB 或 DSB 的处理)可以只更新特征空间的元素的子集。在其中值改变事件被从 SM 内核 305 通信至提取器 320 的实施例中, 期望(尽管不是要求的):只有特征空间的元素的受特定净荷影响的值在该净荷的处理时被从 SM 内核 305 通信至提取器 320。在其中特征空间内的所有值被连续地从 SM 内核 305 驱动至提取器 320 的实施例中, 受特定净荷影响的值可以与从例如用于通信的 SM 私有存储器到提取器 320 的不受影响的特征空间的之前的值组合。

[0103] 系统 300 可以包括处理器 355。处理器 355 例如可以是单个或多个微处理器、现场可编程门阵列(FPGA)元件或者数字信号处理器(DSP)。处理器 355 的具体示例例如是 x86 处理器、ARM 处理器、MIPS 微处理器、8051 微控制器, 等等。处理器 355 可以经由总线 360 耦合至 SM 内核 305、主存储器 370、测试仪 I/F 365 或者它们的一些组合。在一些实施例中, 处理器 355 可以被配置成与 SM 内核 305 直接通信、经由 SM 内核 305 对安全存储器 310 进

行读取并编程、检索 SM 内核 305 的状况和系统状态、将命令发送至 SM 内核 305、从 SM 内核 305 接收用于由处理器 355 执行而被授权的软件的密码散列（诸如，启动程序、操作系统组件、应用，等等）或者它们的一些组合。另外，可以多个进行这些访问的处理器。另外，在一些实施例中，处理器 355 具有例如在 Ring 0 中、利用 ARM 的 TrustZone® 或者在安全的虚拟机器监测器（SVMM）中运行较高特权代码的能力。较低特权的处理器 355 或者处理可以利用 SM 内核 305 的一些或所有能力被阻挡。寄存器接口 358 可以用于通信请求的身份和特权级别，并且 SM 内核 305 能够在接受和处理横跨寄存器接口 358 接收的 SM 命令时把请求者的特权级别考虑进去。

[0104] 系统 300 可以包括主存储器 370。主存储器 370 可以是易失性的（例如，SRAM、DRAM 或其他半导体存储器）或非易失性的（例如，硬盘、R/W 光盘、闪存驱动器）或者它们的一些组合。主存储器 370 被可操作性地耦合至处理器 355、SM 内核 305、测试仪 I/F 365 或者它们的一些组合。在该实施例中，主存储器 370 经由总线 360 耦合至系统 300 的一个或多个组件。

[0105] 系统 300 可以包括测试仪 I/F 365。测试仪 I/F 365 是用于测试仪系统（未示出）的接口。测试仪 I/F 365 例如可以被配置成当 SM 内核 305 处于制造状态时、当 SM 被启用的 IC 在内场时、当处理器 355 尚未操作（或误动作）时或者它们的一些组合时提供到达 SM 内核 305 的通信路径。测试仪 I/F 365 可以是扫描接口、测试接口、联合测试行动小组（“JTAG”）接口、通用串行总线接口、先进的外围总线（“APB”）接口，等等。测试仪系统可以耦合至系统 300 使得能够对系统 300 测试以用于校正操作。例如，测试仪系统能够被配置成确保系统 300 正确地启用特征、禁用特征、对安全存储器 310 进行编程，等等。测试仪系统可以包括一个或多个处理器和存储器，并且可以与用于授权 SM 内核 305 中的操作的委托权限系统通信（或者包括）。

[0106] 系统 300 包括 SM 内核 305。SM 内核 305 可以可操作性地耦合至安全存储器 310、提取器 320 并且经由寄存器接口（“I/F”）358 和总线 360 可操作性地耦合至处理器 355、主存储器 370 以及测试仪 I/F 365。另外，在一些实施例（未示出）中，SM 内核 305 可以被直接连接至处理器 355、主存储器 370 和测试仪 I/F 365 中的一些或所有。SM 内核 305 包括一个或多个 SM 私有存储器（未示出）。这些一个或多个私有存储器可以用于存储由 SM 内核使用的数据，包括一个或多个安全密钥（例如，基本密钥、个人化密钥、传送密钥、网表密钥、根或委托权限公钥，等等）、针对在安全存储器 310 内的位置的一个或多个指针、用于封装器 315 的指令、与特征地址相关联的当前配置状态、命令处理中间体，等等。在一些实施例中，一个或多个安全密钥和产品芯片 ID 可以硬接线至 SM 内核 305 内（例如，根权限公钥、必须在安全存储器 310 误动作或未配置时可用的基本密钥，等等）。一个或多个安全密钥可以包括对称密钥、公共非对称密钥、私有非对称密钥或者它们的一些组合。在一些实施例中，一个或多个安全密钥对于 SM 内核是特定的，并且其他的可以在一系列的 SM 内核之中共享。SM 内核系列是指可以以一些方式相关的 SM 内核的集合。例如，从给定的掩模设计制造出的 SM 被启用的 IC 中的所有 SM 内核可以被视为一系列。备选地，一族类似的 SM 被启用的 IC 中的任何一个中的所有 SM 内核可被视作一系列。

[0107] 在示例性实施例中，SM 内核 305 被配置成接收一个或多个签名块，该签名块可以包括根签名块（“RSB”）以及零个或多个委托签名块（“DSB”），这将参照图 4 进一步进行

讨论。SM 内核 305 被配置成验证与签名块相关联的签名，并且提取相关联的净荷，从而指定约束 / 绑定（见下面）以及预期用于一个或多个特征（例如，325、330、335）的值（例如，配置设定或密钥）。约束的示例包括 SM 内核应该接受净荷所在的限制（诸如，指明了具体装置 ID 的限制，或者存储在特征地址空间内的值的要求状态，或者特征能够被操纵所在的限制，等等）。SM 内核 305 可以被配置成利用根权限的公钥来认证净荷，并且利用例如建立到 SM 被启用的 IC 内或从存储在安全存储器 210 中的值导出的私钥从签名块中提取（例如，解密）净荷。SM 内核 305 被配置成经由提取器 320 将一些净荷或处理净荷的结果分布至预期的一个或多个特征（例如，325、330、335）。

[0108] 在一些实施例中，SM 内核 305 可以被配置成执行更新 SM 被启用的 IC 的特征状态的指令、便于密钥传递至特征、启用安全存储器 310 的配置（诸如，以配置用于写入安全存储器 310 所需的参数，如果有安全存储器的话），等等。例如，SM 内核 305 可以被指示以启用特征 325 或启用特征 330。取决于实施例和所提供的指令，SM 内核 305 可以做出永久性改变（例如，通过更新安全存储器 310）、非永久性改变（例如，通过更新 SM 私有存储器）或两者。永久性改变是在 SM 被启用的 IC 被断电之后永久的那些改变，使得改变在 IC 启用芯片重新启动之后永久存在。非永久性改变是持续预定时间段或事件的那些改变。例如，非永久性改变可以只对于某些数量的执行是良好的，直到电力在装置上丢失为止，等等。SM 内核 305 可以被配置用于管理和传递用于安全数字（“SD”）卡加密、闪存 / 硬盘加密、高带宽数字内容保护（“HDCP”）、数字权益管理（“DRM”）系统、虚拟专用网络（“VPN”）、支付工具（例如，EMV）、口令管理器、无线电链路加密、外围认证、其他安全操作，等等。

[0109] 另外，SM 内核 305 可以被配置成接收可以用在 IC 配置处理中的硬件（“HW”）常量。HW 常量可以包括例如产品芯片 ID、用于根权限系统的一个或多个密钥（诸如，RSA 或 EC-DSA 公钥）、来自委托权限系统的一个或多个密钥、一个或多个基板密钥、一个或多个附加的安全密钥、用于 SM 内核 305 操作的参数（例如，存储器使用率、所支持的命令，等等）、错误校正数据，等等。产品芯片 ID 能够用身份值唯一地标识特定 SM 被启用的 IC 或者特定的 SM 被启用的 IC 系列。安全密钥可以是对称的或非对称的（并且，如果非对称的话，是公共的还是私有的）。在一些实施例中，一个或多个基本密钥可以从万能密钥、SM 被启用的 IC 系列的身份码、芯片特定的标识符或者它们的一些组合导出。错误校正数据可以包括例如与安全密钥的一个或多个相关的校验和。

[0110] SM 内核 305 可以被配置成生成到处理器 355 的中断。例如，SM 内核 305 可以被配置成当 SM 被启用的 IC 的特征状态已经被更近时、准备接收附加的 I/O 时、密钥已经被输出时等生成中断。

[0111] SM 内核 305 可以被配置成执行一个或多个内置的自我校验。例如，SM 内核 305 可以被配置成当首次上电时、在测试接口的控制下时等进行自我校验。

[0112] 在一些实施例中，系统 300 是将图 3 中示出的组件中的所有或者组件中的大多数（诸如除了处理器 355 和主存储器 370 以外的一切）组合的单个 IC（诸如片上系统）。

[0113] 在一些实施例中，系统 300 中的所有或一些可以被构造成抵抗由外界源产生的篡改。例如，SM 内核 305 可以包括安全网孔（未示出）或者在安全网孔下制作。安全网孔是例如利用在集成电路上的顶部金属层中的一个或多个而在主逻辑电路的顶部制作出的导线网络。安全网孔可以与预期检测包括了网孔的导线的损坏的有源传感器网络配对。在该

实施例中,SM 内核 305 被配置成当有源传感器表明安全网孔配线中的一些已经被损坏时拒绝进行敏感性操作。另外,SM 内核 305 可以被配置成进行诸如擦除安全存储器 310 等的其他对策。

[0114] 图 4 描绘了示例性 SM 内核 305 的框图。示例性 SM 内核 305 可以包括密码机模块 410、执行引擎模块 420、通信模块 430 和数据存储模块 440 或者它们的一些组合。应该理解的是,这些模块中的一个或多个可以被删除、修改或者与其他模块组合到一起。

[0115] 密码机模块 410 可以是配置成提供认证、加密功能性、解密功能性或者它们的组合的硬件组件、软件组件或者它们的一些组合。例如,密码机模块 410 可以被配置成提供对称加密功能性、对称解密功能性、非对称签字 / 签名验证、密钥协商或者它们的一些组合。在一些实施例中,密码机模块 410 可以被配置成验证与根签名块 (“RSB”) 相关联的一个或多个数字签名。RSB 可以包括例如一个或多个 SM 命令、命令模版、一个或多个委托许可、一个或多个密钥 (例如,委托公钥) 或者它们的一些组合。RSB 包含由根权限的私钥 (即,根权限系统 217 的私钥) 签名的至少一个数字签名。密码机模块 410 可以被配置成利用相应的根权限公钥来认证 RSB 的数字签名。在一些实施例中,认证可以利用 RSA、DSA 或 ECDSA 来进行。在其他实施例 (诸如从 SM 被启用的 IC 中提取认证秘密不是问题的那些等) 中,认证可以利用诸如 HMAC 等的对称认证方案来进行。认证方案可以使用这些或其他算法的组合。认证方案可以实现诸如 PKCS#1 或 ANSI X9 等的标准,或者可以是专有的。

[0116] 另外,密码机模块 410 可以被配置成验证与委托签名块 (“DSB”) 相关联的一个或多个数字签名。DSB 可以包括例如一个或多个 SM 命令、净荷 (加密的或未加密的)、一个或多个密钥或者它们的一些组合。在一个实施例中,各 DSB 总是以对委托权限的公钥进行指定和授权的 RSB 为先导。DSB 可以包含由委托权限系统 (例如,委托权限系统 222) 签名的至少一个数字签名。在收到并验证有效的 DSB 之后,密码机模块 410 可以 (如适用于 DSB) 利用 SM 被启用的 IC 中的一个或多个基本密钥导出一个或多个混合密钥,一个或多个传送密钥、一个或多个验证子 (例如,用于密钥验证的值) 或者它们的一些组合。另外,密码机模块 410 可以被配置成将多个密钥拆分组合以形成一个或多个基本密钥。

[0117] 另外,在一些实施例中,RSB 和 / 或 DSB 可以包含加密的净荷部分。在该实施例中,密码机模块 410 可以被配置成例如利用基本密钥或从基本密钥导出的密钥对加密的净荷部分进行解密和查验。密码机模块 410 被配置成一旦 RSB 或 DSB 或两者都被认证,就将经过验证的命令提供至执行模块 420。密码机模块 410 可以耦合至执行引擎模块 420、通信模块 430 和数据存储模块 440。

[0118] 另外,依照可允许的许可的集合,DSB 可以表明其与另一下面的 DSB 相关联,并且可以进一步将下面的 DSB 限制为与第一个 DSB 不同的 (例如,较窄的) 可允许许可的集合。

[0119] 在一些实施例中,密码机模块 410 可以被配置成利用寄存器 I/F (例如,寄存器 I/F 358) 与诸如测试仪或 CPU 应用等的 SM 内核外部的装置或组件来协商随机的会话密钥。经过协商的会话密钥可以例如用于打开在随后的 RSB、DSB 或两者中通信的安全通道或保护秘密。

[0120] 另外,下面参照图 5 至图 9B 详细地讨论了示例性 RSB 和 DSB 的方面。

[0121] 执行引擎模块 420 可以是配置成接收和执行 SM 命令的硬件组件、软件组件或它们的组合。SM 命令可以从根权限系统 (例如,根权限系统 217)、委托权限系统 (例如,委托权

限系统 222)、与 SM 内核 305 相关联 (例如,在启动处理期间) 的安全存储器 (例如,安全存储器 310) 或者它们的一些组合接收。SM 命令可以包括例如装载命令、密钥导出命令、解密命令、安全存储器写入命令、条件操作、策略配置操作,等等。加载命令例如可以使得能够对传递至特征的配置输出和 / 或对在内部用于 SM 内核的状态进行非永久性的改变。密钥导出命令可以用于利用例如密钥树从基本密钥导出一个或多个安全密钥,如下面所详细讨论的。解密命令可以用在对接收到的净荷进行解密和对输出至特征的秘密密钥进行解密 / 输出中。安全存储器写入命令可以用于将特定命令或其他改变写入安全存储器。(例如,写入命令可以用于对 SM 被启用的 IC 做出永久性改变。) 条件操作可以用于确定是否 (或哪个) 其他命令适合于在特定 SM 内核上运行。测量配置操作可以用于指定什么其他命令可以做上的限制 (见下文)。

[0122] 除了上面讨论的 SM 命令以外,一些 SM 命令 (例如,测量配置命令) 例如可以将 RSB 或 DSB 的使用约束为 :特定产品芯片 ID ;产品芯片 ID 的范围 ;特定产品制造商 ;基于由 SM 内核管理的任何特征配置的值的给定芯片系列 ;要求委托在使用区块时测试某些特征 ;或它们的一些组合。在一些实施例中,SM 命令也可以通过要求并入到由 SM 内核导出 (例如,基于随机数量的发生器) 的随机一次性挑战的 RSB/DSB 数字签名内而将 RSB 或 DSB 或两者约束为通过“单个使用”。策略配置命令还可以基于从其他硬件连接至 SM 内核的信号、例如来自篡改检测电路的输出、安全存储器 310 的错误状况等信号的状态而强加限制。执行引擎模块 420 可以耦合至密码机模块 410、通信模块 430 和数据存储模块 440。

[0123] 通信模块 430 可以是配置成用作 SM 内核 305 与外界之间的接口的硬件组件、软件组件或它们的组合。例如,通信模块 430 可以被配置成与 CPU(例如,处理器 355)、主存储器 (例如,主存储器 370)、安全存储器 (例如,安全存储器 310)、提取器 (例如,提取器 320)、测试仪接口 (例如,测试仪 I/F 365)、IC 上的任何其他组件或者它们的一些组合接口。通信模块 430 可以被配置成接收来自一个或多个总线 (例如,经由总线 360)、安全存储器等等的命令。另外,通信模块 430 可以帮助发送信息至各种特征 (例如,直接地,或经由提取器 320,或以两种方式)。在一些实施例中,通信模块 430 包括安全存储器封装器 (例如,封装器 315)。安全存储器封装器被配置成将来自 SM 内核 305 的命令翻译成可由与 SM 内核 305 相关联的安全存储器认可的格式。通信模块 430 可以耦合至密码机模块 410、执行引擎模块 420 和数据存储模块 440。

