(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112074836 B
(45)授权公告日 2023.11.03

(21)申请号 201980030106.7
(22)申请日 2019.04.24
(65)同一申请的已公布的文献号
申请公布号 CN 112074836 A
(43)申请公布日 2020.12.11
(30)优先权数据
15/971,498 2018.05.04 US
(85)PCT国际申请进入国家阶段日
2020.11.03
(86)PCT国际申请的申请数据
PCT/CN2019/083997 2019.04.24
(87)PCT国际申请的公布数据
WO2019/210794 EN 2019.11.07
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 莫志军 叶剑飞

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
专利代理师 申健
(51)Int.Cl.
G06F 21/62(2006.01)
H04L 9/32(2006.01)

(56)对比文件
EP 2953290 A1,2015.12.09
EP 3293653 A1,2018.03.14
US 2010229219 A1,2010.09.09
US 2016234176 A1,2016.08.11
US 2016254904 A1,2016.09.01

审查员 姜晓庆

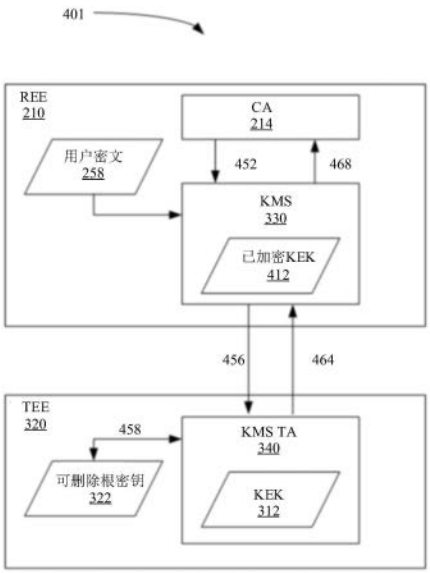
权利要求书3页 说明书10页 附图10页

(54)发明名称

通过可信执行环境保护数据的设备和方法

(57)摘要

本发明提供了一种计算设备，包括：可信执行环境，其可以访问存储有可删除根密钥的存储器，所述存储器无法由第二执行环境访问；可在所述可信执行环境中运行的至少一个处理器，在所述可信执行环境中操作时，所述至少一个处理器用于：基于来自所述第二执行环境的请求，对所述第二执行环境使用的加密密钥执行根密钥操作，以保护所述第二执行环境可访问的数据；在检测到安全事件之后，删除所述根密钥。



CN 112074836 B

1.一种计算设备,其特征在于,包括:

可信执行环境,其可以访问存储有可删除根密钥的存储器,所述存储器无法由第二执行环境访问;

可在所述可信执行环境中运行的至少一个处理器,在所述可信执行环境中操作时,所述至少一个处理器用于:

基于来自所述第二执行环境的请求,使用所述存储器中的可删除根密钥对所述第二执行环境使用的加密密钥执行根密钥操作,以保护所述第二执行环境可访问的数据;

在检测到安全事件之后,删除所述存储器中的所述根密钥。

2.根据权利要求1所述的计算设备,其特征在于,

在所述可信执行环境中操作时,所述至少一个处理器用于检测所述安全事件,其中,所述检测所述安全事件包括:检测系统完整性漏洞或从所述第二执行环境接收指示可疑活动的消息。

3.根据权利要求1或2所述的计算设备,其特征在于,在所述可信执行环境中操作时,所述至少一个处理器用于生成所述根密钥。

4.根据权利要求1或2所述的计算设备,其特征在于,在所述可信执行环境中操作时,所述至少一个处理器用于:

从所述第二执行环境接收解密已加密数据密钥的请求;

在所述根密钥已删除时,向所述第二执行环境发送错误消息。

5.根据权利要求1或2所述的计算设备,其特征在于,在所述可信执行环境中操作时,所述至少一个处理器用于:基于从所述第二执行环境中运行的密钥管理业务(key management service,KMS)接收到的请求执行密钥管理业务可信授权(key management service trusted authority,KMS TA),以进行所述根密钥操作。

6.根据权利要求1或2所述的计算设备,其特征在于,在所述可信执行环境中操作时,所述至少一个处理器用于:

生成密钥加密密钥(key encryption key,KEK)或从所述第二执行环境接收所述KEK;

使用所述根密钥加密所述KEK;

向所述第二执行环境发送所述已加密KEK。

7.根据权利要求1或2所述的计算设备,其特征在于,在所述可信执行环境中进行操作时,所述至少一个处理器用于:

从所述第二执行环境接收数据密钥和已加密密钥加密密钥(key encryption key,KEK);

使用所述根密钥解密所述已加密KEK;

使用所述解密后的KEK加密所述数据密钥;

向所述第二执行环境发送所述已加密数据密钥。

8.根据权利要求1或2所述的计算设备,其特征在于,在所述可信执行环境中进行操作时,所述至少一个处理器用于:

从所述第二执行环境接收已加密数据密钥和已加密密钥加密密钥(key encryption key,KEK);

使用所述根密钥解密所述已加密KEK;

使用所述KEK解密所述已加密数据密钥；

向所述第二执行环境发送所述数据密钥。

9.根据权利要求1或2所述的计算设备，其特征在于，所述第二执行环境为富执行环境(rich execution environment,REE)。

10.一种计算机实现的数据保护方法，其特征在于，包括：

将可删除根密钥存储在计算设备的可信执行环境可访问的存储器中，所述存储器无法由第二执行环境访问；

基于来自所述第二执行环境的请求，所述可信执行环境中运行的所述计算设备的至少一个处理器使用所述存储器中的可删除根密钥对所述第二执行环境使用的加密密钥执行根密钥操作，以保护所述第二执行环境可访问的数据；

在检测到安全事件之后，删除所述存储器中的所述根密钥。

11.根据权利要求10所述的计算机实现的数据保护方法，其特征在于，包括：

所述可信执行环境中运行的所述计算设备的所述至少一个处理器检测所述安全事件，检测所述安全事件包括：检测系统完整性漏洞或从所述第二执行环境接收指示可疑活动的消息。

12.根据权利要求10或11所述的计算机实现的数据保护方法，其特征在于，包括：生成所述可删除根密钥并存储在所述可信执行环境可访问的所述存储器中。

13.根据权利要求10或11所述的计算机实现的数据保护方法，其特征在于，包括：

所述可信执行环境中运行的所述计算设备的所述至少一个处理器接收来自所述第二执行环境的解密已加密数据密钥的请求；

在所述根密钥已删除时，向所述第二执行环境发送错误消息。

14.根据权利要求10或11所述的计算机实现的数据保护方法，其特征在于，所述可信执行环境中运行的所述计算设备的所述至少一个处理器用于：基于从所述第二执行环境中运行的密钥管理业务(key management service,KMS)接收到的请求提供密钥管理业务可信授权(key management service trusted authority,KMS TA)，以进行所述根密钥操作。

15.根据权利要求10或11所述的计算机实现的数据保护方法，其特征在于，包括：

所述可信执行环境中运行的所述计算设备的所述至少一个处理器生成密钥加密密钥(key encryption key,KEK)或从所述第二执行环境接收所述KEK；

所述可信执行环境中运行的所述计算设备的所述至少一个处理器使用所述根密钥加密所述KEK；

向所述第二执行环境发送所述已加密KEK。

16.根据权利要求10或11所述的计算机实现的数据保护方法，其特征在于，包括：

所述可信执行环境中运行的所述计算设备的所述至少一个处理器从所述第二执行环境接收数据密钥和已加密密钥加密密钥(key encryption key,KEK)；

所述可信执行环境中运行的所述计算设备的所述至少一个处理器使用所述根密钥解密所述已加密KEK；

所述可信执行环境中运行的所述计算设备的所述至少一个处理器使用所述KEK加密所述数据密钥；

向所述第二执行环境发送所述已加密数据密钥。

17.根据权利要求10或11所述的计算机实现的数据保护方法,其特征在于,还包括:

所述可信执行环境中运行的所述计算设备的所述至少一个处理器从所述第二执行环境接收已加密数据密钥和已加密密钥加密密钥(key encryption key,KEK);

所述可信执行环境中运行的所述计算设备的所述至少一个处理器使用所述根密钥解密所述已加密KEK;

所述可信执行环境中运行的所述计算设备的所述至少一个处理器使用所述已解密KEK解密所述已加密数据密钥;

向所述第二执行环境发送所述数据密钥。

18.根据权利要求10或11所述的计算机实现的数据保护方法,其特征在于,所述第二执行环境为富执行环境(rich execution environment,REE)。

19.一种计算机可读存储介质,其特征在于,其上存储有计算机可执行指令,在执行所述计算机可执行指令时,可信执行环境中运行的计算设备的至少一个处理器执行权利要求10至18中任一项所述的方法。

通过可信执行环境保护数据的设备和方法

相关申请案交叉申请

[0001] 本申请要求于2018年5月4日递交的发明名称为“通过可信执行环境保护数据的设备和方法”(DEVICE AND METHOD FOR DATA SECURITY WITH A TRUSTED EXECUTION ENVIRONMENT)的第15/971,498号美国专利申请案的在先申请优先权,该在先申请的全部内容以引入的方式并入本文本中。

技术领域

[0002] 本文涉及数据安全,具体地,本发明实施例涉及计算设备和可信执行环境的数据安全的方法。

背景技术

[0003] 现代计算设备用于多种用途,其中许多都涉及用户或其它实体的私有、专有或敏感数据。例如,智能电话等计算设备通常用于存储账号等财务数据、支付证书、指纹等生物统计数据、PIN和密码。此外,计算设备通常存储加密密钥等,以用于安全通信和文档存储或用于受版权保护的媒介的回放等。这种数据对于用户和其它实体(例如软件开发人员、企业、金融机构以及媒介所有者和发行者)都是有价值的数据。因此,保护敏感数据(尤其是防止未经授权访问此类数据)非常重要。

发明内容

[0004] 根据本发明的一方面,提供了一种计算设备,包括:可信执行环境,其可以访问存储有可删除根密钥的存储器,所述存储器无法由第二执行环境访问;可在所述可信执行环境中运行的至少一个处理器,在所述可信执行环境中操作时,所述至少一个处理器用于:基于来自所述第二执行环境的请求,对所述第二执行环境使用的加密密钥执行根密钥操作,以保护所述第二执行环境可访问的数据;在检测到安全事件之后,删除所述根密钥。

