



[12] 发明专利申请公开说明书

[21] 申请号 03813396.2

[43] 公开日 2005 年 8 月 24 日

[11] 公开号 CN 1659494A

[22] 申请日 2003.3.28 [21] 申请号 03813396.2

[30] 优先权

[32] 2002. 4. 12 [33] US [31] 10/121,807

[86] 国际申请 PCT/US2003/009640 2003. 3. 28

[87] 国际公布 WO2003/088019 英 2003. 10. 23

[85] 进入国家阶段日期 2004. 12. 9

[71] 申请人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 J·萨顿二世

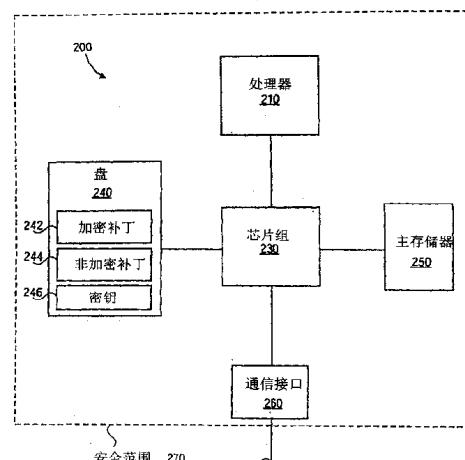
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 钱慰民

权利要求书 4 页 说明书 10 页 附图 6 页

[54] 发明名称 微码补丁验证

[57] 摘要

在将微码补丁传送到安装微码补丁的目标处理器之前对其进行编码。目标处理器在安装之前确认微码补丁。通过以下措施的一个或多个使处理的安全性得到增强：1) 在安全存储器中进行确认、2) 使用公开/秘密密钥对对微码补丁进行加密和解密、3) 使用至少一个嵌入在目标处理器内并且不能由非安全软件读取的密钥以及4) 使用嵌入在目标处理器内的散列值确认至少一个非嵌入的密钥。