[0124] 数据存储模块 440 可以包括一个或多个 SM 私有存储器。数据存储模块 440 可以被配置成存储一个或多个安全密钥 (例如,装置密钥或装置密钥组)、产品芯片 ID、一个或多个 SM 命令、启动指令、特征数据、配置数据、永久性特征信息,等等。在一些实施例中,数据存储模块可以另外地存储用于在 SM 内核 305 操作中做出永久性改变的信息,诸如关于存储器的布局和使用率的信息等。数据存储模块 440 可以包括一个或多个 SM 内核 305 外部的存储器结构 (诸如静态 RAM 等) 或与之接口接合,或者可以并入有内部存储器 (例如,寄存器、寄存器文件、静态 RAM、等等,如果这样的存储器是易失性的话,或者如果可用的话,可以使用易失性存储器)。数据存储模块 440 还可以存储诸如委托权限系统公钥等的密码值。数据存储模块 440 可以耦合至密码机模块 410、执行引擎模块 420 和通信模块 430。

[0125] 3. 安全管理器功能性

[0126] 对于根权限请求 SM 被启用的 IC 中的 SM 内核进行操作 (例如,更新密钥或特征状

态),根权限系统限定了就一个或多个 SM 命令而言的操作。SM 命令在被执行时可以(除其他事项外)更新由 SM 被启用的 IC 中的 SM 内核管理的特征状态。根权限系统以由 SM 内核认可的二进制格式将 SM 命令编码,并且包括对于命令的数字签名。命令和签名的组合被称为签名块。来自根权限系统的签名块被称作根签名块(“RSB”),并且来自委托权限系统的签名块被称作委托签名块(“DSB”)。

[0127] 在不牵涉到委托签名块的简单情况下,SM 被启用的 IC 中的 SM 内核接收来自根权限系统的命令。根权限系统公钥可以被内置到 SM 被启用的 IC 内。图 5 是用于生成包括了由根权限系统签名的命令的根签名块的示例性方法的流程图。在步骤 500 中,根权限系统例如从签名请求或输入文件接收一个或多个 SM 命令。SM 命令的区块接着由根权限系统利用根权限系统私钥进行数字签名(510)以创建 RSB。在步骤 520 中,由根权限系统提供完成的 RSB。RSB 的接收方可以是根权限能够与之通信(例如,经由测试仪 I/F 365)的 SM 内核,或者 RSB 可以在被 SM 内核最终接收之前通过任何数量的实体(例如,中间体、服务器、组件、应用、网络、存储位置 / 文件,等等)。

[0128] 图 6 是用于由 SM 被启用的 IC 中的 SM 内核来处理图 5 中生成的 RSB 的示例性方法的流程图。在步骤 600 中,在 SM 内核接收 RSB。SM 内核接着获得(610)根权限系统公钥,该公钥例如可以存储在 SM 被启用的 IC 内并且被作为软件常量供应至 SM 内核,或者可以存储在安全存储器(例如,安全存储器 310)内。

[0129] SM 内核接着利用根权限系统公钥来验证(620)RSB 的数字签名。如果数字签名验证结果(630)表明签名无效,则处理结束(690)。如果数字签名有效,则 SM 内核对包含在 RSB 中的一个或多个 SM 命令进行处理(640)。如果在处理 SM 命令时发生错误(650),则利用例如寄存器 I/F 358 或中断器报告错误(660),并且处理结束(690)。例如,如果 SM 命令对产品芯片 ID 是否落入特定范围内进行校验,并且对于 SM 内核已知的产品芯片 ID 落入该范围外,则可能发生错误。如果在处理期间发生错误,则 SM 内核确定(670)是否有任何附加的 SM 命令剩下待处理。如果有需要处理的附加的 SM 命令,则流程返回至步骤 640,并且处理继续直到所有 SM 命令都被处理为止。一旦所有 SM 命令都被处理,SM 内核就利用例如寄存器 I/F 358 或中断器来报告成功(680),并且处理结束(690)。

[0130] 图 7 是用于生成能够与 DSB 相关联的 RSB 的示例性方法的流程图。在步骤 700 中,根权限系统接收一个或多个输入参数。输入参数可以包括一个或多个 SM 命令、用于委托预期签名什么的命令模版、委托许可、委托权限系统公钥、其他数据或者它们的一些组合。委托权限系统公钥具有由委托权限系统控制的相应的委托权限系统私钥。

[0131] 如上面所讨论的,SM 命令可以包含引导 SM 内核以影响 SM 被启用的 IC 的状态的信息。另外,当 RSB 与 DSB 相关联时(例如,包含委托权限系统公钥),SM 命令可以(如与上面的只有 RSB 的情况一样)包括基于某些条件而使处理停止的命令。例如,RSB 可以包括确认在与 RSB 处理连续或许可相关联的 DSB 运行之前芯片是处于制造的某阶段、或者是在特定产品芯片 ID 范围内、或者是在特定序列号范围内、或者具有与特定组或子集相关联的设定、或者是 / 不是处于特定错误状态等等的命令。注意,把条件建立在由 SM 内核维持的状态(诸如,装置生命周期、产品 OEM 标识符、用户类型、地理区域、组标识符、零售 SKU、日期等等)之上的能力允许在控制哪个装置能够接受给定的 RSB 以及 RSB 将在这些装置上做什么时很大的灵活性。因此,DSB 可以被防止在不满足根权限系统所阐述的准则的装置上

执行。

[0132] 在一些实施例中,根权限系统还可以接收和签名指明了 DSB 的形式或内容或两者的命令模版。委托权限系统可以作为确保仅签名预期形式的 DSB 的方式来验证根权限系统的签名。在命令模版内可以是被包括的 SM 命令的描述,以及可以做出什么调节。委托权限系统中的硬件安全模块可以验证模版上的根签名、做出许可的修改(或者仅验证已经做出的许可的修改)、接着(如果成功的话)签名委托签名块(DSB)。注意,该途径许可根权限在委托上强加限制(借助于委托权限系统)。注意,委托签名上的这样的限制是由 SM 内核强加的限制的补充(例如,如果 RSB 包括确认产品芯片 ID 处于给定范围内的测试,则将在 DSB 的在该范围外侧的装置上运行时的任何接受之前发生错误)。

[0133] 委托许可典型地描述了根权限允许委托相对于 SM 内核具有的能力。例如,委托许可可以包括授权用于更新的特定特征、授权写入安全存储器 310 内的物理地址的范围、授权哪个 SM 命令可以在处理 DSB 的同时由 SM 内核执行、授权用于安全密钥的传输的目的地、授权访问一个或多个密钥总线、授权访问一个或多个外设、或者它们的一些组合。

[0134] RSB(或者,如果授权的话,DSB)可以设定在 SM 内核内的许可数据字段。这些字段可以例如被映射至特征空间内的地址。这样的设定可以持续进行除非(或者直到)他们被另一 RSB 改变或者直到芯片被复位。例如,由 SM 内核处理时的示例性 RSB 可以设定能力掩码的系列中的位,以指定某些能力是否可以行使。在另一示例中,由 SM 内核处理时的 RSB 可以对控制 SM 内核做出安全存储器 310 的布局和配置的假定的 SM 内核中的指针进行调节。

[0135] 由 SM 内核处理时的 RSB 还可以准备可供随后的 DSB 使用的数据。例如,RSB 可以引起数据被存储在数据存储模块(例如,数据存储模块 440)中,并且 DSB 可以引起该数据被从数据存储模块中检索。另外,在 RSB 的执行之前,处理器(例如,处理器 355)可以利用寄存器 I/F 358 引起数据被存储在数据存储模块内。RSB 可以引起 SM 内核检验用于与某些准则一致,并且如果满足准则的话的数据是否在数据存储模块 440 中留下该数据以供随后的 DSB 使用。在该情况下,尽管数据是由处理器而不是根权限系统提供,但是数据也依照根权限系统的批准。例如,这使得能够为装置上的固件提供未由根或委托权限签名的参数。

[0136] RSB 可以要求 DSB 签名包括一定量的 RSB 指定形式的“绑定数据”。这迫使 DSB 签名处理分别对于绑定数据改变的每个情况而进行。例如,RSB 可以引导 SM 内核以采样由随机数量的发生器生成的值,并且要求 DSB 签名包括被采样的值,这迫使 DSB 签名权限处于与 SM 内核的“现场”连接中并且防止 DSB 的重新播放。在另一示例中,RSB 能够将绑定数据设定为包括装置 ID 和生命周期状态,防止了已签名的 DSB 在其他装置上重新播放。因为绑定数据被委托权限系统并入签名内(并且因此对于委托权限系统是已知的,并且可以在被报告给安全服务 120 的委托权限系统日志中),所以 RSB 也可以为根权限希望确保的绑定数据和参数被精确地记入日志。

[0137] 在一些实施例中,由 SM 内核处理时的 RSB 能够写入与 SM 内核相关联的一次性可编程(OTP)存储器(例如,安全存储器 310)。例如,包含在 OTP 存储器内的指令可作为启动处理的一部分启用 SM 被启用的 IC 的特征 X。RSB 可以引导 SM 内核修改安全存储器 310 使得在启动处理期间特征 X 被启用或者不再被启用。另外,在一些实施例中,DSB 也可以被授予对可编程的 OTP 存储器的内容做出(典型地受限的)改变的许可。

[0138] 在步骤 710 中,输入参数被形成为根签名块,该签名块被利用根权限系统私钥由

根权限系统数字签名以创建 RSB。在步骤 720 中, RSB 被传递至例如委托权限系统或监督委托权限系统的安全服务(例如,安全服务 120)。

[0139] 图 8 是用于生成 DSB 的示例性方法的流程图。在步骤 800 中, 委托权限系统接收一个或多个委托输入参数。委托输入参数可以包括例如图 7 中生成的 RSB、用于包括在 DSM 中的一个或多个 SM 命令、其他净荷数据(加密的或未加密的)、一个或多个密钥或者它们的一些组合。SM 命令可以包括当执行时更新 SM 被启用的 IC 的特征状态的 SM 命令。SM 命令可以被接收作为由根权限系统签名的命令模版的一部分, 如早先描述的。在步骤 800 中, 委托输入参数可以由委托权限系统数字签名(利用与包含在 RSB 内的委托权限公钥对应的私钥)以创建 DSB。在步骤 820 中, DSB 被提供至例如 SM 被启用的 IC(或者直接地或者经由各种中间体)并且由 SM 内核处理。

[0140] 在未示出的一些实施例中, 委托权限系统在数字签名委托输入参数之前验证 RSB 内的委托许可。这可以例如帮助防止 RSB 被损坏或者委托权限系统已经被请求签名从根权限所授权的那些超出的一些事情的问题。

[0141] 图 9A 是用于用 SM 内核来处理图 8 中生成的 DSB(以及相关联的 DSB)的示例性方法的流程图。在步骤 900 中, 与 DSB 相关联的 RSB 在 SM 内核处被接收。SM 内核接着利用根权限公钥来验证(905) RSB 的数字签名。如果数字签名无效, 则 RSB 被拒绝并且处理结束(915)。如果数字签名有效, 则 SM 内核开始处理(912) 包含在 RSB 内的 SM 命令。

[0142] 如果一个或多个 SM 命令中的任何一个都不能处理或者以其他方式产生了错误(920), 则 RSB 被拒绝并且处理结束(915)。例如, 如果委托权限系统配置成具有受限的 SM 编程能力所在的产品芯片 ID 的范围被 RSB 中的 SM 命令指明了, 并且 SM 被启用的 IC 拥有在范围外的产品芯片 ID, 则 SM 内核将失败并且拒绝 RSB(915)。在该实施例中, 如果处理在步骤 915 结束, 并且如果相关联的 DSB 到达了, 则可以在不处理的情况下将其忽略并丢弃。在未示出的其他实施例中, SM 内核可以同时接收 RSB 和 DSB。在这样的实施例中, 如果处理在处理 RSB 的同时归因于错误而结束, 则 DSB 可以在未被处理的情况下忽略和丢弃。在未示出的其图示示例中, SM 内核可以与 RSB 的处理同时地或者在接收 RSB 之前接收 DSB。不管 SM 内核的特定实施例接收 RSB 和 DSB 的方式如何, 如果 RSB 被拒绝, 则 SM 内核可以拒绝处理(或以其他方式拒绝)任何相关联的 DSB。

[0143] 如果 RSB 内的 SM 命令被成功地处理了, 则 SM 内核从 RSB 中提取(925) 委托许可和委托权限公钥。在步骤 926 中, SM 内核接收与 RSB 相关联的 DSB。如上面所提及的, 在未示出的一些实施例中, DSB 和 RSB 可以同时或不同时地接收。

[0144] SM 内核利用包括在 RSB 中的委托权限公钥来验证(930) DSB 的数字签名。如果数字签名无效, 则拒绝 DSB 并且处理结束(935)。如果数字签名有效, 则 SM 内核从委托 DSB 中提取(940) SM 命令。SM 内核接着确定(945) 提取的 SM 命令是否被许可。SM 内核通过将提取的 SM 命令与委托许可进行比较并且对用于与包含在 RSB 中的委托许可一致的 SM 命令进行检验来做出该确定。如果提取的 SM 命令未被委托许可允许, 则不执行提取的 SM 命令、报告错误(950), 并且流程进行到步骤 960。错误可以被报告给在可以进而通知委托权限、根权限或视情况而定的其他实体的 SM 被启用的 IC、测试仪等等上运行的软件。

[0145] 如果提取的 SM 命令被许可, 则 SM 内核执行(955) 提取的 SM 命令。在未示出的一些实施例中, 可能在 SM 命令的执行期间发生错误, 在该情况下流程可以进行到步骤 950。

[0146] SM 内核接着确定 (960) 是否有任何提取的 SM 命令留下待处理。如果所有提取的 SM 命令都已经被处理了，则 SM 内核报告 (965) DSB 的成功执行。报告可以被报告给 SM 被启用的 IC 的用户、委托权限、根权限或者它们的一些组合。但是，如果附加的 SM 命令剩下待处理，则流程进行到步骤 945。

[0147] 在未示出的一些实施例中，当提取的 SM 命令未被许可并且报告了错误 (960) 时，处理接着结束并且拒绝 DSB 区块。

[0148] 图 9B 是用于通过 SM 内核来处理从 RSB 检索的 SM 命令的示例性方法的流程图。步骤 900、905 和 915 如图 9A 中所示。图 9B 中其余部分详述了处理 SM 命令 (912) 和校验来自图 9A 的结果 (920) 的步骤的示例性实施例。一旦数字签名被确认有效，图 9B 中的细节就开始。SM 内核从 RSB 提取 (970) 一个或多个 SM 命令。SM 内核确定 (975) 约束是否实际上许可提取的 SM 命令的执行。如果命令未授权，则步骤 975 触发错误。步骤 975 接着尝试运行命令，这也可能触发错误。一旦发生错误，SM 内核就报告错误 (980) 并且拒绝 RSB 的其余部分（并且结果是拒绝任何相关联的 DSB(915)）。如果提取的 SM 命令成功运行，则 SM 内核接着确定 (985) 提取的 SM 命令是否剩下待处理。如果有任何进一步的命令等候，则处理继续下一命令。一旦所有提取的 SM 命令都已经处理了，方法就行进至图 9A 中的步骤 925。

[0149] 比较测试（例如，在 RSB 中和 / 或 RSB 中）可以例如测试两个值是否大于或小于彼此、等于彼此，等等。另外，在一些实施例中，比较测试可以并入有位掩码或者其他任何其他种类的测试。比较的结果可以是立即错误，或者是随后的操作的流程控制改变（例如，诸如跳转等）或修改 / 跳过。

[0150] 在一些实施例中，委托权限系统可以被要求测试某些特征空间值。这可以在特定特征空间值对于根权限系统不可用时有用。例如，根权限系统可以希望授权委托权限系统产生对单个 SM 被启用的装置的针对例如网络中所有 SM 被启用的装置的某些特征的配置进行修改的 DSB。在该实施例中，根权限系统仅产生单个 RSB，而不是对于其特征待修改的一个或多个 SM 被启用的装置中的每一个产生不同的 RSB。注意，迫使 DSB 绑定至单个装置迫使委托权限系统对于各装置签名做出新的 DSB—由此确保了由委托权限系统强加在签名操作的数量上的限制有效地限制了委托权限能够配置的装置的数量。

[0151] 作为示例，SM 被启用的 IC 可以在处理从 RSB 提取的 SM 命令的同时将值（例如，产品芯片 ID，或随机的一次性挑战）写入中间存储位置。当 SM 内核验证 DSB 的签名时，SM 内核在签名验证处理中牵涉到的密码散列操作中并入有中间存储的内容。例如，中间存储中的值可以在计算密码散列时与 DSB 命令联系起来。如果，当 SM 被启用的 IC 验证 DSB 签名时中间存储中的值与当产生 DSB 时由委托权限系统使用的值不同，则计算出的散列将与签名的散列不匹配，并且 SM 内核可能接着拒绝 DSB。

