(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1914849 B
(45)授权公告日 2011.11.16

(21)申请号 200480041616.8

(22)申请日 2004.12.13

(30)优先权数据
60/528,890 2003.12.11 US
10/815,454 2004.03.31 US

(85)PCT申请进入国家阶段日
2006.08.11

(86)PCT申请的申请数据
PCT/US2004/041909 2004.12.13

(87)PCT申请的公布数据
WO2005/060151 EN 2005.06.30

(73)专利权人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 戴维·惠勒 约翰·布里扎克
莫伊纳尔·卡恩 阿尼沙·科纳

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 钱慰民

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
US 6631472 B2,2003.10.07, 全文.
US 6453415 B1,2002.09.17, 全文.
EP 0534419 A2,1993.03.31, 第11页第17-43行.
US 20020080958 A1,2002.06.27, 全文.
JONES R W.ser functions for the generation anddistribution of encipherment keys.Advances in Cryptology-EUROCRYPT'84,LNCS209.1985,317-334.

审查员 费聿辉

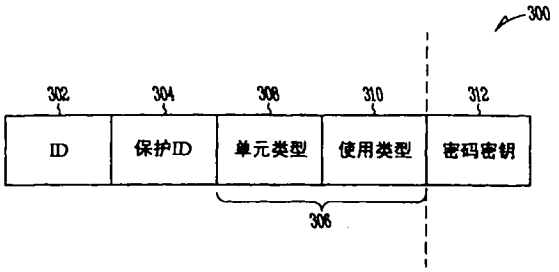
权利要求书 2 页 说明书 14 页 附图 8 页

(54)发明名称

受信移动平台体系结构

(57)摘要

在实施方案中,装置包括一个或更多个密码单元。装置还包括存储器,所述存储器储存一个或更多个数据加密密钥和用于所述一个或更多个数据加密密钥的相关联的头部。所述相关联的头部定义所述一个或更多个密码单元中的哪些使用所述数据加密密钥。



CN 1914849 B

1. 一种用于提供受信移动平台体系结构的装置，包括

控制器；

密码处理器，包括多于一个密码单元；以及

存储器，所述存储器储存多于一个数据加密密钥以及用于所述数据加密密钥中每一个的相关联的头部，其中，所述相关联的头部包括单元类型，所述单元类型定义所述密码单元中的哪些使用相关联的数据加密密钥，并且所述相关联的头部进一步定义用于相关联的数据加密密钥的使用类型，

其中所述使用类型识别可以使用所述数据加密密钥来执行的一种或更多种操作类型；

所述控制器基于用于所述数据加密密钥的所述相关联的头部中所识别的单元类型来约束所述密码单元中的哪些使用所述数据加密密钥；以及

所述控制器基于用于所述数据加密密钥的所述相关联的头部中识别的使用类型来约束操作类型。

2. 如权利要求 1 所述的装置，其中，所述使用类型包括签署、加密储存、以及证明身份密钥 (AIK) 操作。

3. 如权利要求 1 所述的装置，其中，所述相关联的头部定义用来加密所述多于一个数据加密密钥的密钥加密密钥的标识。

4. 如权利要求 1 所述的装置，其中，所述多于一个密码单元选自由高级加密标准单元、数据加密标准单元、消息摘要单元和安全哈希算法单元或幂运算单元组成的组。

5. 一种用于提供受信移动平台体系结构的方法，包括：

将原语指令接收到密码处理器中，以用于使用数据加密密钥的密码操作的执行，所述数据加密密钥在所述密码处理器中受保护，所述密码处理器包括多于一个密码单元；

取得所述数据加密密钥和用于所述数据加密密钥的相关联的头部，其中，所述相关联的头部包括单元类型，所述单元类型定义所述密码单元中的哪些使用所述数据加密密钥，并且所述相关联的头部进一步定义用于相关联的数据加密密钥的使用类型；以及

在由所述相关联的头部所定义的所述密码单元中的一个中使用所述数据加密密钥来进行操作；

基于用于所述数据加密密钥的所述相关联的头部中所识别的单元类型来约束所述密码单元中的哪些使用所述数据加密密钥；以及

基于用于所述数据加密密钥的所述相关联的头部中识别的使用类型来约束操作类型；

其中所述使用类型识别可以使用所述数据加密密钥来执行的一种或更多种操作类型。

6. 如权利要求 5 所述的方法，其中，所述使用类型识别包括签署、加密储存、以及证明身份密钥 (AIK) 操作。

7. 如权利要求 6 所述的方法，其中，所述使用所述数据加密密钥来进行操作的步骤包括，当所述使用类型定义了所述操作类型时，使用所述数据加密密钥来进行操作。

8. 一种用于提供受信移动平台体系结构的设备，所述设备包括：

用于将原语指令接收到密码处理器中，以用于使用数据加密密钥的密码操作的执行，所述数据加密密钥在所述密码处理器中受保护的装置，所述密码处理器包括多于一个密码

单元；

用于取得所述数据加密密钥和用于所述数据加密密钥的相关联的头部的装置，其中，所述相关联的头部包括单元类型，所述单元类型定义所述密码单元中的哪些使用所述数据加密密钥，并且所述相关联的头部进一步定义用于相关联的数据加密密钥的使用类型；以及

用于在由所述相关联的头部所定义的所述密码单元中的一个中使用所述数据加密密钥来进行操作的装置；

用于基于用于所述数据加密密钥的所述相关联的头部中所识别的单元类型来约束所述密码单元中的哪些使用所述数据加密密钥的装置；以及

用于基于用于所述数据加密密钥的所述相关联的头部中识别的使用类型来约束操作类型的装置；

其中所述使用类型识别可以使用所述数据加密密钥来执行的一种或更多种操作类型。

9. 如权利要求 8 所述的设备，其中，所述使用类型包括签署、加密储存、以及证明身份密钥 (AIK) 操作。

10. 如权利要求 9 所述的设备，其中，用于使用所述数据加密密钥来进行操作的装置包括：用于当所述使用类型定义了所述操作类型时，使用所述数据加密密钥来进行操作的装置。

受信移动平台体系结构

[0001] 相关申请：本文档要求2003年12月11日递交的、标题为“Trusted Mobile PlatformArchitecture(受信移动平台体系结构)”的美国临时申请No.60/528,890的优先权，其整篇说明书以引用的方式被包含进来。本申请与2004年3月31日递交的、标题为“METHODAND APPARATUS FOR A TRUST PROCESSOR(用于信任处理器的方法和装置)”的待审定美国专利申请No.(律师案卷号884.B89US1)相关，该待审定美国专利申请被转让给本文公开的实施方案的受让人——英特尔公司。

技术领域

[0002] 本发明总地涉及电子数据处理，并且更具体地，涉及受信移动平台体系结构。

[0003] 背景

[0004] 无线移动设备（例如蜂窝电话、个人数字助理(PDA)等）通常是尺寸小、未系缚的，并且因此易于遗失。正如这样的设备易于遗失，它们也易于偷窃。由于这些设备被偷窃的倾向性，它们容易受到篡改。此外，构建低功率设备的最低限度途径常常使得这些嵌入式系统（在操作系统和硬件方面）过分简单，这又使得它们在有恶意的使用者和/或应用的控制下是易受伤害的。使用者依赖于这些设备用于有价值的用途。特别地，在这样的设备中，使用者储存着诸如收据(receipt)、信用卡号、地址、电话号码、机密文档等的机密信息。因此，由于这些设备能够被轻易地攻击，它们正日益成为窃贼的首要目标。因此，存在着确保设备完整性（包括储存在其中的应用和数据）的需要。

[0005] 附图简要说明

[0006] 通过参照以下描述和示出实施方案的附图可以最好地理解本发明的这些实施方案。被包括在本文中的对图的编号方案是这样的，即图中给定参考号的首个数字与该图号相关联。例如，受信移动计算设备100可以位于图1中。然而，对于在不同图中相同的部件来说参考号是相同的。在附图中：

[0007] 图1根据本发明的一个实施方案，示出具有受信平台体系结构的移动计算设备的简化功能框图。

[0008] 图2根据本发明的一个实施方案，示出受信移动计算设备中的密码处理器的简化功能框图。

[0009] 图3根据本发明的一个实施方案，示出受信移动计算设备中密码处理器中的密钥缓存中的项的一个实施方案。

[0010] 图4根据本发明的一个实施方案，示出用于与密码处理器的接口的操作的流程图。

[0011] 图5根据本发明的一个实施方案，示出密码处理器的初始化的流程图。

[0012] 图6A根据本发明的一个实施方案，示出密码处理器内安全操作的流程图。

[0013] 图6B根据本发明的一个实施方案，示出在密码处理器中使用密码密钥的密码操作的执行的流程图。

[0014] 图7根据本发明的一个实施方案，示出更新密码处理器中的微码的流程图。

[0015] 图 8 根据本发明的一个实施方案，示出其中具有密码操作的受信移动通信设备可以工作的系统配置的简化功能框图。

[0016] 详细描述

[0017] 描述了用于受信移动平台体系结构的方法、装置以及系统。在以下描述中，阐述了大量的具体细节。然而，可以理解，无需使用这些具体细节可以实现本发明。此外，公知电路、结构和技术没有详细示出，以免模糊对本发明的理解。

[0018] 本详细描述被分成三个部分。在第一部分中，介绍了硬件体系结构。在第二部分中，描述了受信 (trusted) 和密码 (cryptographic) 操作。在第三部分中，描述了系统操作环境。

[0019] 硬件体系结构

[0020] 图 1 根据本发明的一个实施方案，示出具有受信平台体系结构的移动计算设备的简化功能框图。具体来说，图 1 示出可以代表多种不同类型的移动计算设备（例如蜂窝电话、PDA 等等）的受信移动计算设备 100。受信移动计算设备 100 包括耦合在一起的芯片上系统 (system-on-a-chip)102、显示器 103、触摸板 104 以及天线 105。显示器可以是多种观察设备，例如液晶显示 (LCD) 屏等等。触摸板 104 可以被用来接收来自受信移动计算设备 100 的用户的输入。例如，触摸板 104 可以是数值 (numeric) 触摸板、键盘等等。尽管未示出，但是受信移动计算设备 100 可以包括多个其他外设，例如用于输入和输出来自用户的音频数据的音频输入 / 输出 (I/O) 逻辑等等。

[0021] 芯片上系统 102 可以是单个芯片，其中，本文描述的组件 (component) 位于例如同一半导体衬底 (substrate) 中。可替换地，芯片上系统 102 可以是多个这样的芯片，所述多个芯片用环氧树脂粘合在一起。