1. 一种提供指令的机器可读取介质，当该指令由一组一个或多个处理器执行时使该组处理器进行操作，该操作包括：

为微码补丁产生散列文摘；

对散列文摘进行加密以产生数字签名；以及

组合数字签名和微码补丁以传送到目标处理器来对目标处理器中的微码打补丁。

2. 如权利要求 1 所述的介质，其特征在于所述组合包括将密钥与数字签名及微码补丁进行组合以传送到目标处理器。

3. 如权利要求 1 所述的介质，其特征在于所述组合包括将密钥的散列值与数字签名及微码补丁进行组合以传送到目标处理器。

4. 一种方法，包括：

为微码补丁产生散列文摘；

用不对称密码算法的秘密密钥对散列文摘进行加密以产生数字签名；以及

组合数字签名和微码补丁以传送到目标处理器来对目标处理器中的微码打补丁。

5. 如权利要求 4 所述的方法，其特征在于还包括：

对微码补丁进行加密；

其中所述产生散列文摘包括在所述对微码补丁进行加密之前产生散列文摘；以及

其中所述组合包括将数字签名与加密的微码补丁进行组合。

6. 如权利要求 4 所述的方法，其特征在于还包括：

对微码补丁进行加密；

其中所述产生散列文摘包括在所述对微码补丁进行加密之后产生散列文摘；以及

其中所述组合包括将数字签名与加密的微码补丁进行组合。

7. 一种包含数据的机器可读取介质，该数据包括：

对目标系统中的微码打补丁的微码补丁；以及

通过将对微码补丁施加散列运算所创建的文摘进行加密所产生的数字签名。

8. 如权利要求 7 所述的介质，其特征在于所述数据还包括：

对数字签名进行解密以产生文摘的密钥。

9. 如权利要求 7 所述的介质，其特征在于所述数据还包括：

确认微码补丁的密钥的散列值。

10. 如权利要求 7 所述的介质，其特征在于微码补丁是加密的。

11. 一种设备，包括：

具有微码的处理器；

耦合到处理器的安全存储器，用于对编码的微码补丁进行解码；以及

耦合到微码的微码补丁存储器，用于保存经解码的微码补丁。

12. 如权利要求 11 所述的设备，其特征在于：

微码包括对编码的微码补丁进行解码的微指令；以及

安全存储器包含编码的微码补丁、解码的微码补丁以及微码补丁解码期间的中间产物中的至少一个。

13. 如权利要求 11 所述的设备，其特征在于：

微码包括对编码的微码补丁进行解码的微指令；以及

安全存储器用于同时包含编码的微码补丁、解码的微码补丁以及微码补丁解码期间的中间产物中的至少一个的仅仅一部分。

14. 如权利要求 11 所述的设备，其特征在于：

处理器包括嵌入式密钥，用于对编码的微码补丁进行解码。

15. 如权利要求 14 所述的设备，其特征在于：

嵌入式密钥是不对称密码算法中的公开密钥。

16. 一种方法，包括：

获取微码补丁和相关的数字签名；

在安全存储器中对数字签名进行解密以获取第一散列文摘；

用微码补丁计算第二散列文摘；

将第一散列文摘与第二散列文摘进行比较；以及

响应于第一和第二散列文摘之间的匹配，在微码补丁存储器中安装微码补

丁。

17. 如权利要求 16 所述的方法，其特征在于进一步包括：

对微码补丁进行解密；

其中所述计算第二散列文摘包括用微码补丁的加密版本计算第二散列文摘。

18. 如权利要求 16 所述的方法，其特征在于进一步包括：

对微码补丁进行解密；

其中所述计算第二散列文摘包括用微码补丁的解密版本计算第二散列文摘。

19. 如权利要求 16 所述的方法，其特征在于：

所述对数字签名进行解密包括使用公开密钥进行不对称解密。

20. 如权利要求 16 所述的方法，其特征在于：

所述对数字签名进行解密包括使用嵌入的密钥。

21. 如权利要求 16 所述的方法，其特征在于：

所述对数字签名进行解密包括使用随微码补丁提供的密钥进行不对称解密。

22. 一种提供指令的机器可读取介质，当该指令由一组具有一个或多个处理器执行时使该组处理器进行操作，该操作包括：

获取微码补丁和相关的数字签名；

在安全存储器中对数字签名进行解密以获取第一散列文摘；

用微码补丁计算第二散列文摘；

将第一散列文摘与第二散列文摘进行比较；以及

响应于第一和第二散列文摘之间的匹配，在微码补丁存储器中安装微码补丁。

23. 如权利要求 22 所述的介质，其特征在于进一步包括：

对微码补丁进行解密；

其中所述计算第二散列文摘包括用微码补丁的加密版本计算第二散列文摘。

24. 如权利要求 22 所述的介质，其特征在于进一步包括：

对微码补丁进行解密；

其中所述计算第二散列文摘包括用微码补丁的解密版本计算第二散列文摘。

25. 如权利要求 22 所述的介质，其特征在于：

所述对数字签名进行解密包括使用公开密钥进行不对称解密。

26. 如权利要求 22 所述的介质，其特征在于：

所述对数字签名进行解密包括使用嵌入的密钥。

27. 如权利要求 22 所述的介质，其特征在于：

所述对数字签名进行解密包括使用随微码补丁以及相关联的数字签名提供的密钥进行不对称解密。

28. 一种系统，包括：

具有微码和嵌入的密钥的处理器；以及

驻留在与处理器耦合的存储设备和基本输入输出系统的至少一个中的微码补丁包，微码补丁包包括对微码打补丁的微码补丁以及数字签名以使用嵌入的密钥对微码补丁进行确认。

29. 如权利要求 28 所述的系统，其特征在于：

在微码补丁包中微码补丁是以加密形式的。

30. 如权利要求 28 所述的系统，其特征在于：

安全存储器在确认期间包含微码补丁。

微码补丁验证

背景

计算机处理器中的一条典型指令用微指令实现一系列的操作，而微指令以微码的形式在非易失性存储区域中定义了被编码的每一操作。微码定义了处理器的所有或一部分可执行指令集，并且还可定义不是以软件可访问代码实现的内部操作。微码通常在制造处理器时置于处理器内的只读存储器（ROM）中。然而，在处理器制造后，甚至在处理器已处于操作中时，有时需要修改微码。微码补丁通过插入新的微指令取代原来的微指令而允许这样的修改。可将微码补丁以不同方式（如通过通信信道下载、由服务技术人员安装或随操作系统提供）传送到处理器，随后存储于处理器用于操作。由于不能简单地改变微码 ROM，微码补丁通常置于处理器内的补丁存储器，如随机存取存储器（RAM），并且对于修改的微指令的引用则被重新定向到补丁 RAM 而不是 ROM。因为补丁 RAM 可以是易失性的，所以通常微码补丁存储于磁盘上或存储于基本输入输出系统（BIOS）中，并在引导系统时将微码补丁加载到补丁 RAM 中。

如果处理器用于安全环境，则在软件和/或硬件设计中应采取各种安全措施，以提供对安全特征操作篡改的保护。将非授权的微码补丁插入处理器中的能力代表了不怀好意的攻击者妨碍传统安全措施的一个方式。

