(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 104471586 A
(43)申请公布日 2015.03.25

(21)申请号 201380036770.5
(22)申请日 2013.07.09
(30)优先权数据
61/671,290 2012.07.13 US
13/931,708 2013.06.28 US
(85)PCT国际申请进入国家阶段日
2015.01.09
(86)PCT国际申请的申请数据
PCT/US2013/049795 2013.07.09
(87)PCT国际申请的公布数据
WO2014/011687 EN 2014.01.16
(71)申请人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 N·巴蒂亚 J·奥多诺霍
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英
(51)Int.Cl.
G06F 21/72(2006.01)
G06F 21/87(2006.01)

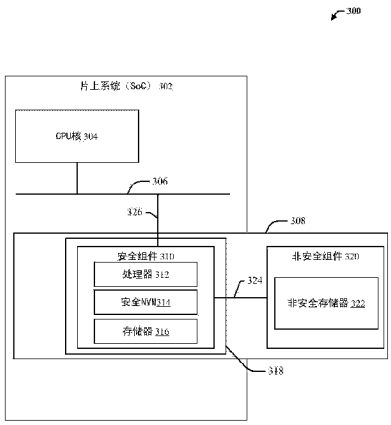
权利要求书3页 说明书10页 附图5页

(54)发明名称

用于将一部分安全单元组件集成在片上系统上的方法和装置

(57)摘要

本发明结合提供高效的SE功能，来提供用于无线通信的方法、装置和计算机程序产品。在一个示例中，通信设备包括SE，其中该SE包括处理器、RAM和NVM、以及安全组件和非安全组件。SE可以被配备为：接收对可通过该SE中存储的信息来访问的功能进行访问的请求；获取在安全组件中存储的与该功能相关联的信息的第一部分；获得在非安全组件中存储的与该功能相关联的信息的第二部分；使用所获取的该信息的第一部分来促进针对该功能的访问，以便能够访问所获得的该信息的第二部分。在一个方面，安全组件可以包括处理器和RAM，非安全组件可以包括几乎所有的NVM。



CN 104471586 A

1. 一种用于通信的装置，包括：

安全单元 (SE)，所述 SE 包括处理器、随机存取存储器 (RAM) 和非易失性存储器 (NVM)，其中，所述 SE 还包括所述 SE 的安全组件、所述 SE 的非安全组件，其中，所述非安全组件和所述安全组件通过接口耦合，并且其中，所述 SE 被配置为：

接收对可通过所述 SE 中存储的信息来访问的功能进行访问的请求；

获取在所述 SE 的所述安全组件中存储的、与所述功能相关联的所述信息的第一部分，其中，所述安全组件包括所述处理器和所述 RAM；

获得在所述 SE 的所述非安全组件中存储的、与所述功能相关联的所述信息的第二部分，其中，所述非安全组件包括基本上所有的所述 NVM；以及

使用所获取的所述信息的所述第一部分来促进对所述功能的访问，以便能够访问所获得的所述信息的所述第二部分。

2. 根据权利要求 1 所述的装置，其中，所述功能是通信设备上存储的应用，并且其中，所述请求是通过所述 SE 和所述通信设备之间的加密安全接口来接收的。

3. 根据权利要求 1 所述的装置，其中，在所述 SE 的所述非安全组件中包括的所述 NVM 包括标准 NVM。

4. 根据权利要求 1 所述的装置，其中，所述 SE 的所述安全组件是使用安全屏蔽来进行安全保护的。

5. 根据权利要求 1 所述的装置，其中，所述 SE 的所述安全组件被集成到片上系统 (SoC)。

6. 根据权利要求 5 所述的装置，其中，所述 SoC 是近场通信控制器 (NFCC)。

7. 根据权利要求 5 所述的装置，其中，所述 SoC 是移动站调制解调器 (MSM) 芯片。

8. 根据权利要求 5 所述的装置，其中，通过仅将所述 SE 的所述安全组件集成到所述 SoC 中，来使所述 SE 在所述 SoC 上的封装最小化。

9. 根据权利要求 8 所述的装置，其中，所述 SE 的所述安全组件具有小于或等于 65nm 的几何尺寸。

10. 根据权利要求 5 所述的装置，其中，用于所述安全组件的安全屏蔽包括：与所述 SoC 相关联的一个或多个现有的金属层。

11. 根据权利要求 1 所述的装置，其中，所述 SE 还被配置为：

在所述 SE 的所述非安全组件和所述 SE 的所述安全组件之间使用高速接口。

12. 根据权利要求 1 所述的装置，其中，以加密格式对在所述 SE 的所述非安全组件中存储的、与所述功能相关联的所述信息的所述第二部分进行存储，所述加密格式基于在所述安全组件中存储的、与所述功能相关联的所述信息的所述第一部分。

13. 根据权利要求 12 所述的装置，其中，所述 SE 还被配置为：

基于所述信息的所述第一部分中包括的一个或多个密码，使用在所述 SE 的所述安全组件中包括的所述处理器，对所述信息的所述第二部分进行解密。

14. 一种使用安全单元 (SE) 进行通信的方法，包括：

接收对可通过所述 SE 中存储的信息来访问的功能进行访问的请求，其中，所述 SE 包括处理器、随机存取存储器 (RAM) 和非易失性存储器 (NVM)；

获取在所述 SE 的安全组件中存储的、与所述功能相关联的所述信息的第一部分，其

中，所述安全组件包括所述处理器和所述 RAM ；

获得在所述 SE 的非安全组件中存储的、与所述功能相关联的所述信息的第二部分，其中，所述非安全组件包括基本上所有的所述 NVM ；以及

使用所获取的所述信息的所述第一部分来促进对所述功能的访问，以便能够访问所获得的所述信息的所述第二部分。

15. 根据权利要求 14 所述的方法，其中，所述功能是通信设备上存储的应用，并且其中，所述请求是通过所述 SE 和所述通信设备之间的加密安全接口来接收的。

16. 根据权利要求 14 所述的方法，其中，在所述 SE 的所述非安全组件中包括的所述 NVM 包括标准 NVM。

17. 根据权利要求 14 所述的方法，其中，所述 SE 的所述安全组件是使用安全屏蔽来进行安全保护的。

18. 根据权利要求 14 所述的方法，其中，所述 SE 的所述安全组件被集成到片上系统 (SoC)。

19. 根据权利要求 18 所述的方法，其中，所述 SoC 是近场通信控制器 (NFCC)。

20. 根据权利要求 18 所述的方法，其中，所述 SoC 是移动站调制解调器 (MSM) 芯片。

21. 根据权利要求 18 所述的方法，其中，通过仅将所述 SE 的所述安全组件集成到所述 SoC 中，来使所述 SE 在所述 SoC 上的封装最小化。

22. 根据权利要求 21 所述的方法，其中，所述 SE 的所述安全组件具有小于或等于 65nm 的几何尺寸。

23. 根据权利要求 18 所述的方法，其中，用于所述安全组件的安全屏蔽包括 ：与所述 SoC 相关联的一个或多个现有的金属层。

24. 根据权利要求 14 所述的方法，其中，所述获得包括 ：在所述 SE 的所述非安全组件和所述 SE 的所述安全组件之间使用高速接口。

25. 根据权利要求 14 所述的方法，其中，以加密格式对在所述 SE 的所述非安全组件中存储的、与所述功能相关联的所述信息的所述第二部分进行存储，所述加密格式基于在所述安全组件中存储的、与所述功能相关联的所述信息的所述第一部分。

26. 根据权利要求 25 所述的方法，其中，所述访问还包括 ：基于所述信息的所述第一部分中包括的一个或多个密码，由在所述 SE 的所述安全组件中包括的所述处理器对所述信息的所述第二部分进行解密。