[0005] 根据本发明的另一方面,提供了一种计算机实现的数据保护方法,包括:将可删除根密钥存储在计算设备的可信执行环境可访问的存储器中,所述存储器无法由第二执行环境访问;基于来自所述第二执行环境的请求,所述可信执行环境中运行的所述计算设备的所述至少一个处理器对所述第二执行环境使用的加密密钥执行根密钥操作,以保护所述第二执行环境可访问的数据;在检测到安全事件之后,删除所述存储器中的所述根密钥。

[0006] 根据本发明的另一方面,提供了一种非瞬时性计算机可读存储介质,其上存储有计算机可执行指令,在执行所述计算机可执行指令时,可信执行环境中运行的计算设备的至少一个处理器执行以下操作:将可删除根密钥存储在所述可信执行环境可访问的存储器中,所述存储器无法由第二执行环境访问;基于来自所述第二执行环境的请求,对所述第二执行环境使用的加密密钥执行根密钥操作,以保护所述第二执行环境可访问的数据;在检测到安全事件之后,删除所述存储器中的所述根密钥。

附图说明

[0007] 将结合附图示仅例性地描述实施例。在附图中：

[0008] 图1图示了计算设备的示意图；

[0009] 图2图示了根据实施例的具有两个执行环境的系统或设备的框图；

[0010] 图3图示了根据实施例的示例加密链各方面的表示的框图；

[0011] 图4A示出了根据一些实施例的图示了在应用程序请求创建密钥加密密钥(key encryption key,KEK)时TEE与REE之间的交互的系统框图；

[0012] 图4B为根据一些实施例的示出了已加密KEK的示例生成方法各方面的流程图；

[0013] 图5A示出了根据一些实施例的图示了TEE与REE之间用于保护数据加密密钥(data encryption key,DEK)的交互的系统框图；

[0014] 图5B为根据一些实施例的示出了已加密DEK的示例生成方法各方面的流程图；

[0015] 图6A示出了根据一些实施例的图示了TEE与REE之间用于对加密链加密的密钥进行解密的交互的系统框图；

[0016] 图6B为根据一些实施例的示出了已加密DEK的示例解密方法各方面的流程图；

[0017] 图7A示出了根据一些实施例的图示了检测到完整性漏洞时TEE与REE之间的交互的系统框图；

[0018] 图7B为根据一些实施例的示出了加密链加密的数据的示例保护方法各方面的流程图。

[0019] 应理解,在整个说明书和附图中,相似的特征由相似的附图标记标识。

具体实施方式

[0020] 方法、系统和装置的实施例通过参考附图描述。

[0021] 以下讨论提供了本发明主题的示例实施例。尽管每个实施例可以表示发明元素的单个组合,但是应认为本发明主题包括所公开元素的所有可能组合。因此,如果一个实施例包括元素A、B和C,而第二个实施例包括元素B和D,则即使未明确披露,也仍认为本发明主题包括A、B、C或D的其它剩余组合。

[0022] 图1图示了根据本发明一实施例的计算设备100的示例的示意图。计算设备100可以是智能电话、平板电脑、笔记本计算机等个人计算机、可穿戴计算设备、物联网(Internet of Things,IoT)设备等。

[0023] 计算设备100包括若干组件,包括处理器102、存储器104、存储设备106和用于连接计算设备100各组件的总线107。计算设备100还可以包括其它组件,例如一个或多个输入/输出(input/output,I/O)设备108和一个或多个网络接口110(以虚线示出)。计算设备100的各组件可以制成在一个或多个半导体芯片中,安装到用于在各组件之间进行通信的印刷电路板上。在一些实施例中,多个组件,例如处理器102和网络接口110,被并入称为片上系统的单个半导体芯片中。在其它实施例中,每个组件为分立芯片。

[0024] 处理器102是任何合适类型的处理器,例如实现ARM或x86指令集的处理器。

[0025] 存储器104是处理器102可访问的任何合适类型的随机存取存储器。存储器104包括安全存储器112。在一些实施例中,安全存储器112是分立的物理模块。在其它实施例中,存储器104会被分段,以在同一物理模块内将安全存储器定义为其它存储器。在一些实施例

中，安全存储器112占用了存储器104的地址空间内的一段存储器地址。在一些实施例中，处理器102可以在不同的存储器空间内访问安全存储器112。

[0026] 存储设备106可以是具有合适容量的一个或多个NAND闪存模块，或者可以是一个或多个永久性计算机存储设备，例如硬盘驱动器、固态驱动器等。存储设备106包括安全存储设备114。在一些实施例中，安全存储设备114驻留在与其它存储设备106共享的设备上。在其它实施例中，安全存储设备114驻留在分立硬盘驱动器、闪存等上。

[0027] 总线107可以是几种总线架构中任何一种或多种，包括存储器总线或存储器控制器以及外围总线。

[0028] I/O设备108包括用户接口设备等，如能够接收触摸形式的输入的电容或电阻式触敏屏，或者具有集成触摸传感器的触摸屏显示器，该触摸屏显示器用于在检测到触摸屏显示器上的触摸时接收输入，并在其上呈现图像作为输出。在一些实施例中，I/O设备108还包括扬声器、麦克风、加速度计和全球定位系统(global positioning system,GPS)接收器等传感器、小键盘、触摸板等中的一个或多个。在一些实施例中，I/O设备108包括用于将计算设备100连接到其它计算设备的端口。在一示例中，I/O设备108包括用于将计算设备100连接到外围设备或主机计算设备的通用串行总线(universal serial bus,USB)控制器。

[0029] 网络接口110能够将计算设备100连接到一个或多个通信网络。在一些实施例中，网络接口110包括一个或多个无线电，诸如Wi-Fi或蜂窝(例如，GPRS、GSM、EDGE、CDMA、LTE等)，用于将计算设备100无线连接至无线通信网络。

[0030] 计算设备100在包括操作系统(operating system,OS)116在内的软件程序的控制下操作。软件程序的计算机可读指令存储在存储设备106或安全存储设备114中，并由处理器102在存储器104或安全存储器112中执行。

[0031] 在一些实施例中，计算系统包括或用于提供多个不同的执行环境。在一些其它实施例中，计算设备100包括或用于提供多个不同的执行环境。在具有多个不同执行环境的计算设备100中，可以允许不同环境访问不同的存储资源和处理资源。这些环境可以使用软件或硬件隔离。在一些实施例中，这些环境之一可以被称为可信执行环境(trusted execution environment,TEE)，并且可以访问隔离的安全存储资源和处理资源。这些资源可以包括单独的处理器(例如，可以将多核处理器中的单个核分配给TEE)和隔离的存储设备(除了与隔离的核关联的寄存器之外，使用这种处理器或协同处理器时可以指示不同的存储器地址范围)。该环境可以支持不同的操作系统，或者可以是应用程序可访问的安全资源集合，其中，整个系统的底层操作系统(例如，OS 116)将该环境分配给所述应用程序使用。在一些实施例中，可以存在通用存储资源(例如，存储设备106)内的安全存储设备114等专用安全存储资源，以及通用存储器资源(例如，存储器104)内的安全存储器112等专用安全存储器。本领域技术人员应理解，在一些实施例中，这些安全资源可以在物理上和逻辑上至少与同一类型的通用资源不同。如上所述，在多核处理器中，一个或多个核可以专用于一个或多个TEE。在其它实施例中，处理器102外部的协同处理器可以为TEE提供安全的处理资源

[0032] 在包括或用于提供两个不同的执行环境的计算设备100中，第一执行环境是安全执行环境，而第二执行环境是潜在的不安全环境。安全执行环境有时称为可信执行环境(trusted execution environment,TEE)，而潜在的不安全环境有时称为富执行环境(rich

execution environment,REE)。

[0033] 在包括或用于提供两个不同的执行环境的计算设备100中,计算设备100等计算设备包括或用于提供安全执行环境,与第一计算设备不同的第二计算设备包括或用于提供可能不安全的第二执行环境。第二执行环境(例如,可能不安全的执行环境)用于与安全执行环境(例如,第一执行环境)通信以请求如本文所述的密钥操作。

[0034] 本文使用以下术语:

[0035] TEE:可信执行环境(Trusted Execution Environment)

[0036] REE:富执行环境(Rich Execution Environment)

[0037] TA:可信应用程序(Trusted Application)

[0038] CA:客户端应用程序(Client Application)

[0039] FDE:全盘加密(Full Disk Encryption)

[0040] FBE:基于文件的加密(File Based Encryption)

[0041] DEK:设备加密密钥(Device Encrypted Key)

[0042] CEK:证书加密密钥(Credential Encrypted Key)

[0043] KEK:密钥加密密钥(Key Encryption Key)

[0044] KMS:密钥管理业务(Key Management Service)

[0045] 在示例实施例中,处理器102包括一个或多个ARM Cortex-A™核,并且包括具有安全监控器逻辑的软件(例如,TrustZone™技术),该软件用于对ARM架构中的处理器进行逻辑划分(例如,虚拟分区),使得在一个逻辑分区中,处理器能够在安全执行环境中执行,在另一个逻辑划分中,处理器在第二执行环境中执行。

[0046] 其它实施方式也是可能的。如上所述,安全存储器112可以位于与存储器104分离的物理存储器模块中。或者可以在不同的地址空间或不同的地址范围中访问安全存储器112。同样,安全存储设备114可以位于单独的物理存储设备中,也可以位于存储设备106的不同分区或扇区中。在一些实施例中,单独的执行环境具有单独的物理处理器和/或其它硬件组件。

[0047] 在一些实施例中,两个不同的执行环境包括或可以访问单独的资源。例如,安全执行环境和第二执行环境都可以具有硬件模块和软件模块。安全执行环境具有安全处理器(可以是处理器102的虚拟分区或单独的硬件组件)、安全存储器(可以是存储器104的虚拟分区或单独的物理存储器)以及包括安全操作系统OS的软件代码。安全OS被加载到安全存储器中并且由安全处理器执行以执行本文所述方法的各方面(以及其它安全OS操作)。可以将安全OS存储在安全存储设备114或存储设备106中(只要使用本文所述的加密密钥链等进行了加密,就无须将安全OS存储在安全存储设备中)。