附图简述

通过参考用于示出本发明实施例的以下描述以及附图可理解本发明。

图 1 根据本发明的一个实施例示出了确认和安装微码补丁的系统框图。

图 2 根据本发明的一个实施例示出了将微码补丁转换为安全传送形式的系统框图。

图 3 根据本发明的一个实施例示出了从图 2 系统传送到图 1 系统的包含各单元的补丁包。

图 4 根据本发明的一个实施例示出了用于制备、传送和确认补丁包的整个过

程的流程图。

图 5 根据本发明的一个实施例示出了用于制备补丁包的过程的流程图。

图 6 根据本发明的一个实施例示出了用于确认补丁包的过程的流程图。

详细描述

在以下描述中，提出了许多特定细节。然而，可以理解，没有这些特定细节也可实现本发明的实施例。在其他实例中，为了便于该描述的理解，没有详细示出熟知的电路、结构和技术。提到的“一个实施例”、“实施例”、“示例实施例”、“各实施例”等表示所描述的实施例可包括特定特点、结构或特征，但不是每个实施例都必须包括这些特定的特点、结构和特征。并且，可将对于不同实施例描述的特点、结构或特征结合到单个实施例中。还有，重复使用短语“在一个实施例中”并不一定指同一实施例，虽然也可以指同一实施例。

这里提到的加密法可包括加密、解密或两者兼而有之。这里提到的“对称”密码、密钥、加密或解密指的是同一密钥被用于加密和相关解密的密码技术。1993年作为联邦信息出版标准 FIPS PUB 46-2 出版的熟知的数据加密标准 (DES) 以及 2001 年作为 FIPS PUB 197 出版的高级加密标准都是对称密码的例子。这里提到的“不对称”密码、密钥、加密或解密指的是加密和相关解密使用不同但相关的密钥的密码技术。所谓的“公开密钥”密码技术，包括熟知的 Rivest-Shamir-Adleman (RSA) 技术，就是不对称密码的例子。不对称密码过程两个相关密钥之一被称作为秘密密钥（因为它通常保持私密的），而另一个则被称作为公开密钥（因为它通常可自由地使用）。在一些实施例中，秘密或公开密钥可用于加密，而其中另一个密钥则用于相关的解密。

可以硬件、固件和软件的其中一个或组合来实现本发明的实施例。本发明的实施例还可实现为存储在机器可读取介质上的指令，它可由至少一个处理器读取并执行以实现这里所描述的操作。机器（如计算机）可读取介质包括任何用于以机器可读取形式存储或发送信息的机制。例如，机器可读取介质包括只读存储器 (ROM)、随机存取存储器 (RAM)、磁盘存储介质、光存储介质、快闪存储器设备、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），等等。

本发明的各个实施例涉及微码补丁（这里还简称为“补丁”）的编码和/或解

码，使得在将补丁安装于目标处理器（希望使用补丁的处理器）中之前将其验证为有效。编码/解码可包括以下的一种或多种：1) 加密/解密、2) 使用密码散列函数、3) 使用数字签名、4) 等等。目标系统是将要安装补丁的系统，而始发系统是制备安全传送到目标系统的补丁的系统。在一个实施例中，为特定类型的计算机系统产生补丁的公用集，其中“类型”可以指特定的代、特定型号、型号内的一些类别等。一旦产生了补丁，就在传送到想要该补丁的每个目标系统之前，以这里所述的方式对其进行编码。在每个目标系统中，可如这里所述对一个或多个补丁进行解码和安装，使得补丁成为目标系统的操作部分。

可使用任何传统的传送方法，包括但不限于，通过通信链路传送、由技术人员安装、由操作系统的制造商包含在操作系统中、包含在基本输入输出系统(BIOS)中。一旦经过传送，补丁可以其编码形式存储直到其被操作安装。操作安装包括对编码的补丁进行解码、确认补丁是授权的以及将补丁置于补丁存储器。确认包括以下任一项或两者：1) 确定自补丁在始发系统中制备用于传送以来没有被修改过；以及2) 确定该补丁在已授权系统中被制备。在一个实施例中，编码的补丁被存储在目标系统的盘上或 BIOS 中，每一次引导系统时，被操作地安装在易失性 RAM 中。在一个实施例中，将编码的补丁操作地安装在非易失性存储器中，并且在后续重引导期间不再安装。

图 1 根据本发明的一个实施例示出了确认和安装微码补丁的系统框图。在图 1 示出的实施例中，系统 100 包括处理器 110、芯片组 130、盘 140、主存储器 150 以及通信接口 (Comm I/F) 160。处理器 110 可包括微码 ROM112、补丁存储器 114、安全存储器 118 以及一个或多个密钥 116。芯片组 130 可包括 BIOS132。可将以后所描述的补丁包存储于盘 140、BIOS132 或包括非易失性存储的系统 100 的另一部分的至少一个中。

在一些实施例中，可由包含在微码 ROM112 中的微指令序列实现对补丁进行解码、确认和安装的操作。在特定实施例中，通过执行将执行传输到序列入口点的特别指令启动该序列。在另一特定实施例中，响应于将预定值写到机器专用寄存器 (MSR) 的预定部分启动该序列。还可使用其它方法启动该序列。