[0022] 芯片上系统 102 包括应用处理器 106、受信引导只读存储器 (ROM)108、通信逻辑 110、控制器 112、非易失性存储器控制器 114、非易失性存储器 116、易失性存储器控制器 118、易失性存储器 120、图形逻辑 122、直接存储器访问 (DMA) 逻辑 124、密码处理器 (cryptographic processor)126、外设逻辑 128、联合测试工作组 (JTAG) 接口 155 和总线 130。应用处理器 106、受信引导 ROM 108、通信逻辑 110、控制器 112、非易失性存储器控制器 114、非易失性存储器 116、易失性存储器控制器 118、图形逻辑 122、JTAG 接口 155 和 DMA 逻辑 124 被耦合到总线 130。因此，总线 130 提供这些组件之间的通信。显示器 103 和触摸板 104 通过外设逻辑 128 耦合到芯片上系统 102。

[0023] 天线 105 被耦合到通信逻辑 110。通信逻辑 110 提供进入和离开受信移动计算设备 100 的 I/O 的接收与传输。例如，通信逻辑 110 可以使用天线 105 来对进入和离开受信移动计算设备 100 的无线通信 (communication) 进行发送与接收。天线 105 可以是贴片、单极、双极、波束、阵列或定向天线等等。如下进一步描述的，天线 105 可以接收导致应用处理器 106 生成用于加密操作的一条或更多条原语指令 (primitive instruction) 的通信。这些原语指令可以被传输到密码处理器 126，以供执行。此外，天线 105 可以输出与由密码处理器 126 完成的密码操作相关的通信。

[0024] 在一些实施方案中，通信逻辑 110 可以包括为受信移动计算设备 100 建立特定通信标准的基带处理器（例如数字信号处理器）。通信逻辑 110 可以是无线接口。例如，如果受信移动计算设备 100 是蜂窝电话，则通信逻辑 110 为受信移动计算设备 100 提供无线

接口——蜂窝网络接口。仅仅作为一些实施例，对于这些无线接口，基带处理器可以建立码分多址 (CDMA) 蜂窝无线电话通信系统，或者宽带 CDMA(W-CDMA) 无线电话通信系统。作为欧洲电信标准协会 (ETSI) 对国际电信联盟 (ITU) 提出的针对用于未来公共陆地移动电信系统 (FPLMTS) 的国际移动电信 (IMT)-2000 的建议，已经明确建议将 W-CDMA 作为第三代（“3G”）的解决方案。基带处理器可以建立其他电信标准，例如全球移动通信系统 (GSM)，ETSI，5.0.0 版 (1995 年 12 月）；或者通用分组无线业务 (GPRS)(GSM 02.60，6.1 版)，ETSI，1997。

[0025] 在将控制转移到要在应用处理器 106 中执行的操作系统之前，受信引导 ROM 108 储存由应用处理器 106 执行的代码。如下面进一步描述的，这样的代码导致多项信任操作的执行（使用密码处理器 126)，以确保操作系统的完整性。在下列 2003 年 12 月 22 日递交、标题为“Securing anElectronic Device（保护电子设备）”的共同待审定、共同转让的美国专利申请 No. 10/745,496 中描述了受信引导操作的更详细的描述。JTAG 接口 155 提供到受信移动计算设备 100 的调试接口。

[0026] 非易失性存储器 116 可以是任何多种不同类型的非易失性可写存储器，例如闪存 (FLASH) 存储器等等。易失性存储器 120 可以是任何多种不同类型的易失性可写存储器，例如随机访问存储器 (RAM)（例如同步动态 RAM(SDRAM)、DRAM、DDR-SDRAM 等）等等。

[0027] 非易失性存储器控制器 114 被耦合到非易失性存储器 116。易失性存储器控制器 118 被耦合到易失性存储器 120。从而，耦合到总线 130 的组件可以分别通过非易失性存储器控制器 114 和易失性存储器控制器 118 来与非易失性存储器 116 和易失性存储器 120 通信。密码处理器 126 和外围设备逻辑 128 通过 DMA 逻辑 124 耦合到总线 130。耦合到总线 130 的组件可以通过 DMA 逻辑 124 来与密码处理器 126 和外围设备逻辑 128 通信。

[0028] 密码处理器 126 还通过私用 (private) 接口，分别经由非易失性存储器控制器 114 和易失性存储器控制器 118 直接耦合到非易失性存储器 116 和易失性存储器 120。如所示出的，受信计算设备 100 中的其他组件（例如应用处理器 106) 可以不通过这些私用接口来访问非易失性存储器 116 和易失性存储器 120。此外，密码处理器 126 和应用处理器 106 可以通过总线 130（公用 (public) 接口）来访问非易失性存储器 116 和易失性存储器 120。

[0029] 密码处理器 126 可以将易失性存储器 120 划分成至少两个不同的部分（公用部分和私用部分）。此外，只有密码处理器 126 可以访问易失性存储器 120 的私用部分中的地址空间。此外，受信移动计算设备 100 中的不同组件可以访问易失性存储器 120 的公用部分中的地址空间。这样的配置允许私用部分被用于安全 / 受信使用，并且阻止应用处理器 106 访问该部分。因此，如果在应用处理器 106 上执行病毒和 / 或恶意代码，则该代码可以不破坏易失性存储器 120 的私用部分。从而，密码处理器 126 可以使用该私用部分来安全地储存要用于在其中执行的操作的已加密密钥等。

[0030] 如下进一步描述，密码处理器 126 包括受保护的储存装置和多个不同的功能单元。密码处理器 126 可以提供与受信移动计算设备 100 相关联或在受信移动计算设备 100 中执行的硬件、软件、配置数据等的认证。例如，作为受信移动计算设备 100 的初始化的部分，密码处理器 126 可以执行横贯 (across) 应用的代码的密码哈希，并且将该哈希与被安全地储存在受信移动计算设备 100 中的已签名证书进行比较。此外，密码处理器 126 还在受信移动计算设备 100 的操作期间提供不同的密码操作。例如，密码处理器 126 可以生成

密码密钥、执行不同类型的加密与解密、生成哈希、数字签名等等。

[0031] 应用处理器 106 可以在第一操作上下文 (context) 中，而密码处理器 126 可以在第二操作上下文中。第一操作上下文和第二操作上下文可以互相独立。如下进一步的描述，应用处理器 106 可以执行驱动器（用于密码处理器 126），所述驱动器（通过 DMA 逻辑 124）在应用处理器 106 和密码处理器 126 上执行的应用之间提供接口。该驱动器从控制应用处理器 106 的操作系统中接收用于不同安全服务（认证、信任、加密、解密等等）的请求。驱动器可以基于安全服务请求生成一个或更多个原语指令。然后，这些原语指令被发布给密码处理器 126 以供执行。此外，密码处理器 126 可以（通过 DMA 逻辑 124 从非易失性存储器 116 和 / 或易失性存储器 120）取得数据，基于原语指令对所述数据进行执行操作。密码处理器 126 可以基于原语指令对所取得的数据执行密码操作。

[0032] 下面结合图 4、5、6A-6B 阐述了受信移动计算设备 100 的操作的更详细的描述。

[0033] 图 2 根据本发明的一个实施方案，示出受信移动计算设备内的密码处理器的简化功能框图。具体来说，图 2 示出密码处理器 126 的一个实施方案的更详细的框图。

[0034] 密码处理器 126 包括 DMA 接口 202、指令序列缓冲区 204、控制器 206、微码存储器 240、补丁标志 (patch flag) 存储器 281、控制寄存器组 208、上下文储存装置 / 平台配置寄存器 210、状态寄存器 212、中间储存装置 214、输出缓冲区 216、输入缓冲区 218、内部易失性存储器 220、算术逻辑单元 (ALU)222、数据加密标准 (DES) 单元 224、消息摘要 (MD) 单元 226、随机数生成器 (RNG) 单元 228、安全哈希算法 (SHA) 单元 230、高级加密标准 (AES) 单元 232 和幂运算单元 234。因此，密码处理器 126 包括多个不同的功能单元（包括多个不同的密码单元）(ALU 222、DES 单元 224、MD 单元 226、RNG 单元 228、SHA 单元 230、AES 单元 232 和幂运算单元 234)。

[0035] 虽然微码存储器 240 可以是不同类型的存储器，但是在一个实施方案中，微码存储器 240 是只读存储器 (ROM)。内部易失性存储器 220 可以是任何类型的易失性可写存储器，例如随机访问存储器 (RAM)（例如同步动态 RAM(SDRAM)、DRAM、DDR-SDRAM 等等）等。如示出的，内部易失性存储器 220 储存密钥缓存 (cache)221、根加密密钥 (rootencryption key)241 和计数器 215。密钥缓存 221 可以储存多个不同的受保护密钥，所述受保护密钥可以是数据加密密钥和 / 或（用于加密数据加密密钥的）密钥加密密钥。下面结合图 3 更详细地描述密钥缓存 221 的一个实施方案。

[0036] 补丁标志存储器 281 可以是多种不同类型的易失性可写存储器中的任何一种，例如随机访问存储器 (RAM)（例如同步动态 RAM(SDRAM)、DRAM、DDR-SDRAM 等等）等。如下面进一步描述的，补丁标志存储器 281 可以储存对应于微码存储器 240 中的段 (segment) 的补丁标志。给定补丁标志指示微码存储器 240 的给定段是否已被修补。下面更详细地描述对补丁标志的使用的更详细描述。

[0037] DMA 接口 202 被耦合，以接收和传输进入和出自密码处理器 126 的数据。DMA 接口 202 耦合到指令序列缓冲区 204、控制寄存器组 208、上下文储存装置 /PCR 210、状态寄存器 212、输出缓冲区 216 和输入缓冲区 218。

[0038] 指令序列缓冲区 204 储存从应用处理器 106 接收的原语指令。控制器 206 可以从指令序列缓冲区 204 取得 (retrieve) 给定原语指令，并且可以从微码存储器 240 中取得相关联的一条或多条微码指令。这些微码指令可以包括要在密码处理器 126 中完成的一连串

操作。例如，一条指令可以导致控制器 206 从易失性存储器 120 取得已加密的数据加密密钥。一条不同的指令可以导致控制器 206 将该密钥传输到功能单元中的一个以供解密。另一条指令可以导致已解码的数据加密密钥被传输到不同的功能单元，以完成密码操作。这一连串微码指令的输出可以被储存到输出缓冲区 216 中。接着，（密码处理器 126 的）驱动器 (driver) 可以取得该输出。下面阐述了这些操作的更详细的描述。

[0039] SHA 单元 230 可以用于生成并验证密码哈希 (hash)。SHA 单元 230 可以进行 SHA-1 操作，以及基于 SHA 的 HMAC 计算。幂运算单元 234 可以用于进行多项不同运算操作的加速。例如，幂运算单元 234 可以用于针对不同类型的加密标准（例如 Riverst、Shaman 和 Adelman(RSA)）完成非对称加密和解密、签署、签名的验证等等。为了图示说明，幂运算单元 234 可以进行模幂、求模化简、乘法、加法、减法等等。