27. 一种用于通信的装置，包括 ：

用于接收对可通过安全单元中存储的信息来访问的功能进行访问的请求的单元，其中，所述 SE 包括处理器、随机存取存储器 (RAM) 和非易失性存储器 (NVM) ；

用于获取在所述 SE 的安全组件中存储的、与所述功能相关联的所述信息的第一部分的单元，其中，所述安全组件包括所述处理器和所述 RAM ；

用于获得在所述 SE 的非安全组件中存储的、与所述功能相关联的所述信息的第二部分的单元，其中，所述非安全组件包括基本上所有的所述 NVM ；以及

用于使用所获取的所述信息的所述第一部分来促进对所述功能的访问，以便能够访问所获得的所述信息的所述第二部分的单元。

28. 根据权利要求 27 所述的装置，其中，所述功能是通信设备上存储的应用，并且其

中，所述请求是通过所述 SE 和所述通信设备之间的加密安全接口来接收的。

29. 根据权利要求 27 所述的装置，其中，在所述 SE 的所述非安全组件中包括的所述 NVM 包括标准 NVM。

30. 根据权利要求 27 所述的装置，其中，所述 SE 的所述安全组件是使用安全屏蔽来进行安全保护的。

31. 根据权利要求 27 所述的装置，其中，所述 SE 的所述安全组件被集成到片上系统 (SoC)。

32. 根据权利要求 31 所述的装置，其中，所述 SoC 是近场通信控制器 (NFCC)。

33. 根据权利要求 31 所述的装置，其中，所述 SoC 是移动站调制解调器 (MSM) 芯片。

34. 根据权利要求 31 所述的装置，其中，通过仅将所述 SE 的所述安全组件集成到所述 SoC 中，来使所述 SE 在所述 SoC 上的封装最小化。

35. 根据权利要求 34 所述的装置，其中，所述 SE 的所述安全组件具有小于或等于 65nm 的几何尺寸。

36. 根据权利要求 31 所述的装置，其中，用于所述安全组件的安全屏蔽包括 ：与所述 SoC 相关联的一个或多个现有的金属层。

37. 根据权利要求 36 所述的装置，其中，所述用于获得的单元还被配置为 ：在所述 SE 的所述非安全组件和所述 SE 的所述安全组件之间使用高速接口。

38. 根据权利要求 27 所述的装置，其中，以加密格式对在所述 SE 的所述非安全组件中存储的、与所述功能相关联的所述信息的所述第二部分进行存储，所述加密格式基于在所述安全组件中存储的、与所述功能相关联的所述信息的所述第一部分。

39. 根据权利要求 38 所述的装置，其中，所述用于促进访问的单元还被配置为 ：基于所述信息的所述第一部分中包括的一个或多个密码，对所述信息的所述第二部分进行解密。

40. 一种计算机程序产品，包括 ：

计算机可读介质，其包括用于执行以下操作的代码 ：

接收对可通过所述 SE 中存储的信息来访问的功能进行访问的请求，其中，所述 SE 包括处理器、随机存取存储器 (RAM) 和非易失性存储器 (NVM) ；

获取在所述 SE 的安全组件中存储的、与所述功能相关联的所述信息的第一部分，其中，所述安全组件包括所述处理器和所述 RAM ；

获得在所述 SE 的非安全组件中存储的、与所述功能相关联的所述信息的第二部分，其中，所述非安全组件包括基本上所有的所述 NVM ；以及

使用所获取的所述信息的所述第一部分来促进对所述功能的访问，以便能够访问所获得的所述信息的所述第二部分。

用于将一部分安全单元组件集成在片上系统上的方法和装置

[0001] 基于 35U.S.C. § 119 要求优先权

[0002] 本专利申请要求享受2012年7月13日提交的、标题为“METHODS AND APPARATUSES FOR INTEGRATING A PORTION OF SECURE ELEMENT COMPONENTS ON A SYSTEM ON CHIP”的临时申请 No.61/671,290 的优先权，该临时申请已经转让给本申请的受让人，故以引用方式将其明确地并入本文。

技术领域

[0003] 概括地说，所公开的方面涉及设备之间和 / 或之内的通信，具体地说，所公开的方面涉及用于使用安全单元的方法和系统，其中该安全单元的一部分集成在片上系统 (SoC) 中。

背景技术

[0004] 技术的提高使得生产出越来越小和越来越强大的个人计算设备。例如，当前存在多种多样的便携式个人计算设备，其包括诸如便携式无线电话、个人数字助理 (PDA) 和寻呼设备之类的无线计算设备，它们每一个都是小型、轻型和用户容易携带的。具体而言，例如，便携式无线电话还包括通过无线网络来传输语音和数据分组的蜂窝电话。制造的很多这种蜂窝电话的计算能力都具有相对很大的提升，故它们变得等价于小型个人计算机和手持型 PDA。此外，制造这些设备以便能使用多种频率和适当的覆盖区域 (例如，蜂窝通信、无线局域网 (WLAN) 通信、近场通信 (NFC) 等) 来进行通信。

[0005] 当前，在设备中，一些应用可以被配置为使用高级别的安全，其包括防止物理和 / 或软件入侵。这些应用可以主存在安全单元 (SE) 中。如本申请所使用的，SE 可以包括已被硬化以防止未授权访问的完整计算平台 (例如，随机存取存储器 (RAM)、只读存储器 (ROM)、非易失性存储器 (NVM)、加密加速器、中央处理单元 (CPU) 等)。虽然这些 SE 可以实现非常高级别的安全，但当将它们集成到设备中时，也是相对昂贵的。例如，通常使用独立的硅工艺来产生 SE，因此，其不能通过集成的 SoC 上的可能的成本效益中获益。

[0006] 因此，期望用于提供高效的 SE 功能的改进方法和装置。

发明内容

[0007] 为了对一个或多个方面有一个基本的理解，下面给出了这些方面的简单概括。该概括部分不是对所有预期方面的详尽概述，也不是旨在标识所有方面的关键或重要元素或者描述任意或全部方面的范围。其唯一目的是用简单的形式呈现本发明的一个或多个方面的一些概念，以此作为后面的详细说明的前奏。

[0008] 根据一个或多个方面以及其相应公开内容，本申请结合提供高效 SE 功能，来描述各个方面。在一个示例中，通信设备包括 SE，其包括处理器、RAM 和 NVM、安全组件、以及非安全组件。在一个方面，所述非安全组件和所述安全组件通过一种接口进行耦合。SE 可以

被配备为：接收对可通过该SE中存储的信息来访问的功能进行访问的请求；获取在所述SE的安全组件中存储的与该功能相关联的信息的第一部分；获得在所述SE的非安全组件中存储的与该功能相关联的信息的第二部分；使用所获取的该信息的第一部分来促进针对该功能的访问，以便能够访问所获得的该信息的第二部分。在一个方面，所述安全组件可以包括处理器和RAM，所述非安全组件可以包括几乎所有的NVM。

[0009] 根据有关的方面，提供了一种用于提供高效SE功能的方法。该方法可以包括：接收对可通过所述SE中存储的信息来访问的进行访问的请求。在一个方面，所述SE可以包括处理器、RAM和NVM。此外，该方法还可以包括：获取在所述SE的安全组件中存储的与所述功能相关联的信息的第一部分。在一个方面，所述安全组件可以包括所述处理器和所述RAM。此外，该方法还可以包括：获得在所述SE的非安全组件中存储的与所述功能相关联的信息的第二部分。在一个方面，所述非安全组件可以包括几乎所有的所述NVM。此外，该方法还可以包括：使用所获取的所述信息的第一部分来促进针对所述功能的访问，以便能够访问所获得的所述信息的第二部分。

[0010] 另一个方面与被启用以提供高效的SE功能的通信装置有关。该通信装置可以包括：用于接收对可通过所述SE中存储的信息来访问的功能进行访问的请求的单元。在一个方面，所述SE可以包括处理器、RAM和NVM。此外，该通信装置还可以包括：用于获取在所述SE的安全组件中存储的与所述功能相关联的信息的第一部分的单元。在一个方面，所述安全组件可以包括所述处理器和所述RAM。此外，该通信装置还可以包括：用于获得在所述SE的非安全组件中存储的与所述功能相关联的信息的第二部分的单元。在一个方面，所述非安全组件可以包括几乎所有的所述NVM。此外，该通信装置还可以包括：用于使用所获取的所述信息的第一部分来促进针对所述功能的访问，以便能够访问所获得的所述信息的第二部分的单元。

[0011] 另一个方面涉及一种通信装置。该装置可以包括SE，其包括处理器、RAM和NVM、所述SE的安全组件、以及所述SE的非安全组件。所述SE可以被配置为：接收对可通过所述SE中存储的信息来访问的功能进行访问的请求。此外，所述UE还可以被配置为：获取在所述SE的安全组件中存储的与所述功能相关联的信息的第一部分。在一个方面，所述安全组件可以包括所述处理器和所述RAM。此外，所述UE还可以被配置为：获得在所述SE的非安全组件中存储的与所述功能相关联的信息的第二部分。在一个方面，所述非安全组件可以包括几乎所有的所述NVM。此外，所述UE还可以被配置为：使用所获取的所述信息的第一部分来促进针对所述功能的访问，以便能够访问所获得的所述信息的第二部分。