[0048] 第二执行环境包括处理器102、存储器104和存储设备106的不安全部分。第二执行环境的软件代码可以包括不安全OS,不安全OS存储在存储设备中,在运行时加载到存储器104以供由处理器102执行从而进行OS操作。

[0049] 在一些实施例中,如全球平台TEE系统架构所定义,安全执行环境是可信执行环境(trusted execution environment,TEE),第二执行环境是富执行环境(rich execution environment,REE)。例如,在一些实施例中,计算设备100符合全球平台TEE系统架构v1.0,并包括符合全球平台TEE系统架构v1.0定义的可信执行环境规范的一个安全操作系统。在

一些实施例中，安全操作系统、操作系统116和计算设备100实现TEE客户端API规范v1.0和TEE内核API规范v1.1.1.1等全球平台TEE API规范，并且安全操作系统与操作系统116之间的通信根据这些规范进行，所有这些规范以引入的方式并入本文本中。

[0050] 在本文所述的一些实施例中，“REE”可以指第二执行环境或不安全执行环境，这些术语可以互换使用。类似地，“TEE”可以指第一执行环境或安全执行环境，这些术语也可以互换使用。在其它实施例中，第二执行环境也可以是安全执行环境，因为第二执行环境可以访问另一执行环境不可访问的数据和/或资源。

[0051] 可以使用第一安全执行环境和第二执行环境以及一串加密密钥来加密第二执行环境中的数据。

[0052] 常规计算设备包括存储在安全存储器中并且只能由TEE访问的不可变唯一根密钥。不可变密钥在硬件中编码，或在制造时永久存储在TEE的安全存储设备中。可以将用于保护REE中的数据的加密密钥发送给TEE，以使用不可变根密钥进行加密。然后将加密的加密密钥存储在REE中。

[0053] 当要撤销对数据的访问权时，REE删除加密的加密密钥。如果没有加密的加密密钥，则无法恢复由未加密的加密密钥加密的任何数据或由未加密的加密密钥加密的第二加密密钥。

[0054] 但是，如果REE被破坏，则删除加密的加密密钥可能会被拦截、停止或回退。例如，恶意用户可能会备份加密的加密密钥，并在删除加密的加密密钥后恢复加密的加密密钥，以重新访问数据。

[0055] 一种实现防回退密钥的可能方式可以通过以下操作实现：记录TEE中已经用不可变根密钥加密的所有加密的加密密钥的哈希值，并将这些哈希值存储在安全存储设备中。当删除加密密钥时，TEE还可以从安全存储设备中删除其哈希值。从而，如果回退了任何已删除加密密钥，由于缺少密钥的对应哈希值，TEE可以拒绝使用不可变根密钥为恶意客户端提供服务。但是，如果TEE受到破坏，则TEE可以合作并为恶意客户端提供服务。

[0056] 受到破坏的REE备份和恢复(例如，回退)加密的加密密钥(或加密密钥的哈希值)的能力以及受到破坏的TEE使用不可变根密钥解密恢复的加密的加密密钥的能力使恶意软件未经授权便能访问使用包含加密的加密密钥的加密密钥链进行加密的敏感数据。

[0057] 在某些实例中，例如，如本文实施例所示的本发明各方面可以使计算设备的恶意软件或用户备份和恢复(例如，回退)加密密钥链的加密密钥的能力下降或消失，这使得从密码学而言，不可能解密使用加密密钥链的加密密钥加密的敏感数据，从而提高了加密数据的安全性。

[0058] 参考图2和图3，在一些实施例中，安全执行环境包括或具有对存储可删除根密钥(例如，可以从存储器中移除、擦除或删除的根密钥)的存储器的访问权限。该存储器为安全存储器，或无法由第二执行环境中或安全执行环境之外执行的应用程序访问。

[0059] 在一些实施例中，安全执行环境将执行安全执行环境中的任务与第二执行环境隔离。在一些实施例中，安全执行环境中的任务由可以在安全执行环境内的操作系统级别、固件级别或任何其它合适的抽象级别上运行的应用程序执行。

[0060] 在一些实施例中，软件模块应用程序用于在检测到触发条件时删除可删除根密钥。

[0061] 在一些实施例中,软件模块用于检测指示在第二操作系统或系统中其它地方检测到可疑活动或完整性漏洞的触发条件。

[0062] 如此处所述或在一些实施例中,术语“模块”可以指代可由处理器等硬件组件执行的软件模块或代码/指令集。在一些实施例中,术语“模块”可以包括硬件组件或电路等硬件模块。在一些实施例中,模块可以包括用于执行本文所述过程的一个或多个方面的软件和/或硬件组件的组合。

[0063] 图2为示出两个不同执行环境(例如,安全执行环境和第二执行环境)的各方面的框图。安全执行环境(例如,TEE 320)包括可以执行要在TEE 320内执行的安全功能的应用程序,例如用于对TEE 320的操作系统使用的加密密钥执行根密钥操作的应用程序。在一些平台中,TEE 320中的应用程序称为可信应用程序(trusted application,TA)222。在一些实施例中,可信应用程序可执行一些功能,例如充当密码密钥库,或者可以提供安全功能,该安全功能可以从在第二执行环境中运行的应用程序中卸载,或与之相关联。

[0064] 在一些实施例中,第二执行环境(例如,REE)210可以操作一个或多个应用程序,一个或多个应用程序可以包括电子邮件客户端或网络浏览器等用户应用程序。在图2所示实施例中,REE 210包括一个称为客户端应用程序(client application,CA)214的应用程序,CA 214可以调用TA 222或与TA 222交互,以分流敏感操作。在一些实施例中,CA 214和TA 222可以经由受控的环境间接口和/或API发送或传递数据。尽管在图2中描绘了一个CA 214,但是本领域普通技术人员将认识到在替代性实施例中,REE 210可以包括多个客户端应用程序,并且每个客户端应用程序CA 214可以调用多个TA或与多个TA交互,以分流敏感操作。

[0065] 在一些实施例中,客户端应用程序214可以包括REE 210中的密钥管理系统,例如KMS 330(图4A),该密钥管理系统调用函数或与对应的可信应用程序的密钥管理系统交互,该可信应用程序的密钥管理系统可以为TEE 320中的KMS TA 340(图4A)等。

[0066] 在一些实施例中,在TEE中运行的应用程序可以包括用于监控REE 210中的运行活动的系统监控模块324。例如,在一些实施例中,系统监控模块周期性地监控或在有访问触发时监控系统或进程的完整性,系统或进程可以为密钥管理系统或提供对TEE 320的访问权限的任何数量的硬件和/或软件组件(例如,入口模块或内置的anti-root/反恶意软件模块)。如果攻击者更改了这样的系统(其代码或数据)以绕过某些权限检查或将其强制关闭,则系统监控模块324将检测到此类事件(例如,通过验证代码和数据的被监控部分的摘要或签名),并触发适当操作以保护敏感数据。在REE 210中检测到可疑活动(例如异常)或危险(例如完整性系统漏洞)时,系统监控模块324可以删除可删除根密钥或触发可删除根密钥的删除。完整性系统漏洞的一个示例为检测到对REE 210与TEE 320之间的入口模块或其它接口或通信机制中的被监控数据或代码的修改。如下所述或其它地方所述,在没有已删除根密钥的情况下,TEE 320无法验证或解密REE 210的已加密密钥(例如KEK 312)。因此,即使随后破坏了TEE 320,也不能使用回退的(例如备份和恢复的)已加密KEK 312来访问数据252。在一些实施例中,删除可删除根密钥322的功能在TEE 320内执行,从而恶意软件或对REE 210的攻击不能阻止删除。

[0067] 图3为根据本发明实施例的用于在计算设备100上加密和解密数据的示例加密密钥链350的各方面的逻辑表示的框图。加密密钥链350的一部分保护在TEE 320中,其它部分

存储在REE 210中或可以由REE 210访问。

[0068] 加密密钥链350包括用于加密/解密数据252的文件加密密钥(file encryption key,FEK)254。FEK 254使用一个或多个加密密钥(例如DEK或CEK)256加密。REE 210中使用的加密密钥256可以使用REE 210中生成的KEK 312加密。用户密文(例如,用户密码和/或用户证书)258可以提供对加密密钥256的访问权限。用户密文258可以包括用户密码、个人识别码(personal identification number,PIN)、图案或生物特征。用户密文258可以用于保护KEK 312和授权KEK 312的使用(而不是直接访问DEK 256)。为了增加安全性,KEK 312使用TEE 320中的隐藏可删除根密钥322,如下文进一步的详细描述。在一些实施例中,KEK 312可以被加密并存储在REE 210侧,用密码学方式将KEK 312的加密绑定到用户密文258(从而,绑定到可删除根密钥322)。当用户提供正确的密文时,TEE 320能够以明文形式解密和检索正确的KEK 212,以便随后对DEK 256进行加密或解密。

[0069] 可删除根密钥322仅在TEE 320中可访问,从不脱离TEE 320,并且只能由TA 222等可信应用程序从TEE 320永久删除。可删除根密钥322是在TEE 320中随机生成或从TEE 320中其它受TEE保护的密钥派生。可删除根密钥322可以在软件中生成,并存储在存储器中(例如,重放保护存储区(replay protected memory block,RPMB)等安全存储区域)。

[0070] 将KEK 312链接到仅可在TEE 320中访问的隐藏可删除根密钥322,从而使KEK 312不会回退。从密码学而言,删除根密钥322后将无法恢复KEK 312。即使REE 210侧系统受到破坏,删除TEE 320内的可删除根密钥322也会使KEK 312无效。

[0071] 此处或其它地方描述的实施例可以适用于FDE或FBE中的根密钥管理。FDE和FBE在它们的加密密钥链(例如,图3)中都使用根密钥。因此,删除FDE或FBE中的根密钥能防止(恶意)用户访问安全数据252(例如,使用加密密钥链350加密的数据)。如果使用FDE,则在分区级别而非文件级别分离工作/个人(或敏感/不敏感)数据。