可将对补丁进行解码、确认和安装操作期间要运行的数据置于安全存储器 118 中，可将其设置为用非安全代码无法进行访问。在一些实施例中，安全存储器 118

在不同时间包含编码的补丁、解码的补丁以及在对编码补丁进行解码期间所产生的中间产物。在一个实施例中，安全存储器 118 没有足够的容量来保存以上提到的补丁和/或中间产物，并且它也可同时包含编码补丁、解码补丁和中间产物中一个或多个的仅仅一部分。

在一个实施例中，安全存储器 118 是专用 RAM 存储器，它可置于处理器 110 的内部或外部，仅仅用于安全操作。在另一实施例中，安全存储器 118 是处理器 110 的专用高速缓存，并且在补丁的解码、确认和安装期间，对于所有其它操作，对该专用高速缓存的访问是阻塞的。其他实施例可使用在所述操作期间提供安全存储器 118 的其他方法。

虽然系统 100 示出了特定实施例，但还可使用其它实施例。例如，在一个实施例中，BIOS132 可包括在处理器 110 中，而另一实施例没有芯片组 130。

在一个实施例中，密钥 116 是嵌入处理器 110 中的一个或多个安全密钥（在编码和/或解码中使用的一些值）。可以以下方式将“嵌入式”密钥制造入处理器 110 中，即阻止系统 100 的软件对密钥进行改变并阻止非安全软件对密钥进行读取。在特定实施例中，嵌入式密钥无法由任何软件进行直接读取，但是一个或多个特定指令可使特定的嵌入式密钥传输到其他硬件中以用于解码序列中。

在一个实施例中，特定的嵌入式密钥是不对称密码算法的两个密钥的其中一个，而其中另一个在安全控制下保存在补丁始发系统中。在另一实施例中，特定的嵌入式密钥包括不对称密码算法的公开密钥的散列值、与相关补丁一起传送的公开密钥。其他实施例可包括其他类型的密钥作为嵌入式密钥。

在一些实施例中，微码 112 置于非易失性存储器（如只读存储器（ROM））中，并且在制造之后无法直接改变。补丁可置于补丁存储器 114 中用于系统操作，使得响应于对修改的微码部分的引用，将该访问重新定向到补丁存储器 114 以对修改的微码进行存取。在一个实施例中，补丁存储器 114 包括 RAM，并且每当系统 100 重启和/或重新引导时，将补丁安装于补丁存储器 114 的 RAM 中。在另一实施例，补丁存储器 114 包括非易失形式的存储器，如快闪存储器，并且一旦安装了，每一补丁在补丁存储器 114 中保持完整直到该补丁由后续补丁替代。

安装之前，可将编码的补丁存储于非易失性存储器（如 BIOS132）中或盘 140 上，以在每次将补丁安装于补丁存储器 114 中时对补丁进行解码和确认。在一个实

施例中，来自 BIOS 厂商的补丁可存储于 BIOS132 中并由驻留于 BIOS 的代码在初始引导过程期间进行安装。在另一实施例中，来自操作系统 (OS) 厂商的补丁可存储于盘上并以后在引导过程中由 OS 引导加载程序安装。两个实施例可组合在同一系统中。

在一个实施例中，通过通信连接（如因特网）传送补丁、通过 Comm I/F160 接收并存储该补丁用于使用。在其他实施例中，可通过其它方式传送补丁。

图 2 根据本发明的一个实施例示出了将微码补丁转换为安全传送形式的系统框图。在图 2 所示的实施例中，系统 200 包括处理器 210、芯片组 230、盘 240、主存储器 250 和通信接口 260。这些设备中每一个的基本功能类似于图 1 中的相应部分。然而，在一个实施例中，作为补丁的始发方，系统 200 是处于可保护的集中式安装，其中为整个系统 200 提供防止攻击者的保护。在示例实施例中，可由安全范围 270 提供该保护。如这里所使用的，术语“范围”是概念上的而不是物理上的，并且安全范围 270 可包括多种保护性措施，包括但不限于系统 200 的物理保护、个人对系统 200 的有限访问、防火墙或其他保护软件设备等以阻止通过通信接口 260 对系统的未授权入侵。系统 200 还可类似于图 1 所示的使用内部安全特性。在一个实施例中，使用系统 200 为单个类型的目标系统产生补丁包。在另一实施例中，使用系统 200 为多个类型的目标系统产生不同补丁包。补丁的代码可在系统 200 中产生，也可在其他地方产生，并将其传送到系统 200 以用于制备相关补丁包。待使用并存储于 200 中的信息可包括但不限于以下的一种或多种：非加密补丁 244、加密补丁 242 以及相关的密钥 246，以上所有都示出存储在盘 240 上。由于不同目标系统需要不同补丁并涉及不同密钥，盘 240 可分为不同存储区域。每个存储区域针对单独的补丁集及相关密钥。