[0012] 另一个方面涉及一种计算机程序产品，所述计算机程序产品可以具有计算机可读介质，所述计算机可读介质包括：用于接收对可通过所述SE中存储的信息来访问的功能进行访问的请求的代码。在一个方面，所述SE可以包括处理器、RAM和NVM。此外，所述计算机可读介质可以包括：用地获取在所述SE的安全组件中存储的与所述功能相关联的信息的第一部分的代码。在一个方面，所述安全组件可以包括所述处理器和所述RAM。此外，所述计算机可读介质可以包括：用于获得在所述SE的非安全组件中存储的与所述功能相关联的信息的第二部分的代码。在一个方面，所述非安全组件可以包括几乎所有的所述NVM。此外，所述计算机可读介质可以包括：用于使用所获取的所述信息的第一部分来促进针对所述功能的访问，以便能够访问所获得的所述信息的第二部分。

[0013] 为了实现前述和有关的目的，一个或多个方面包括下文所详细描述和权利要求书中具体指出的特征。下文描述和附图详细描述了一个或多个方面的某些示例性特征。但是，这些特征仅仅说明可采用这些各个方面之基本原理的各种方法中的一些方法，并且该描述旨在包括所有这些方面及其等同物。

附图说明

[0014] 下面结合附图来描述本发明的所公开方面，提供的这些附图用于说明而不是限制所公开的方面，其中相同的附图标记表示相同的元素，其中：

[0015] 图 1 是根据一个方面，一种基于感应通信系统的简化框图；

[0016] 图 2 是根据一个方面，一种基于感应系统的简化示意图；

[0017] 图 3 是根据一个方面，具有集成的 SE 的 SoC 的框图；

[0018] 图 4 是根据一个方面，描述用于使用集成到 SoC 中的 SE 的示例方法的流程图；

[0019] 图 5 是根据本发明的通信设备的方面的框图；

[0020] 图 6 根据一个方面，描绘了用于提供高效 SE 功能的示例通信设备的框图。

具体实施方式

[0021] 现在参照附图来描述各个方面。在下文描述中，为了说明起见，为了对一个或多个方面有一个透彻理解，对众多特定细节进行了描述。但是，显而易见的是，可以在不使用这些特定细节的情况下实现这些方面。

[0022] 通常，通信设备可以通过 SE 的使用，来访问各种功能。SE 提供一种存储信息的环境，其中 SE 通常已被硬化以防止未授权的访问。此外，SE 可以包括各种组件，例如但不限于：RAM、ROM、NV 存储器 (NVM)、加密加速器、CPU 等。如本申请所使用的，给出了一种系统体系结构，其中该 SE 的组件中的一个或多个可以是独立的，并包括（例如，集成）在 SoC 中。因此，可以使用集成的并且低成本体系结构，来实现与传统单片 SE 设计方案相兼容的安全级别。

[0023] 图 1 根据本发明的各个示例性实施例，描绘了一种基于感应的通信系统 100。向发射机 104 提供输入功率 102，以产生用于提供能量传输的辐射场 106。接收机 108 耦接到辐射场 106，产生用于存储或者由一个设备（没有示出）使用的输出功率 110，其中该设备耦接到输出功率 110。发射机 104 和接收机 108 相隔一定的距离 112。在一个示例性实施例中，根据相互共振关系，对发射机 104 和接收机 108 进行配置，当接收机 108 的谐振频率和发射机 104 的谐振频率非常接近时，在接收机 108 位于辐射场 106 的“近场”之中时，发射机 104 和接收机 108 之间的传输损耗最小。

[0024] 此外，发射机 104 还包括发射天线 114，以提供用于能量传输的单元，接收机 108 还包括接收天线 118，以提供用于能量接收的单元。根据应用场景以及与之相关联的设备，设计发射天线和接收天线的尺寸。如上所述，通过将发射天线的近场中的能量的一大部分耦接到接收天线，而不是将电磁波中的能量的大部分传播到远场，来实现高效的能量传输。当处于近场之中时，可以在发射天线 114 和接收天线 118 之间开发一种耦合模式。天线 114 和 118 周围的实现这种近场耦合的区域，本申请称为耦合模式区域。

[0025] 图 2 示出了近场基于感应通信系统的简化示意图。发射机 204 包括振荡器 222、功

率放大器 224 以及滤波和匹配电路 226。振荡器被配置为按照期望的频率来产生信号，其中可以响应于调整信号 223 来调整该期望频率。功率放大器 224 可以使用响应于控制信号 225 的放大量，对该振荡器信号进行放大。可以包括滤波和匹配电路 226，以便过滤掉谐波或者其它不想要的频率，并使发射机 204 的阻抗与发射天线 214 相匹配。

[0026] 接收机 208 可以包括匹配电路 232 与整流器和开关电路 234，以产生 DC 电源输出，对如图 2 中所示的电池 236 进行充电，或者对耦接到接收机（没有示出）的设备进行供电。可以包括匹配电路 232，以便使接收机 208 的阻抗与接收天线 218 相匹配。接收机 208 和发射机 204 可以在不同的通信信道 219（例如，蓝牙、zigbee、蜂窝等）上进行通信。

[0027] 参见图 3，该图描绘了根据一个方面的 NFC 系统体系结构 300 的框图。NFC 系统体系结构 300 可以包括 SoC 302，其可以被配置为通过使用共享总线 306，实现一个或多个 CPU 核 304 的处理。在一个方面，SoC 302 可以代表移动站调制解调器 (MSM) 芯片。在另一个方面，SoC 302 可以代表 NFC 控制器 (NFCC)。

[0028] 此外，NFC 系统体系结构 300 还包括 SE 308。在一个方面，SE 308 可以是用户识别模块 (SIM) 卡、安全数字 (SD) 卡、微 SD 卡和 / 或嵌入式 SE 308。SE 308 可以包括安全组件 310 和非安全组件 320。安全组件 310 和非安全组件可以通过接口 324 相耦合。在一个方面，接口 324 可以被配置为使用支持加密的总线接口。在另一个方面，接口 324 可以是标准高速接口。在该方面，接口 324 提供将代码、小应用程序等从非安全存储器 322 高效地装载到 SE 308 的安全组件 310 以进行处理。

[0029] 安全组件 310 可以包括处理器 312、安全 NVM 314 和存储器 316。在一个方面，处理器 312 可以是与 SE 308 相关联的专用处理器 312。在另一个方面，处理器 312 可以是能通过 SoC 302 可用的处理器，其具有另外的安全保护（例如，加密、签名等）以帮助维持 SE 308 中的安全性和完整性。在一个方面，安全 NVM 314 可以包括足够的存储器，以保存可以通过保护来获益的各个项（例如，根密钥、证书等）。在一个方面，存储器 316 可以包括足够的存储能力，以允许非安全存储器 322 中存储的信息的高效装载和处理。

[0030] 此外，安全组件 310 可以是使用安全屏蔽 318 来变得安全的。在一个方面，安全屏蔽 318 可以提供针对硬件和 / 或软件攻击的各种预防措施（例如，差分功率分析 (DPA)、简单功率分析 (SPA)、激光攻击、电压改变、温度改变、激光探测等）。安全屏蔽 318 预防措施可以包括但不限于：用于使内部操作的观察更加困难的金属层；当包装被打开时，禁用操作的光传感器；用于类似操作的多个硬件路径等。在一个方面，安全屏蔽 318 可以使用与 SoC 302 相关联的现有金属层，来实现用于形成安全屏蔽的数字或模拟 IP。

[0031] 非安全组件 320 可以包括非安全存储器 322。在一个方面，非安全存储器 322 可以专用于向安全存储设备、标准 NVM、RAM、任何存储器存储设备或者其任意组合提供任务。在一个方面，非安全存储器 322 可以配置有近似 1.2M 字节的空间。在另一个方面，非安全存储器 322 可以用于存储：与可通过 SE 308 访问的各种功能相关联的代码、小应用程序等。在该方面，非安全存储器 322 可以用于应用（例如，计算机代码）和数据的非易失性存储，安全 NVM 314 可以用于存储与这些应用相关联的密钥系统。在一个方面，为了帮助维持代码和数据的安全性和完整性，防止通过外部接口的攻击，只要当数据离开 SoC 302 时，就对该数据进行加密（以确保安全）和签名（以保证完整性）。因此，可以使非安全存储器 322 中的信息的安全，达到在安全组件 310 中所使用的加密操作所提供的能力的程度。