[0152] 另外，在一些实施例中，RSB 引起 SM 内核对可以利用中间存储由 DSB 进行以保持一个或多个 SM 命令的活动进行约束或修改。在该实施例中，RSB 中的 SM 命令可以引起数据被写入中间存储。SM 内核接着验证 DSB 签名，并且如果有效，则 SM 内核接着作为命令对被写入中间存储的数据进行处理，并且执行该数据。例如，中间存储中的数据可能是命令“将值 64 写入特征地址 X”（例如，其中 X 可以配置无线电频率）的表示。通过制定整体命令，该示例中的 RSB 授权委托权限系统仅将频率设定为仅 64，而不是任何其他值。在该实施例的扩展中，RSB 可以包含允许 DSB 修改中间存储的有限部分的委托许可，由此授权 DSB 做出

命令的有限变型。例如,如果委托仅被允许改变参数的与频率相对应的最不显著的 4 位,则这将允许委托权限系统将频率设定为从 64 到 79 的任何值。

[0153] 在实施例中,SM 内核对用于过滤特征和密钥管理用的控制报文的安全时间参考进行管理。时间参考可以被维持在 SM 内核内或者可以在将时间提供至 SM 内核的单独的区块内。在该示例中,签名块(例如,RSB、DSB)可以引导密钥输出或特征调节,但仅当时间在一定时间窗内才能够使用。签名块包括引起 SM 内核进行与当前时间值的被引导的比较的命令。例如,这能够用于防止试用密钥或试用特征在试用期外被加载。对于增加的安全性,可以通过 SM 特征信号来管理和设定时间参考(例如,使得时间可追踪至安全服务器上的时钟)。在该情况下,前述 RSB 指定的绑定数据可以用于要求在与用作签名权限的根或委托权限系统的现场交互中进行时间设定。备选地,可信时间源可以通过允许参考由不可信软件调节来创建,但是其中追踪值(或者 SM 内核内部的或者外部的)监测装置时间参考是否自从时间参考经由与可信时间服务器的现场 RSB 和 / 或 DSB 交互被标志为有效的而已经被调节、断电或者复位。

#### [0154] 3.1 特征管理

[0155] 特征管理可以用于控制 SM 被启用的 IC 的配置和其他特征状态是否并且以什么方式更新。SM 被启用的 IC 的特征状态可以控制 SM 被启用的装置的能力,例如,能够启用、禁用或以其他方式安全地配置特征的操作、能够基于产品芯片 ID 来配置硬件能力、基于 SM 被启用的 IC 的地理位置来配置硬件能力、配置特性设定、允许或配置某些外部接口的使用、分路操作的某些模式的使用(例如,启用 / 禁用分路操作的某些功能性模式、修补 ROM、调节微码等等的程序错误修正模式)、启用或禁用测试模式(例如,控制诊断和调试模式)、控制特定模式或特征被激活的时间(例如,仅在制造过程期间被激活)、能够调节由特征使用的参数、调节 SM 被启用的 IC 的配置、进行审核操作以证明配置或其他信息对于 SM 内核是可访问的、在内场装置上安全地进行诊断活动、校准或调谐模拟电路以补偿处理变化、设定装置配置数据(例如,配置用于特定产品中的输入时钟和期望的操作频率的 PLL)、基于适用于特定产品或区域的规章要求来调节无线电的功率和频率、配置由内部热失效安全强加的限制(热限制可以基于不同产品中使用的封装和冷却溶液而变化)、配置电池充电电路、启用 SM 被启用的 IC 的潜在能力或更新、禁用 SM 被启用的装置上的广告报文的显示(例如,通过向软件提供配置状况)、启用内场更新至 SM 被启用的 IC 上的 CUP 等的较高操作特性,等等(或者它们的组合)。例如,控制诊断和调试模式可以临时地(例如,直到下一复位)启用调试特征。另外,在一些实施例中,特征状态是否更新取决于费用是否已经支付(例如,如由计费和报告服务 122 管理)。

[0156] SM 内核(以及 SM 被启用的 IC)的示例性架构假定特征配置设定不是秘密的,但是特征设定的更改要求特权(例如,源自根权限)。对于秘密密钥,可以另外要求保护值的秘密性,所以秘密值可以通过使用密钥管理功能性来操纵,将在下一部分中更加详细地讨论。数字签名可以用于确保特征改变(以及密钥相关的操作)仅由被授权方进行。

[0157] 特征管理可以包括在非易失性存储器(例如,安全存储器 310)中记录特征改变、启用仅直到下一复位为止被激活的特征改变、启用仅对于固定时间段(如由时钟周期计数器或实时时钟测量)有效的特征改变、启用操作的选定模式(例如,控制诊断和调试模式、PLL 配置等等)或者它们的一些组合。

[0158] 图 10 是用于 SM 被启用的 IC 的特征管理的示例性方法的流程图。在步骤 1005 中，SM 被启用的 IC 接收一个或多个签名块（例如，一个或多个 RSB、DSB 或它们的组合）。签名块包含当由 SM 被启用的 IC 中的 SM 内核处理时启用 SM 内核以更新所管理的特征状态的更新信息。信息可以例如包括一个或多个 SM 命令、一个或多个密钥或者它们的组合。SM 内核利用相应的公钥来查验（1015）数字签名的有效性。例如，如果签名块是 RSB，则 SM 内核使用根权限公钥（例如，存储在 SM 被启用的 IC 中）来查验数字签名的有效性。类似地，如果签名块是 DSB，则 SM 内核可以使用委托权限公钥（来自 RSB）来查验 DSB 的数字签名的有效性。在可选的实施例中，SM 被启用的 IC（或者包含 IC 的装置）可以联系根权限系统、委托权限系统、第三方服务器或者它们的一些组合，以检索适当的公钥或其他需要的信息。

[0159] 如果数字签名无效，则处理结束（1020）。如果数字签名有效，则 SM 内核确定（1025）当前许可是否允许所请求的特征更新。在该实施例中，许可可以从 SM 命令或者安全存储器 310、RSB、DSB 或它们的一些组合中的设定来设定。如果许可不允许特征更新，则处理接着结束（1020）。如果许可允许特征更新，则 SM 接着确定（1030）SM 命令是否被执行为永久性特征更新。（永久性特征更新是在 SM 被启用的 IC 复位之后、例如因为改变被记录在非易失性存储器中而继续的更新）。如果是，则 SM 内核视情况而定地保存（1035）SM 命令、密钥值、特征配置值或者它们的组合以对非易失性安全存储器（例如，安全存储器 310）进行永久性特征更新，并且还可选地更新（1040）SM 内核中的相应的特征状态。如果 SM 命令未被执行为永久性特征更新，则处理移至步骤 1040，更新由 SM 内核管理的特征状态并且处理完成（1045）。

### [0160] 3.2 密钥管理

[0161] 密钥管理功能性可以用于安全地传递净荷，例如秘密密钥或其他值。目的地可以包括在 SM 被启用的 IC、硬件区块或甚至包含 SM 被启用的 IC 的装置的其他部件上执行的软件。SM 被启用的 IC 包含数个永久性存储的装置特定的对称密钥（基本密钥）。基本密钥可以用于引导附加的密钥的安全传递。在接收包含净荷的签名块之后，SM 被启用的 IC 在提取净荷之前查验区块以及任何相关联的许可的签名的有效性。一旦遇到密钥管理命令，SM 被启用的 IC 就进行如下的密钥解开处理：首先从基本密钥导出传送密钥，接着使用传送密钥将包含在命令中或由命令引用的密钥解密，并且最后将经过解密的密钥传给另一硬件单元。如上面所讨论的，参见图 3，经过解密的密钥可以例如被直接地或经由提取器、密钥接口以及子提取器传给硬件单元密钥管理命令不需要在安全设施中运行；净荷可以在不可信通信信道之上被内场传递至包含 SM 被启用的 IC 的产品。

[0162] 在一个实施例中，密钥解开处理使用提供了抵抗侧信道和故障感应攻击的保护的密钥树构造。密钥树构造使能够从单个开始的密钥创建多个不同的密钥，并且所创建的密钥中的每一个都可以接着陆续地用于创建多个附加的不同密钥。密钥解开处理的可选实施例可以使用区块密码（诸如 AES 等）、非对称算法（例如 RSA），等等。

[0163] 图 11 是用于生成净荷的安全传送用的 DSB 的示例性方法的流程图。如上面所讨论的，净荷可以包括秘密密钥。在步骤 1100 中，委托权限系统接收用于其计算的基本密钥。基本密钥可以例如是全局基本密钥或者芯片特定的基本密钥。委托权限系统可以从例如 IC 制造商 110、产品供应商 125 或安全服务 120 接收基本密钥。委托权限系统还可以通过解密或以其他方式处理存储在产品中（例如，在用于 SM 内核的安全存储器 310 中）的值来确定

基本密钥。

[0164] 在各种实施例中，全局基本密钥可以由多个 SM 被启用的 IC 使用。例如，全局基本密钥可以是作为 HW 常量被提供至 SM 被启用的 IC 的根权限系统密钥。在其他实施例中，基本密钥是装置特定的密钥，例如被编程到 SM 内核内的基本密钥。在一些场合中，装置特定的密钥部分由产品芯片 ID 导出。在另一实施例中，委托权限系统获取混合密钥或者混合密钥的前体（而不是基本密钥）。例如，如果各芯片具有唯一的装置特定的装置密钥  $K_{CHIP}$ ，则根权限可以分布（例如，经由安全服务 120）给委托权限系统用于各芯片的  $F(K_{CHIP}, \text{委托 ID})$  的表格 / 数据库，其中  $F$  是诸如散列等的密码操作，允许了委托用具使用用于芯片的表格项目作为其固定密钥（或者以形成固定密钥），而 RSB 可以引导 SM 内核计算用于特定委托的委托 ID 的  $F(K_{CHIP}, \text{委托 ID})$  以到达相同值。更通常地，委托基本密钥可以被传递作为委托密钥数据库的一部分，并且利用对于 SM 内核已知的主基本密钥、或者对于 SM 内核已知或者可以被传递至 SM 内核（例如，在 RSB 和 / 或 DSB 中）的参数值（诸如委托 ID 等）以及一个或多个密钥生成功能导出。例如，混合密钥可以利用密钥梯、HMAC、散列功能或其他密钥导出方法来导出。数据库可以例如每个芯片或每多个芯片包含一个委托基本密钥。委托基本密钥可以由根权限系统生成。例如，根权限可以利用例如 AES 和一系列单向函数从万能密钥导出特定的基本密钥。以该方式的导出和密钥控制可以帮助防止较高值的密钥万一第三方不正确地管理了密钥而被损害。

[0165] 在步骤 1105（除非混合密钥已经在早先被导出，例如每上述可选实施例中的）中，委托权限系统导出混合密钥。委托权限系统可以通过使用关于之前步骤中导出的密钥的一系列的一个或多个单向函数来导出混合密钥。例如，混合密钥可以用密钥树操作、HMAC 计算、散列函数或其他密钥导出方法导出。来自基本密钥的附加的抽取可以帮助保护基本密钥不受直接攻击。

[0166] 在步骤 1110 中，委托权限系统利用一些列单向函数从混合密钥导出一个或多个传送密钥。步骤 1110 可以牵涉到对称密码术、非对称密码术、单向密码功能或者它们的一些组合。委托权限系统可以接着获取净荷密钥，例如通过从万能密码导出净荷密钥、或者从预计算的数据表格中检索净荷密钥或者在网络之上取出净荷密钥。在一些实施例中，预计算的表格可以由发布密钥的第三方（诸如对发布用于特定系统或诸如 HDCP、EMV 等协议的密钥有责任的实体）生成，或者先前由委托权限系统生成。净荷密钥可以由作为获取（1120）净荷密钥的处理的一部分的委托权限系统加密接着解密而被存储。

[0167] 在步骤 1130 中，委托权限系统利用一个或多个传送密钥将净荷密钥加密。

[0168] 在步骤 1135 中，委托权限系统利用经过加密的净荷密钥和混合密钥（或另一密钥）导出验证子。具体地，验证子可以通过将经过加密的净荷密钥和混合密钥作为输入提供至其最终输出是验证子的一系列的一个或多个单向函数。验证子使得 SM 内核（或经过加密的净荷密钥的潜在的其他接收方）能够验证经过加密的净荷密钥是有效的并且未经修改。

[0169] 在步骤 1140 中，委托权限系统接收一个或多个委托输入参数（除了在签名中牵涉到的其他值以外，其还可以包括 SM 内核以及提取器 / 子提取器最终应该将净荷传递至的位置的地址）。并且，在步骤 150 中，委托输入参数、经过加密的净荷密钥以及验证子接着利用委托权限系统私钥被委托权限系统数字签名，以创建 DSB。在步骤 1160 中，提供了 DSB。

[0170] 备选地,在未示出的一些实施例中,步骤 1135 被省略,并且于是在步骤 1150 中,验证子未被数字签名并且不是被提供的 DSB 的一部分 (1160)。

[0171] 图 12 是用于通过 SM 内核来处理包括了净荷的一个或多个签名块的示例性方法的流程图。例如,一个或多个签名块可以是 RSB 和相关联的 DSB(例如,经由图 11 的处理生成)。在另一实施例中,净荷在没有 DSB 的情况下可以被包括在 RSB 内。

[0172] 在步骤 1200 中,在 SM 内核处接收一个或多个签名块(例如,一个或多个 RSB、DSB 或者它们的组合)。还可以接收附加的未签名的数据(诸如具有验证子的经过加密的净荷等)。这些元素可以被同时或不同时地接收。

[0173] 在步骤 1210 中,SM 内核验证一个或多个签名块的数字签名,并且验证任何 DSB 的委托许可是否有效。验证处理与参照图 9A 和图 9B 进行上述验证处理相同。如果用于一个或多个签名块的数字签名无效,或者委托许可无效,则 SM 内核拒绝 (1215) 一个或多个签名块并且处理结束 (1250)。然而,如果数字签名和许可有效,则 SM 内核利用对 SM 内核已知的基本密钥(例如,全局密钥或委托基本密钥)、例如利用用于生成混合密钥的相同算法(例如,与图 11 有关的描述)来导出 (1220) 混合密钥。SM 内核接着可以利用基本密钥和图 11 中的用于生成传送密钥的相同算法来导出 (1225) 传送密钥。

[0174] SM 内核从 DSB(或者从 RSB 或从未签名的数据,如果该 RSB 或未签名的数据是经过加密的净荷存在所在位置的话)中提取 (1230) 经过加密的净荷密钥,并且采用图 11 中用于生成传送密钥的相同算法利用经过加密的净荷密钥和混合密钥导出 (1235) 验证子。SM 内核可以接着确定 (1240) 验证子是否正确。SM 内核通过将在步骤 1235 中导出的验证子与用净荷密钥(例如,在 DSB 中)接收到的验证子进行比较来做出该确定。如果验证子不匹配,则这是个错误 (1215) 并且处理结束 (1250)。如果验证子匹配,则 SM 内核利用传送密钥将经过加密的净荷密钥解密 (1245) 并且处理结束 (1250)。

[0175] 备选地,在未示出的一些实施例中,步骤 1235 和 1240 被省略,并且于是经过加密的净荷密钥可以在不使用验证子的情况下被解密。步骤 1235 和 1240 还可以用验证验证子的其他方法取代,例如通过验证没有单独进行计算的验证子(诸如通过验证 RSA、EC-DSS 或验证子中包含的其他数字签名)。

[0176] 另外,在一些实施例(未示出)中,经过加密的净荷密钥不是从 DSB(1230) 中提取,但是可以(例如)从 RSB(或其他签名块)、从安全存储器(例如,安全存储器 310)检索、与检测器 I/F(例如,寄存器 I/F 358)之上的签名块单独地被提供或者从 SM 内核内的私有存储器检索。

### [0177] 3.3 审核

[0178] 在各个时间都可能期望验证 SM 被启用的 IC 的状态。审核能力可以例如用于确保先前的特征管理命令已经被正确地施加至装置,或者用于验证装置的效力。例如,如果客户请求启用了特征的交易的退款,则可能期望验证特征在退款购买价格之前已经被禁用。

[0179] 通常审核处理可以包括从审核实体接收挑战。该挑战可以是随机参数,并且被包括以允许响应于特定请求而生成的确认。在接收到挑战之后,SM 被启用的 IC 可以生成如下证明演示:(1)它知道秘密密钥(例如,审核命令中指定的基本密钥),并且(2)它知道或者适当的状态的值或者状态的性质(例如,它满足挑战中指定的准则)。例如,响应于审核命令,示例性 SM 内核可以计算出作为秘密密钥的以及正被审核的特征状态中的位的