[0072] 尽管附图中示出的示例实施例示出了两个执行环境,但是本发明各方面可以适用于任何数量的执行环境。在一些实施例中,第一操作系统和第二执行环境可以在不同的物理设备上运行。例如,TEE 320可以在除运行REE 210的主中央处理器(central processing unit,CPU)之外的专用芯片上运行。在另一示例中,REE 210可以在IoT设备上操作,并且相应的TEE 320可以在与IoT设备通信的通信设备上操作,反之亦然。

[0073] 本文描述的示例实施例示出了单个可删除根密钥;然而,在其它实施例中,可以对一个或多个REE的不同密钥链使用多个可删除根密钥。

[0074] 图4A是示出了TEE 320与REE 210的各方面之间的交互的系统401框图。在该示例实施例中,CA 214请求创建KEK(例如,KEK 312)。在图4A的示例中,密钥管理任务由REE 210中的密钥管理系统(key management system,KMS)330处理,该KMS 330与TEE 320中的密钥管理系统可信应用程序(key management system trusted application,KMS TA)340交互。在一些操作系统中,例如Android™OS中,KMS被称为密钥库。

[0075] 尽管本文所述示例实施例提及的为KMS 330和KMS TA 340,但是在其它实施例中,KMS 330和KMS TA 340提供的功能可以同样由其它合适的客户端应用程序和可信应用程序提供。

[0076] KMS 330与KMS TA 340之间的交互将参考图4B进一步描述。图4B示出了生成KEK 312和从KEK 312生成已加密KEK 412的示例性方法400的各方面的流程图。

[0077] 已加密KEK 412可以在多种情况下生成，例如，在创建新的已加密数据文件开始时，在接收到创建新用户账户的请求之后等。KMS 330可以从在REE 210中执行的CA 214接收创建KEK 312的请求。KMS 330接收KEK密钥创建请求消息452，并获取454与KEK 312相关联的用户密文258。在一些实施例中，用户密文258可以从CA 214接收，从存储器104检索，通过用户输入设备接收或者可以通过任何其它机制获得。

[0078] KMS 330发送指示或提示TEE 320的KMS TA 340生成KEK 312的密钥创建请求消息456。可选地，密钥创建请求消息456可以包括用户密文258或与用户密文258关联的值(例如，哈希值或由用户密码或用户证书解锁的密钥或其它值)。KMS TA 340获取458(即，如果以前已生成，则生成或检索)可删除根密钥322。可删除根密钥322是在TEE 320中生成的随机数。KMS TA 340然后可以生成KEK 312，KEK 312是一个与用户密文258关联的随机数。在一些实施例中，KEK 312以加密方式绑定到用户密文258。KMS TA 340然后使用可删除根密钥322加密462 KEK 312并生成已加密KEK 412。在一些实施例中，在生成460 KEK 312的步骤之后执行获取458可删除根密钥322的步骤。KMS TA 340加密462 KEK 312后，KMS TA 340会向KMS 330发送密钥返回响应消息464以及已加密KEK 412，其中密钥返回响应消息464包含密钥blob。收到密钥返回响应消息464后，KMS 330可能会生成466 KEK句柄，并向CA 214发送包含该KEK句柄的KEK句柄返回消息468。

[0079] 出于安全原因，未加密的KEK 312不会发送到KMS 330并存储在REE 210的不安全存储器中。相反，在已加密KEK的返回消息464中向KMS 330发送包含已加密KEK 412的密钥blob。密钥blob是已加密KEK 412的表示形式(即加密或环绕未加密的KEK 312)，也可以包括与KEK 312相关的其它信息，例如版本、密钥特征(例如，大小、预期用途等)、授权方法、摘要或签名(用于完整性检查)等。密钥blob可以由KMS 330在内部管理，而不会将密钥blob直接公开给请求KEK 312的CA 214。为了使用密钥blob，CA 214 可以使用KMS 330生成的句柄作为密钥blob的唯一引用。只有KMS 330知道唯一句柄与实际密钥blob之间的映射。

[0080] 图5A为图示了TEE 320与REE 210之间的交互的系统501框图。在本示例实施例中，CA 214生成加密密钥链350中待保护的DEK 256。这些应用程序之间的交互将参考图5B进一步描述，图5B为示出了已加密DEK 256的示例生成方法500的各个方面的流程图。应理解，方法500也可以应用于使用KMS TA 340生成的KEK 312进行加密的任何密钥(例如密钥X)。

[0081] 方法500的开始步骤为：REE 210中的CA 214生成552 DEK 256(例如，Android™OS中的DE/CE)。然后，CA 214可以向KMS 330发送DEK加密请求消息554。DEK加密请求消息554可以包括生成的DEK 256、与DEK 256关联的用户密文258以及包含已加密KEK的密钥blob 412。然后，KMS 330可以向TES 320中的KMS TA 340发送DEK加密请求消息556，以便使用KEK 312加密DEK 256。DEK加密请求消息556包括DEK 256、已加密KEK 412和用户密文258。然后，KMS TA 340可以验证用于生成KEK 312的用户密文258。例如，对摘要的检查将能够识别用户密文258是否正确(即不正确的用户证书258将无法解密与KEK 312相关的其它项目，例如摘要)。然后，KMS TA 340可以检索558可删除根密钥322，并使用可删除根密钥322以及用户密文258解密560已加密KEK 412，以获取KEK 312(以及密钥blob 412中包含的任何附加信息)。KMS TA 340然后使用KEK 312加密DEK 256，并通过DEK加密响应消息564向REE 210中执行的CA 214发送已加密DEK 506。

[0082] 应注意，在本发明中，发送任何用户密文258并不限于仅发送用户密文258本身。在

一些实施例中，在通过受控的环境间接口、API和/或其它从REE 210传递到TEE 320之前，可以将用户密文258与其它信息(例如盐值或用户标识)进行转换、哈希化或混合。在一些实施例中，用户密文258可以是可用于解锁与TEE 320中的KEK关联的密钥或其它密文值的用户密码或用户证书。只要TEE 320接收到完全相同的密文(例如，每个比特都相同)，用作用于创建KEK 312的密文，TEE 320就可以正确地解密已加密KEK 412。

[0083] 图6A为图示了TEE 320与REE 210的各方面之间的交互的系统601框图。在该示例实施例中，CA 214请求访问已由图3所示的加密密钥链350加密的DEK。这些应用程序之间的交互将参考图6B进一步描述，图6B示出了用于已加密DEK 506的示例解密方法600的各方面的流程图。

[0084] CA 214有权访问已加密DEK 506，但使用DEK 256来访问存储在存储设备106中已使用加密密钥链350加密的数据。方法600的开始步骤为：CA 214向REE 210中的KMS 330发送DEK解密请求消息652。DEK解密请求消息652可以包括已加密DEK 506、与已加密DEK 506关联的用户密文258和已加密KEK 312。然后，KMS 330向TEE 320中的TMS TA 340发送DEK解密请求消息654，以使用KEK 312解密已加密DEK 506。DEK解密请求消息654包括待解密的已加密DEK 506和已加密KEK 312。在一些实施例中，DEK解密请求消息654还包括用户密文258。类似于上述过程或其它过程，KMS TA 340可以验证用户密文258并从安全存储设备114中检索656可删除根密钥322。然后，KMS TA 340使用可删除根密钥322解密658已加密KEK 312，以获取KEK 312。然后，KMS TA 340使用KEK 312解密660已加密DEK 506，以获得DEK 256。然后，KMS TA 340可通过DEK解密返回消息662向REE 210的KMS 330发送DEK 256。

[0085] 图7A为图示了TEE 320与REE 210的各方面之间的交互的系统701框图。在该示例实施例中，系统完整模块324检测REE 210处的潜在的完整性漏洞。这些应用程序之间的交互将参考图7B进一步描述，图7B示出了用于保护使用图3所示的加密密钥链350进行加密的数据的示例方法700的各方面的流程图。

[0086] 在752处，系统完整模块324监控并检测到REE 210处的潜在的完整性漏洞。然后，KMS TA 340从系统完整模块324接收用于删除可删除根密钥322的信号或消息754。在收到信号或消息754后，KMS TA 340删除756可删除根密钥322。从而，无法再解密已加密KEK 412。没有KEK 312就无法解密已加密DEK 506，并访问使用图3所示的加密密钥链进行加密的数据。可选地，KMS TA 340可以向REE 210中的KMS 330发送KEK删除消息758，以指示KMS 330删除或以使REE 210上的已加密KEK 412无效。

[0087] 在REE 210受到破坏，并且恶意攻击者尝试在可删除根密钥322已删除之后使用已删除的已加密KEK 412的回退版本(例如，备份和恢复的版本)发送DEK解密请求消息654的情况下(或者如果REE不知道根密钥已删除)，KMS TA 340解密已加密KEK 412将会失败762，因为就密码学而言，在没有可删除根密钥322(已删除)的情况下不可能解密KEK。从而，KMS TA 340将无法解密已加密DEK 506。将向CA 214发送错误消息764。

[0088] 在一些实例中，本文描述的实施例的各方面可以增加存储在计算设备上的已加密信息的安全性。在某些实例中，利用从未脱离安全执行环境的可删除根密钥允许(例如，具有正确的证书)可信用户进行授权访问，并降低了恶意软件或攻击者能够获得用于解密已加密敏感数据所需的加密密钥的访问权限的可能性。在检测到可疑活动后，即使安全执行环境随后遭到破坏，安全执行环境中的进程删除可删除根密钥仍可以永久防止攻击者访问

或备份和恢复(例如,回退)解密已加密敏感数据所需的加密密钥。

[0089] 本文描述的设备、系统和方法的实施例可以以硬件和软件的组合实现。这些实施例可以在可编程计算机上实现,每台计算机包括至少一个处理器、数据存储系统(包括易失性存储器或非易失性存储器或其它数据存储元件或其组合)以及至少一个通信接口。