[0032] 在一个操作方面中，在称为‘公共标准’的指导方针下，SE 308 可以被证实为安全。这些指导方针对于将规定的评价指标 (TOE) 进行评估，其中在该 TOE 中，对安全进行评估。如图 3 中所示，可以将包括安全组件 310 和非安全组件 320 的 SE 308 评估成一个 TOE。换言之，为了保持可以合理地类似于当前所使用的 TOE 的 TOE，可以使安全组件 310 和 SoC 302 的其它组件之间的接口 326 减到最少。在该方面，接口 326 可以被配置为：允许某些电熔丝 (eFuse) 数据仅仅可用于 SE 308。在另一个方面，可以将接口 326 加密保护到 SoC 302 的内部 (RAM) 存储器，因此防止 SoC 302 中的其它处理器 (例如，CPU 核 304) 观察 SE 308 的操作。在另一个方面，与 SoC 302 上的其它组件 (例如，304) 相比，安全组件 310 可以使用独立的功率域和 / 或功率管理。在另一个方面，安全组件 310 可以例如使用二进制通用异步接收机 / 发射机 (UART) 接口，限制与其它处理器 (例如，304) 的交互。

[0033] 因此，给出了一种可以将 SE 308 的各种功能分割到安全组件 310 和非安全组件 320 中的 NFC 系统体系结构 300，其中安全组件 310 可以使用 SoC302 上的小的几何形状来高效实现，非安全组件 320 可以更高效地实现在更大更昂贵的几何形状上。

[0034] 图 4 描绘了根据本发明的各个方面的各种方法。虽然，为了便于解释目的，将方法示出和描述为一系列的动作或者顺序步骤，但应当理解和明白的是，本发明并不受这些动作的顺序的限制，这是因为某些动作可以以不同的顺序发生和 / 或与本申请示出和描述的其它动作一起同时发生。例如，本领域普通技术人员应当理解和明白的是，一个方法可以替代地表示成一系列相互关联的状态或事件，如在状态图中。此外，实现根据本发明的方法，并不需要所有描绘的动作。此外，还应当理解的是，下文所公开的和贯穿本说明书的方法能够保存在制品上，以便于向计算机传送和传输这些方法。如本申请所使用的，术语制品旨在涵盖可从任何计算机可读器件、载体或介质访问的计算机程序。

[0035] 现参见图 4，该图描绘了用于描述使用 SE 的处理 400 的示例流程图，其中该 SE 至少部分地与 SoC 集成在一起。在一个方面，处理 400 可以由包括 SE(例如，SE 560) 的通信设备 (例如，通信设备 500) 来执行。

[0036] 在方框 402 处，SE 可以接收对访问一种功能 (例如，应用) 的请求。在一个方面，该请求可以是响应于一种应用的激活而接收的、从一个或多个传感器获得的测量值、响应于从另一个设备接收的数据等。在一个方面，该请求可以是响应于下面情形而接收的：一种应用的激活、从一个或多个传感器获得的测量值、从另一个设备接收的数据等。在一个方面，该请求可以是通过该 SE 和通信设备之间的加密安全接口来接收的。

[0037] 在方框 404 处，SE 可以从该 SE 的安全组件获取与该功能相关联的信息的一部分。在一个方面，该信息可以包括：与以安全方式来访问所请求的功能相关联的密钥、证书等。在另一个方面，可以将 SE 的安全组件集成到 SoC 中 (例如但不限于 MSM 芯片、NFCC 等)。在一个方面，可以通过只将 SE 的安全组件集成到 SoC 中，来使 SE 在 SoC 上的封装 (footprint) 最小化。在另一个方面，SE 的安全组件可以具有小于或等于 65nm 的几何尺寸。

[0038] 在方框 406 处，SE 可以从该 SE 的非安全组件中的存储设备，获得与该功能相关联的信息的一部分。在一个方面，非安全组件可以包括标准 NVM，其可以存储与可通过该 SE 访问的各种功能相关联的代码、小应用程序等。在另一个方面，可以通过高速接口，将所获取的信息的部分传输给 SE 的安全组件。在该方面，可以将所获取的信息部分放置在 SE 的安全组件中可用的存储器里。在一个方面，可以以基于在安全组件中存储的信息部分的加密

格式，对于在 SE 的非安全组件中存储的信息部分进行存储。

[0039] 在方框 408 处，SE 可以基于从该 SE 的非安全组件获得的信息和从该 SE 的安全组件获得的信息，来促进针对该功能的访问。在一个方面，当以加密格式来存储在 SE 的非安全组件中保存的信息部分时，促进访问可以包括：对该信息进行解密。

[0040] 因此，处理 400 提供了一种用于使用 SE 的方法，其中该 SE 至少部分地集成到 SoC 中。

[0041] 在参见图 3 时，但现在还转到图 5，该图描绘了通信设备 500 的示例性体系结构。如图 5 中所示，通信设备 500 包括接收机 502，其从例如接收天线（没有示出）接收信号，对所接收的信号执行动作（例如，滤波、放大、下变频等），并数字化所调节的信号以获得采样。接收机 502 可以包括解调器 504，其可以对所接收的符号进行解调，并将它们提供给处理器 506 以用于信道估计。处理器 506 可以是专用于分析接收机 502 接收的信息和 / 或生成由发射机 520 发送的信息的处理器、用于控制通信设备 500 的一个或多个组件的处理器、和 / 或既分析由接收机 502 接收的信息、生成由发射机 520 发送的信息，又控制通信设备 500 的一个或多个组件的处理器。此外，发射机 520 通过调制器 518 对信号进行传输准备，其中调制器 518 可以对处理器 506 所处理的信号进行调制。

[0042] 另外，通信设备 500 还可以包括存储器 508，其操作性地耦合至处理器 506，其中存储器 508 可以存储要发送的数据、接收的数据、与可用信道有关的信息、TCP 流、与分析的信号和 / 或干扰强度相关联的数据、与分配的信道有关的信息、功率、速率等、以及用于估计信道和通过该信道进行通信的任何其它适当信息。此外，处理器 506 和 / 或设备主机 534 可以被配置为辅助 NFC 系统的控制。

[0043] 在一个方面，处理器 506、NFCC 530 和 / 或 SE 560 可以提供：用于接收对可通过 SE 560 中存储的信息来访问的功能进行访问的请求的单元；用于获取在 SE 560 的安全组件 562 中存储的与该功能相关联的信息的第一部分的单元；用于获得在 SE 560 的非安全组件 564 中存储的与该功能相关联的信息的第二部分的单元；用于使用所获取的所述信息的第一部分来促进针对该功能的访问，以便能够访问所获得的所述信息的第二部分的单元。在一个方面，SE 560 可以包括处理器 506、RAM 和 NVM。在一个方面，安全组件 562 可以包括该处理器和 RAM。在一个方面，非安全组件 564 可以包括几乎所有的 NVM。

[0044] 应当理解的是，本申请描述的数据存储器（例如，存储器 508）可以是易失性存储器或 NVM，或者可以包括易失性存储器和 NVM 二者。通过示例而不是限制的方式，NVM 可以包括只读存储器 (ROM)、可编程 ROM(PROM)、电可编程 ROM(EPROM)、电可擦写 PROM(EEPROM) 或者闪存。易失性存储器可以包括充当为外部高速缓冲存储器的随机存取存储器 (RAM)。通过示例而不是限制的方式，RAM 能以多种形式可用，例如同步 RAM(SRAM)、动态 RAM(DRAM)、同步 DRAM(SDRAM)、双倍数据速率 SDRAM(DDR SDRAM)、增强型 SDRAM(ESDRAM)、同步链接 DRAM(SLDRAM) 和直接型 Rambus RAM(DRRAM)。本发明的系统和方法的存储器 508 可以包括，但不限于，这些和任何其它适当类型的存储器。

[0045] 在另一个方面，通信设备 500 可以包括 NFC 控制器接口 (NCI)550。在一个方面，NCI 550 可用于实现 NFC 启用天线（例如，502、520）和 NFC 控制器 530 之间的通信。NCI 550 可以被配置为以监听模式和 / 或轮询模式进行工作。

[0046] 在另一个方面，通信设备 500 可以包括一个或多个安全单元 560。在一个方面，所

述一个或多个安全单元 560 可以耦接到 NFC 控制器 530，和 / 或至少部分地集成在 NFC 控制器 530 之中。在一个方面，所述一个或多个安全单元 560 可以耦接到 MSM 芯片（例如，处理器 506），和 / 或至少部分地集成在 MSM 芯片之中。在一个方面，所述一个或多个安全单元 560 可以是安全单元或者近场控制器执行环境 (NFCEE)。在一个方面，所述一个或多个安全单元 560 可以包括具有各种模块（例如，但不限于 SIM、CSIM 等）的 UICC。在另一个方面，所述一个或多个安全单元 560 可以被配置为执行图 4 中所描述的处理。