图 3 根据本发明的一个实施例示出了可从图 2 系统传送到图 1 系统的包含各单元的补丁包。在一个实施例中，补丁包 300 包括补丁标头 310、补丁 320 以及数字签名 330。另一实施例还包括一个或多个可传送密钥 340。补丁标头 310 包含可标识以下（但不限于）的一种或多种的标识信息：想要补丁的目标系统类型、补丁类型、在哪里使用补丁、如何使用补丁以及目标系统 100 需要的任何其他相关信息。在一个实施例中，没有对补丁标头 310 进行加密，以在补丁的验证和/或解密之前便于目标系统 100 对补丁包 300 的识别和处理。补丁 320 包含用于在补丁存储器

114 中进行替换的微码，虽然补丁 320 可以处于加密形式并同时在补丁包 300 中。可使用补丁 320 的加密以保护可从补丁本身得到的商业秘密或其他机密信息。数字签名 330 包括用于确认待安装补丁的真实性，使得可检测到补丁包制备之后对补丁的改变。在一个实施例中，仅为补丁 320 产生数字签名 330。在另一实施例中，为补丁 320 和补丁标头 310 产生数字签名 330，使得可由目标系统 100 监测对任何一个的未授权的改变。在另一实施例中，还可为补丁包 300 的其他部分产生数字签名 330。

在一个实施例中，在制造时将目标系统 100 所需的所有密钥嵌入处理器 110 中。对于特定实施例，补丁包 300 不包括用于对补丁进行解码的任何密钥。在另一特定实施例中，将由系统 100 使用的一个或多个密钥传送到系统 100 作为补丁包 300 的一部分，并且在这里将这些密钥指定为可传送密钥 340（复数术语“密钥”涵盖了只有单个可传送密钥的实施例）。可传送密钥 340 可与用于目标系统 100 或始发系统 200 的其他密钥相关联。例如，在特定实施例中，可传送密钥包括不对称密码算法中公开/秘密密钥对的公开密钥，而秘密密钥保留在始发系统 200 中，并且从公开密钥获得的散列值嵌入处理器 100 中并用于确认所传送公开密钥的真实性。还可使用所嵌入的散列值确认通过其它方式提供的一个或多个密钥，例如置于盘上用于操作系统升级的密钥或置于 BIOS 中用于 BIOS 升级的密钥。其他实施例可使用其它密钥组合和加密方案。在以后描述中更详细地描述补丁包 300 的各单元。

在另一实施例中，嵌入式密钥或散列值可与一密钥证书链一起使用。在一个这样的实施例中，使用嵌入式密钥或散列值确认第二密钥，该第二密钥用于确认第三密钥，以此类推，这样就用与特定层相关联的每一密钥提供多个安全层。可将这些密钥通过一个或多个先前提到的传送方法和/或通过没有描述过的其他方法进行传送。

图 4 根据本发明的一个实施例示出了用于制备、传送和确认补丁包的整个过程的流程图。在图 4 示出的实施例中，流程图 400 由两个部分。框 410-430 示出了补丁始发过程，其中补丁始发系统制备现有的补丁以进行安全传送。框 440-495 示出了在目标系统中进行的补丁确认/安装过程。

在一个实施例中，补丁始发过程以框 410 对补丁进行加密开始。如前所述，

一些实施例可不对补丁进行加密，因为考虑补丁的内容不是秘密的而不需要保护。不管是否对补丁进行加密，都可使用框 420 和 430 的操作，从而能够在补丁安装到目标系统之前监测对补丁的窜改。在框 420，为补丁产生一数字签名。在一个实施例中，为补丁标头和补丁两者产生数字签名，从而没有一个会被窜改而被检测到。在另一实施例中，为补丁而不是为补丁标头产生数字签名。在另一实施例中，还为可传送密钥产生数字签名。在框 430，数字签名和补丁以及任何其他包括的单元组合在一起形成补丁包。如果在框 410 对补丁进行了加密，则在框 430 包括了加密的补丁。

在创建补丁包之后，可将补丁包通过任何可行的方式传送到目标系统。在框 440 以接收和存储补丁包的方式开始在目标系统中进行的补丁确认/安装过程。补丁包可存储在盘 140 上、存储在 BIOS132 中或存储在系统 100 中任何可行的存储位置。在一个实施例中，直到引导系统时才在操作条件下安装补丁，引导过程开始于框 450。在框 460，对补丁包的数字签名进行解密并在框 470 用于对补丁的确认。如之后所述，解密和确认可采用若干形式中的任何一种。如果在框 410 对补丁进行了加密，则在框 480 对其进行解密以揭示实际的补丁。在框 490，以可操作的方式将所揭示的补丁安装在处理器 110 中。在框 495，处理器 110 使用修补的微码进行操作。