[0040] AES 单元 232 可以完成多种不同类型的加密（对称，非对称）。AES 单元 232 可以基于可变的轮数 (number of rounds) 进行加密，所述轮数取决于加密密钥长度。AES 单元 232 可以支持 128 位 (bit)、192 位和 256 位的密钥长度，所述 128 位 (bit)、192 位和 256 位的密钥长度分别产生 10 轮、12 轮和 14 轮加密。AES 单元 232 可以用于以不同的密钥（被称为密钥加密密钥）加密数据加密密钥。

[0041] 这样的操作使得在易失性存储器 220 的密钥缓存 221 中数据加密密钥的安全储存能够进行。可以用加密密钥层级来配置密码处理器 126。例如，AES 单元 232 可以用密钥加密密钥来加密数据加密密钥。AES 单元 232 可以用根加密密钥 241 来加密密钥加密密钥。当数据加密密钥和密钥加密密钥呈已加密格式时，它们可以被储存到在密码处理器 126 外部的存储器（例如易失性存储器 116，非易失性存储器 120）中。为了确保安全性，根加密密钥 241 不对外暴露给密码处理器 126。

[0042] DES 单元 224 可以进行多种不同类型的加密和解密。例如，DES 单元 224 可以基于 64 位密钥加密和解密 64 位数据块。MD 单元 226 可以基于多种不同的标准生成哈希（消息摘要）。例如，MD 单元 226 可以基于 MD-5、MD-4 等生成哈希。MD 单元 226 可以接收具有任意长度的消息块，并生成 128 位的摘要。MD 单元 226 还可以进行密钥哈希消息认证码 (HMAC) 操作。

[0043] ALU 222 可以为信任和加密操作进行多项不同的运算和逻辑操作。例如，ALU 222 可以进行加法、减法、乘法、除法、位对齐、移位操作、不同的逻辑功能（例如 AND，OR，XOR 等等）等。

[0044] RNG 单元 228 可以进行不同类型随机数的生成。RNG 单元 228 可以使用线性反馈移位寄存器 (LFSR) 来生成随机位序列。此外，LFSR 的输出可以被传递通过 SHA 单元 230，以获得额外的随机化。

[0045] 控制寄存器组 208 可以储存用于控制密码处理器 126 的数据。因此，在密码处理器 126 外部的组件可以将数据储存在与密码处理器 126 的控制和配置有关的控制寄存器组 208 中。上下文储存装置 /PCR 210 可以储存与受信移动计算设备 100 有关的上下文和配置数据。例如，上下文储存装置 /PCR 210 可以储存来自信任操作的密码哈希，所述信任操作与在应用处理器 106 上执行的不同应用的认证有关。状态寄存器 212 可以用于储存关于密码处理器 126 内给定操作的状态、不同功能单元的状态等等。中间储存装置 214 可以用于储存要被输入到不同功能单元的中间结果，所述中间结果可以是来自一个功能单元的输

出。

[0046] 输入缓冲区 218 可以储存数据，针对所述数据执行给定操作。例如，如果对于给定原语指令，要横贯应用的代码执行密码哈希，则将所述代码储存在输入缓冲区 218 中。

[0047] 如示出的，密码处理器 126 包括多个功能单元（包括多个不同的密码单元）和不同的易失性储存装置。此外，密码处理器 126 可以完成多项不同的操作，其中中间结果是安全的。如下面进一步描述的，控制器 206 可以控制这些不同功能单元的操作，以及这些不同功能单元之间的数据流。

[0048] 如将被描述的，密码处理器 126 允许通过提供其中操作的原子性 (atomicity) 和 / 或完整性来允许安全的操作。操作的原子性被定义，从而其中的外向 (outgoing) 操作不会被预占 (preempted)，并且因此被执行直至完成。操作的完整性被定义，从而密码处理器 126 规定中间数据和结果的不透明性。密码处理器 126 工作为受信移动计算设备 100 的核心 (core)，用于创建更高级的安全性服务。这样的服务可以包括安全储存、安全或已加密通信的受信执行加速、随机数生成等等。

[0049] 密码处理器 126 可以工作在非受保护模式和受保护模式两种模式下。在非受保护模式下，密码处理器 126 可以工作为用于加密和解密的非安全硬件加速器。例如，密码处理器 126 可以接收请求，以对在应用处理器 106 上执行的应用进行整体加密 (bulk encryption) 操作。在受保护模式下，密码处理器 126 可以进行多项不同的安全原子操作。在下面阐述了这些操作更详细的描述。

[0050] 图 3 根据本发明的一个实施方案，示出受信移动计算设备内密码处理器中密钥缓存中的项 (entry) 的一个实施方案。具体来说，图 3 示出易失性存储器 220 的密钥缓存 221 中的项的一个实施方案。密钥缓存 221 可以包括一个到多个项，所述项包括受保护的密码密钥 312 和头部 300。头部提供对密钥使用的多个不同的标识 (identification) 以及限制。

[0051] 如示出的，头部 300 包括标识 302、保护标识 304 和多个标志 306。所述多个标志 306 包括单元类型 308 和使用类型 310。标识 302 可以是标识受保护的密码密钥 312 的字母数字值。密码处理器 126 中的不同功能单元和 / 或控制器 206 可以使用标识 302 来访问受保护的密码密钥 312。保护标识 304 可以是标识用于加密该受保护的密码密钥 312 的密钥加密密钥的字母数字值。如果受保护的密码密钥 312 是数据加密密钥，则保护标识 304 可以是针对密钥加密密钥中一个的标识。如果受保护的密码密钥 312 是密钥加密密钥，则保护标识 304 可以是根加密密钥 241。

[0052] 单元类型 308 标识密码处理器 126 中可以访问受保护的密码密钥 312 的一个或更多个功能单元。此外，如果原语指令导致试图使功能单元访问未被单元类型 308 标识的给定受保护密码密钥 312 的微码指令的生成，则访问被拒绝，并且密码处理器 126 可以向请求该执行的应用返回错误信息 (error)。使用类型 310 标识可以使用受保护的密码密钥 312 来执行的一种或更多种类型的操作。操作类型可以包括签署、加密储存、证明身份密钥 (AIK) 操作等等。

[0053] 受信和密码操作

[0054] 现在描述受信和密码操作的更详细的描述。图 4 根据本发明的一个实施方案，示出用于与密码处理器的接口的操作的流程图。具体来说，图 4 示出在应用处理器 106 上执

行以与密码处理器 126 接口的（用于密码处理器 126 的）驱动器的操作的流程图 400。

[0055] 在框 402，接收对受信或密码操作的安全服务请求。参照图 1 的实施方案，在应用处理器 106 上执行的驱动器接收对受信或密码操作的安全服务请求。例如，该驱动器可以从在应用处理器 106 上执行的操作系统或其他应用接收该安全服务请求。安全服务请求可以是用于认证应用、硬件、配置信息等的信任操作。安全服务请求可以针对密码操作（例如哈希、密钥生成、加密、解密等等）。控制在框 404 处继续。

[0056] 在框 404，基于安全服务请求生成至少一条原语指令。参照图 1 的实施方案，用于密码处理器 126 的驱动器基于安全服务请求生成至少一条原语指令。例如，安全服务请求可以包括一项到多项不同的密码操作。从而，驱动器可以为不同的操作生成原语指令。控制在框 406 处继续。

[0057] 在框 406，将一条或多条原语指令传输到密码处理器。参照图 1 的实施方案，用于密码处理器 126 的驱动器将一条或多条原语指令传输到密码处理器 126。驱动器通过 DMA 逻辑 124 进行该传输操作。控制在框 408 处继续。

[0058] 在框 408，从密码处理器中接收一条或多条原语指令的结果。参照图 1 的实施方案，密码处理器 126 通过输出缓冲区 216（使用 DMA 接口 202）将一条或多条原语指令的结果传输回用于密码处理器 126 的驱动器。例如，如果原语指令与用于给定应用的认证的信任操作有关，则结果可以是指示应用是否被认证的布尔 (Boolean) 值。在另一个实施例中，如果原语指令是对解密操作的请求，则结果可以是指示解密操作是否成功以及该解密的结果被储存在何处或该解密的结果的布尔值。在不同的实施例中，如果原语指令是对随机数的请求，则结果可以包括随机数。流程图 400 的操作完成。

[0059] 现在描述密码处理器 126 对原语指令的处理的更详细的描述。图 5 根据本发明的一个实施方案，示出密码处理器的初始化的流程图。具体来说，在实施方案中，流程图 500 示出在密码处理器 126 中的操作执行之前所完成的那些操作。成功执行流程图 500 的操作之后，密码处理器 126 处于受信状态。

[0060] 在框 502，进行验证操作来确保 RNG 单元 228 正生成适当的随机数。参照图 2 的实施方案，控制器 206 执行该验证操作。这样的验证可以包括向 RNG 单元 228 请求随机数的一连串请求。例如，控制器 206 可以使用从 FIPS 140 针对随机性指定的测试来验证从那里输出的不同随机数是不同的并且具有随机值。控制在框 504 处继续。

[0061] 在框 504，进行验证操作来确保计数器处于适当的状态。计数器可以是单调计数器，所述单调计数器是仅在一个方向（例如向上）计数的软件或硬件计数器。计数器可以用于事务中和认证协议中，以确保消息被重放 (replay) 或者被使用多于一次。参照图 2 的实施方案，控制器 206 进行计数器 215 的该验证操作。计数器 215 的值可以被储存在非易失性存储器 116 中的被加密状态文件中。因此，该验证操作可以包括从非易失性存储器 116 中读取已加密状态文件以确保计数器 215 的该值未曾被递减，以及算术校验 (arithmeticcheck)，以确保计数器 215 的该值未处于它的上界 (upper range)。控制在框 506 处继续。

[0062] 在框 506，进行验证操作来确保功能单元正生成适当的结果。参照图 2 的实施方案，控制器 206 进行该验证操作。该验证操作可以包括在不同功能单元中执行不同的操作以及对这些操作的输出的验证。例如，控制器 206 可以命令 DES 单元 224 对不同数据进行一

连串的加密操作。接着，控制器 206 可以命令 DES 单元 224 解密这些数据。控制器 206 可以命令 ALU 222 将这些操作之前的数据与这些操作之后的数据进行比较。可以进行功能单元的其他类型的验证操作。例如，功能单元可以接收标准测试输入，并且可以将来自那里的输出与来自给定标准（例如国家标准技术研究所 (NIST) 提出的联邦信息处理标准 (FIPS)）的公开发表的值进行比较。控制在框 508 处继续。