[0047] SE 560 可以包括安全组件 562 和非安全组件 564。安全组件 562 和非安全组件可以通过一种接口相耦合。在一个方面，该接口可以被配置为使用支持加密的总线接口。在另一个方面，该接口可以是标准高速接口。在该方面，该接口提供将代码、小应用程序等从非安全存储器 322 高效地装载到 SE 560 的安全组件 562 以进行处理。

[0048] 安全组件 562 可以包括安全存储器 568。在一个方面，安全存储器 568 可以包括足够的存储器，以保存可以通过保护来获益的各个项（例如，根密钥、证书等）。在一个方面，安全存储器 568 可以包括 5 到 10K 比特的空间。在一个方面，安全存储器 568 可以包括足够的存储能力，以允许非安全存储器 564 中存储的信息的高效装载和处理。

[0049] 此外，安全组件 562 可以是使用安全屏蔽 566 来变得安全的。在一个方面，安全屏蔽 566 可以提供针对基于硬件攻击的各种预防措施，例如，但不限于：用于使内部操作的观察更加困难的金属层；当包装被打开时，禁用操作的光传感器；用于类似操作的多个硬件路径等。在一个方面，安全屏蔽 566 可以使用与 SoC 相关联的现有金属层，来实现用于形成安全屏蔽的数字或模拟 IP。

[0050] 非安全组件 564 可以包括非安全存储器 570。在一个方面，非安全存储器 570 可以专用于向安全存储设备、标准 NVM 或者其任意组合提供任务。在一个方面，非安全存储器 570 可以配置有近似 1.2M 字节的空间。在另一个方面，非安全存储器 570 可以用于存储：与可通过 SE 560 访问的各种功能相关联的代码、小应用程序等。在该方面，非安全存储器 570 可以用于应用（例如，计算机代码）和数据的非易失性存储，安全存储器 568 可以用于存储与这些应用相关联的密钥系统。在一个方面，为了帮助维持代码和数据的安全性和完整性，防止通过外部接口的攻击，只要当数据离开 SoC560 时，就对该数据进行加密（以确保安全）和签名（以保证完整性）。因此，可以使非安全存储器 570 中的信息的安全，达到在安全组件 562 中所使用的加密操作所提供的能力的程度。

[0051] 另外，通信设备 500 可以包括用户接口 540。用户接口 540 可以包括用于生成针对通信设备 500 的输入的输入装置 542、以及用于生成由通信设备 500 的用户使用的信息的输出装置 544。例如，输入装置 542 可以包括诸如键或键盘、鼠标、触摸屏显示器、麦克风等之类的装置。此外，例如，输出装置 544 可以包括显示器、音频扬声器、触觉反馈装置、个域网 (PAN) 收发机等。在所描绘的方面，输出装置 544 可以包括用于以图像或视频格式呈现媒体内容的显示器，或者用于以音频格式呈现媒体内容的音频扬声器。

[0052] 图 6 描述了可用于促进使用 SE 308 的高效功能的示例性通信系统 600 的框图，其中 SE 308 可以至少部分地集成到一个通信设备中。例如，通信系统 600 可以至少部分地位于通信设备（例如，通信设备 500）之内。此外，SE 308 可以至少部分地位于该通信设备（例如，通信设备 500）之内。应当明白的是，系统 600 表示为包括一些功能模块，而这些功能模块表示由处理器、软件或者其组合（例如，固件）实现的功能。系统 600 包括协力操作

的电子组件的逻辑组 602。

[0053] 例如，逻辑组 602 可以包括可以提供用于接收对可通过 SE 中存储的信息来访问的功能进行访问的请求的单元的电子组件。例如，该用于接收的单元可以包括 SE 308 的安全组件 310 和处理器 312、和 / 或通信设备 500 的处理器 506。

[0054] 此外，逻辑组 602 可以包括可以提供用于获取在 SE 的安全组件中存储的、与该功能相关联的信息的第一部分的单元 606 的电子组件。在一个方面，该安全组件可以包括所述处理器和 RAM。例如，该获取单元 606 可以包括 SE 308 的安全组件 310、安全 NVM 314 和 / 或处理器 312。

[0055] 此外，逻辑组 602 可以包括可以提供用于获得在 SE 的非安全组件中存储的、与该功能相关联的信息的第二部分的单元 608 的电子组件。在一个方面，该非安全组件可以包括几乎所有的 NVM。例如，该获得单元 608 可以包括 SE 308 的安全组件 310、非安全组件 320、安全 NVM 314、非安全存储器 322 和 / 或处理器 312。在一个方面，该获得单元 608 可以被配置为：在该 SE 的非安全组件和该 SE 的安全组件之间使用高速接口。

[0056] 此外，逻辑组 602 可以包括可以提供用于使用所获取的信息的第一部分来促进对所述功能的访问，以便能够访问所获得的信息的第二部分的单元 610 的电子组件。在一个方面，该用于促进访问的单元 610 可以包括 SE308 的安全组件 310、非安全组件 320、安全 NVM 314、非安全存储器 322 和 / 或处理器 312。

[0057] 在一个可选的方面，逻辑组件 602 可以包括可以提供用于对与一个功能相关联的信息进行解密的单元 612 的电子组件。例如，该用于解密的单元 612 可以包括 SE 308 的安全组件 310 和 / 或处理器 312。

[0058] 另外，系统 600 可以包括存储器 614，存储器 614 保存用于执行与电子组件 604、606、608、610 和 612 相关联的功能的指令，存储由电子组件 604、606、608、610、612 等使用或者获得的数据。在一个方面，存储器 614 可以包括存储器 508，和 / 或被包括在存储器 508 中。虽然图中将电子组件 604、606、608、610 和 612 示为位于存储器 614 之外，但应当理解的是，电子组件 604、606、608、610 和 612 中的一个或多个可以位于存储器 614 之内。在一个示例中，电子组件 604、606、608、610 和 612 可以包括至少一个处理器，或者每一个电子组件 604、606、608、610 和 612 可以是至少一个处理器的相应模块。此外，在另外的或者替代的示例中，电子组件 604、606、608、610 和 612 可以是包括计算机可读介质的计算机程序产品，其中每一个电子组件 604、606、608、610 和 612 可以是相应的代码。

[0059] 如本申请所使用的，术语“组件”、“模块”、“系统”等旨在包括与计算机相关实体，例如，但不限于：硬件、固件、硬件和软件的结合、软件或运行中的软件。例如，组件可以是，但不限于是：在处理器上运行的处理、处理器、对象、可执行文件、执行的线程、程序和 / 或计算机。举例而言，在计算设备上运行的应用和计算设备都可以是组件。一个或多个组件可以存在于处理和 / 或执行线程中，组件可以位于一个计算机中和 / 或分布在两个或更多计算机之间。此外，这些组件能够从在其上具有存储的各种数据结构的各种计算机可读介质中执行。这些组件可以通过诸如根据具有一个或多个数据分组的信号（例如，来自一个组件的数据，该组件与本地系统、分布式系统中的另一个组件进行交互和 / 或以信号的方式通过诸如互联网之类的网络与其它系统进行交互），以本地和 / 或远程处理的方式进行通信。

[0060] 此外，本申请结合终端（其可以是有线终端或无线终端）描述了各个方面。终端也可以称作为系统、设备、用户单元、用户站、移动站、移动台、移动设备、远程站、移动装备 (ME)、远程终端、接入终端、用户终端、终端、通信设备、用户代理、用户设备或用户装备 (UE)。无线终端可以是蜂窝电话、卫星电话、无绳电话、会话发起协议 (SIP) 电话、无线本地环路 (WLL) 站、个人数字助理 (PDA)、具有无线连接能力的手持设备、计算设备或连接到无线调制解调器的其它处理设备。此外，本申请结合基站描述了各个方面。基站可以用于与无线终端进行通信，基站还可以称为接入点、节点 B、或某种其它术语。

[0061] 此外，术语“或”意味着包括性的“或”而不是排外的“或”。也就是说，除非另外说明或者从上下文中明确得知，否则“X 使用 A 或 B”意味任何正常的或排列。也就是说，如果 X 使用 A ；X 使用 B ；或者 X 使用 A 和 B，那么在任何上述实例中都满足“X 使用 A 或 B”。此外，本申请和所附权利要求书中使用的冠词“一个 (a)”和“一 (an)”通常应当解释为意味“一个或多个”，除非另外说明或者从上下文中明确得知其针对于单数形式。