图 5 根据本发明的一个实施例示出了用于制备补丁包的过程的流程图。流程图 500 示出了图 4 补丁始发过程更详细的描述。图 5 中示出的实施例包括补丁的加密以及文摘的创建以用于确认所接收的补丁是否正确。在一个实施例中，用对称加密算法（如 AES、DES 等）对补丁进行加密。如这里所使用的，文摘是通过对数据块进行操作而获得的参数，其中相同的数据块产生相同的文摘，但是数据块中的任何改变可能会产生不同的文摘。在一个实施例中，该文摘是散列文摘，即通过将散列算法应用于补丁而产生的文摘。在一个实施例中，首先创建文摘并随后对补丁进行加密，而在另一实施例中，首先对补丁进行加密随后为加密的补丁创建文摘。图 5 示出了两个实施例。在第一实施例中，在框 510 对未加密的补丁和补丁标头施加散列过程以创建文摘。在特定实施例中，散列过程使用安全散列算法（SHA-1），它是 1994 年根据联邦信息出版标准 FIPS PUB 180-1 出版的。随后在框 520，对补丁进行加密。如果没有对补丁进行加密，就可省略框 520。在第二实施例中，在框

530 首先对补丁进行加密，并在框 540 对加密的补丁和补丁标头施加散列过程以创建文摘。在任一实施例中，如果后续操作需要文摘由一定数量的比特组成，则在框 550 可对文摘进行填充（即将数据添加到其中），从而如所需增加比特数。填充可包括预定数据或随机数据。在框 560，对填充的文摘进行加密以创建数字签名。在一个例子中，使用不对称加密过程中公开/秘密密钥对的秘密密钥对填充的文摘进行加密。在特定实施例中，加密遵循使用 2048 个比特的秘密密钥的 RSA 加密过程。如所熟知的，在 RSA 加密过程中，密钥和所加密的消息都具有相同的比特数，这样如果文摘少于密钥则在框 550 就必须对文摘进行填充。在另一实施例中，文摘和密钥已经是相同尺寸了，这样就可以免除在框 550 的填充。在另一实施例中，使用密钥和消息无需相同尺寸的加密方法，在这样的情况下也可免除框 550 的填充。在框 570，将数字签名、补丁（加密的或未加密地）和补丁标头组合到补丁包中以传递到目标系统。在一个实施例中，补丁包还包括其他信息，这取决于系统的需要。

图 6 根据本发明的一个实施例示出了用于确认补丁包的过程的流程图。流程图 600 示出了图 4 补丁确认和安装过程更详细的描述。在框 610，从目标系统内获取补丁包。在一个实施例中，先前由目标系统接收补丁包并置于存储器中，随后从该存储器中获取该补丁包。在另一实施例中，在框 610 目标系统一接收到补丁包就获取补丁包，而无需中间存储。而在一个实施例中，获取由始发系统传送的整个补丁包，在另一实施例中，在获取补丁包之前去掉补丁的任何非必要单元。

在补丁包中传送密钥的一个实施例中，在框 612 为密钥计算散列值。如果所计算的散列值与处理器 110 中嵌入的相关联的散列值相匹配，则确认该密钥并可将其用于后续确认操作。如果所计算的散列值与嵌入的散列值不匹配，那么确认就失败并将控制移到框 690，这在之后进行描述。在不涉及传送密钥的实施例中，可省略框 612 和 614 的操作。

在框 620，对数字签名进行解密以获取在始发系统中创建的文摘。在一个实施例中，借助使用公开/秘密密钥对的秘密密钥的不对称加密算法产生数字签名，这样就使用相关联的公开密钥进行框 620 的解密。如果在创建期间对文摘进行了填充，那么框 620 的操作就获取该填充的文摘，并在框 630，去除填充以揭示先前在框 510 或 540 产生的文摘。如果文摘在创建期间没有进行填充，那么框 620 的操作产生非填充的文摘，框 630 就可省略。

在该点，之后的过程取决于流程图 500 中文摘是在对补丁进行加密之前还是之后创建的。在如框 510 和 520 所示的加密之前创建文摘的实施例中，就在框 640 对补丁进行解密，并且在框 650 对解密的补丁和补丁标头施加散列函数以获得所计算的文摘。在框 660 将所计算的文摘与在框 620–630 获取的实际文摘进行比较以知道两个文摘是否匹配。如果两个文摘是等同的，则确认该补丁并在框 680 安装补丁。在一个实施例中，安装补丁包括将补丁以以下方式置于处理器 110 的补丁存储器 114 中，即任何对所修补微码的所尝试的访问都将定向到补丁存储器 114 而不是初始微码 112。