[0063] 在框 508，进行易失性存储器的验证。参照图 2 的实施方案，控制器 206 可以验证易失性存储器 120 和 / 或易失性存储器 220。该验证可以包括确定易失性存储器未包括储存在其中的数据。另一个验证可以包括翻转其中的位，以验证数据可以被适当地储存在其中。流程图 500 的操作完成。

[0064] 图 6A 根据本发明的一个实施方案，示出密码处理器内安全操作的流程图。

[0065] 在流程图 600 的框 602 中，接收原语指令和 / 或相关联的数据。参照图 1 的实施方案，密码处理器 126 从用于密码处理器 126 的（在应用处理器 106 上执行的）驱动器接收原语指令。如上所述，这些原语指令可以用于不同类型的安全操作，例如信任操作、密码操作等等。参照图 2 的实施方案，密码处理器 126 通过 DMA 接口 202 接收原语指令，并且将该指令储存在指令序列缓冲区 204 中。

[0066] 此外，对于多个这样的指令，密码处理器 126 可以接收用于原语指令的相关联数据。参照图 2 的实施方案，密码处理器 126 通过 DMA 接口 202 将相关联数据接收到输入缓冲区 218 中。例如，如果原语指令与认证要在应用处理器 106 中执行的应用（例如用于应用处理器 106 的操作系统）的信任操作有关，则相关联的数据是用于所述应用的代码，所述代码从非易失性存储器 116 中取得 (retrieve)。

[0067] 为了进一步图示说明，密码处理器 126 可以被用来加密机密或需要被保护以避免修改的数据。因此，这样的操作可以被受信移动计算设备 100 用来保护文件不被其他应用或受信移动计算设备 100 的使用修改或查看。此外，密码处理器 126 可以被用在是数字版权运动的部分的受信移动计算设备 100 中，以保护内容和数字版权（许可）对象。因此，密码处理器 126 可以被用来解密移动图像专家组 (MPEG) 音频层 3(MP3) 文件，所述文件已经根据数字版权运动受到数字化保护。

[0068] 这样的数据的另一个实施例可以包括用于整体解密 (bulk decryption) 操作的数据，其中，所述数据从远程设备（例如不同的移动设备、服务器等等）接收到受信移动计算设备 100。相关联的数据可以包括要连同公钥被加密的数据，所述公钥用来进行解密操作。

[0069] 密码处理器 126 可以通过非易失性存储器 116 和 / 或易失性存储器 120 的公共接口来接收用于原语指令的相关联数据。回到流程图 600，控制在在框 604 处继续。

[0070] 在框 604，取得用于原语指令的微码指令。参照图 2 的实施方案，控制器 206 从微码存储器 240 取得用于原语指令的微码指令。给定的原语指令可以包括一条到多条不同的微码指令。例如，如果原语指令要基于对应用的已签署证书与密码哈希的比较来认证应用，则微码指令可以包括从非易失性存储器 116 取得已签署证书的指令。另一条微码指令可以包括从非易失性存储器 116 取得加密密钥，所述加密密钥用于密码哈希。另一条微码指令可以包括将加密密钥移动到 SHA 单元 230 的移动操作，而不同的微码指令可以命令 SHA 单元 230 进行所述密码哈希。另一条微码指令可以包括将密码哈希的结果和已签署证书移动到 ALU 22 的移动操作，而不同的微码指令可以命令 ALU 222 执行这两个值的比较。另一条

微码指令可以导致比较操作的结果被储存在输出缓冲区 216 中（所述结果被传输回应用处理器 106）。

[0071] 如所描述的，给定原语指令可以包括一连串微码指令。因此，用于给定原语指令的中间结果对于在密码处理器 126 外部的组件来说是不透明的。回到流程图 600，控制在框 606 处继续。

[0072] 在框 606，确定在密码处理器中是否基于用于该原语指令的微码指令进行敏感操作。参照图 2 的实施方案，控制器 206 作出该确定。敏感操作的实施例可以包括使用根加密密钥 241 的任何操作、使用（密钥缓存 221 中的）任何受保护密钥的任何操作和 / 或访问计数器 215 或任何平台配置寄存器 210 的任何操作。确定在密码处理器中未基于用于该原语指令的微码指令执行敏感操作后，控制在框 610 处继续，这在下面更详细地描述。

[0073] 在框 608，确定在密码处理器中基于用于该原语指令的微码指令执行敏感操作后，确定密码处理器是否处于受信状态。参照图 2 的实施方案，控制器 206 作出该确定。在实施方案中，如果密码处理器 126 未被适当地初始化（如上面结合图 4 的流程图 400 所描述的），则密码处理器 126 可能未处于受信状态。如果曾执行非法操作，则密码处理器 126 可能未处于受信状态。非法操作的实施例可以是当数据被尝试从一个位置不适当地移动到第二个位置时进行的操作（如本文关于数据移动约束的描述）。如果认证失败，或者如果密钥未被适当地加载到密码单元中，或者如果与原语指令 502 相关联的参数未在合适范围内等等，则密码处理器 126 也可能未处于受信状态。在加载密钥期间使用认证，并且使用口令 (password) 和两个随机数来组成 HMAC-SHA 计算，其中一个随机数由密码处理器 126 生成并且另一个随机数由应用或用户生成。HMAC 计算还可以包括来自原语指令 502 的值或要被加载的密钥的属性。

[0074] 在一些实施方案中，希望将密码密钥加载到密码处理器 126 的一个功能单元中以供执行的应用使用用于所述密钥的口令来计算 HMAC。应用可以具有口令的先验知识。例如，当密钥被创建时，应用可以设置密码。应用可以将期望的 HMAC 计算结果作为参数提供给原语指令 502。密码处理器 126 还生成 HMAC 计算，并且将它的结果与原语指令 502 上的期望的结果参数进行比较。如果两个结果匹配，则认证成功并且密钥被加载。如果结果不匹配，则认证失败并且密钥不被加载。

[0075] 在框 609 中，取消 (abort) 原语指令。参照图 2 的实施方案，控制器取消该原语指令。控制器 206 终止 (terminate) 任何额外的微码指令，并且还可以向在应用处理器 106 上执行的驱动器发送失败通知。然后，流程图 600 的操作完成。

[0076] 在框 610 中，确定密码处理器 126 处于受信状态后，进行与原语指令相关联的操作。参照图 2 的实施方案，控制器 206 基于微码操作来控制不同操作的执行顺序。因此，控制器 206 可以将用于执行的控制指令传输到密码处理器 126 内适当的功能单元、非易失性存储器控制器 114 或易失性存储器控制器 118。密码处理器 126 内适当的功能单元、非易失性存储器控制器 114 或易失性存储器控制器 118 进行所述操作。对于在原语指令的执行期间访问非易失性存储器 116 和易失性存储器 120，密码处理器 126 可以通过用于非易失性存储器 116 和易失性存储器 120 的私用接口 (private interface) 来执行该访问。例如，假设储存在易失性存储器 120 中的已加密数据加密的密钥要被用于针对原语指令的密码操作。控制器 206 可以通过用于易失性存储器 120 的私用接口来取得该已加密数据加密密钥。此

外，与原语指令相关联的操作的其他实施例在针对框 604（在上面阐述）的描述中示出。

[0077] 控制器 206 可以在不同的功能单元之间移动数据。然而，可以用一个或更多个数据移动约束来配置密码处理器 126。这样的约束确保流氓进程 (rogue process) 不能暗中从密码处理器 126 读取出任何敏感信息。这样的约束可以被储存在微码存储器 240 中。例如，一个数据约束阻止储存在密钥储存装置 220 中的数据被写到输出缓冲区 216 中。这样的约束防止加密密钥以未加密格式被读取出密码处理器 126。

[0078] 另一个示例性约束可以阻止储存在输入缓冲区 218 中的数据被写到上下文储存装置 /PCR 210 中。这样的约束防止对密码处理器 126 的平台配置的覆写。另一个示例性约束可以阻止储存在输入缓冲区 218 中的数据被写到密钥缓存 221。这样的约束防止对储存在密钥缓存中的加密密钥的覆写。回到流程图 600，控制在框 612 处继续。

[0079] 在框 612，确定是否有额外的微码指令要执行。参照图 2 的实施方案，控制器 206 作出该确定操作。如上面描述的，控制器 206 为给定原语指令从微码存储器 240 中取得一条到多条微码指令。因此，控制器 206 确定是否这些不同的指令已被执行。在确定要为给定原语指令执行额外的微码指令之后，控制在框 606 处继续，其中不同的微码指令被执行。在确定无需为给定原语指令执行额外的微码指令之后，微码执行清除 (clean-up) 操作，以确保密码处理器 126 停留在受信状态中。清除操作包括诸如从密码单元移除在操作中使用过的密钥、用 0 或 1 覆写中间储存装置 214 中的中间结果、重新设置密码处理器中的状态标志以指示操作完成或密码不再可用等等的操作。在清除操作结束之后，流程图 600 的操作完成。

[0080] 流程图 300 和 600 的操作可以用于多种不同的受信和密码操作。一个这样的实施例包括对非易失性存储器 116 的写访问。非易失性存储器 116 可以被分成多个不同的块。例如，如果非易失性存储器 116 的大小为 8 兆字节，则非易失性存储器 116 可以包括 8 个 1 兆字节的块。所述多个不同的块可以具有相关联的使能信号 (enable)，以控制对其的写访问。在要被储存到给定块的数据已经被认证之后，密码处理器 126 可以允许对所述给定块的使能信号的断言 (assertion)。相应地，密码处理器 126 的驱动器接收对非易失性存储器 116 中给定块的写访问的安全性服务请求。接着，驱动器生成原语指令，所述原语指令请求对要被储存在所述块中的数据的认证。所述原语指令连同已签署证书以及数据被传输到密码处理器 126。接着，密码处理器 126 可以执行多条不同的微码指令，以横贯所述数据生成与所述已签署证书进行比较的密码哈希。密码处理器 126 可以基于所述比较认证所述数据。这样的实施例可以用于认证被下载到受信移动计算设备 100 中的给定应用的新补丁。

[0081] 因此，如所描述的，本发明的实施方案可以在同一处理器上进行受信操作和密码操作两者，所述处理器处于独立于受信移动计算设备内的应用处理器的可执行上下文的可执行上下文中。因此，该密码处理器可以用于进行信任操作（例如用于认证应用处理器的操作系统的受信引导操作），同时还使用相同的功能单元进行受信引导操作后续的不同类型的密码操作。