[0090] 程序代码应用于输入数据,以执行本文描述的功能并生成输出信息。输出信息应用于一个或多个输出设备。在一些实施例中,通信接口可以是网络通信接口。在元件可以组合的实施例中,通信接口可以是软件通信接口,例如用于进程间通信的接口。在其它实施例中,通信接口的组合可以实现为硬件、软件及其组合。

[0091] 在前文的讨论中,大量引用了服务器、服务、接口、门户、平台或由计算设备形成的其它系统。应理解,应认为使用这些术语表示具有至少一个处理器的一个或多个计算设备,该处理器用于执行存储在计算机可读有形非瞬时性介质上的软件指令。例如,服务器可以包括一种或多种能够实现所述角色、职责或功能的网络服务器、数据库服务器或其它类型计算机服务器的计算机。

[0092] 实施例的技术方案可以是软件产品的形式。软件产品可以存储在非易失性或非瞬时性存储介质中,非易失性或非瞬时性存储介质可以是只读光盘(compact disk read-only memory,CD-ROM)、USB闪存盘或移动硬盘。该软件产品包括许多使计算机设备(个人计算机、服务器或网络设备)能够执行实施例提供的方法的指令。

[0093] 本文描述的实施例由包括计算设备、服务器、接收器、发送器、处理器、存储器、显示器和网络的物理计算机硬件实现。本文描述的实施例提供了有用的物理机器以及特别配置的计算机硬件布置。

[0094] 尽管已经详细描述了实施例,应理解,本文可以进行各种改变、替换和变更。

[0095] 此外,本发明的范围并不局限于说明书中所述的过程、机器、制造、物质组分、构件、方法和步骤的具体实施例。所属领域的一般技术人员可从本发明的公开中轻易地了解,可根据本发明使用现有的或即将开发出的,具有与本文所描述的相应实施例实质相同的功能,或能够取得与所述实施例实质相同的结果的过程、机器、制造、物质组分、构件、方法或步骤。相应地,所附权利要求范围包括这些过程、机器、制造、物质组分、构件、方法或步骤。

[0096] 可以理解,以上描述和示出的示例仅为示例性。

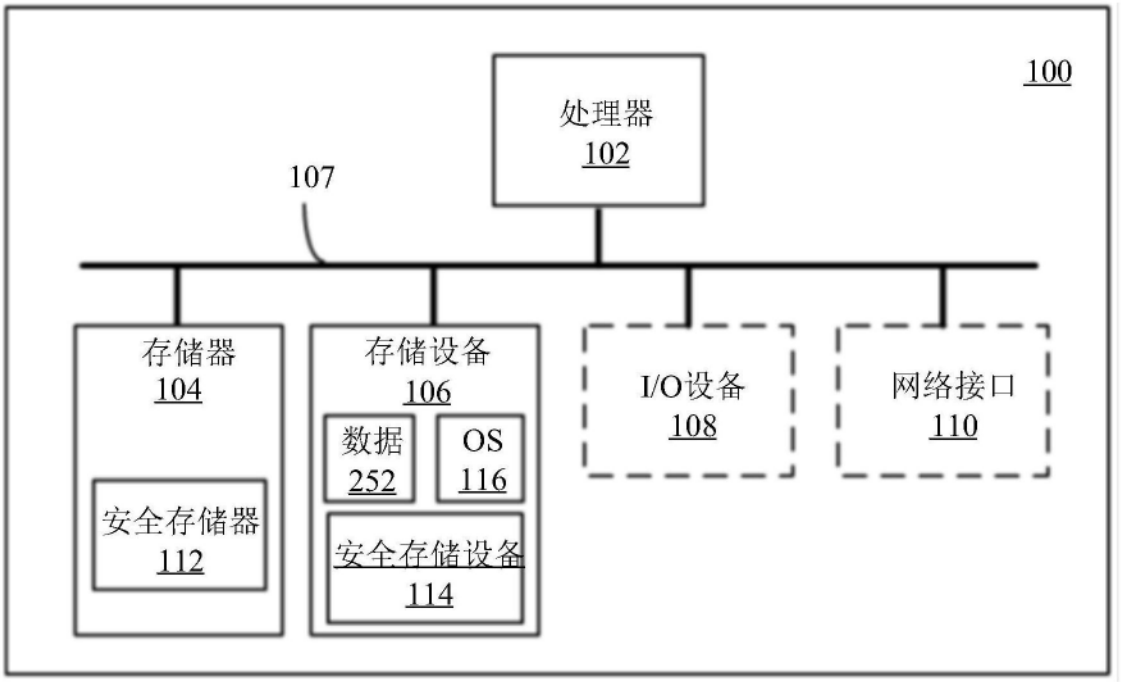

100
处理器
102
107
存储器
104
安全存储器
112
存储设备
106
数据
252
OS
116
安全存储设备
114
I/O设备
108
网络接口
110