[0062] 本申请所描述的技术可以用于各种无线通信系统，比如 CDMA、TDMA、FDMA、OFDMA、SC-FDMA 及其它系统。术语“系统”和“网络”经常可以交换使用。CDMA 系统可以实现诸如通用陆地无线接入 (UTRA)、CDMA2000 等之类的无线技术。UTRA 包括宽带 CDMA(W-CDMA) 和 CDMA 的其它变形。此外，CDMA2000 覆盖 IS-2000、IS-95 和 IS-856 标准。TDMA 系统可以实现诸如全球移动通信系统 (GSM) 之类的无线技术。OFDMA 系统可以实现诸如演进的 UTRA(E-UTRA)、超移动宽带 (UMB)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、Flash-OFDMA 等之类的无线技术。UTRA 和 E-UTRA 是通用移动通信系统 (UMTS) 的一部分。3GPP 长期演进 (LTE) 是 UMTS 的采用 E-UTRA 的版本，其在下行链路上使用 OFDMA，并在上行链路上使用 SC-FDMA。在来自名为“第三代合作伙伴计划”(3GPP) 的组织的文档中描述了 UTRA、E-UTRA、UMTS、LTE 和 GSM。另外，在来自名为“第三代合作伙伴计划 2”(3GPP2) 的组织的文档中描述了 CDMA2000 和 UMB。此外，这些无线通信系统还可以包括对等的（例如，移动台对移动台的）ad hoc 网络系统，其通常使用不成对的未经许可的频谱、802.xx 无线 LAN、蓝牙 (BLUETOOTH)、近场通信 (NFC-A、NFC-B、NFC-F 等）和任何其它短程或远程无线通信技术。

[0063] 本申请围绕包括多个设备、组件、模块等的系统来呈现各个方面或特征。应当理解和明白的是，各个系统可以包括另外的设备、组件、模块等和 / 或可以不包括结合附图讨论的所有设备、组件、模块等。还可以使用这些方法途径的组合。

[0064] 用于执行本申请所述功能的通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其它可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件部件或者其任意组合，可以用来实现或执行结合本申请所公开方面描述的各种示例性的逻辑、逻辑框、模块和电路。通用处理器可以是微处理器，或者，该处理器也可以是任何常规的处理器、控制器、微控制器或者状态机。处理器也可以实现为计算设备的组合，例如，DSP 和微处理器的组合、若干微处理器、一个或多个微处理器与 DSP 内核的结合，或者任何其它此种结构。另外，至少一个处理器可以包括可用于执行上述的一个或多个步骤和 / 或动作的一个或多个模块。

[0065] 此外，结合本申请所公开方面描述的方法或者算法的步骤和 / 或动作可直接实现为硬件、用处理器执行的软件模块或者实现为两者的组合。软件模块可以位于 RAM 存储器、

闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、移动硬盘、CD-ROM 或者本领域已知的任何其它形式的存储介质中。可以将一种示例性的存储介质连接至处理器，从而使该处理器能够从该存储介质读取信息，并且可向该存储介质写入信息。或者，存储介质也可以是处理器的组成部分。此外，在一些方面，处理器和存储介质可以位于 ASIC 中。另外，该 ASIC 可以位于用户终端中。当然，处理器和存储介质也可以作为分立组件存在于用户终端中。另外，在一些方面，方法或算法的步骤和 / 或动作可以作为代码和 / 或指令集中的一个或任意组合位于机器可读介质和 / 或计算机可读介质上，其中所述机器可读介质和 / 或计算机可读介质可以并入到计算机程序产品中。

[0066] 在一个或多个方面，本申请所述功能可以用硬件、软件、固件或其任意组合的方式来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是计算机能够存取的任何可用介质。通过示例的方式而不是限制的方式，这种计算机可读介质可以包括 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储、磁盘存储介质或其它磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机进行存取的任何其它介质。此外，几乎任何连接都可以称为计算机可读介质。例如，如果软件是使用同轴电缆、光纤光缆、双绞线、数字用户线 (DSL) 或者诸如红外线、无线和微波之类的无线技术从网站、服务器或其它远程源传输的，那么同轴电缆、光纤光缆、双绞线、DSL 或者诸如红外线、无线和微波之类的无线技术包括在所述介质的定义中。如本申请所使用的，磁盘和光盘包括压缩盘 (CD)、激光碟、光碟、数字多用途光碟 (DVD)、软盘和蓝光光碟，其中磁盘通常磁性地复制数据，而光盘则用激光来光学地复制数据。上面的组合也应当包括在计算机可读介质的保护范围之内。

[0067] 虽然上述公开内容讨论了示例性的方面和 / 或一些方面，但应当注意的是，在不脱离所描述的方面和 / 或如所附权利要求书所规定方面的保护范围的基础上，可以对本申请做出各种改变和修改。此外，虽然用单数形式描述或主张了所描述方面和 / 或一些方面的元素，但除非明确说明限于单数，否则复数形式是可以预期的。此外，除非另外说明，否则任何方面和 / 或方面的所有部分或一部分可以与任何其它方面和 / 或方面的所有部分或一部分一起使用。

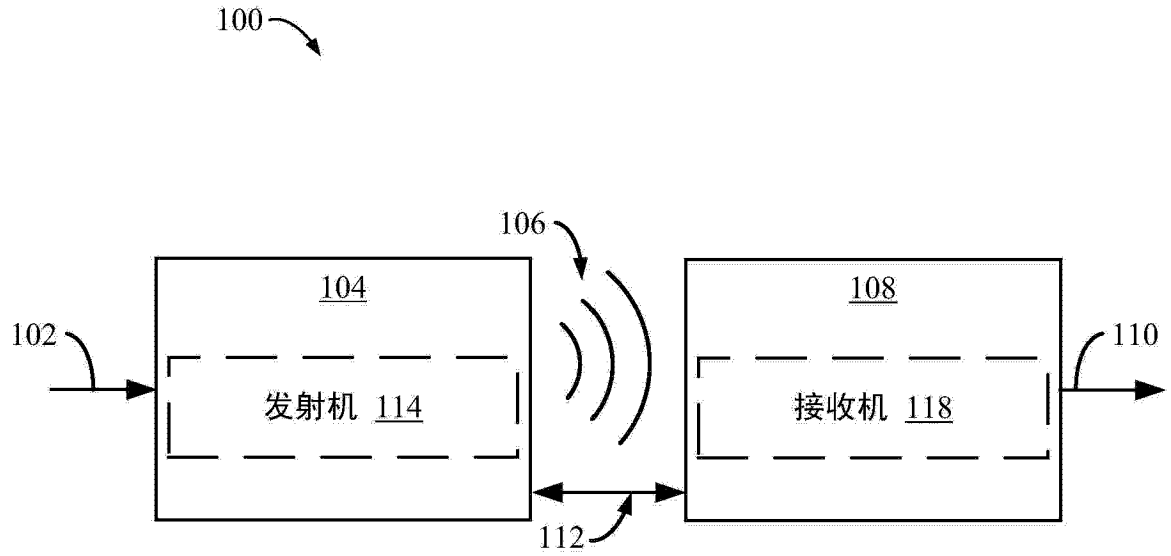

100
106
104
108
102
110
发射机 114
接收机 118
112

图 1

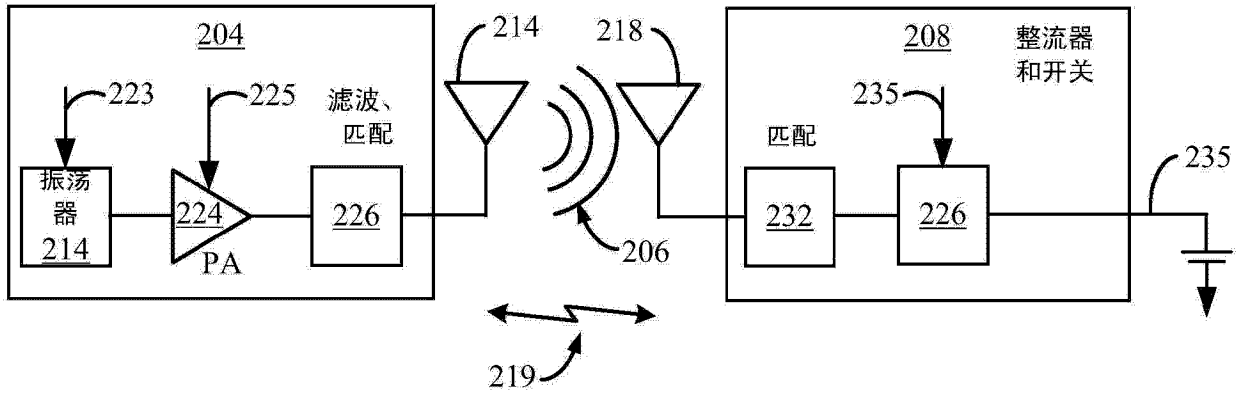

204
214
218
208
整流器
和开关
223
225
滤波、
匹配
235
匹配
振荡
器
214
224
PA
226
206
232
226
235
219