[0082] 此外，如所描述的，密码处理器 126 可以确保信任相关的加密密钥不被对外（未加密地）暴露。密码处理器 126 可以确保密码操作的中间、部分结果也不被对外暴露。此外，密码处理器 126 可以确保一旦密码操作被发起，所述密码操作不能从密码处理器外部的组件被修改或篡改。

[0083] 现在描述密码操作的执行的更详细的描述，所述密码操作包括对密码密钥的使用。具体来说，图 6B 根据本发明的一个实施方案，示出在密码处理器中使用密码密钥的密码操作的执行的流程图。流程图 650 示出在密码处理器 126 中的操作执行中使用密码密钥之前，对所述密码密钥的验证和认证操作。

[0084] 在框 652，接收原语指令，以在密码处理器中进行包括密码密钥使用的操作。参照图 2 的实施方案，控制器 206 可以接收该原语指令。所述密码密钥可以在密码处理器 126 外部被生成。这样的密码密钥可以在所述原语指令的接收之间已经被加载到密码处理器 126 内的存储器中。可替换地，所述密码密钥可以连同所述原语指令被加载到密码处理器 126 中。所述密码密钥可以由密码处理器 126 中的功能单元在内部生成。所述密码密钥可以通过保护加密密钥被加密。此外，密码密钥的单元类型和 / 或使用类型（下面结合图 3 更详细地描述）可以与所述密码密钥相关联。控制在框 654 处继续。

[0085] 在框 654，确定密码密钥的单元类型和 / 或使用类型是否被授权。参照图 2 的实施方案，控制器 206 可以作出此确定。回到图 3 以帮助图示说明，控制器 206 可以取得用于所述密码密钥的头部。控制器 206 可以确定要使用该密码密钥的功能单元是否被列为单元类型 308 中的一个。此外，控制器 206 可以确定要使用该密码密钥进行的操作是否被列为使用类型 310 中的一个。在确定该密码密钥的单元类型和 / 或使用类型未被授权之后，控制在框 664 处继续，这在下面更详细地描述。

[0086] 在框 656，确定该密码密钥的单元类型和 / 或使用类型被授权后，生成质询 (challenge)。参照图 2 的实施方案，控制器 206 可以导致质询的生成。被加载到密码处理器 126 中的密码密钥可以包括相关联的口令。所述相关联的口令在密码处理器 126 中已知，并且为发出该原语指令的应用所已知。控制器 206 可以生成质询，所述质询被输出回在应用处理器 106 上执行的应用。所述质询可以请求来自应用的、对相关联口令的哈希的响应。虽然口令的哈希可以是多种不同类型的，但是在一个实施方案中，哈希基于 HMAC 操作。控制在框 658 处继续。

[0087] 在框 658，接收对质询的响应。参照图 1 的实施方案，在应用处理器 106 上执行的（请求执行原语指令的）应用将响应传输回密码处理器 126。控制器 206 接收对此质询的响应。控制在框 660 处继续。

[0088] 在框 660，确定响应是否正确。参照图 2 的实施方案，控制器命令 SHA 单元 230 生成所述口令的哈希。例如，SHA 单元 230 可以基于 HMAC 操作生成哈希。控制器 206 可以命令 ALU 222 比较从应用接收到的哈希和由 SHA 单元 230 生成的哈希。如果哈希相等，则响应被认为是正确的。在确定响应不正确后，控制在框 664 处继续，这在下面更详细地描述。

[0089] 在框 662，在确定响应正确后，密码密钥被加载到指定的功能单元以进行执行。参照图 2 的实施方案，控制器 206 导致密码密钥被加载到指定的功能单元以进行执行。接着，（如上面在流程图 600 中所描述的）该功能单元可以执行指令。接着，流程图 650 的操作完成。

[0090] 在框 664，原语指令被取消。参照图 2 的实施方案，控制器 206 取消该原语指令。控制器 206 终止任何额外的微码指令，并且还可以向在应用处理器 106 上执行的驱动器发送失败通知。接着，流程图 650 的操作完成。

[0091] 流程图 650 示出用于授权密码密钥在密码处理器 126 中的使用的质询 / 响应的一

个实施例。具体来说，流程图 650 示出使用与密码密钥相关联的口令的哈希的质询 / 响应。本发明的实施方案可以使用用于授权的其他类型的质询 / 响应操作。

[0092] 储存在微码存储器 240 中的微码指令可以被修补或更新。然而，如果微码存储器 240 是只读存储器，则补丁可以被储存在易失性存储器 220 中，从而补丁中的指令被用来代替微码存储器 240 中的那些指令。为了维护密码处理器 240 的安全性和可信赖状态，可以在安装之前认证这样的补丁 / 更新。现在描述对这些微码指令的这样的更新的一个实施方案。具体来说，图 7 根据本发明的一个实施方案，示出更新密码处理器中的微码的流程图。

[0093] 在框 702，为密码处理器发起受信引导操作。参照图 1 的实施方案，基于储存在受信引导 ROM 108 中的指令引导密码处理器 126。作为受信引导操作的一部分，微码存储器 240 中的指令可以被修补（这在流程图 700 中更详细地描述）。在以下 2003 年 12 月 22 日递交、标题为“Securing an Electronic Device（保护电子设备）”的共同待审定、共同转让的美国专利申请 No.10/745,496 中描述了受信引导操作的更详细的描述。控制在框 704 处继续。

[0094] 在框 704，（作为受信引导操作的一部分）确定是否存在针对微码的补丁。参照图 2 的实施方案，非易失性存储器 116 包括指定段，用于对微码指令的补丁的储存。因此，控制器 206 可以基于指定段中的数据是否包括补丁来确定是否存在针对微码的补丁。确定不存在补丁后，流程图 700 的操作完成。

[0095] 在框 706，确定存在用于微码的补丁后，所述补丁以及用于所述补丁的密码密钥和签名被加载。参照图 2 的实施方案，控制器 206 将所述补丁、用于所述补丁的密码密钥和签名加载到非易失性存储器 120 中。控制在框 708 处继续。

[0096] 在框 708，确定用于补丁的密码密钥是否是合法 (valid) 的。参照图 2 的实施方案，非易失性存储器 116 可以包括被定义为“一次可编程”的段。具体来说，该段可以被写一次，由此阻止流氓或恶意进程修改储存在该段中的数据。该段可以包括用于补丁的密码密钥的哈希。因此，控制器 206 可以分别从非易失性存储器 116 以及易失性存储器 120 中取得该哈希和密码密钥。控制器 206 命令 SHA 单元 230 生成密码密钥的哈希。接着，控制器 206 可以命令 ALU 222 将该哈希结果与从非易失性存储器 116 取得的哈希进行比较，以确定这两个值是否相同。如果这两个值相等，则用于补丁的密码密钥是合法的。

[0097] 在框 710，确定用于补丁的密码密钥不合法后，用于补丁的密码密钥和签名被删除。参照图 2 的实施方案，控制器 206 将补丁、用于补丁的密码密钥和签名从易失性存储器 120 中删除。因此，补丁内的指令将不会被加载到密码处理器 126 中或被密码处理器 126 执行。接着，流程图 700 的操作完成。

[0098] 在框 712，确定用于补丁的密码密钥合法后，确定用于补丁的签名是否合法。参照图 2 的实施方案，控制器 206 将补丁加载到 SHA 单元 230 中。接着，控制器 206 命令 SHA 单元 230 生成补丁的摘要。控制器 206 将伴随补丁的数字签名连同密码密钥加载到幂运算单元 234 中。接着，控制器 206 可以命令幂运算单元 234 解密所述签名。控制器 206 可以检查幂运算单元 234 的输出，以确定所述签名是否被适当地解密。适当解密签名后，控制器 206 命令 ALU 222 将已解密签名与由 SHA 单元 230 生成的摘要进行比较。如果两个值相等，则用于补丁的签名是合法的，并且所述补丁是用于密码处理器 126 的被适当授权的补丁。

[0099] 在框 714，确定用于补丁的签名合法后，补丁标志以及用于被修补的微码的标签项

(tagentry) 被加载。参照图 2 的实施方案，除了是补丁的一部分的指令之外，补丁可以包括一组补丁标志，所述补丁标志指示微码存储器 240 的哪些段被修补。控制器 206 可以将这些补丁标志加载到补丁标志存储器 281 中。这样的补丁标志可以是用于微码存储器 240 中每个段的 1 位表示。补丁标志存储器 281 中被置位 (set) 的位指示微码存储器 240 中的对应段具有补丁。例如，如果在补丁标志存储器 240 中位 5 被置位，则微码存储器 240 中的段 5 具有对应的补丁。相应地，包括补丁的文件可以包括补丁标志、以补丁标签开头的一连串补丁段、对补丁标志以及所述一连串补丁段和补丁标签的数字签名。用于微码存储器 240 中的段的给定补丁标签储存补丁中要替代微码存储器 240 的段被执行的段的标识。因此，在微码存储器 240 的段中的指令的执行期间，如果标志指示该段被修补，则控制器 206（使用标签项）从补丁中取 (fetch) 指令，以供替代来自微码存储器 240 的指令进行执行。在一些实施方案中，当要执行补丁的段中的指令时，仅将所述补丁的段从易失性存储器 120 加载到易失性存储器 220 中。此外，该段可以保留在易失性存储器 220 中。因此，如果所述段中的指令要被重新执行，控制器 206 不必要从易失性存储器 120 中重新取该指令。流程图 700 的操作完成。

[0100] 因此，如所描述的，密码处理器 126 中的微码可以仅仅基于包括密码密钥的认证操作被修补，所述密码密钥基于储存在“一次可编程”储存装置中的哈希进行验证。认证操作还被基于横贯补丁的签名使用被验证的密码密钥进行验证。

[0101] 系统操作环境

[0102] 在这部分，介绍系统概述。系统概述介绍结合本发明的实施方案使用的网络配置。系统概述还介绍网络配置的一般功能性。

[0103] 图 8 根据本发明的一个实施方案，示出其中具有密码操作的受信移动通信设备可以工作的系统配置的简化功能框图。图 8 示出包括多个受信移动计算设备 100A-100N 以及多个服务器 806A-806N 的系统 800，所述多个受信移动计算设备 100A-100N 和多个服务器 806A-806N 通过网络 804 耦合在一起。网络 804 可以是广域网、局域网，或者是在多个受信移动计算设备 100A-100N 和多个服务器 806A-806N 之间提供通信的不同网络的组合。例如，多个受信移动计算设备 100A-100N 可以是不同类型的无线计算设备，其中，网络 804 的一部分被配置为处理无线通信，而网络 804 的不同的部分可以被配置成为与多个服务器 806A-806N 的通信处理有线通信。

[0104] 如上文所描述的，多个受信移动计算设备 100A-100N 可以执行多项信任和密码操作。例如，多个受信移动计算设备 100A-100N 的用户可以用在多个服务器 806A-806N 上执行的不同应用来进行不同的电子商务交易。