图1

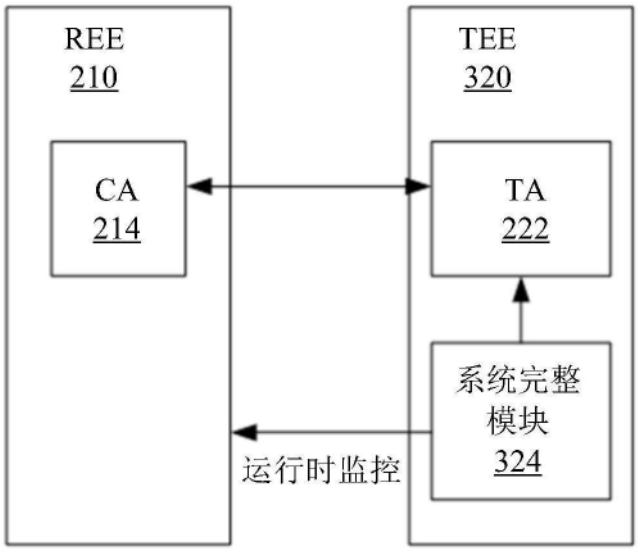

REE
210
CA
214
TEE
320
TA
222
系统完整
模块
324
运行时监控

图2

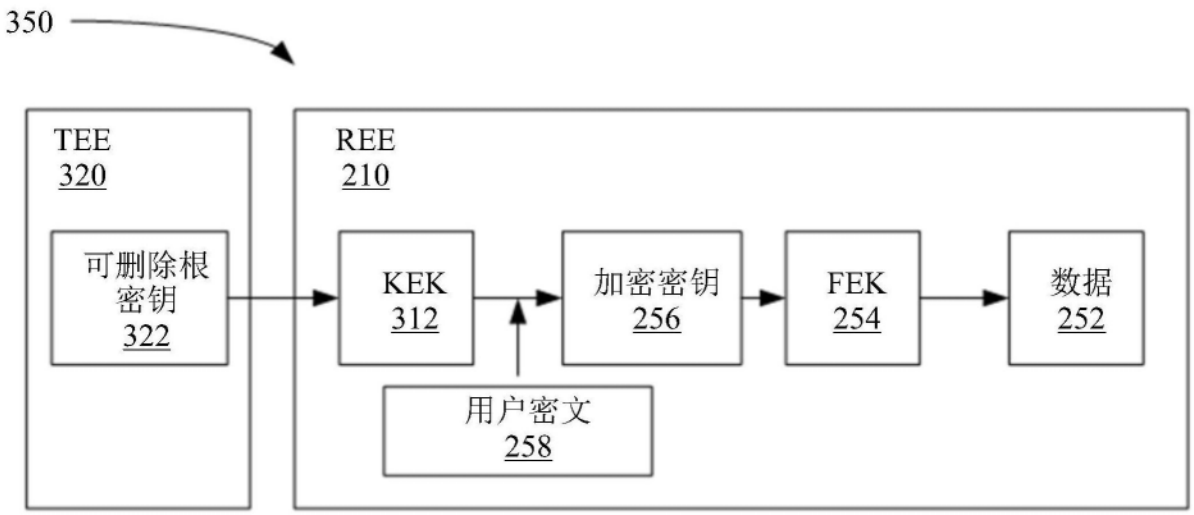

350
TEE
320
可删除根
密钥
322
REE
210
KEK
312
加密密钥
256
FEK
254
数据
252
用户密文
258

图3

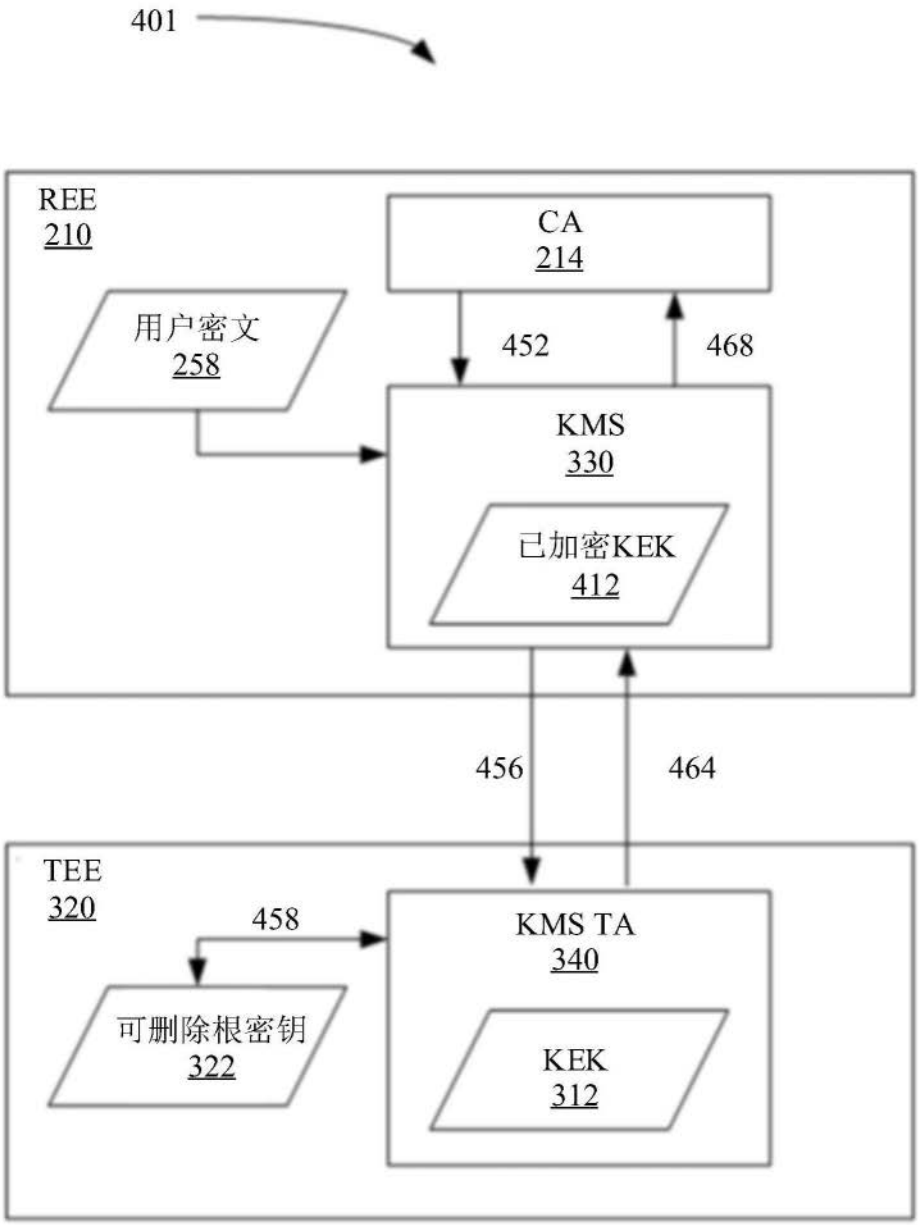

401
REE
210
CA
214
用户密文
258
452
468
KMS
330
已加密KEK
412
456
464
TEE
320
458
KMS TA
340
可删除根密钥
322
KEK
312

图4A

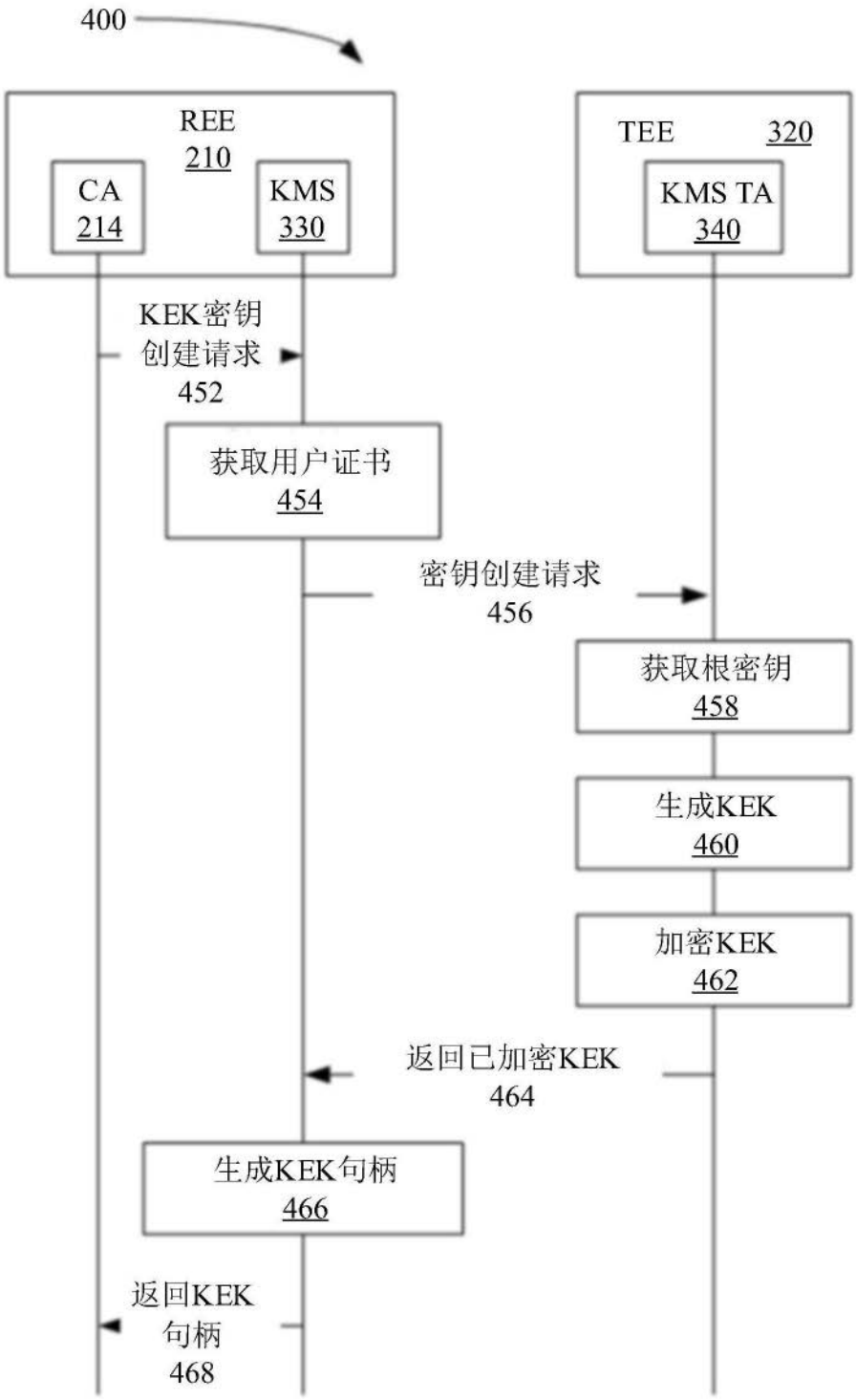

400
REE
210
CA
214
KMS
330
TEE
320
KMS TA
340
KEK密钥
创建请求
452
获取用户证书
454
密钥创建请求
456
获取根密钥
458
生成KEK
460
加密KEK
462
返回已加密KEK
464
生成KEK句柄
466
返回KEK
句柄
468