函数的审核证明。在审核计算中包括秘密密钥防止不知道秘密密钥的对手伪造审核响应。审核实体最终验证响应。状态审核可以使用对称密码术（诸如报文认证码等）并且 / 或者公钥密码术（诸如数字签名等）以保证证明安全。

[0180] 在示例性实施例中，审核请求可以可选地包含命令签名者也知道选定的秘密密钥的验证子演示。如果该验证子与内部计算出的参考匹配，则 SM 内核例如可以仅产生审核证明。关于请求的验证子可以帮助防止未授权方调用审核命令。

[0181] 包括了 SM 内核内部特征的任何特征状态的值都可以潜在地被审核。例如，为了使用验证先前的特征管理命令已经被正确地应用至 SM 被启用的 IC 的审核功能性，先前的命令可以设定表明了其成功的内部位，接着该位可以随后被审核。如果审核实体的目的仅是验证包含了 SM 内核（但不是其状态）的装置的效力，则任何特征状态都不必要被并入到响应中。

[0182] 审核可以利用 SM 内核可用的任何密钥来进行，包括全局密钥、装置特定的密钥、由一些列 SM 被启用的 IC 共享的密钥或者它们的一些组合。在利用装置特定的密钥的实施例中，密钥的数据库可以做成对于审核员（例如，通过根权限、IC 制造商、产品供应商、安全服务，等等）是可用的，以便于审核响应的验证（以及可能的审核请求的创建）。

#### [0183] 4. 配置器和编译器功能性

[0184] 配置器系统（例如，配置器系统 280）可以在 SM 被启用的 IC 的设计过程期间使用。配置器系统在 ASIC 设计过程期间被操作，以对 SM 内核管理的特征空间和密钥的到 IC 中的特征以及其他目的地或使用的映射进行追踪并使其自动化。图 13A 是用于在 SM 被启用的 IC 的设计过程期间利用配置器系统的示例性方法的流程图。在步骤 1310 中，配置器系统接收配置器输入数据。配置器输入数据可以包括一个或多个配置器输入文件、硬件（“HW”）常量或它们的一些组合。

[0185] 一个或多个配置器输入文件限定了关于用于 SM 被启用的 IC 的期望的配置的信息。例如，这些文件可以指定如下这样的事物：用于应该被传递至各特征的配置值的名称和大小（例如，位的数量）、配置值的在特征地址空间内的分组或位置、用于配置值的默认（例如，上电）值、用于安全密钥总线目的地的名称和属性、安全密钥总线属性（诸如用于目的地的密钥大小等）、安全存储器映射属性（诸如关于安全存储器 310 的布局的信息）或它们的一些组合。

[0186] HW 常量可以被包含在配置器输入文件或者被单独地接收。输入配置器的 HW 常量的示例可以包括例如产品芯片 ID、来自根权限（潜在地包括根权限公钥）的一个或多个密钥、来自委托权限的一个或多个密钥、一个或多个基本密钥、一个或多个附加安全密钥、错误校正数据等等。

[0187] 在步骤 1320 中，配置器系统生成 IC 设计文件。这些 IC 设计文件可以包括提取器硬件限定、子提取器硬件限定以及状态缓存数据（例如，IC 配置映射信息）。在一些实施例中，在先的 IC 配置映射信息可以在步骤 1310 中被包括有配置器输入数据，以使并入了对 SM 被启用的 IC 设计做出的改变时的现有电路设计的修改最小化。在该情况下，配置器力图标识出最小冲击的方式来进行请求的改变。例如，如果新的值待被插入到特征地址空间内，则这可以包括利用先前的映射来标识出用于插入（例如，与重新创建用于现有值的位置相反）的先前未使用的位置。同样，如果值被从特征地址空间中去除，则配置器可以使用先前

的映射信息以留下与重新定位剩余特征相反的间隙。

[0188] 芯片设计被锁定（步骤 1330），例如因为芯片设计被准备用于大规模的制造。在这一点上，影响制造中使用的掩码设定的配置器输出不能再被改变。图 13B 是在芯片设计被提交用于制造之后可以如何利用配置器的示例性处理的流程图。

[0189] 在步骤 1340 中，配置器系统接收配置器可操作性输入数据。配置器可操作性输入数据可以包括图 13A 中生成的 IC 配置映射以及附加的数据（例如，在可操作性 SM 配置文件中）。可操作性 SM 配置文件可以描述例如关于与特定 SM 被启用的 IC 相关联的特征和密钥可以如何使用的策略、对命名约定做出的改变、用于安全存储器 310 的 SM 内核的使用的布局和配置约定以及内部特征的到特征地址的映射。

[0190] 在步骤 1350 中，配置器系统在内部生成可操作性配置映射。因为图 13B 中的步骤可以比图 13A 中的那些步骤晚地进行，所以在步骤 1350 处生成的映射可以是能够比图 13A 期间准备的映射更加全面且最新的特征地址范围的映射，而图 13B 中的处理通常必须假定实际影响芯片硬件的来自 13A 的输出不能被改变。

[0191] 在步骤 1360 中，配置器系统从其可操作性配置映射生成映射文件。这些映射文件包括一个或多个命令映射文件以及一个或多个固件映射文件。命令映射文件是例如用于将命令映射成为能够由 SM 内核理解的形式的文件。例如，如果根权限系统希望将特定配置值输送至给定特征，则该文件可以帮助根权限系统标识与该配置值和特征对应的特征空间地址。固件映射文件是包含软件开发（例如，C 或 C++ 标头和源文件，等等）所需的限定和结构的文件。在一些实施例中，可操作性配置映射可以在步骤 1340 中包括有配置器可操作性输入数据，以使当并入对可操作性输入数据做出的附加改变时的现有可操作设计的修改最小化。

[0192] 另外，在一些实施例中，配置器系统生成文档文件。文档文件提供 SM 被启用的 IC 设计的概要，诸如特征空间中的分配的命名以及相关联的地址的列表、该配置值被发送至各特征的列表、关于所支持的密钥的信息、用于特征地址空间中的值的默认值。另外，文档文件可以包括软件组件的设计中使用的环境和构造原理。文档文件可以以诸如 XML、HTML、text、PDF、WORD 等的格式输出。

[0193] 5. 可操作性生态系统

[0194] 5.1 安全存储器命令分段和上电处理

[0195] 在示例性实施例中，命令分段区域存在于作为 SM 被启用的 IC 的一部分的安全存储器 310 内。该区域对由 SM 被启用的 IC 在各复位上执行的 SM 命令进行保持。储存的 SM 命令在分段中被组织，并且可以用于影响特征空间中的值的永久性设定以及期望 SM 被启用的 IC 在各复位上执行命令（例如，传递诸如固件解密密钥等的密钥）和 / 或在 SM 被启用的 IC 内永久性地携带配置操作的其他情况。

[0196] 安全存储器典型地是永久性的并且在一些实施例（诸如使用一次性可编程存储器的那些等）中不可以被容易地重写，这可能使提高坚固性的措施成为必要。一个可能的故障是“撕裂（tearing）”，这是例如归因于电源故障而在写入处理期间的中断。期望被中断的命令分段写入不会致使 SM 被启用的 IC 不能在将来的复位上使用。另一可能的故障是存储在安全存储器中的数据例如归因于硅劣化或外部条件的损坏。再次期望冲击最小并且单个损坏事件应该不可能致使 SM 被启用的 IC 不可用。还期望安全存储器的损坏（例如作

为攻击的一部分)不会启用在SM被启用的IC的操作上的由SM内核强加的任何约束的环境。

[0197] SM命令可以包含控制SM内核写入安全存储器的方式的信息。例如,有可能是防撕裂的标志(防撕裂模式)、或在错误上恢复的标志(错误上恢复模式)或者组合。

[0198] 当防撕裂模式被激活时,示例性SM内核在写入命令分段的处理(或其他写入操作)开始时将“跳过字符”写入安全存储器。如果写入未完成,则跳过字符引起SM内核在随后的复位中认出它(例如,使得能够跳过包含部分被写入的数据的区域)。在写入跳过字符之后,SM内核可以写入净荷(例如,主命令分段内容),并且接着最后擦掉(例如,通过将字中的所有位设定为1的值)跳过字符。当未使用防撕裂模式时,SM被启用的IC不写入跳过字符,这节约了安全存储器的一个字符,但是意味着如果写入未完成则SM内核可能记住在随后的复位上的严重故障。(严重故障可能引起SM内核进入SM被启用的IC所进入的功能缩减的状态,例如因为继续进行操作通常可能会危及安全。)一旦擦掉了跳过字符,分段变成强制性的并且将用在各随后的复位上(即,如果在跳过字符被擦掉之后当读取分段时遇到不可改正的问题,则SM被启用的IC将引发严重故障)。是否使用防撕裂模式的选择可以取决于编程环境,例如禁用防撕裂模式的提高了的效率可以在受控的工厂环境中是优选的,而防撕裂可以对于内场写入是强制性的。

[0199] 对于错误上恢复模式,SM被启用的IC在命令分段标头中设定标志,如果在从安全存储器中读取分段时有问题,则该标志可接受忽略命令分段。例如,错误上恢复标志可以设定在启用SM被启用的IC的能力的分段上。如果SM被启用的IC跳过分段,则因为不能从安全存储器中读取,同时SM被启用的IC的能力可能比分段被正确读取和处理时的低,所以没有创建安全风险。

[0200] SM被启用的IC可以既不允许防撕裂标志和错误上恢复标志中的一个也不允许两者被指定用于写入安全存储器的任何给定的分段(或其他数据值)。SM被启用的IC也可以要求对于安全存储器的所有写入使用模式的特定组合。

[0201] 在复位之后,SM内核由于被存储在其安全存储器(例如,安全存储器310)中的命令分段引导而自动地将特征和密钥状态初始化。图14是用于SM被启用的IC的初始化的示例性方法的流程图。

[0202] 在步骤1405中,SM被启用的IC被上电或复位。SM内核可以作为该步骤的一部分被复位。SM内核接着检索(1410)与SM被启用的IC相关联的产品芯片ID以及完整性校验值。(完整性校验值可以是与例如奇偶校验、汉明码等相关联的值)。SM被启用的IC进行完整性校验(1415)以确定是否发生完整性错误(例如,产品芯片ID或完整性校验值已经被损坏)。如果发生了完整性错误,则报告错误(1420),处理被中止(1445)并且SM内核可以进入“严重故障”状态。如果未发生完整性错误,则SM内核从安全存储器检索(1425)命令分段。

[0203] SM内核以可预知的顺序对包含在安全存储器中的命令分段进行处理。例如,分段可以连续地位于安全存储器中,或者各分段可以包含待处理的下一分段的存储器地址。在一些情况下,错误(1430)可能引起SM被启用的IC不能可靠地确定待处理的下一命令分段的定位,在该情况下,内核可以尝试利用撤退机制(例如,搜索已知的标头值)来定位下一分段,或者将其处理为严重故障。如果未发生错误,则SM内核执行(1435)命令分段中的命

令。SM 内核接着确定 (1440) 是否有任何附加的命令分段被留下来待执行。如果是，则流程移至步骤 1425。

[0204] 如果没有命令分段留下，则 SM 内核通知 (1455) 系统外部（例如，处理器 355、SM 被启用的 IC 的特征或其他部分、或者并入有 SM 被启用的 IC 的装置）初始特征状态准备就绪。该通知可以由 SM 被启用的 IC 用来将芯片的其他部分的启动排序，例如，通过保持 SM 被启用的 IC 的除 SM 内核以外的所有部分处于复位来确保来自 SM 内核的必要值在其他组件需要他们之前准备就绪。处理接着结束（步骤 1460）。

[0205] 返回参见步骤 1430，如果发生错误，则 SM 被启用的 IC 确定是否许可跳到下一命令分段 (1445)。例如，命令分段的标头可能包含指示 SM 内核跳过有问题的命令分段的跳过字符或错误上恢复标志。如果许可跳过有问题的命令分段，则 SM 被启用的 IC 可以报告没有致命错误 (1450)（例如，通过保存错误信息用于以后分析）并且移至步骤 1440。如果 SM 被启用的 IC 确定不许可跳过有问题的命令分段，则报告更严重的错误 (1420)，并且处理被中止 1445。

[0206] SM 内核可以例如在图 14 中描述的初始化处理之前、期间或之后将基本密钥初始化。为了最大的特性和灵活性，SM 内核可以仅将启动期间进行的命令分段所要求的基本密钥初始化，接着在 SM 被启用的 IC 的其余部分被释放以启动之后将余下的基本密钥初始化。

[0207] 在一些实施例中，安全存储器中的错误（例如，存储器完整性错误）可以由根权限系统修复。错误可能是由在先 RSB 或 DSB 写入的。根权限系统可以发送包含允许 SM 被启用的 IC 跳过引起错误的命令分段的重写命令的 RSB。另外，RSB 可以包含替换或校正故障命令分段的附加的 SM 命令。另外，在一些实施例中，如果安全存储器中的错误数据是由来自委托权限系统的 DSB 写入的，则不同的委托权限系统可以发送包含允许 SM 被启用的 IC 跳过引起错误的命令分段的重写命令的 DSB。另外，DSB 可以包含进行由故障命令分段事先处理的任务的附加 SM 命令。

#### [0208] 5.2 个性化

[0209] 个性化是指在制造期间将密钥（例如，装置特定的）和数据（例如，命令分段）编程到 SM 被启用的 IC 内。个性化的秘密密钥可以用于密钥管理和审核功能性。首先编程到 SM 被启用的 IC 内的值中的一个可以是产品芯片 ID。

[0210] 密钥信息可以被存储为密钥拆分。在初始化期间，SM 内核从例如密钥拆分、包含在网表中的信息或从两者重构装置密钥。例如，P1 密钥拆分可以作为在装置中编程的第一密钥拆分在晶片测试时被编程。P2 密钥拆分可以在封装模具测试时被编程。P1 和 P2 密钥拆分通过 SM 内核被组合以形成基本密钥。组合函数可以选择为使得或者 P1 密钥拆分或者 P2 密钥拆分（但不是两者一起）的知识对于确定基本密钥都是不充分的。另外，一个或多个附加的密钥拆分可以在装置组装期间被存储并且可以由 SM 内核使用以确定附加的基本密钥。例如，产品制造商可能希望作为其制造过程的一部分存储对于 IC 提供商或 IC 制造商未知的密钥。除了个性化数据以外，SM 被启用的 IC 可以被编程有唯一的产品芯片 ID、制造追踪 / 日期信息、批次 ID、晶片 ID、产品类型、装置历史数据以及其他信息的所以方式。

[0211] 图 15 以框图形式图示了示例性个性化处理。在步骤 1510 中，委托权限系统得到待编程到 SM 被启用的 IC 内的信息。信息可以包括例如一个或多个基本密钥、一个或多个

密钥拆分（例如，P1、P2，等等）、产品芯片 ID 或者它们的一些组合。待编程的信息可以从耦合至委托权限系统的安全存储器或安全装置（例如，智能卡或 HSM）得到。

[0212] 在步骤 1520 中，委托权限系统将包含适当的存储器写入命令的 DSB 转送至装置测试仪。被转送的信息可以被加密。装置测试仪将 DSB（与其随附的 RSB 一起）转送至 SM 被启用的 IC，在那里被接收、验证并且（如果有效）由 SM 内核执行对存储器进行编程。

[0213] 在步骤 1530 中，委托权限系统可以用表明了一个或多个 SM 被启用的 IC 被成功个性化了的信息来更新审核日志，并且处理结束（1540）。如先前所描述的，这些审核日志可以接着被转送至安全服务 120。

[0214] 另外，输入到 SM 被启用的 IC 的任何密钥都可以处于未加密或已加密的形式。SM 被启用的 IC 和 / 或 SM 内核可以支持用于个性化的加密密钥转送的一个或多个机制。例如，SM 内核可以使用先前编程的密钥（例如，来自根权限的一个或多个密钥、来自委托权限的一个或多个密钥、嵌在硅内的一个或多个基板密钥、一个或多个附加的安全密钥，等等）将待编程的数据解密。另外，SM 内核可以允许利用非对称加密进行会话密钥的更换或生成，例如，以便产生与能够使用共享密钥的委托权限系统共享的密钥以在转送至 SM 被启用的 IC 之前将个性化密钥加密。会话密钥由 SM 内核使用以解密待编程的密钥。在一些实施例中，该协议可以通过将会话密钥与对于 SM 内核可用的附加对称密钥值组合而被扩展，例如，以在 SM 内核与个性化中牵涉到的外部装置（例如，委托权限系统）之间提供相互认证。