[0105] 在描述中，阐述了大量具体细节，例如逻辑实现、操作代码、指定操作数的方法、资源划分 (partitioning)/ 共用 / 复制的实现、系统组件的类型和相互关系，以及逻辑划分 / 集成的选择，以提供对本发明的完整理解。然而，本领域的技术人员将意识到，无需使用这些具体的细节可以实践本发明。此外，控制结构、门级电路和整个软件指令序列未详细示出，以免模糊本发明的实施方案。获悉本文所包含的说明的本领域普通技术人员无需超出常规的试验就能够实现适当的功能性。

[0106] 在说明书中提及的“一个实施方案”、“实施方案”、“示例性实施方案”等指示描述的实施方案可以包括特定特征、结构或特性，但是每个实施方案可以不必包括所述特定特

征、结构，或特性。此外，这样的短语不必是指同一实施方案。此外，当关于某种实施方案来描述具体的特点、结构或特性时，无论是否明确地指出，认为本领域的技术人员在其知识范围内都可以结合其他实施方案来实现这种特点、结构或特性。

[0107] 本发明的实施方案包括可以被实施在由机器可读介质提供的机器可执行指令中的特征、方法或过程。机器可读介质包括以机器（例如计算机、网络设备、个人数字助理、制造工具、具有一组一个或更多个处理器的任何设备，等等）可访问形式提供（即储存和/或传输）信息的任何机制。在示例性实施方案中，机器可读介质包括易失性和/或非易失性介质（例如只读存储器 (ROM)、随机访问存储器 (RAM)、磁盘储存介质、光储存介质、闪存存储器设备等等）以及电、光、声或其他形式的传播信号（例如载波、红外信号、数字信号等等）。

[0108] 使用这样的指令来导致用这些指令编程的通用或专用处理器完成本发明的实施方案的方法或过程。可替换地，通过包括用于完成操作的硬连线逻辑的具体硬件组件或者通过编程的数据处理组件和具体硬件组件的任何组合来完成本发明的实施方案的特征或操作。本发明的实施方案包括软件、数据处理硬件、数据处理系统实现的方法、以及本文进一步描述的各种处理操作。

[0109] 多幅附图根据本发明的实施方案示出用于受信移动平台体系结构的系统和装置的框图。多幅附图根据本发明的实施方案示出图示说明用于受信移动平台体系结构的操作的流程图。将参照在框图中示出的系统/装置来描述流程图的操作。然而，应该理解，流程图的操作可以由与参照框图所讨论的那些系统和装置不同的其他系统和装置的实施方案完成，并且参照系统/装置所讨论的实施方案可以完成与参照流程图所讨论的那些操作不同的其他操作。

[0110] 考虑本文所描述的实施方案的各种改变，该详细的描述仅意图是示意性的，而不应该被视为限制本发明的范围。为了图示说明，虽然参照信任和加密操作作出描述，但是当受信移动计算设备 100 被这样的设备的使用者实际操作时，本发明的实施方案不受这样的限制。例如，密码处理器 126 可以被用来在受信移动计算设备 100 的调试操作期间认证设备。回到图 1 来图示说明，设备可以通过 JTAG 接口 155 耦合到密码处理器 126，以供调试。因此，密码处理器 126 可以通过质询/响应操作来认证该设备。密码处理器 126 可以生成被传输到耦合到 JTAG 接口 155 的设备的质询。接着，该设备生成对质询的响应。因此，如果密码处理器 126 基于响应认证该设备，则设备能够通过 JTAG 接口 155 来执行与受信移动计算设备 100 的通信。

[0111] 为了进一步示出本发明的实施方案的改变，虽然在实施方案中描述为原语指令在密码处理器 126 中被串行地执行，但是，用于不同原语指令的多项不同的微码操作可以至少部分地同时在其中执行。因此，本发明所要求保护的是所有这样的修改，所述修改可以在所附权利要求书及其等同物的范围和可用等同范围内。因此，说明书和附图被视为示意性的，而不是限制性的。

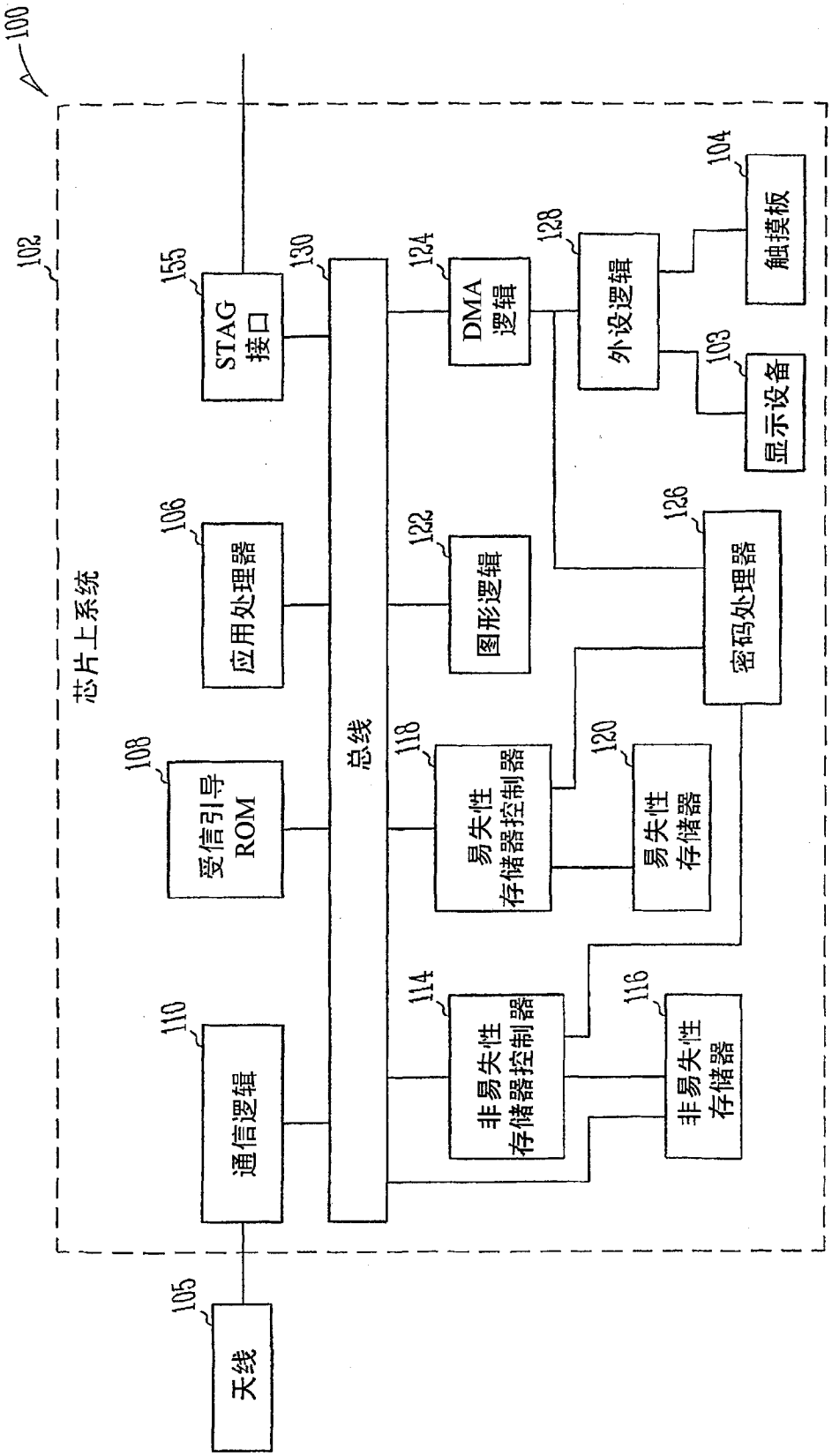

100
102
芯片上系统
155
STAG 接口
130
总线
124
DMA 逻辑
128
外设逻辑
104
触摸板
103
显示设备
106
应用处理器
122
图形逻辑
126
密码处理器
108
受信引导 ROM
118
易失性存储器控制器
120
易失性存储器
110
通信逻辑
114
非易失性存储器控制器
116
非易失性存储器
105
天线