回到框 630，在如框 530 和 540 创建文摘之前对补丁进行加密的实施例中，在框 645，对加密的补丁以及标头施加散列运算以获得所计算的文摘。在框 665，将所计算的文摘与在框 630 所揭示的实际文摘进行比较以了解它们是否匹配。如果发现它们是等同的，则确认该补丁并在框 670 对补丁进行解密。随后在框 680 安装确认和解密的补丁。在两个实施例中，框 645、650 所有的散列运算与框 510、540 所使用的是相同的。

如果在框 660 或 665 所计算的文摘与实际文摘是不匹配的，这就表示自从补丁包产生以来它已经改变了或者它不适合安装。这样的改变/不适合性可能由几个原因，包括但不限于：未授权的人故意试图改变补丁、在传送期间未监测到的/未纠正的传输错误、将补丁包传送到不正确的目标系统、软件或硬件失效或人为错误。不管是什么原因，如果实际文摘与所计算的文摘不匹配，就在框 690 终止补丁安装过程，不安装没有确认的补丁。终止补丁安装可采取若干形式，包括但不限于：1) 试图重新安装补丁、2) 跳过有故障的补丁而安装其他补丁、3) 回复到先前版本的补丁、4) 关闭系统、5) 重新引导系统，等等。

在一个实施例中，对安全存储器 118 中的整个补丁进行框 610–670 的确认过程，并在确认之后，在框 680 在补丁存储器 114 安装整个补丁。在另一实施例中，其中安全存储器 118 没有足够的容量进行整个确认过程，递增地对补丁的各个部分进行框 610–670 的确认过程。如果在这个方式中有任何一部分没有经过确认，就如先前所述在框 690 终止该过程。如果在该方式下确认了所有部分，就可以第二次递增地对补丁进行确认，而每各部分经过确认后就安装在补丁存储器 114 中。如果在第二轮确认中补丁有任何一部分没有通过确认(这表示在第一次确认之后补丁受到窜

改），就在框 690 终止该过程。如果在框 690 终止之前已部分安装了补丁，那么框 690 的终止过程除了一个或多个先前所述过程之外还包括将新安装的补丁从补丁存储器 114 中去除。

以上描述旨在都是示例性的而非限制性的。对于本领域的技术人员可对这些描述进行改变。希望这些改变包括在本发明的各个实施例中，这仅仅由所附权利要求书的主旨和范围所限制。