图4B

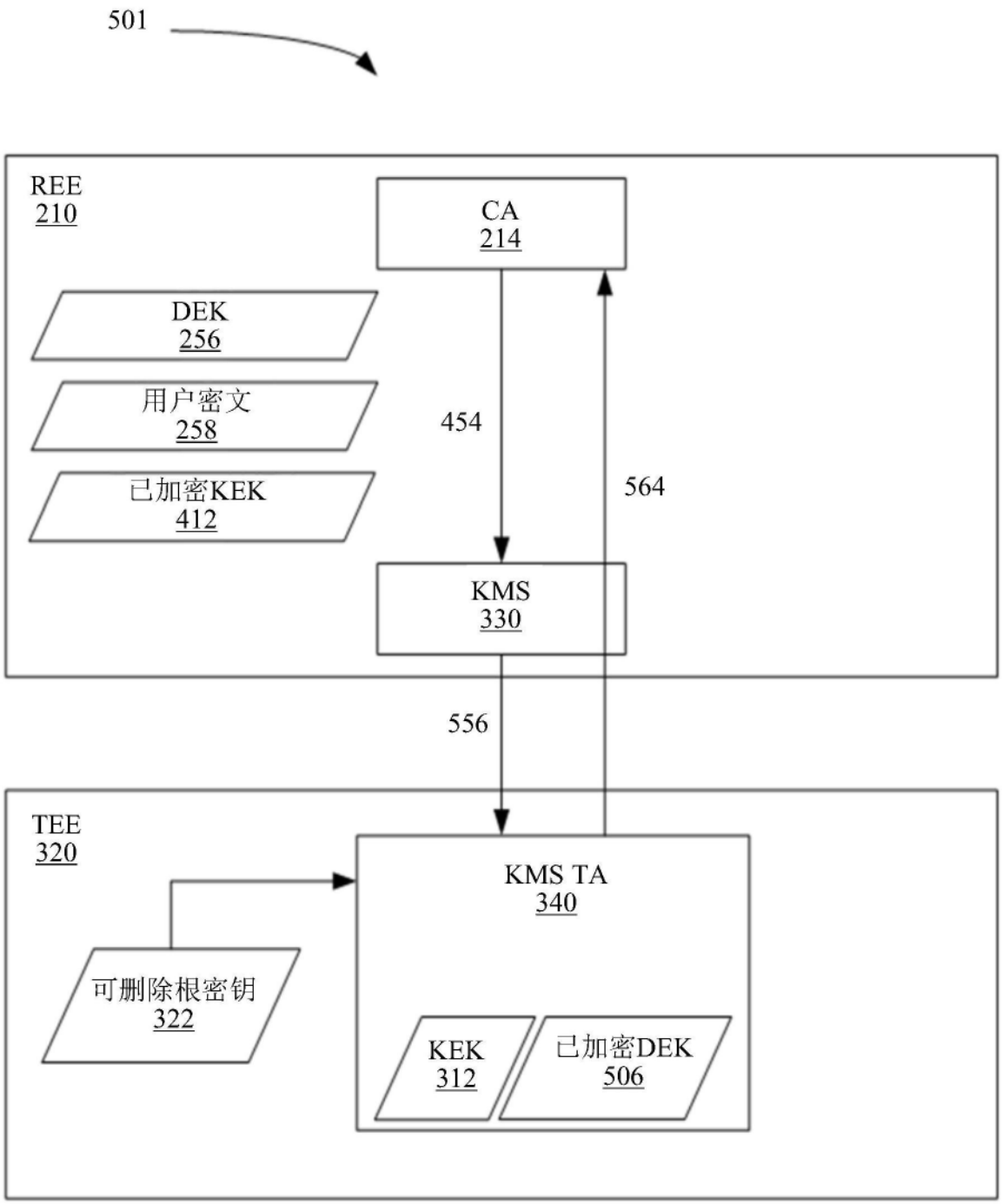

501
REE
210
CA
214
DEK
256
用户密文
258
已加密KEK
412
454
564
KMS
330
556
TEE
320
KMS TA
340
可删除根密钥
322
KEK
312
已加密DEK
506

图5A

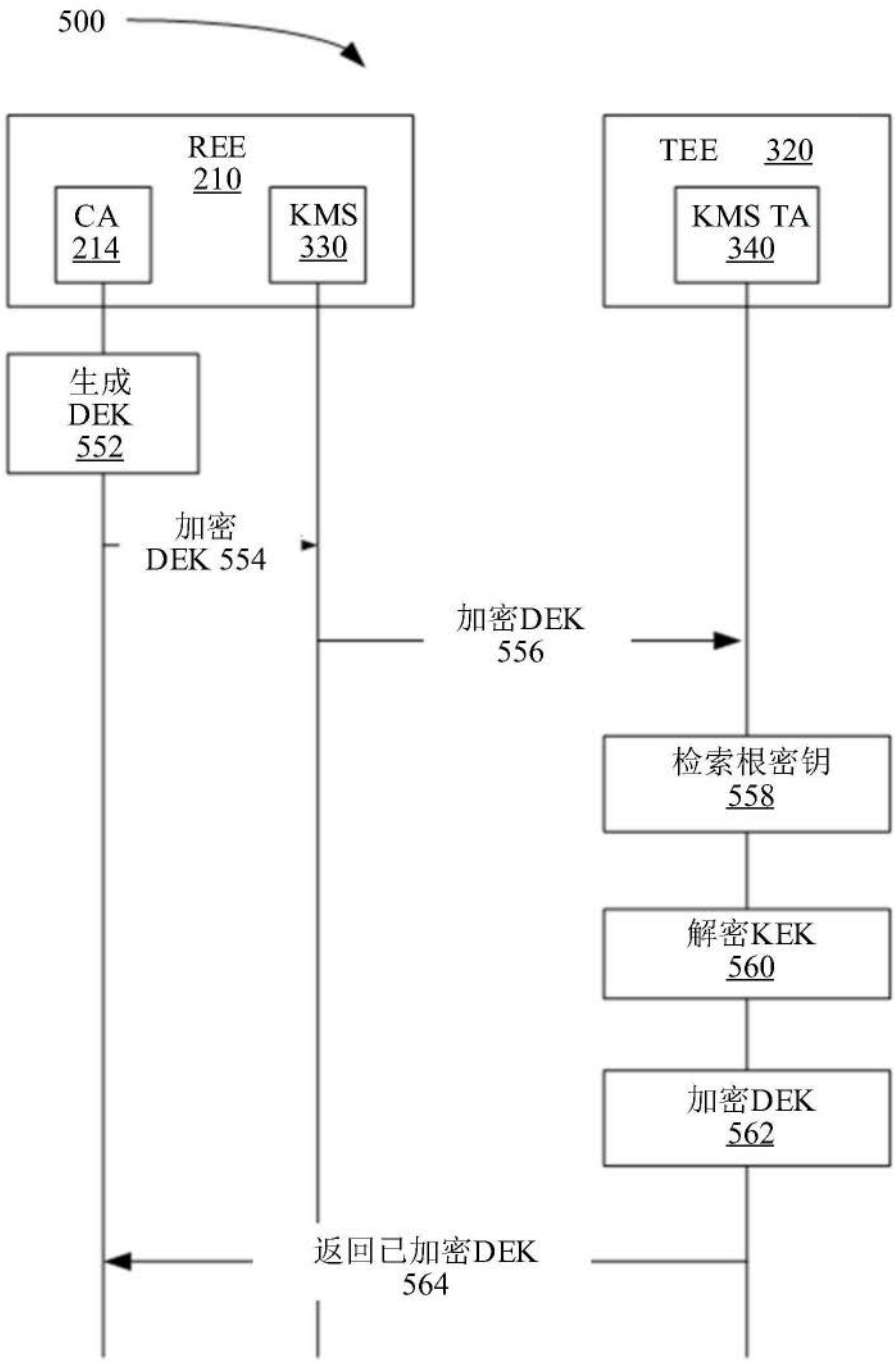

500
REE
210
CA
214
KMS
330
TEE 320
KMS TA
340
生成
DEK
552
加密
DEK 554
加密DEK
556
检索根密钥
558
解密KEK
560
加密DEK
562
返回已加密DEK
564

图5B

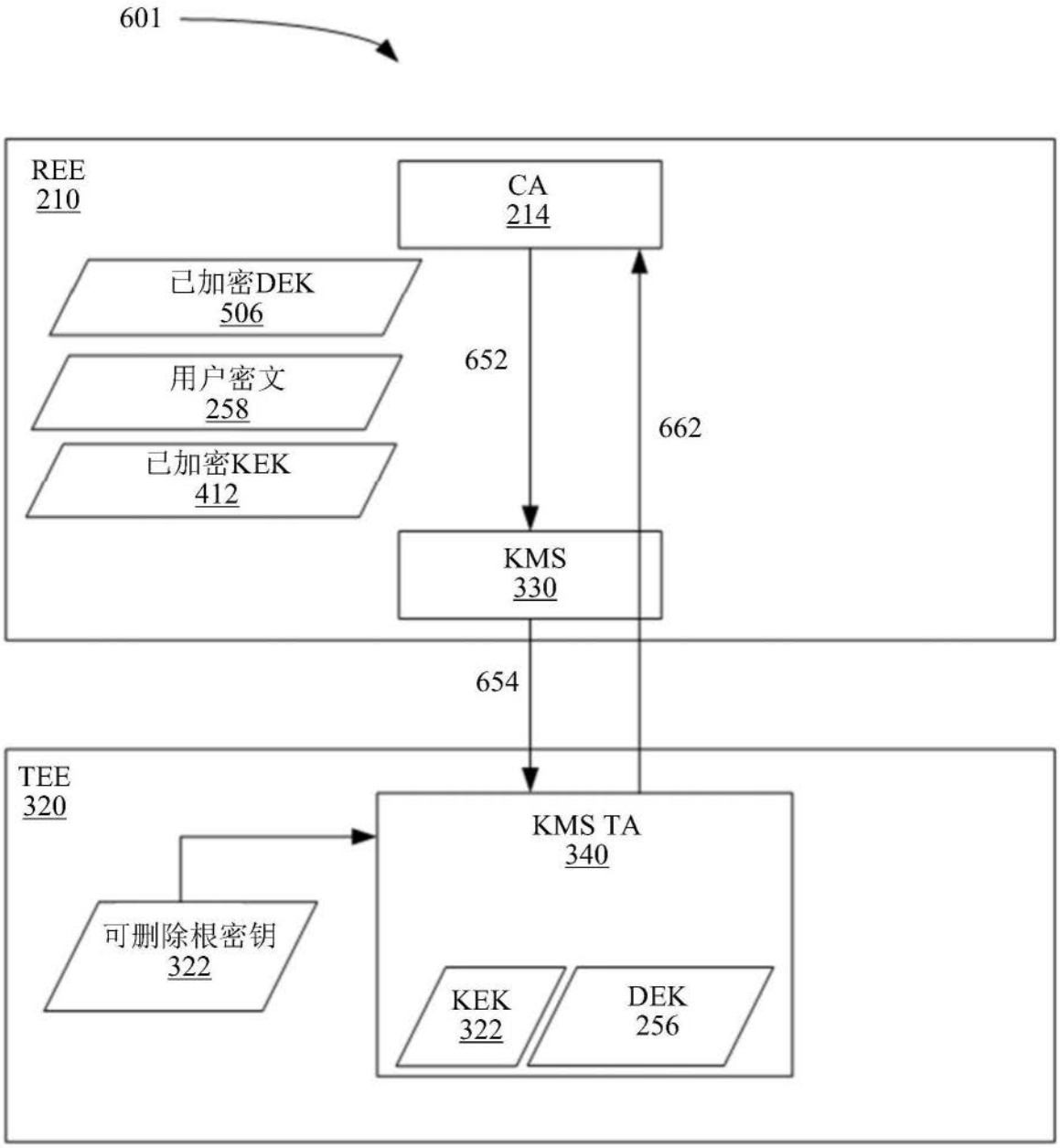

601
REE
210
CA
214
已加密DEK
506
用户密文
258
已加密KEK
412
652
662
KMS
330
654
TEE
320
KMS TA
340
可删除根密钥
322
KEK
322
DEK
256

图6A