图 1

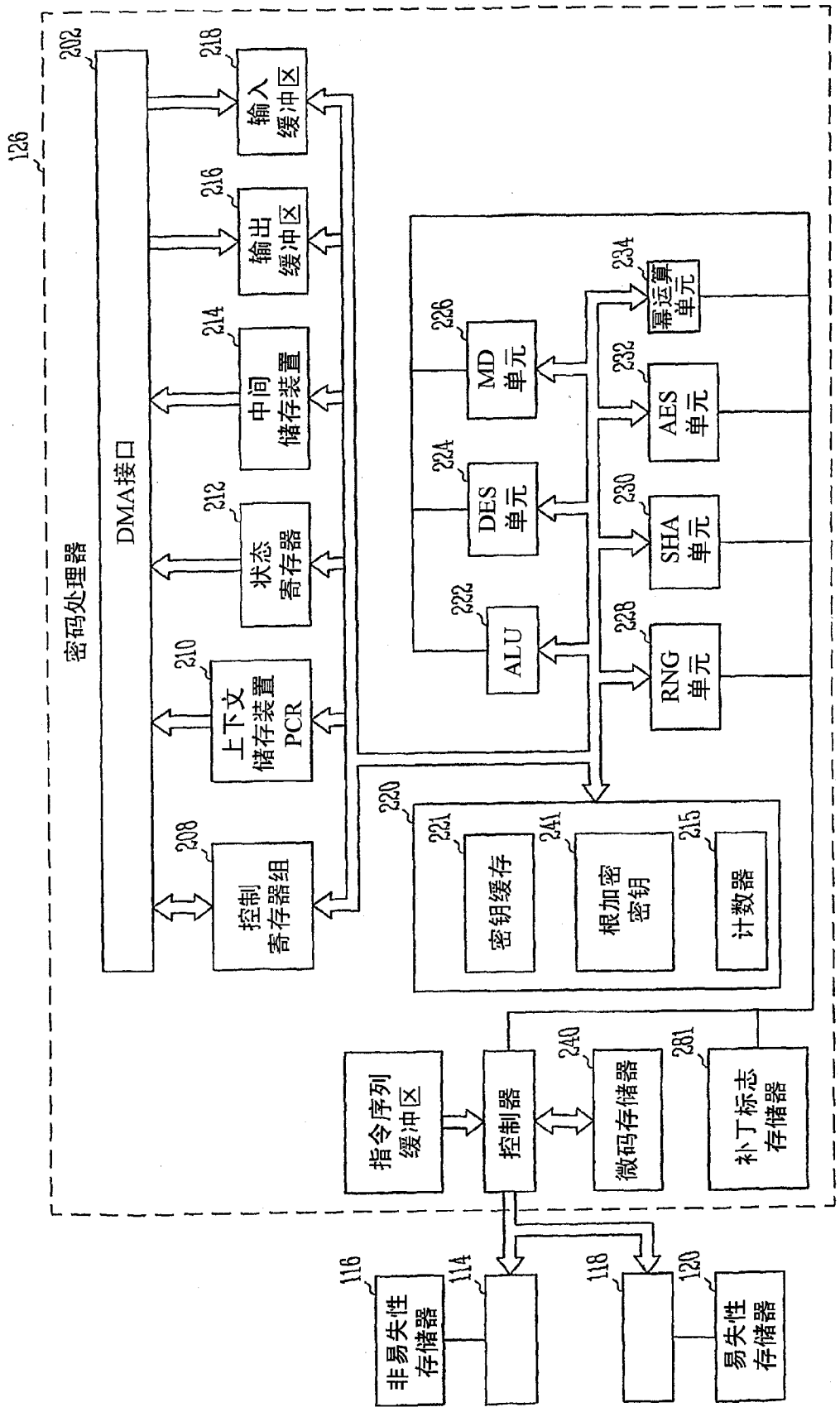

126
密码处理器
202
DMA接口
218
输入缓冲区
216
输出缓冲区
214
中间储存装置
212
状态寄存器
210
上下文储存装置PCR
208
控制寄存器组
220
221
密钥缓存
241
根加密密钥
215
计数器
226
MD单元
224
DES单元
222
ALU
234
幂运算单元
232
AES单元
230
SHA单元
228
RNG单元
指令序列缓冲区
控制器
240
微码存储器
281
补丁标志存储器
116
非易失性存储器
114
118
120
易失性存储器

图 2

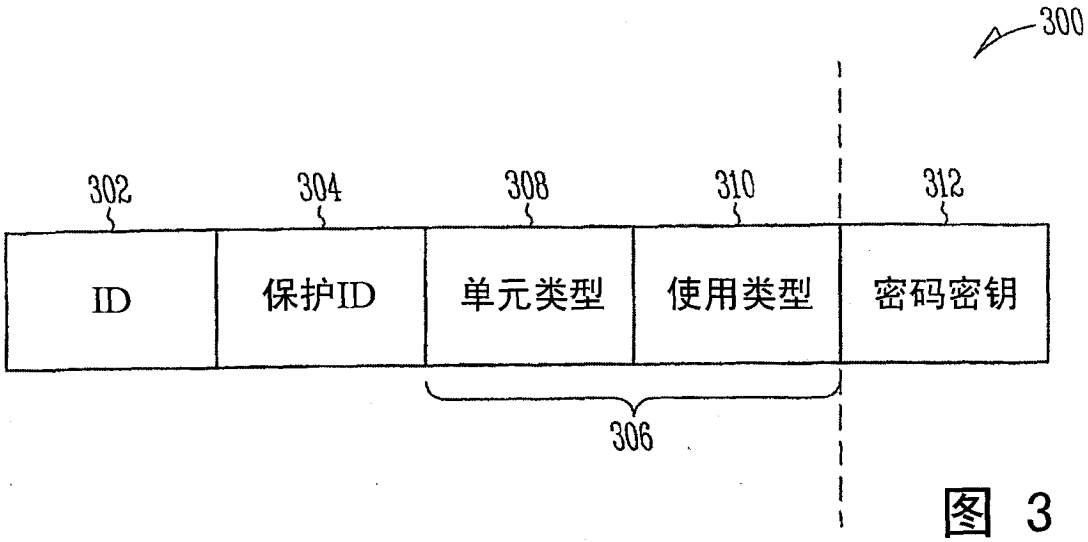

300
302
304
308
310
312
ID
保护ID
单元类型
使用类型
密码密钥
306

图 3

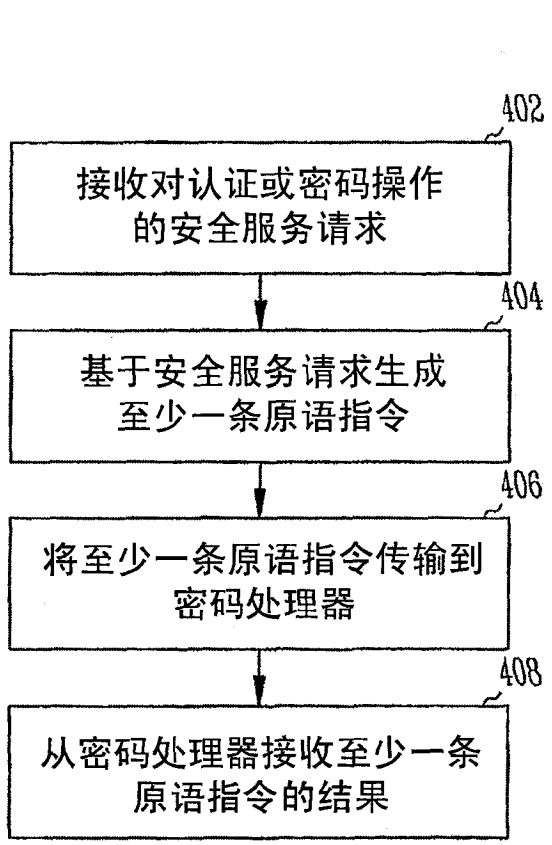

400
402
接收对认证或密码操作的安全服务请求
404
基于安全服务请求生成至少一条原语指令
406
将至少一条原语指令传输到密码处理器
408
从密码处理器接收至少一条原语指令的结果

图 4

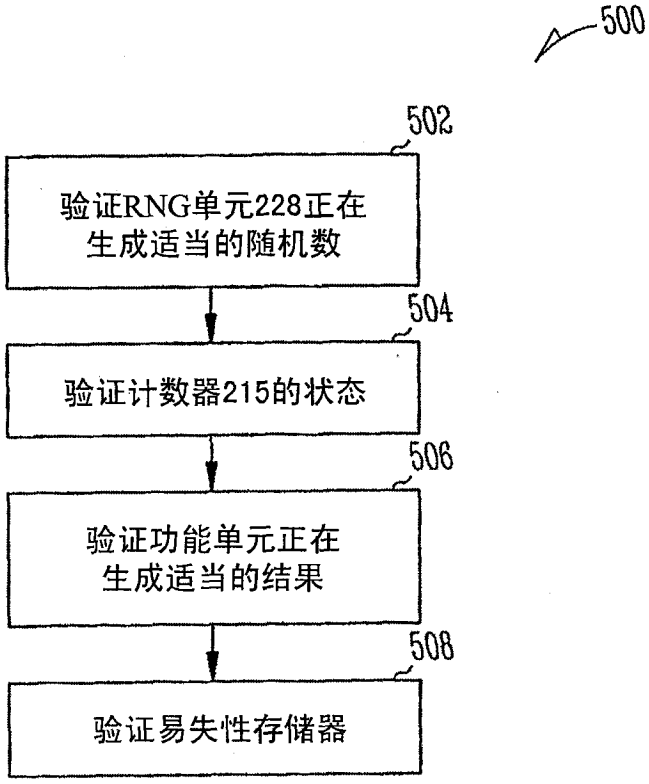

500
502
验证RNG单元228正在生成适当的随机数
504
验证计数器215的状态
506
验证功能单元正在生成适当的结果
508
验证易失性存储器

图 5

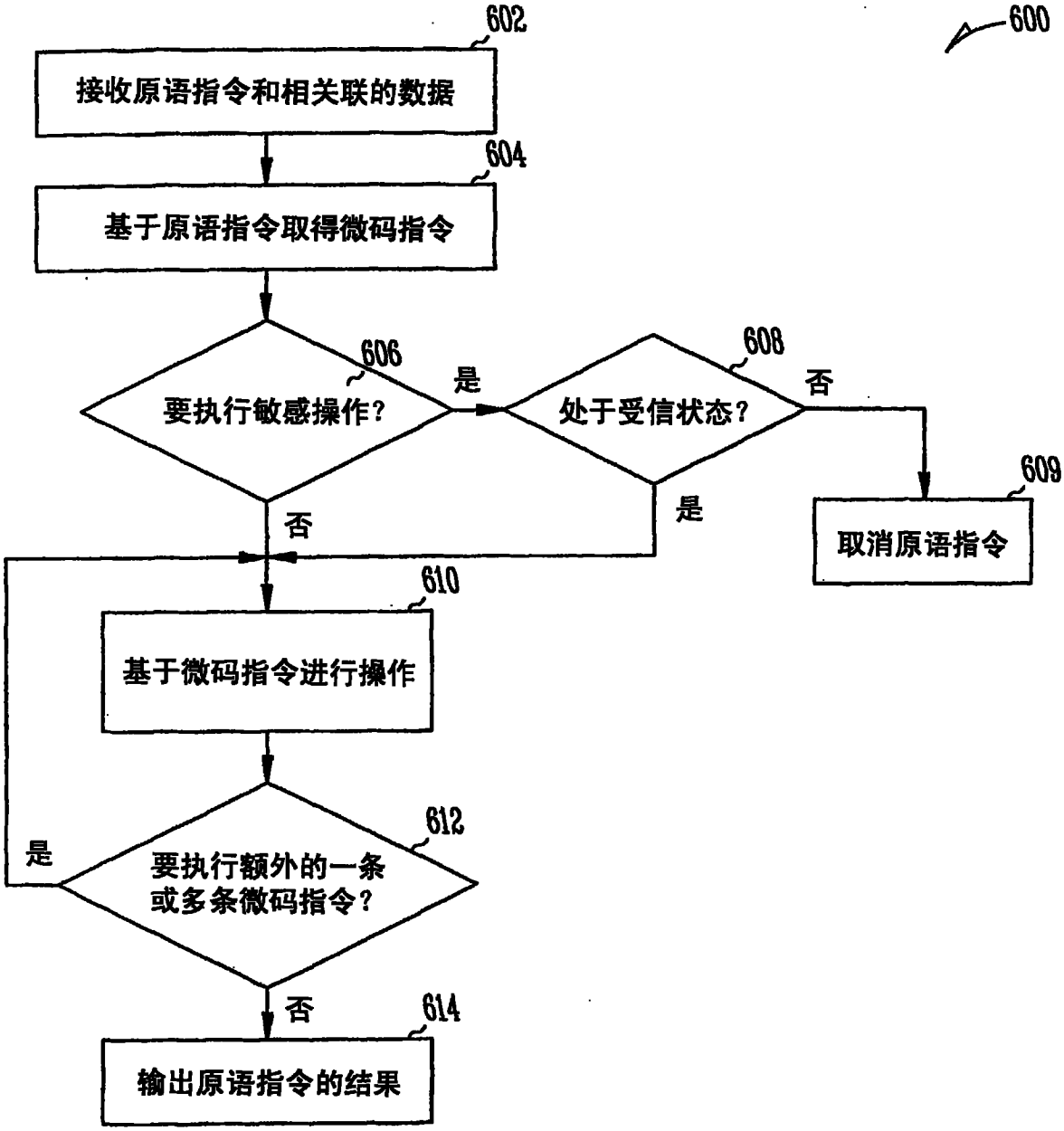

600
602
接收原语指令和相关联的数据
604
基于原语指令取得微码指令
606
要执行敏感操作?
是
608
处于受信状态?
否
609
取消原语指令
是
否
610
基于微码指令进行操作
612
要执行额外的一条或多条微码指令?
是
否
614
输出原语指令的结果