[0215] 密钥转送机制中的任何一个都可以独立于各个性化步骤来选择。另外，SM 被启用的 IC 不一定需要在密钥被个性化的顺序上强加任何约束，允许了从相同原始掩模集产生的芯片能够对于不同应用或客户以不同的序列进行个性化。

[0216] 即使在进行任何个性化之前，委托权限系统也可以能够产生更新了特征状况的 DSB 例如以供测试。在一个实施例中，SM 内核生成了被发送至委托权限系统的随机挑战值。委托权限系统生成并发送被绑定至挑战值并根据期望在非永久性基础上进行特征管理、密钥管理或两者的 DSB。例如，委托权限系统可以被启用 SM 被启用的 IC 的一个或多个特征，直到下一复位为止。因此，允许了 SM 被启用的装置的操作能够被测试。因此，即使芯片的安全存储器被完全损坏或者未被编程，也仍然能够进行安全操作。

[0217] 5.3 对 SM 被启用的装置的特征状况的内场更新

[0218] SM 被启用的装置的用户可以能够请求特征状况的更新。授权这些改变的报文（例如，RSB/DSB）可以是芯片特定的或者以其他方式受限，使得他们可以在不可信信道（诸如因特网等）之上被安全地发送。商人、系统操作员、装置供应商以及装置制造商也可以请求更新 SM 被启用的 IC 中的特征的命令。在一些情形中，请求独立于特征更新通信所使用的方法被转送至 SM 被启用的装置。例如，能够预先计算提供某些特征能力的解锁的一些列报文，其中各报文被制定用于不同的特定产品芯片 ID。该制定的列表可以由不与根权限系统或委托权限系统直接相连的服务器存储。视情况而定（诸如在接收到支付之后等），预计算列表中的实体可以被释放至 SM 被启用的装置。

[0219] 图 16 是用于对针对 SM 被启用的 IC 进行特征更新的请求进行授权的示例性方法的流程图，其中更新由委托权限系统（例如，委托权限系统 222）授权。

[0220] 在步骤 1600 中，委托权限系统接收更新与 SM 被启用的 IC 相关联的特征状态的请求。请求可以是在网络之上的报文、电子邮件、经由门户网站接收的命令、电话请求、SMS 报

文,等等。另外,在一些实施例中,请求可以来自属于处理请求的委托权限系统的子系统。(例如,从属者可以通过确认用户数据库或支付中的凭证来认证请求,接着将经批准的请求发给主委托权限系统。)

[0221] 在步骤 1610 中,委托权限系统做出是否授权该请求的确定。例如,委托权限系统可以为了信息或协助而联系第三方(例如,计费和报告服务 122,或安全服务 120)。如果请求未被批准,则委托权限系统接着将授权失败报告(1620)给用户并且处理结束(1660)。例如,委托权限系统可以发送电子邮件给用户,表明授权失败以及失败的原因。

[0222] 如果,授权请求被批准,则委托权限系统得到(1630)RSB。RSB 可以从根权限系统或安全服务检索,或者如果先前接收的,则 RSB 可以从委托权限系统内部的(或以其他方式相关联的)存储器检索。

[0223] 委托权限系统接着创建(1640)DSB。DSB 可以例如利用参照图 8、图 9A、图 9B 和图 11 进行的上述多个处理中的一个处理或一部分处理来创建。

[0224] 委托权限系统提供(1650)DSB 并且处理结束(1660)。例如,委托权限系统可以经由网络(例如,蜂窝式或因特网)将 DSB 传输至用户的 SM 被启用的装置。或者,在一些实施例中,委托权限系统做出用户可用的 DSB 以供下载(例如,通过张贴在安全网站上)。

[0225] 图 17 是用于对针对 SM 被启用的 IC 进行特征更新的请求进行授权的示例性方法的流程图,其中更新由根权限系统(例如,根权限系统 217)授权。

[0226] 在步骤 1710 中,根权限系统接收更新与 SM 被启用的 IC 相关联的特征状况的请求。请求可以是在网络之上的报文、电子邮件、经由门户网站接收的命令、电话请求、SMS 报文,等等。例如,在一些实施例中,请求可以来自属于处理请求的委托权限系统的子系统。(例如,从属者可以通过确认用户数据库或支付中的凭证来认证请求,接着将经批准的请求发给主委托权限系统。)。请求可以来自委托权限系统。

[0227] 在步骤 1720 中,根权限系统确定是否该授权请求(这可以包括与用于信息或协助的第三方联系)。如果请求未被批准,则根权限系统接着报告(1730)授权失败并且处理结束(1760)。

[0228] 如果授权请求被批准,则根权限系统接着创建(1740)RSB。在该实施例中,RSB 包含引导 SM 内核更新其特征状态的信息。RSB 可以例如利用参照图 5 或图 7 进行的上述处理来创建。

[0229] 根权限系统接着提供(1750)RSB 并且处理结束(1760)。

[0230] 现在将讨论本公开的各种实施例的示例。

[0231] 根据示例 #1,方法可以包括:由集成电路的安全管理器接收根签名块;由安全管理器利用秘密密钥来验证与根签名块相关联的签名;由安全管理器从根签名块提取命令;由安全管理器执行提取的命令,其中所执行的命令适用于集成电路的操作。

[0232] 根据示例 #2,方法可以包括:由集成电路的安全管理器接收委托签名块;由安全管理器标识与委托权限系统相关联的委托许可和密钥;由安全管理器利用与委托权限系统相关联的密钥来验证与委托签名块相关联的签名;由安全管理器从委托签名块中提取命令;由安全管理器利用委托许可来验证提取的命令被许可;并且由安全管理器执行提取处的命令,其中所执行的命令适合于集成电路的操作。

[0233] 根据示例 #3,方法可以包括:由集成电路的安全管理器接收用于更新集成电路的

多个特征中的特征的状态的命令；由安全管理器确定特征的状态的更新是否是永久性的；并且如果更新是永久性的，则将命令保存至存储器，并且执行用于更新特征的状态的命令。在一个实施例中，特征的状态根据包括了时间相关的因素、或者集成电路的特点或者装置的特点在内的一或多个因素来更新。

[0234] 根据示例 #4, 方法可以包括：由集成电路的安全管理器接收适合于集成电路的特征的状态的挑战，挑战接收自审核系统；响应于挑战，由安全管理器计算出作为秘密密钥和特征的状态的函数的审核证明值；并且将审核证明值提供至审核系统。

[0235] 根据示例 #5, 方法可以包括：接收包括了配置器输入文件和硬件常量的配置器输入数据；并且利用输入数据生成集成电路设计文件，其中集成电路设计文件包括提取器硬件限定、一个或多个子提取器硬件限定以及状态缓存。

[0236] 根据示例 #6, 方法可以包括：接收限定了用于集成电路的特征和密钥的策略的配置器可操作性输入数据；利用配置器可操作性输入数据生成用于集成电路的可操作配置映射；并且从可操作性配置映射创建映射文件。

[0237] 根据示例 #7, 方法可以包括：一旦集成电路的上电或复位，就由集成电路的安全管理器接收完整性校验值；由安全管理器通过处理安全存储器中的命令分段来进行完整性校验；并且基于完整性校验值来确定命令段中的任何一个是否具有完整性错误。

[0238] 根据示例 #8, 方法可以包括：由集成电路的安全管理器追踪从实体接收到的命令；将命令与相应的实体相关联；并且基于从各个实体接收到的命令对实体中的每一个进行计费。

[0239] 在本公开中，“计算机”可以包括一个或多个处理器、存储器、数据接口、硬件安全模块、显示器或它们的一些组合。处理器可以是单个或多个微处理器、现场可编程门阵列 (FPGA) 或者能够执行特定指令集的数字信号处理器 (DSP)。由计算机进行的方法中的一些可以利用能够存储在如下介质上的计算机可读指令植入：所述介质是诸如软盘、硬盘、CD-ROM (压缩盘 - 只读存储器) 以及 MO (磁光)、DVD-ROM (数字通用盘 - 只读存储器)、DVD-RAM (数字通用盘 - 随机存取存储器) 等的有形非易失性计算机可读介质，或者半导体 (例如，ROM 或闪存) 存储器。备选地，方法中的一些可以在硬件组件或者诸如例如 ASIC、专门目的的计算机或者通用目的的计算机等的硬件与软件的组合中实现。一些实施例可以不仅在集成电路内而且在计算机可读介质内实现。例如，这些设计可以存储在与用于设计集成电路的软件设计工具相关联的计算机可读介质上或者嵌入其内。示例包括 VHSIC 硬件描述语言 (VHDL) 网表、Verilog 寄存器传输级 (RTL) 网表以及晶体管级 (例如，SPICE 或 SPICE 相关的文件) 网表。注意，这样的网表可以被合成以及是能够合成的。计算机可读介质还包括具有诸如 GDS-II 文件等的布局信息的介质。此外，用于集成电路设计的网表文件或其他计算机可读介质可以用在模拟环境中以进行如上所述的设计的方法。

[0240] 可以做出上述实施例的某些改写和修改。因此，上面讨论的实施例被视为说明性的并且不是限制性的。本申请的实施例不限于任何特定的操作系统、移动装置架构、服务器架构或者计算机编程语言。