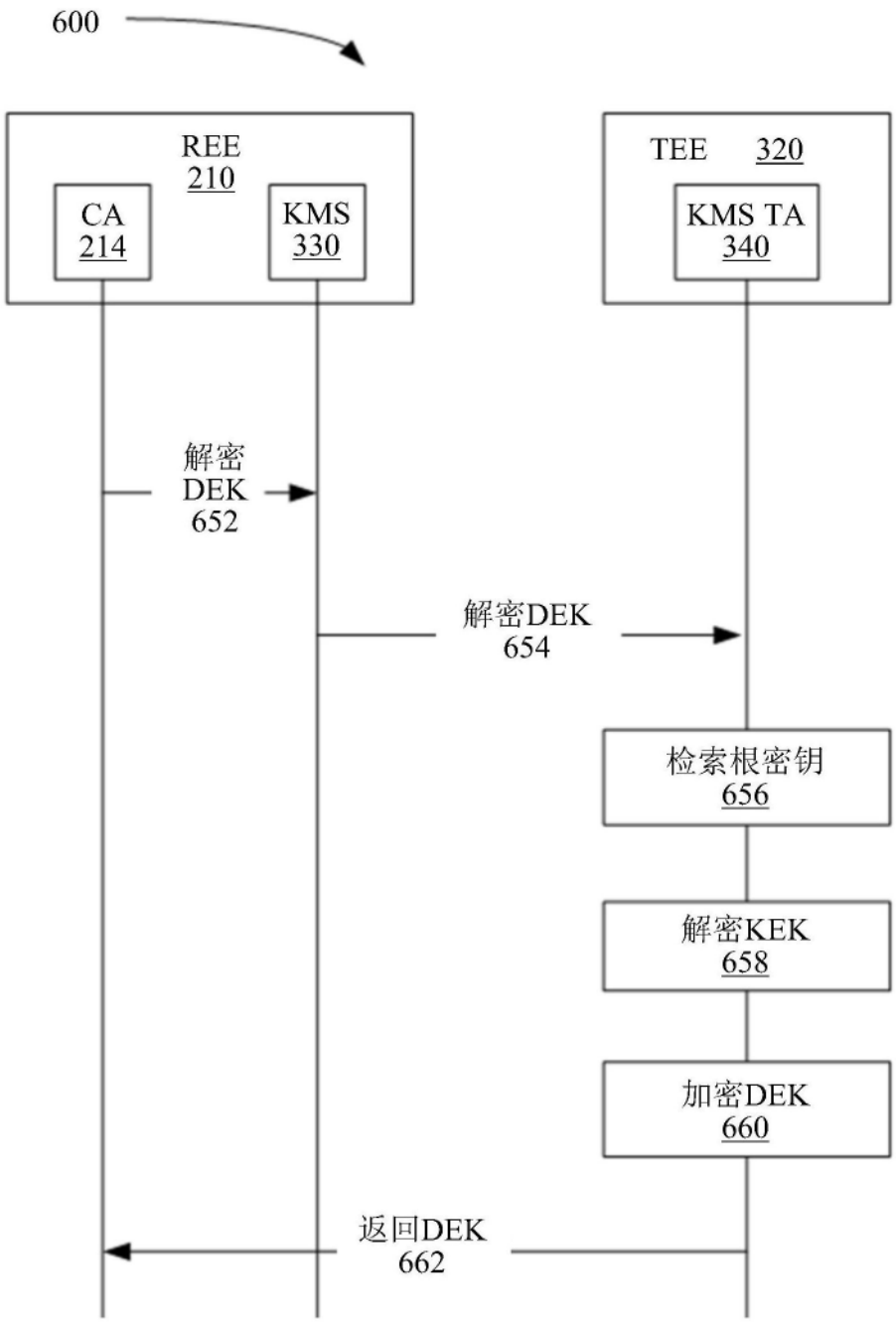

600
REE
210
CA
214
KMS
330
TEE 320
KMS TA
340
解密
DEK
652
解密DEK
654
检索根密钥
656
解密KEK
658
加密DEK
660
返回DEK
662

图6B

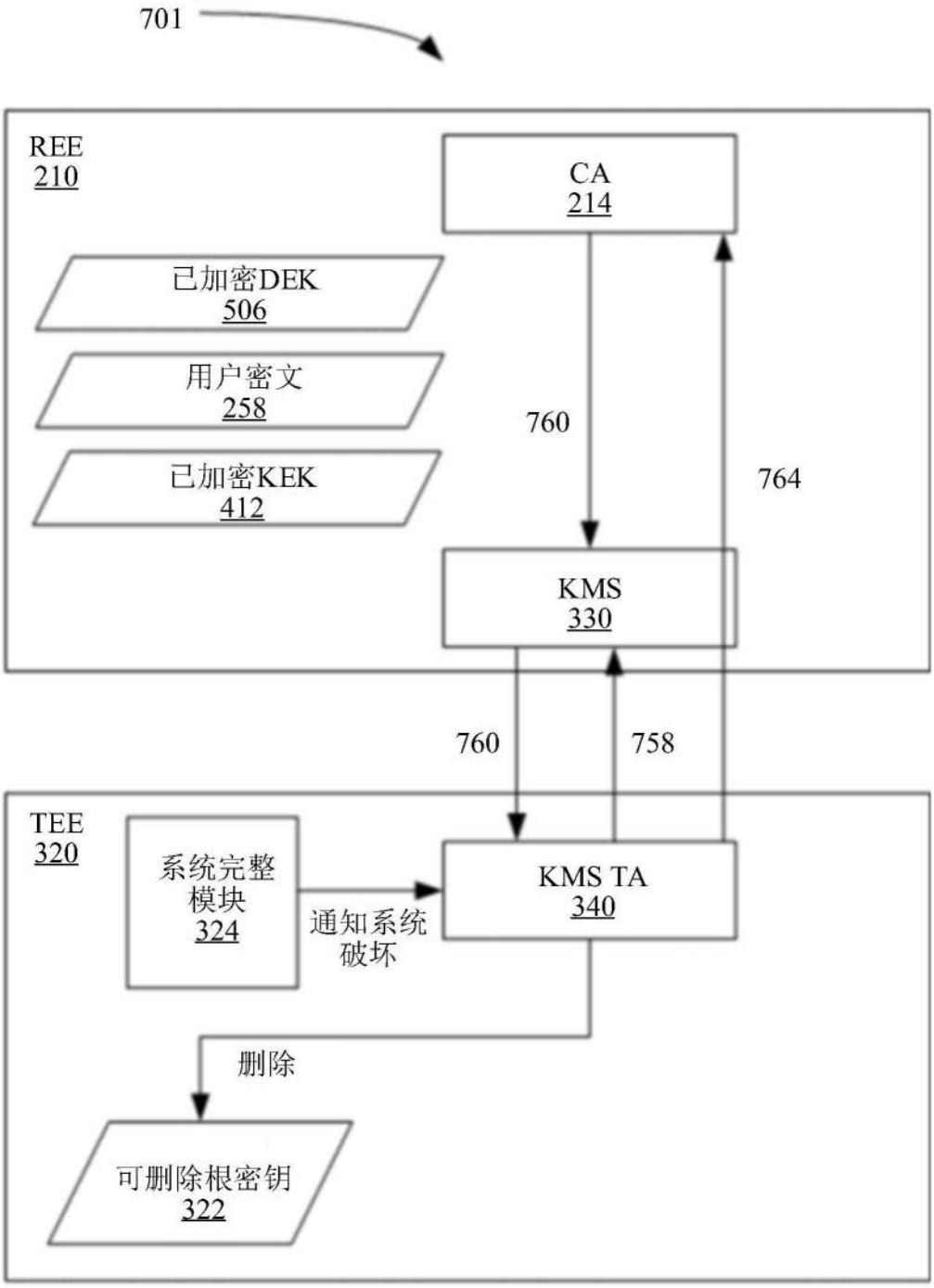

701
REE
210
CA
214
已加密DEK
506
用户密文
258
已加密KEK
412
760
764
KMS
330
760
758
TEE
320
系统完整
模块
324
通知系统
破坏
KMS TA
340
删除
可删除根密钥
322

图7A

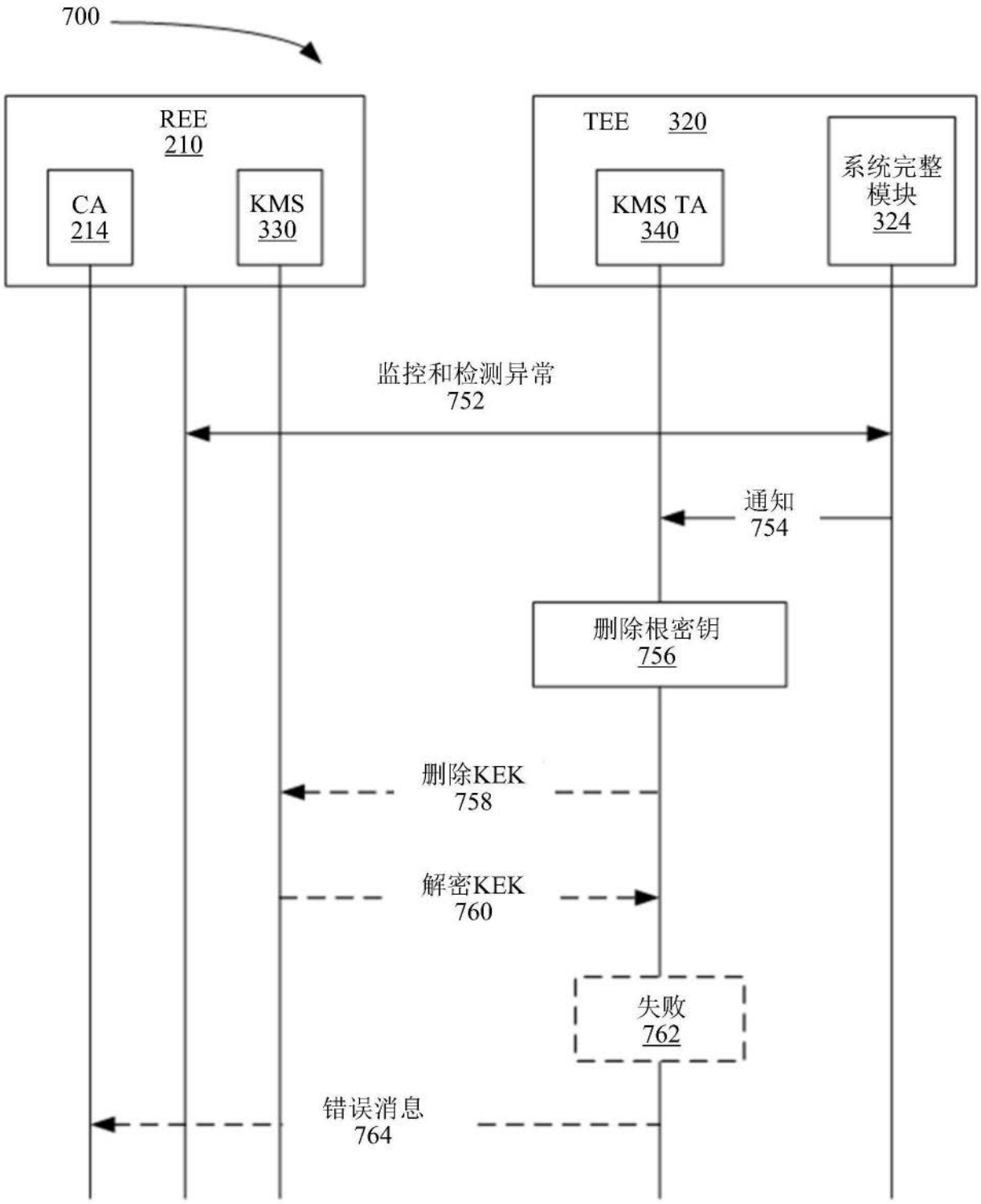

700
REE
210
CA
214
KMS
330
TEE 320
KMS TA
340
系统完整
模块
324
监控和检测异常
752
通知
754
删除根密钥
756
删除KEK
758
解密KEK
760
失败
762
错误消息
764

图7B