图 6A

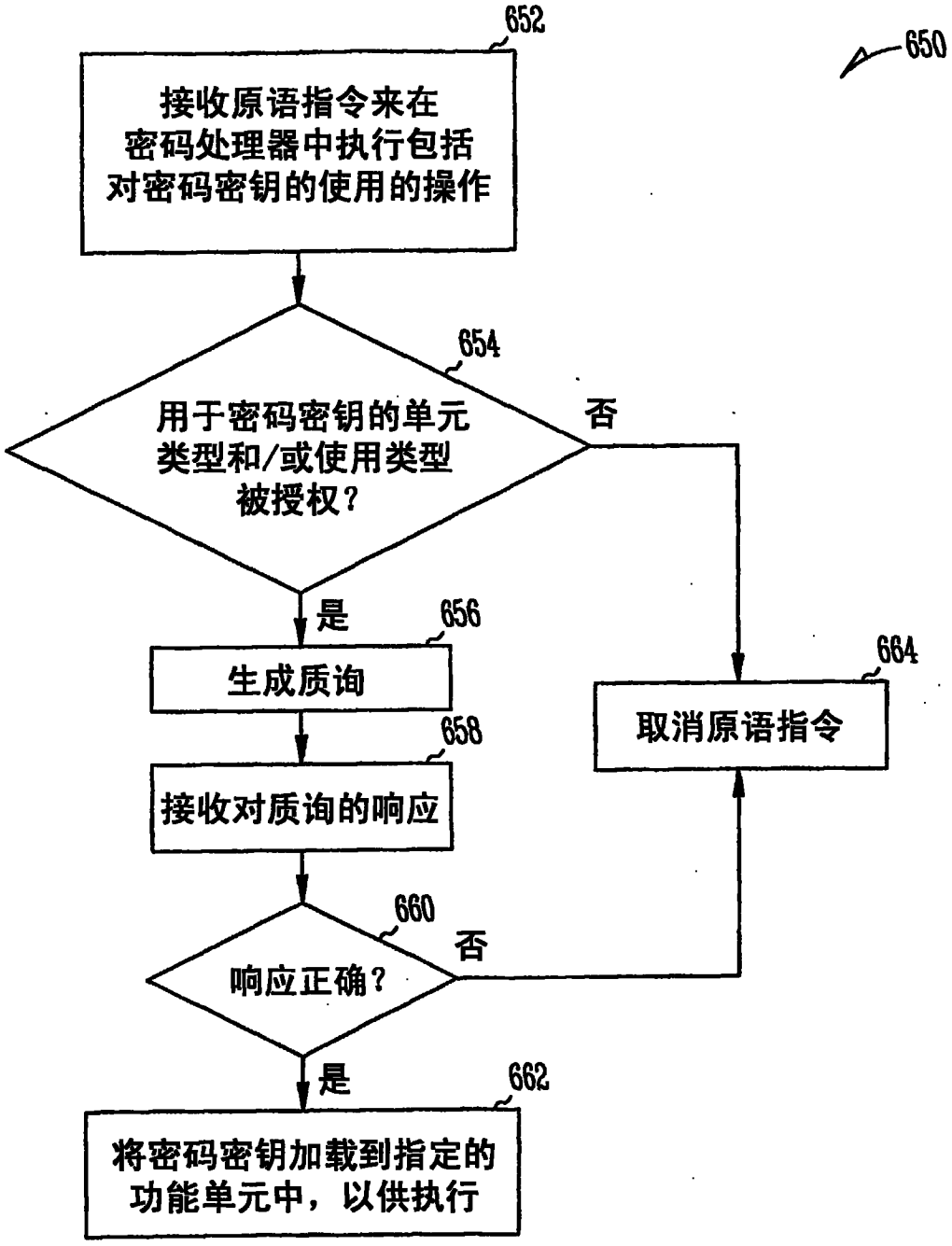

650
652
接收原语指令来在密码处理器中执行包括对密码密钥的使用的操作
654
用于密码密钥的单元类型和/或使用类型被授权？
否
是
656
生成质询
658
接收对质询的响应
660
响应正确？
否
是
662
将密码密钥加载到指定的功能单元中，以供执行
664
取消原语指令

图 6B

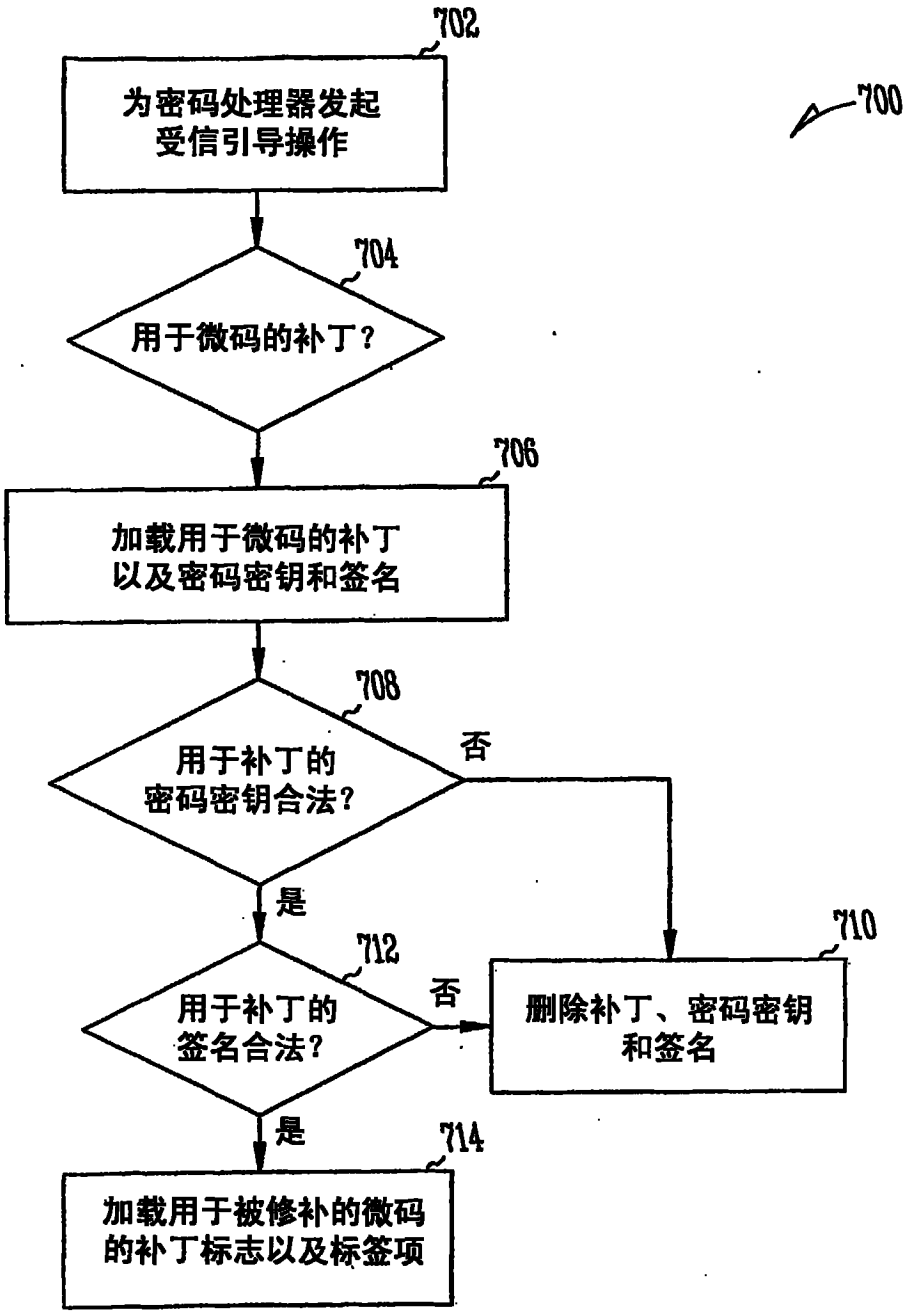

702
为密码处理器发起
受信引导操作
700
704
用于微码的补丁？
706
加载用于微码的补丁
以及密码密钥和签名
708
用于补丁的
密码密钥合法？
否
是
710
712
用于补丁的
签名合法？
否
删除补丁、密码密钥
和签名
是
714
加载用于被修补的微码
的补丁标志以及标签项

图 7

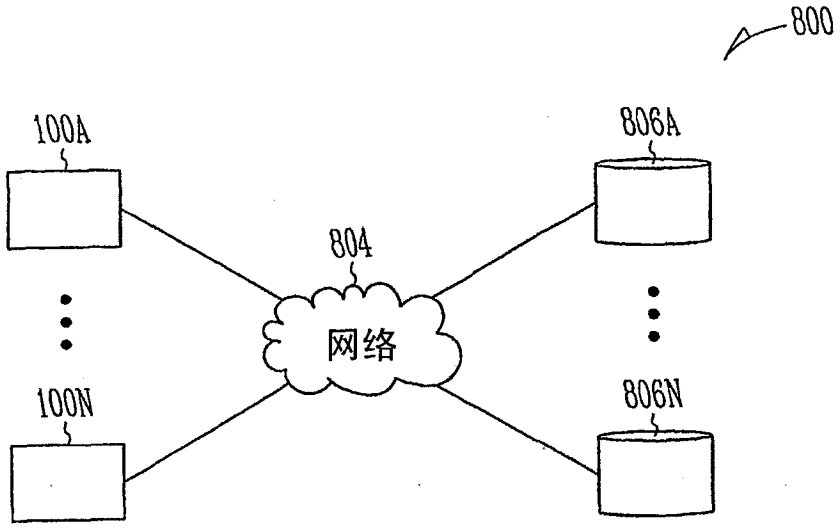


图 8