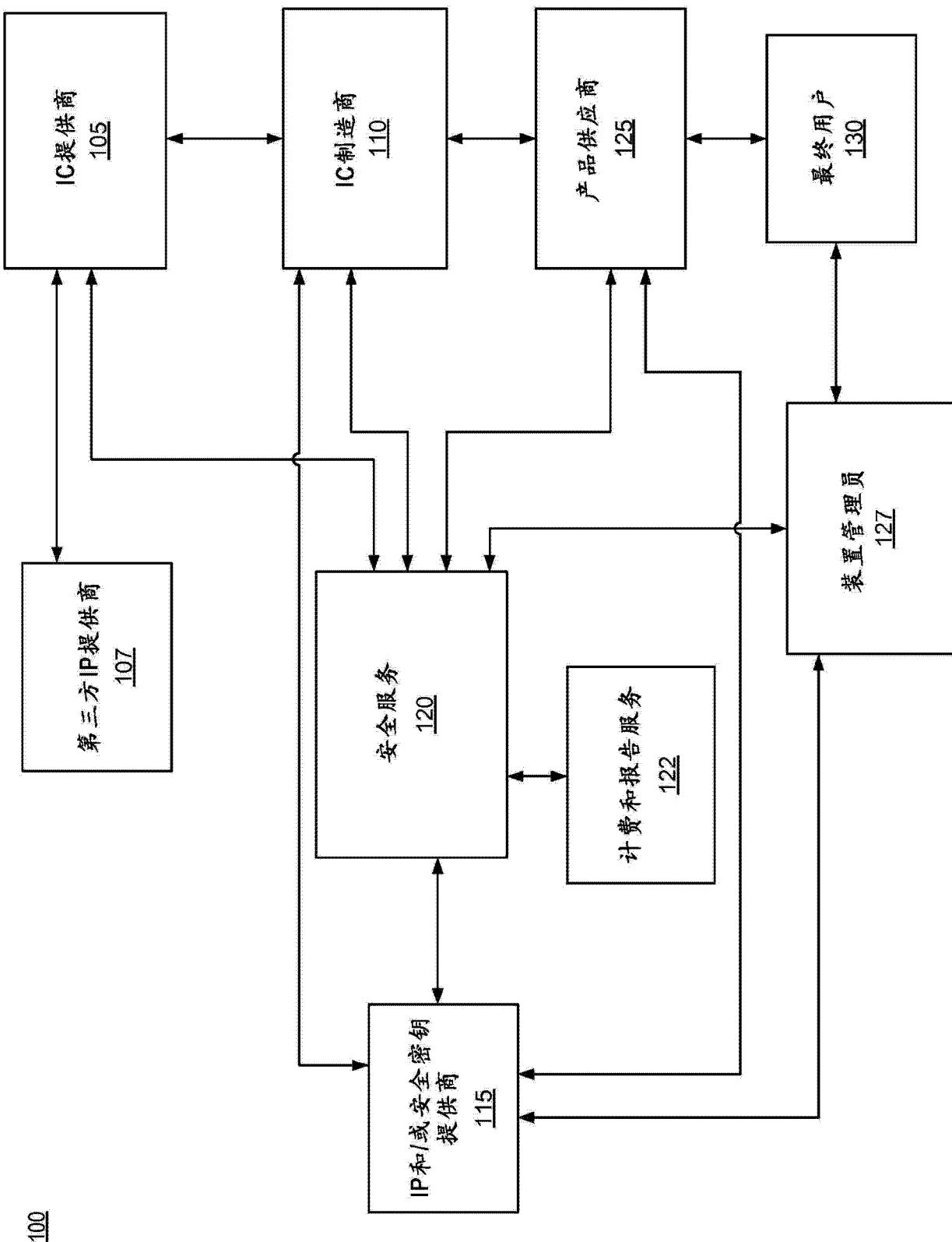


图 1A

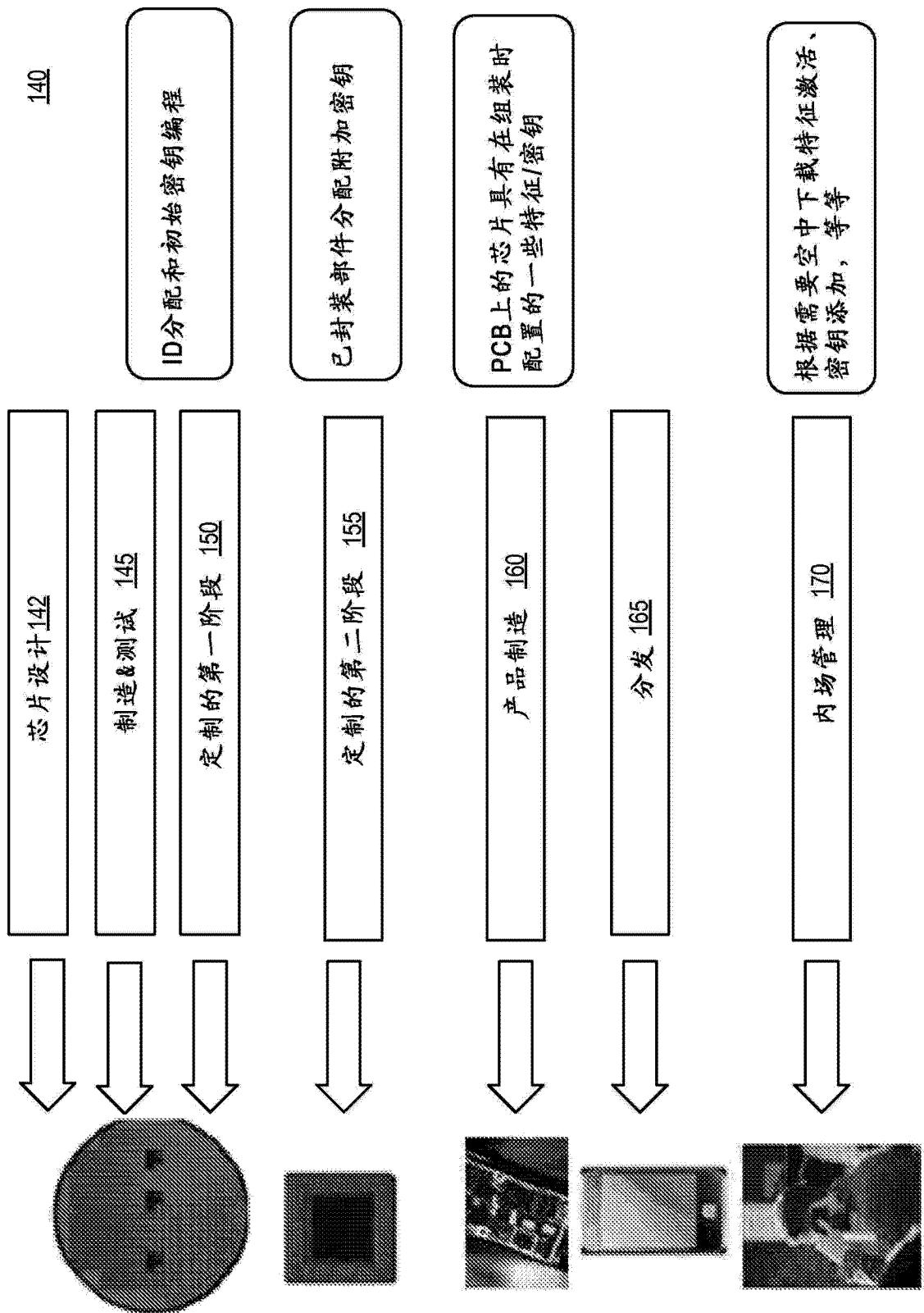


图 1B

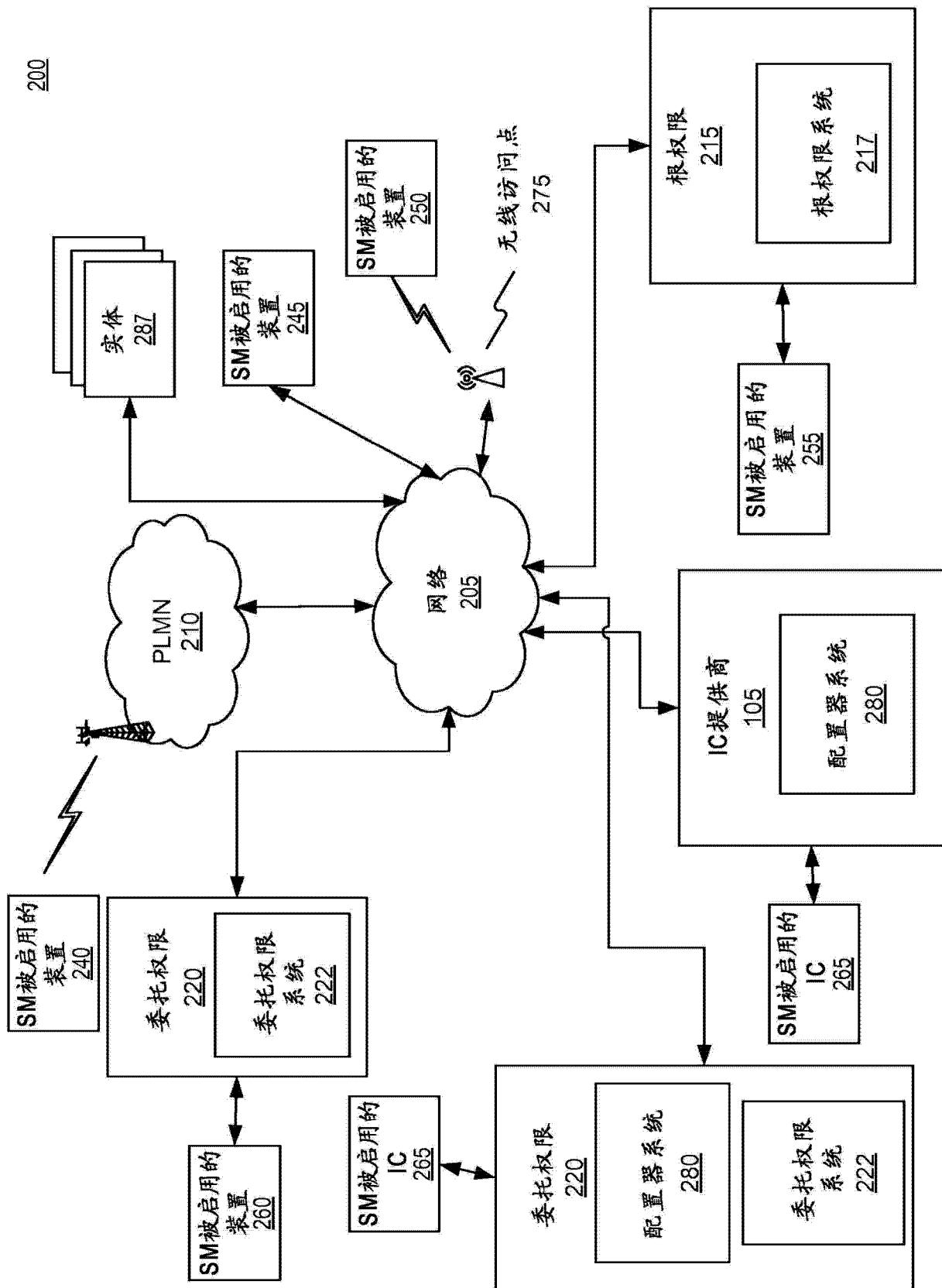


图 2A

	<u>290</u>	<u>295</u>	
0		启用 GPS	
1		启用 Wi-Fi	
2		启用 蓝牙	
3...10		PLL配置 (8位)	
		●	
		●	
		●	
n		第N个值	

图 2B

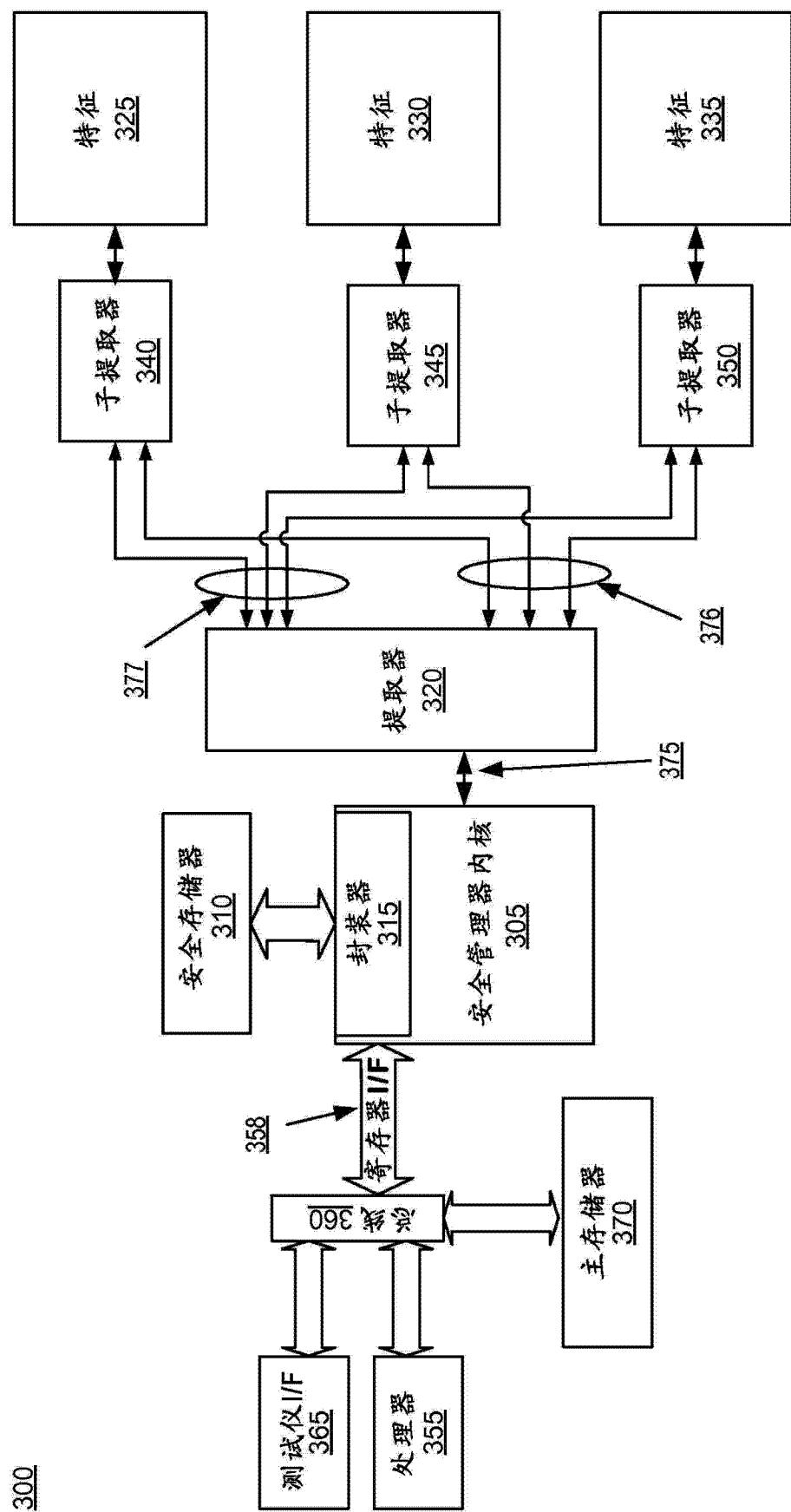


图 3

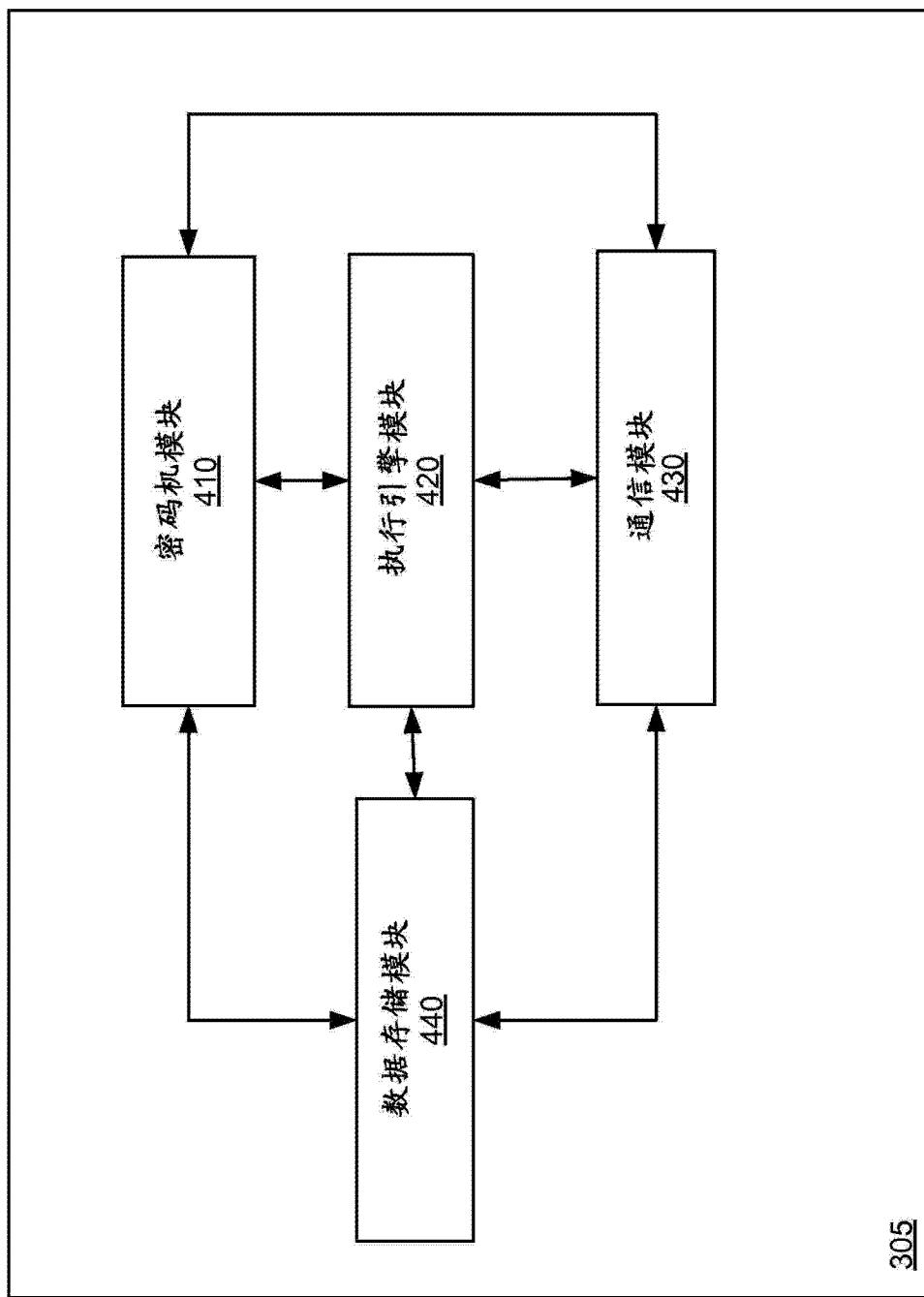


图 4

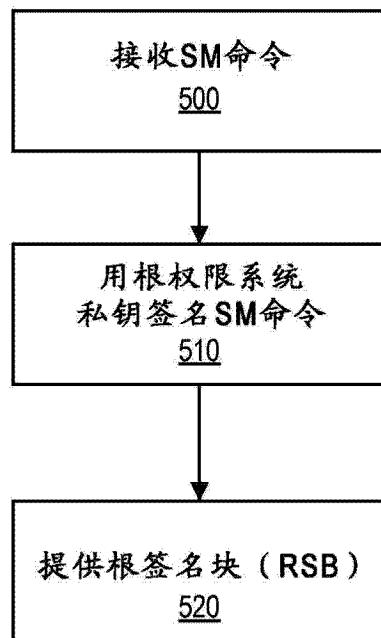


图 5

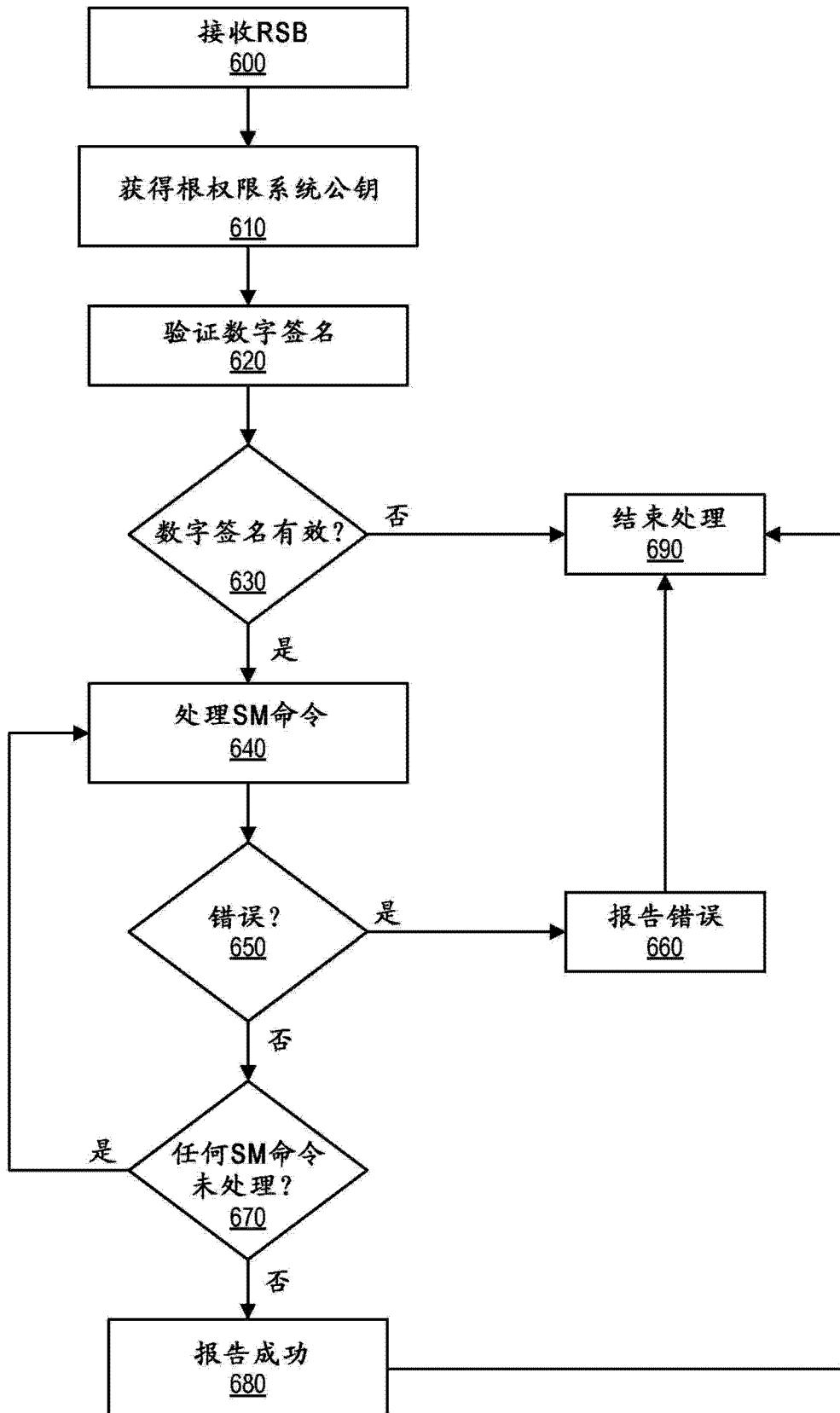
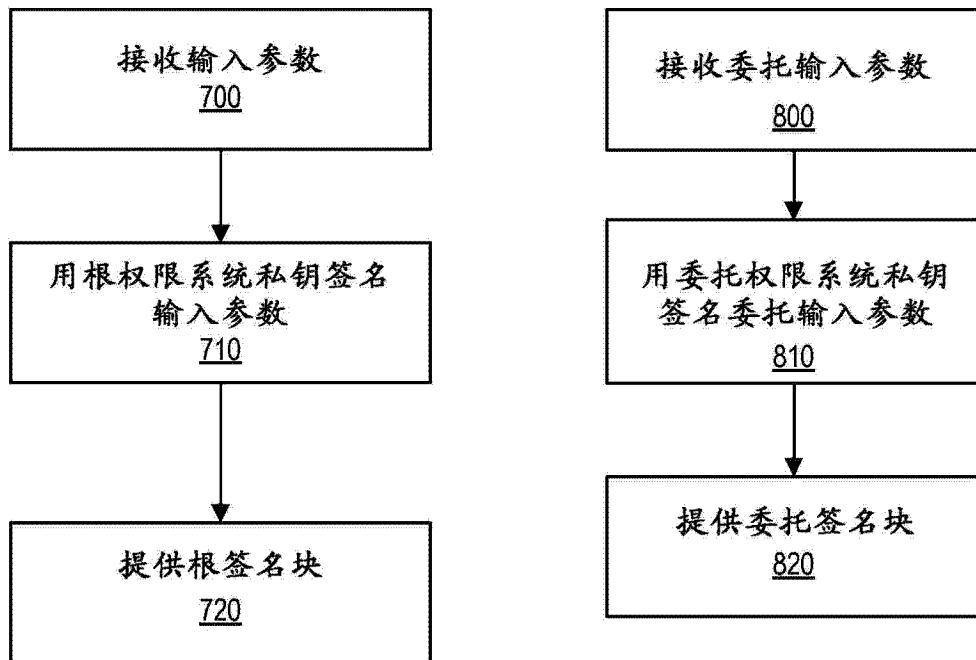