图 2

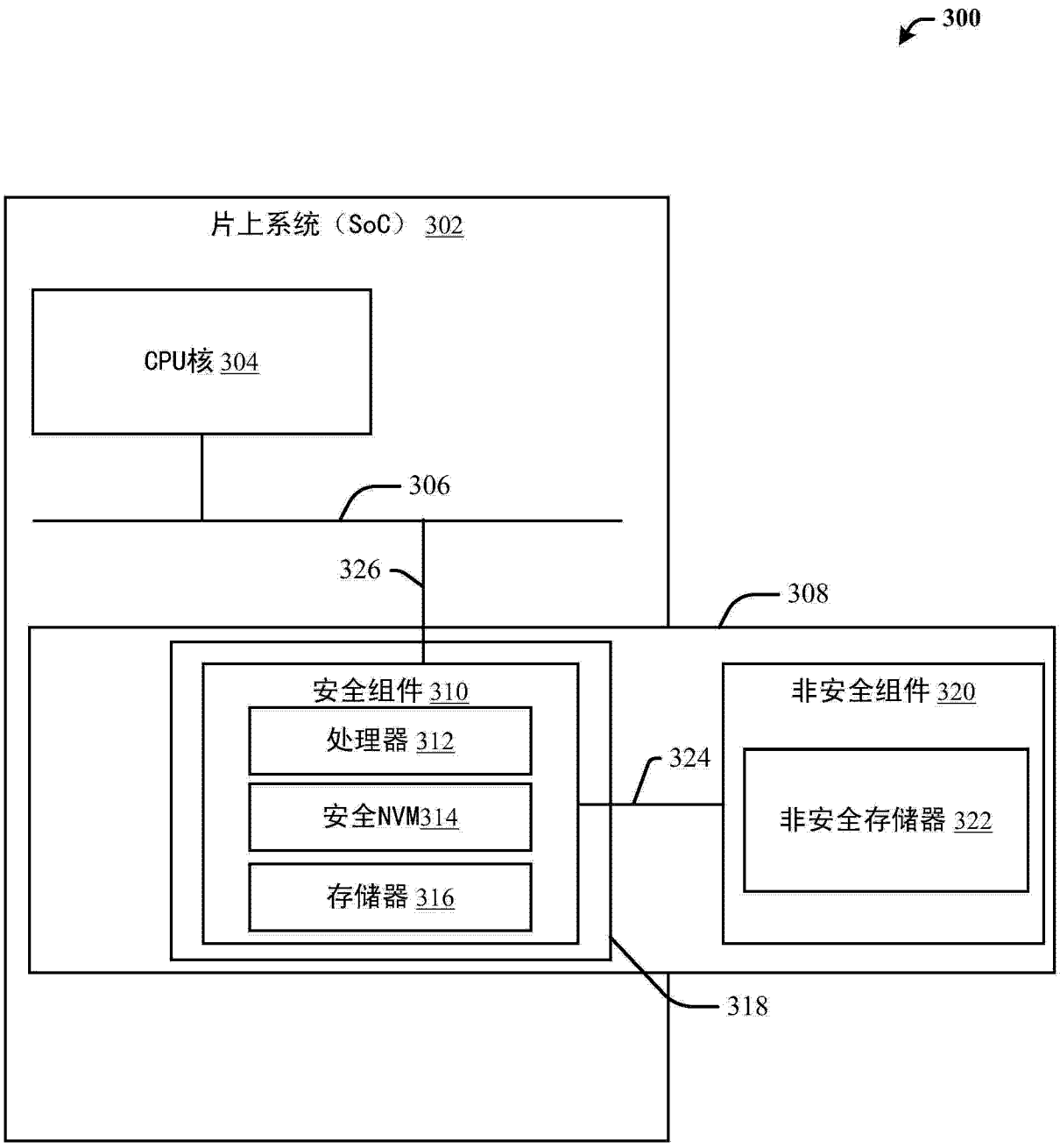

300
片上系统（SoC） 302
CPU核 304
306
326
308
安全组件 310
处理器 312
安全NVM314
存储器 316
非安全组件 320
非安全存储器 322
324
318

图 3

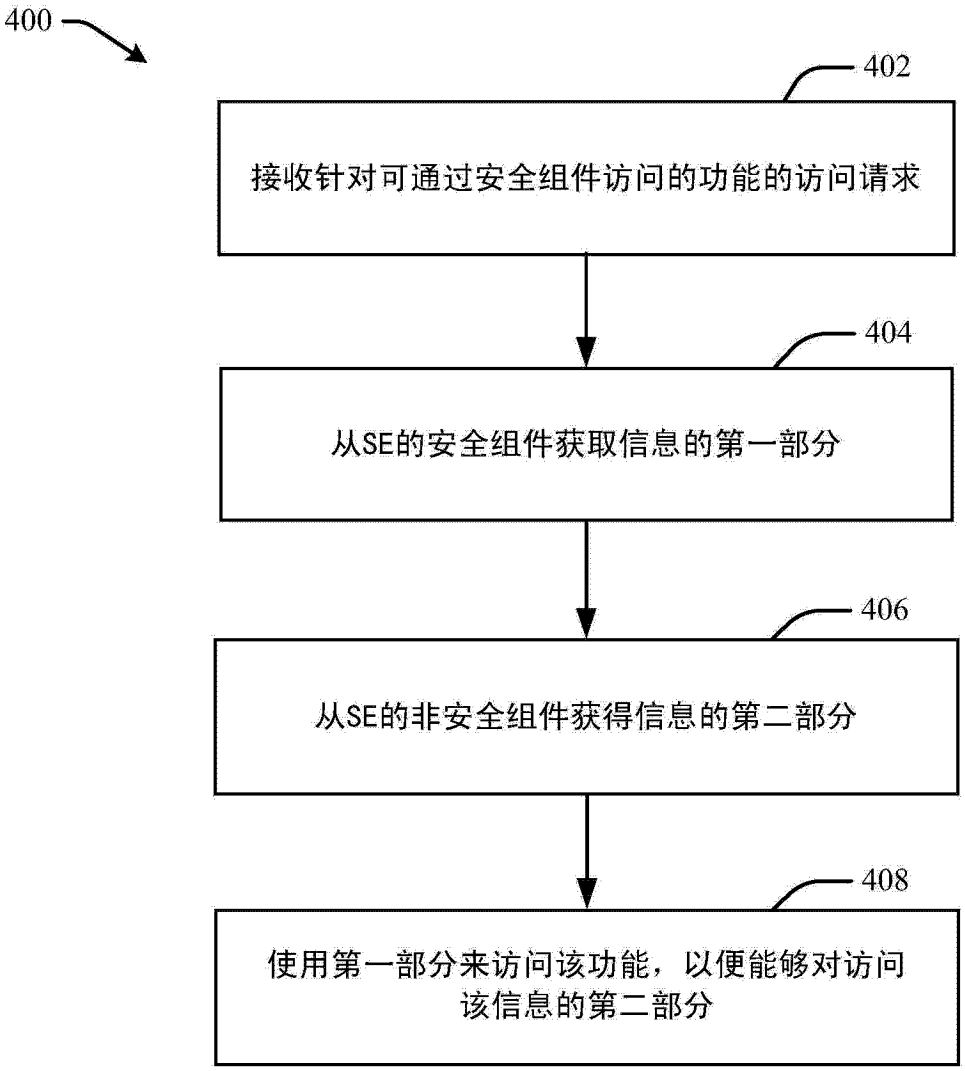

400
402
接收针对可通过安全组件访问的功能的访问请求
404
从SE的安全组件获取信息的第一部分
406
从SE的非安全组件获得信息的第二部分
408
使用第一部分来访问该功能，以便能够对访问该信息的第二部分