图 6



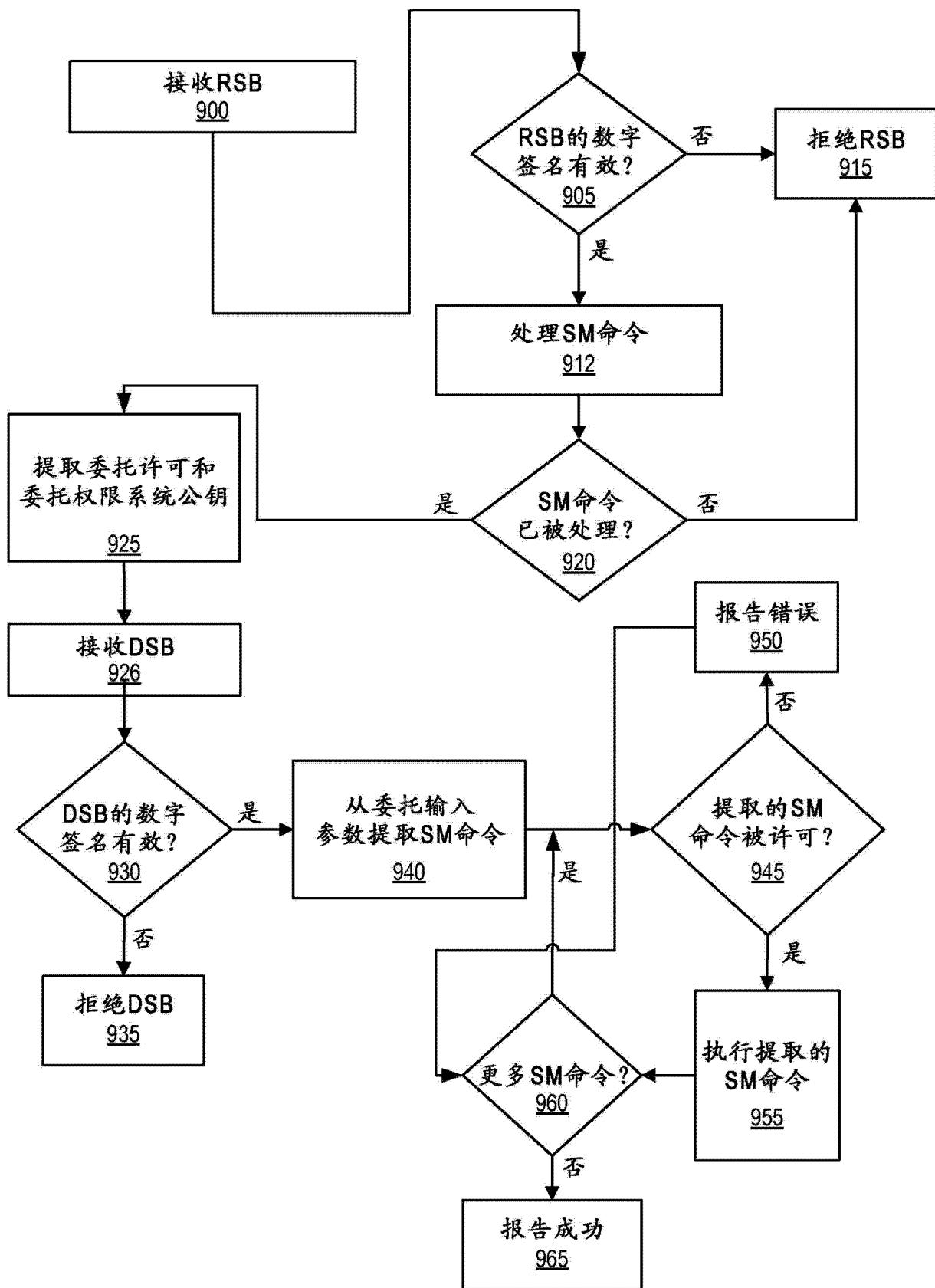


图 9A

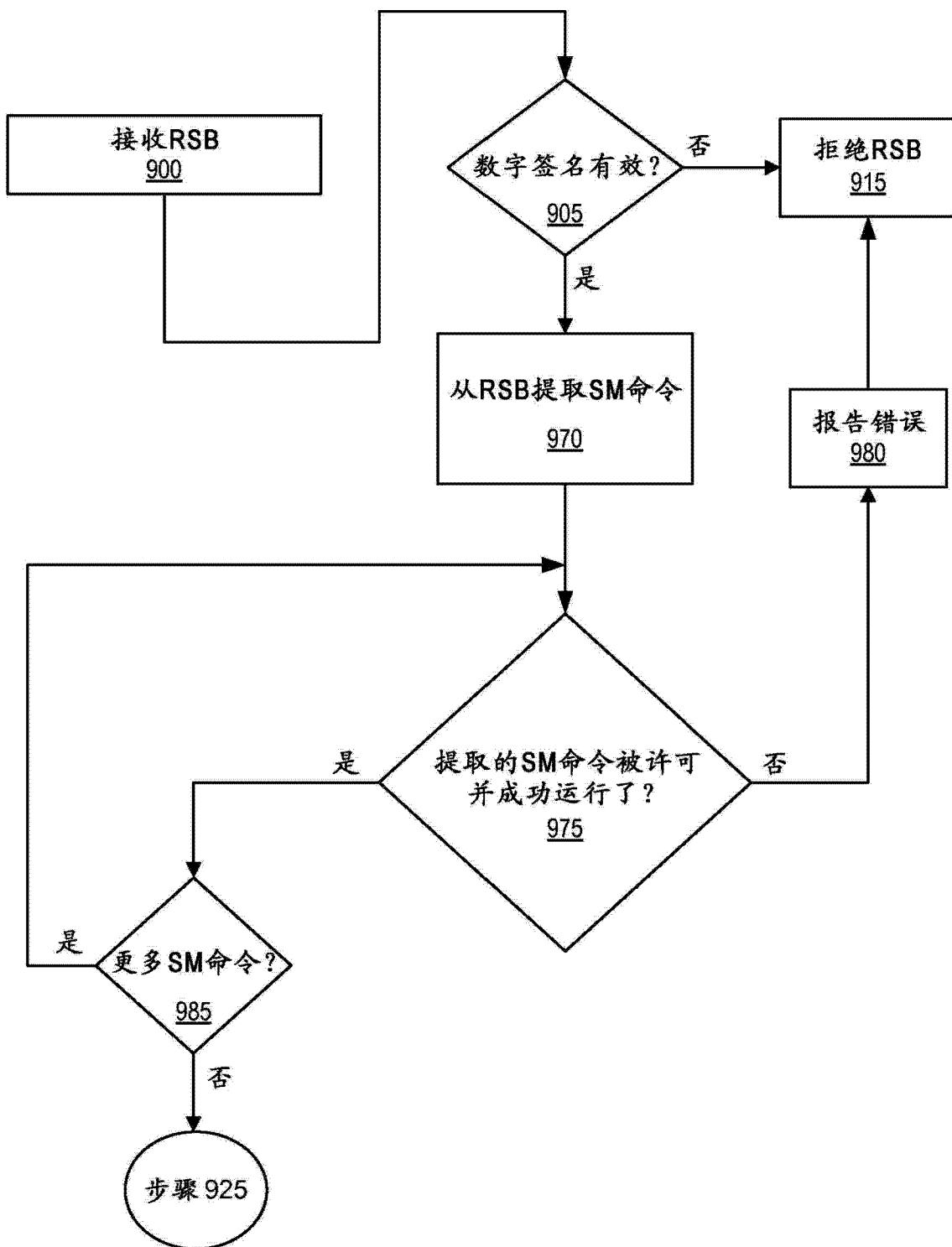


图 9B

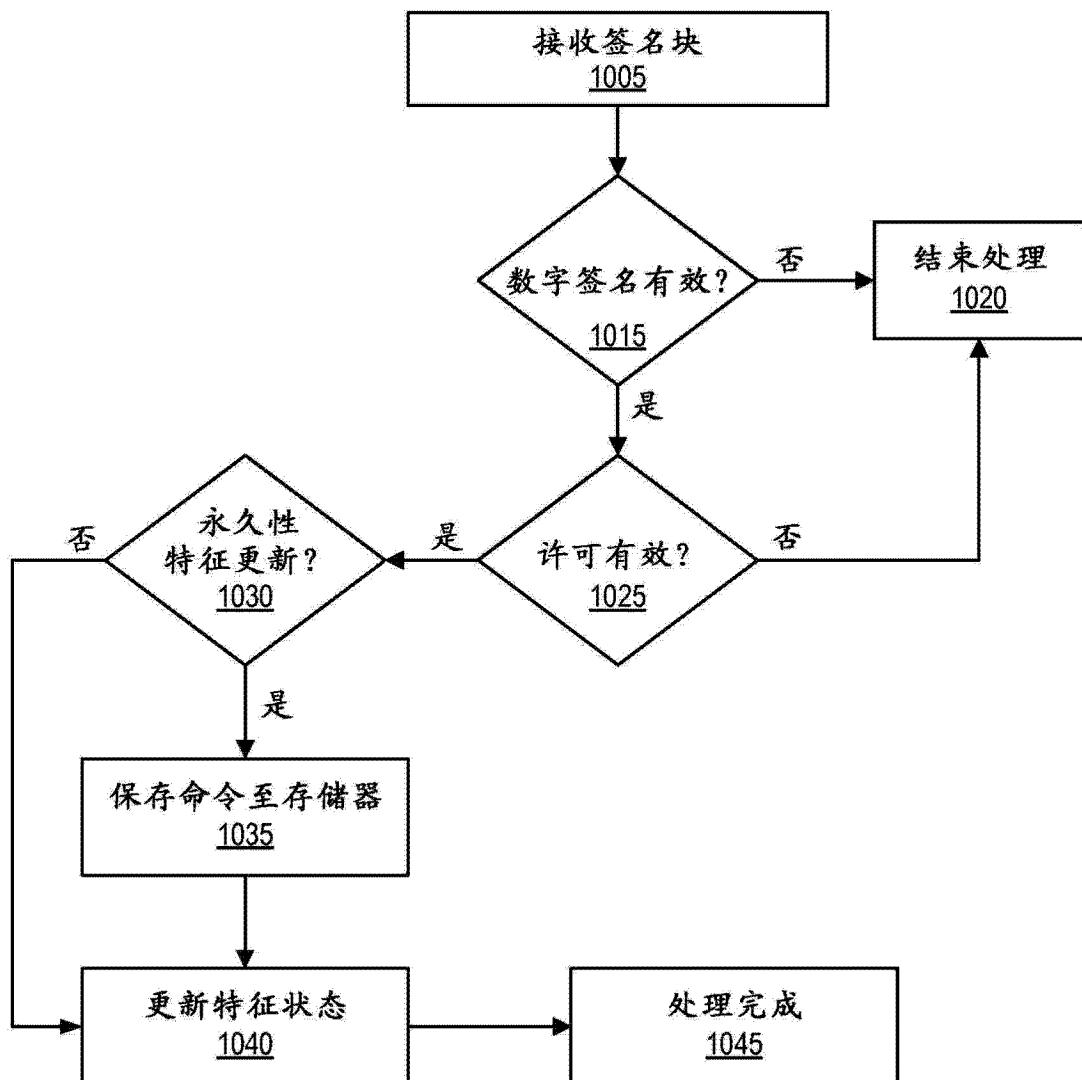


图 10

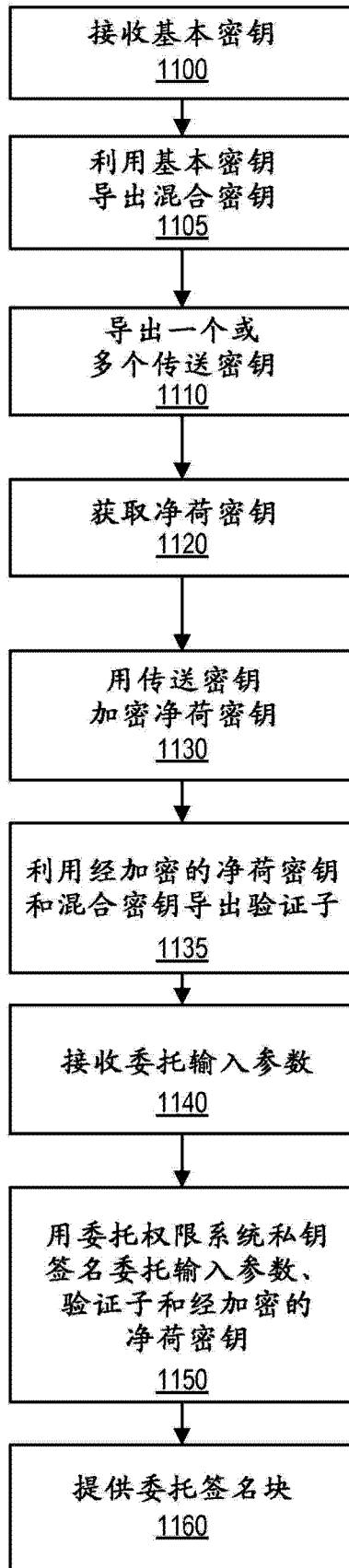


图 11

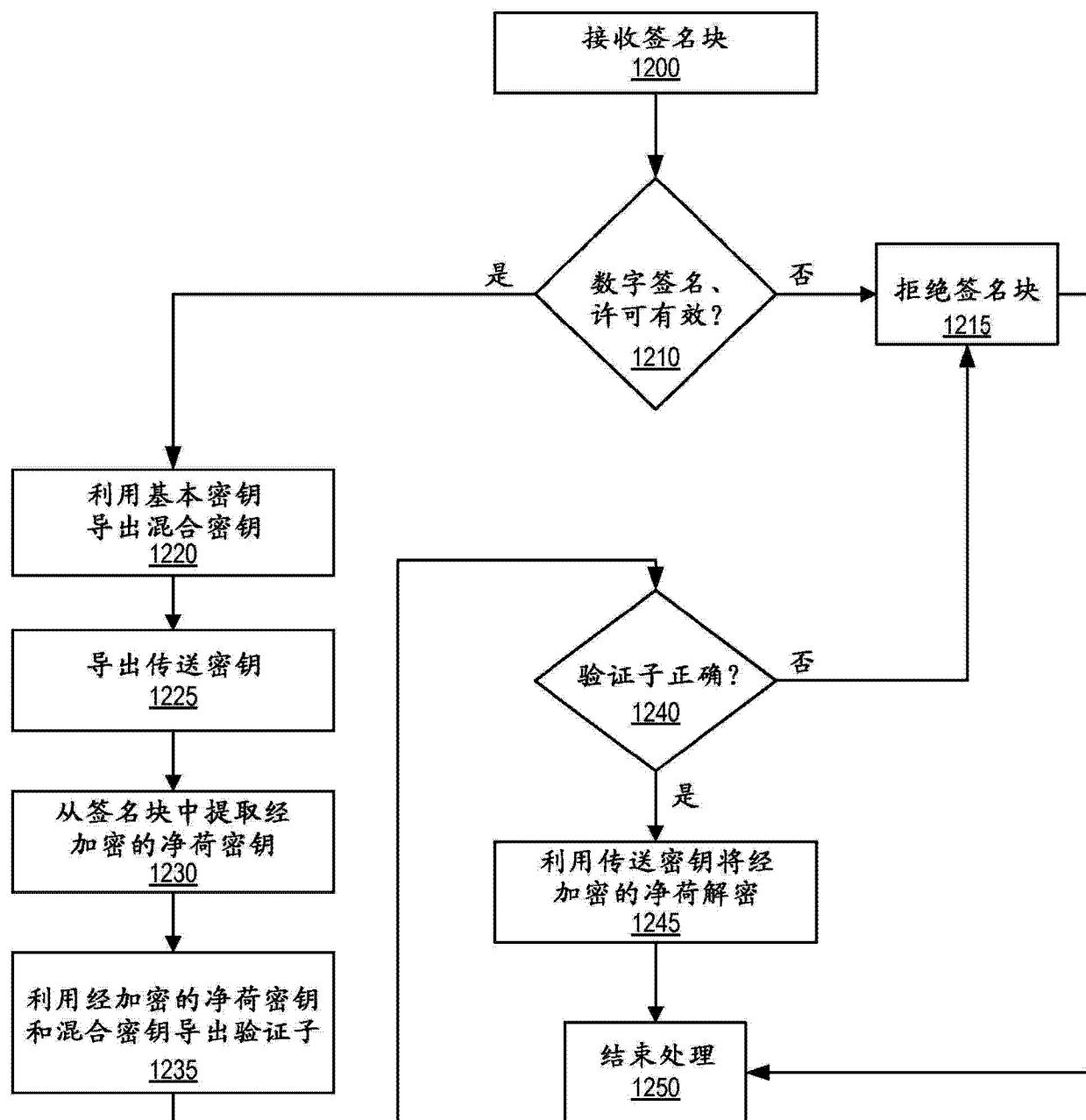


图 12