图 4

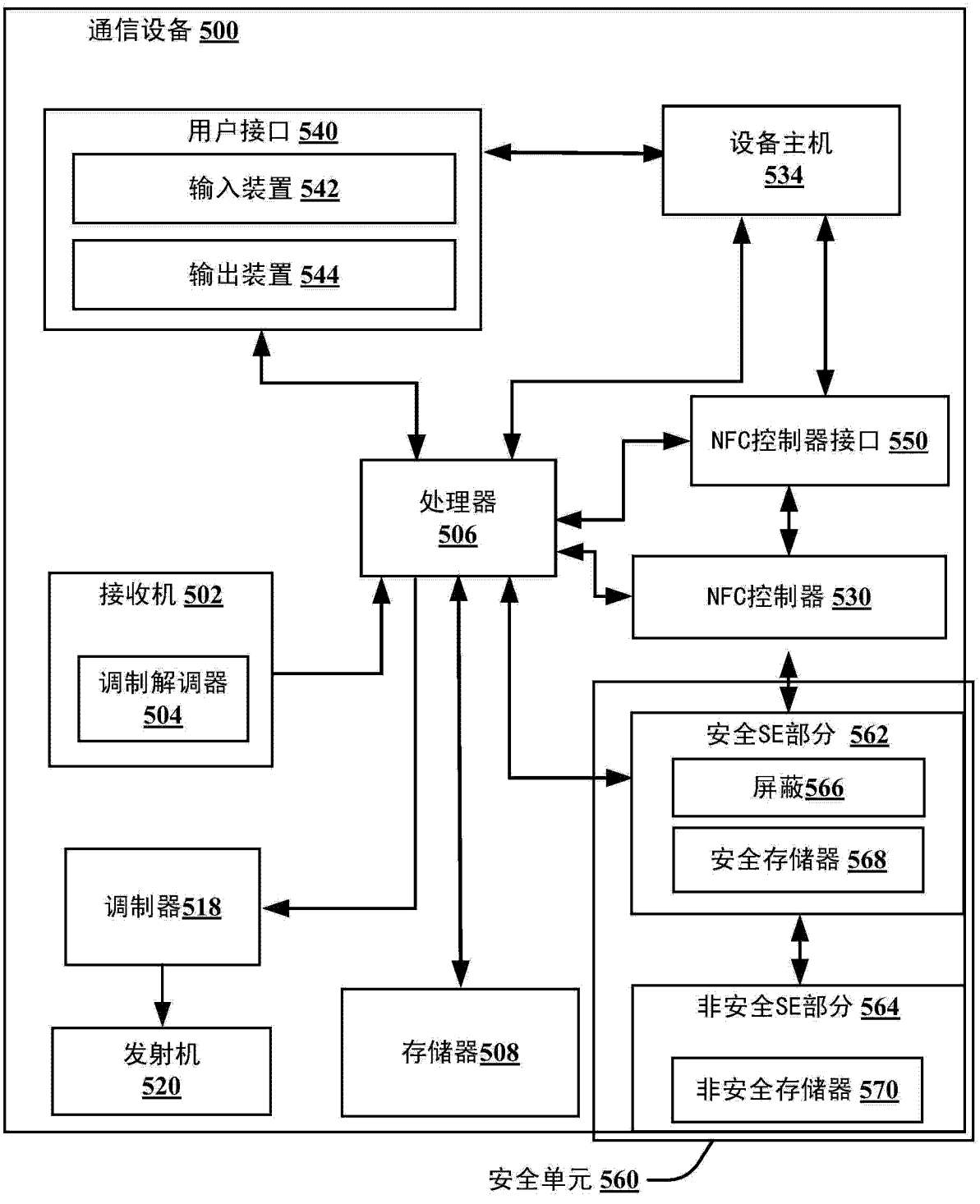

通信设备 500
用户接口 540
输入装置 542
输出装置 544
设备主机 534
NFC控制器接口 550
处理器 506
NFC控制器 530
接收机 502
调制解调器 504
安全SE部分 562
屏蔽566
安全存储器 568
调制器518
非安全SE部分 564
非安全存储器 570
发射机 520
存储器508
安全单元 560

图 5

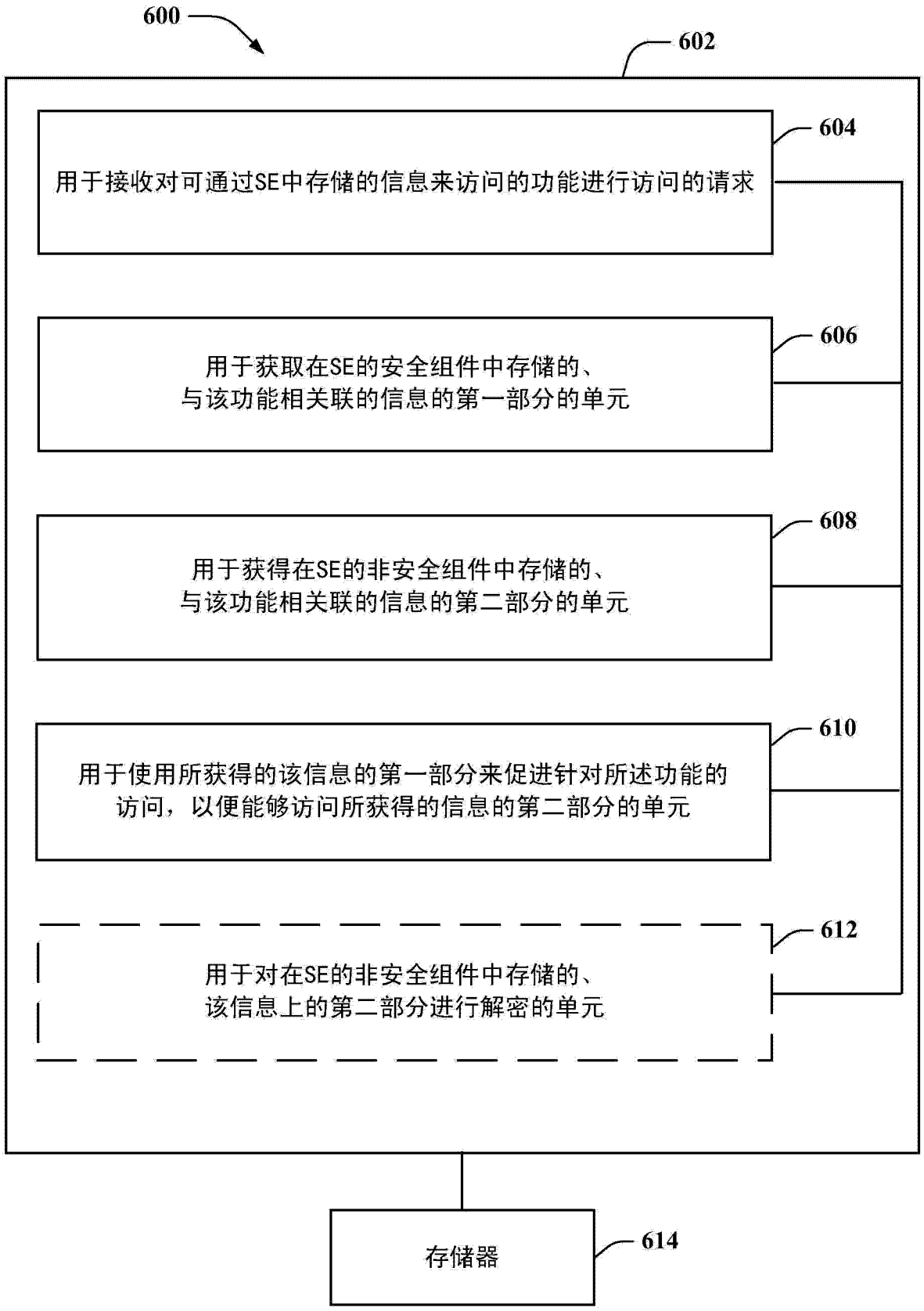

600
602
用于接收对可通过SE中存储的信息来访问的功能进行访问的请求
604
用于获取在SE的安全组件中存储的、
与该功能相关联的信息的第一部分的单元
606
用于获得在SE的非安全组件中存储的、
与该功能相关联的信息的第二部分的单元
608
用于使用所获得的该信息的第一部分来促进针对所述功能的
访问，以便能够访问所获得的信息的第二部分的单元
610
用于对在SE的非安全组件中存储的、
该信息上的第二部分进行解密的单元
612
存储器
614

图 6