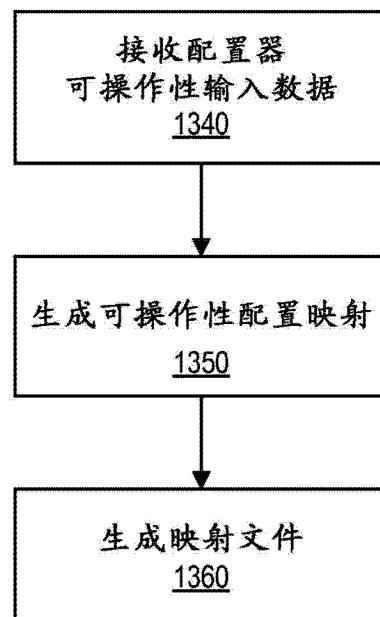
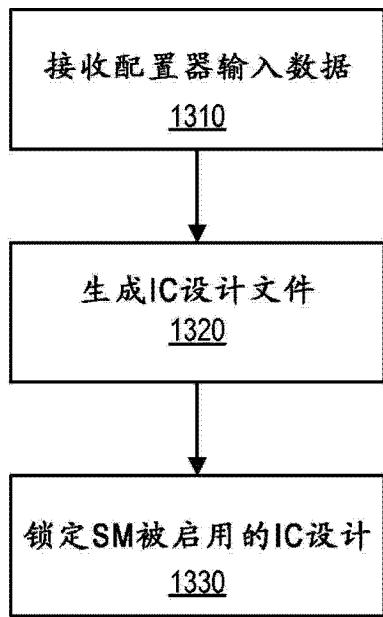


图 13A

图 13B

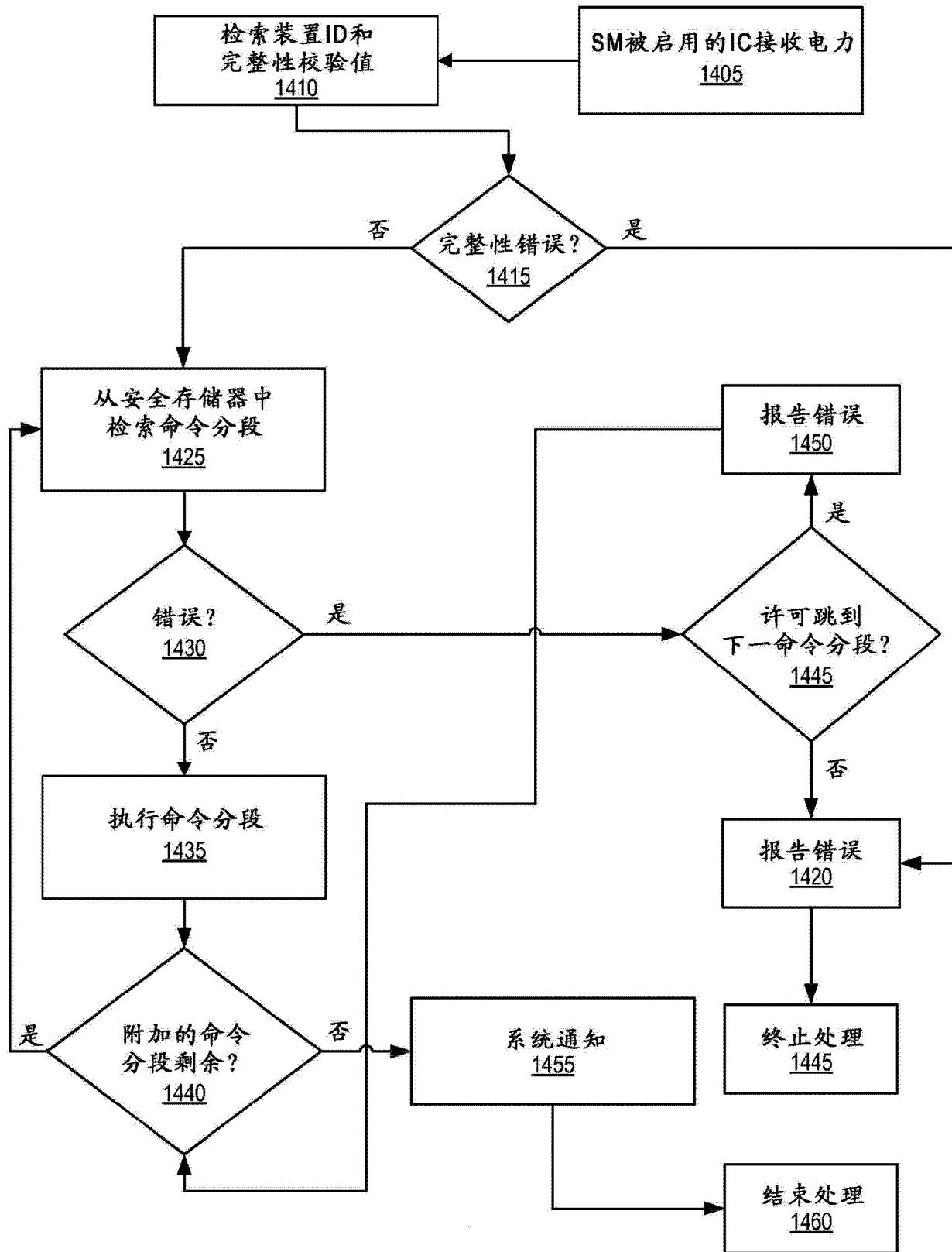


图 14

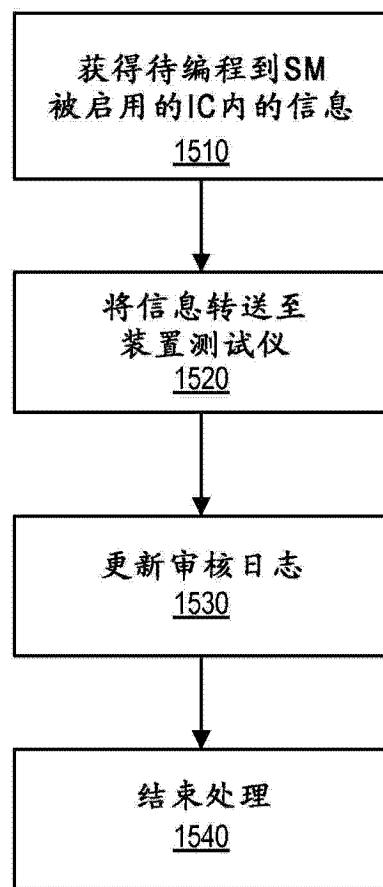


图 15

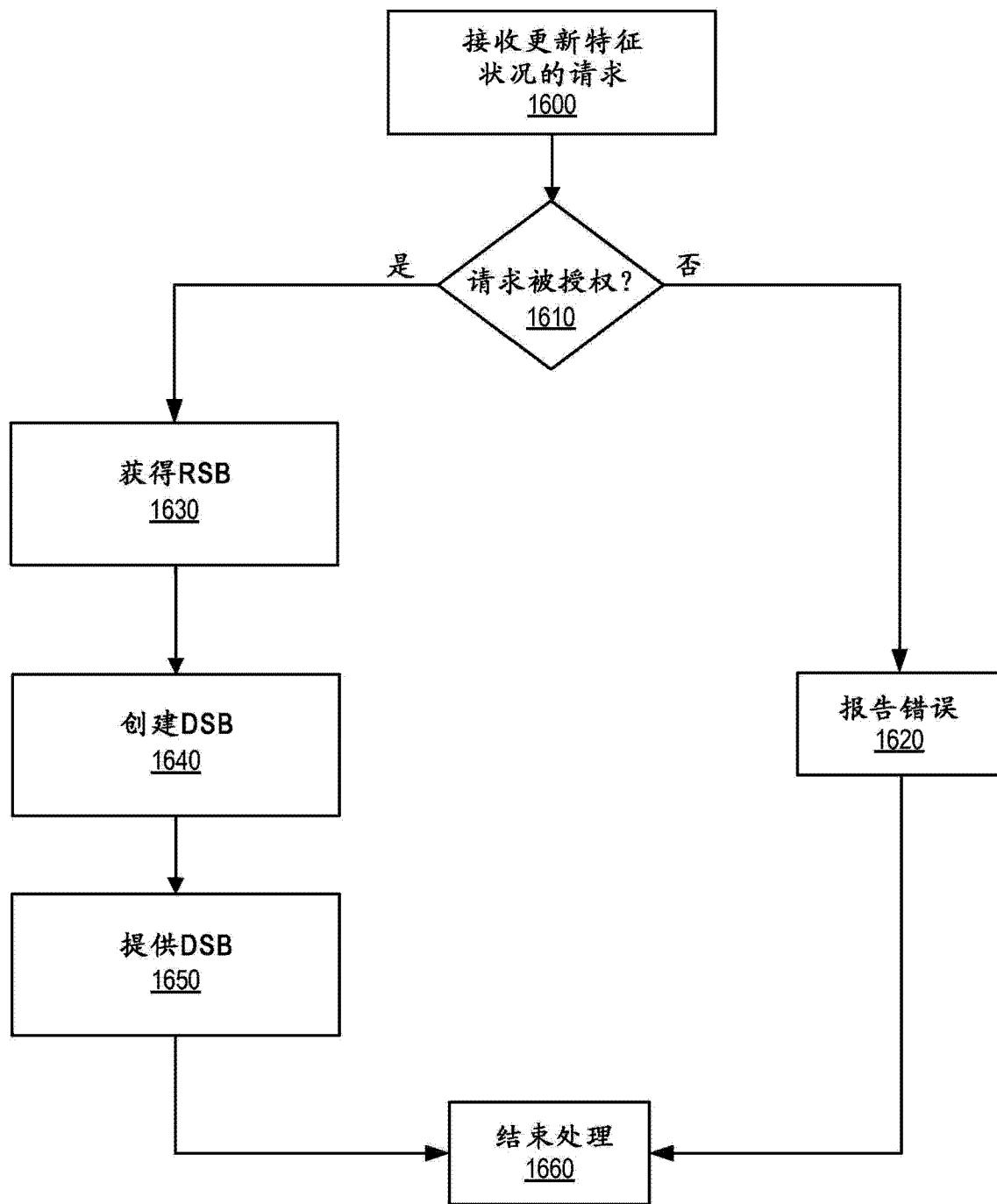


图 16

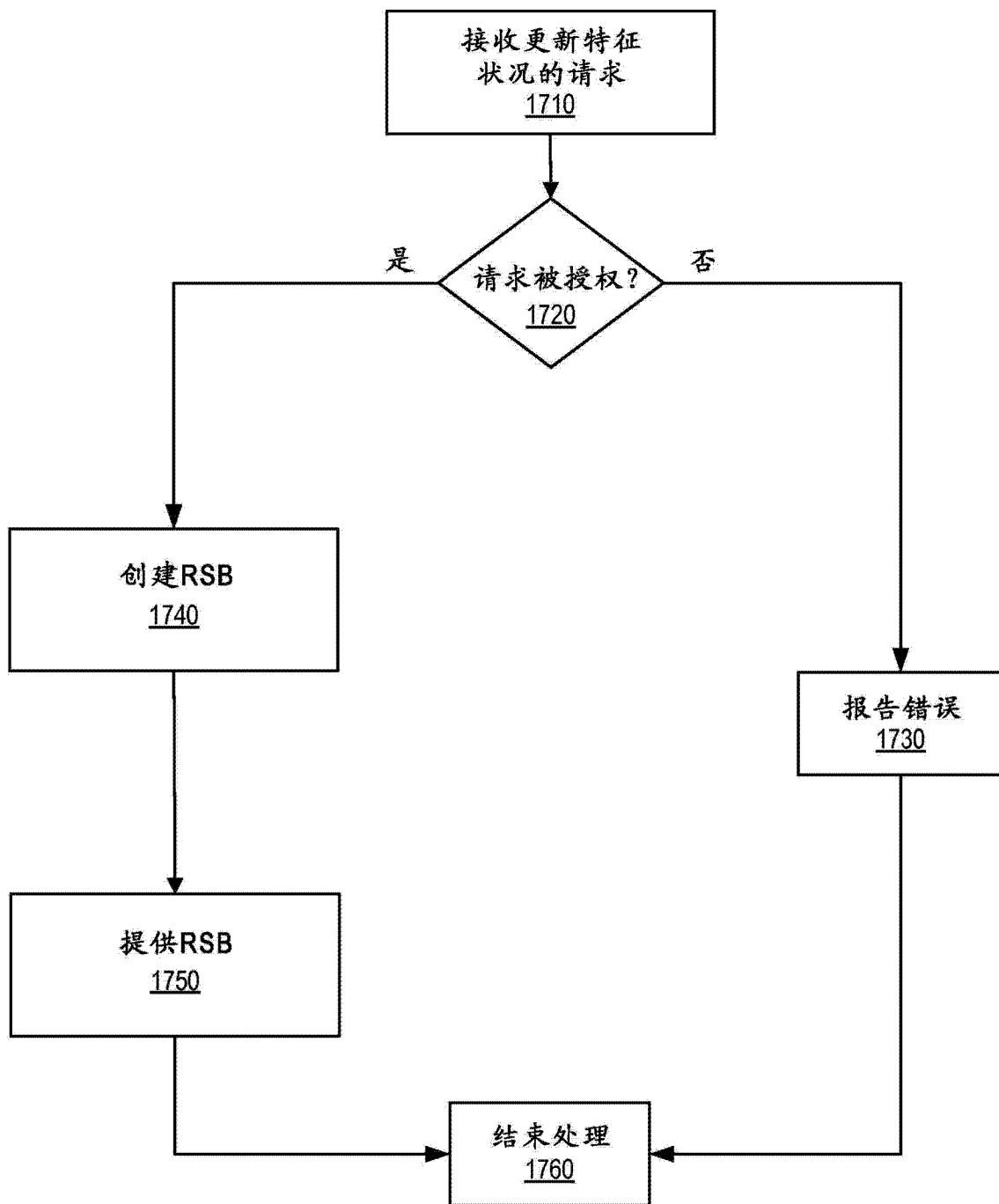


图 17