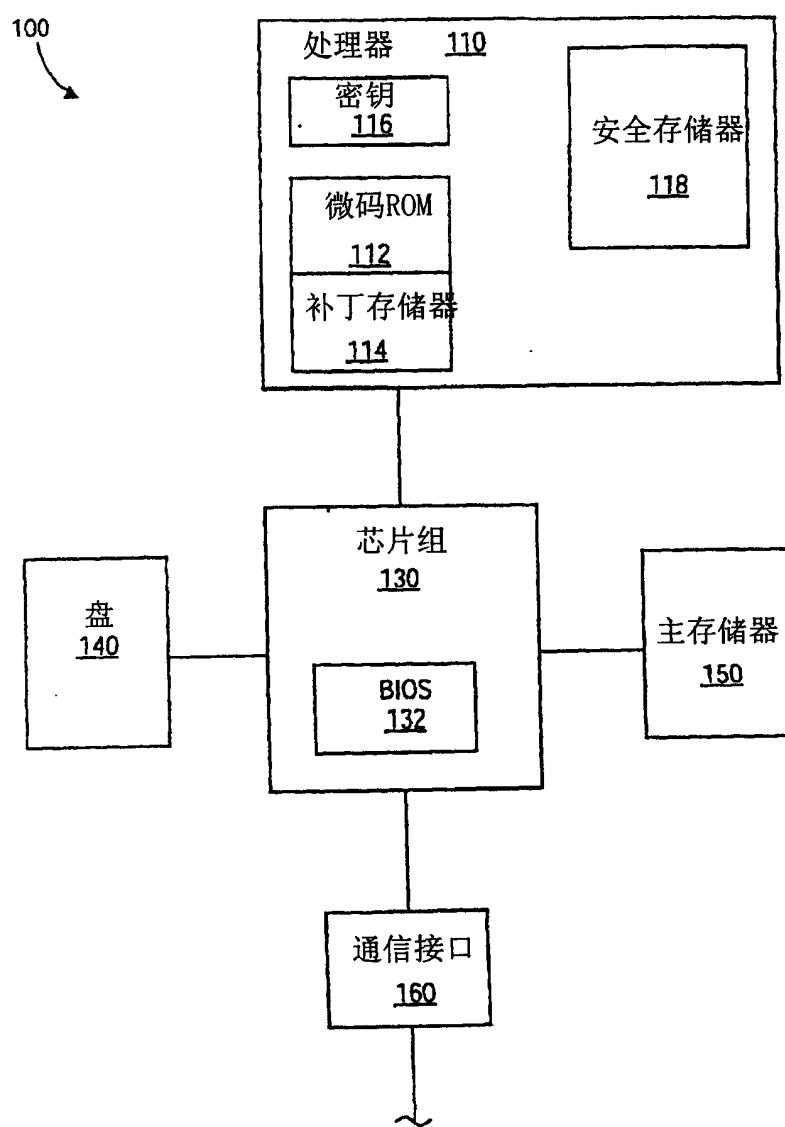


图 1

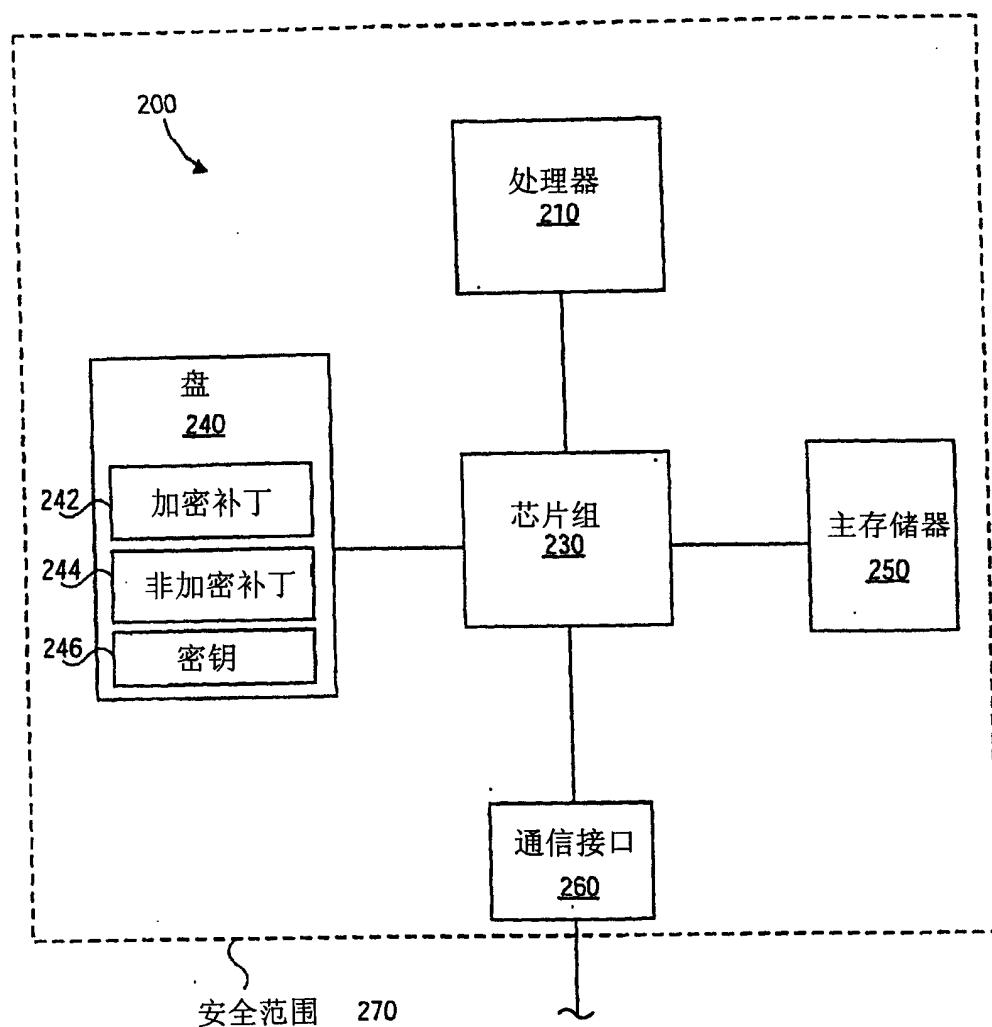


图 2

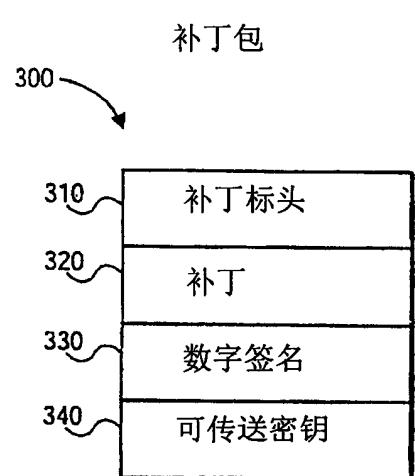


图 3

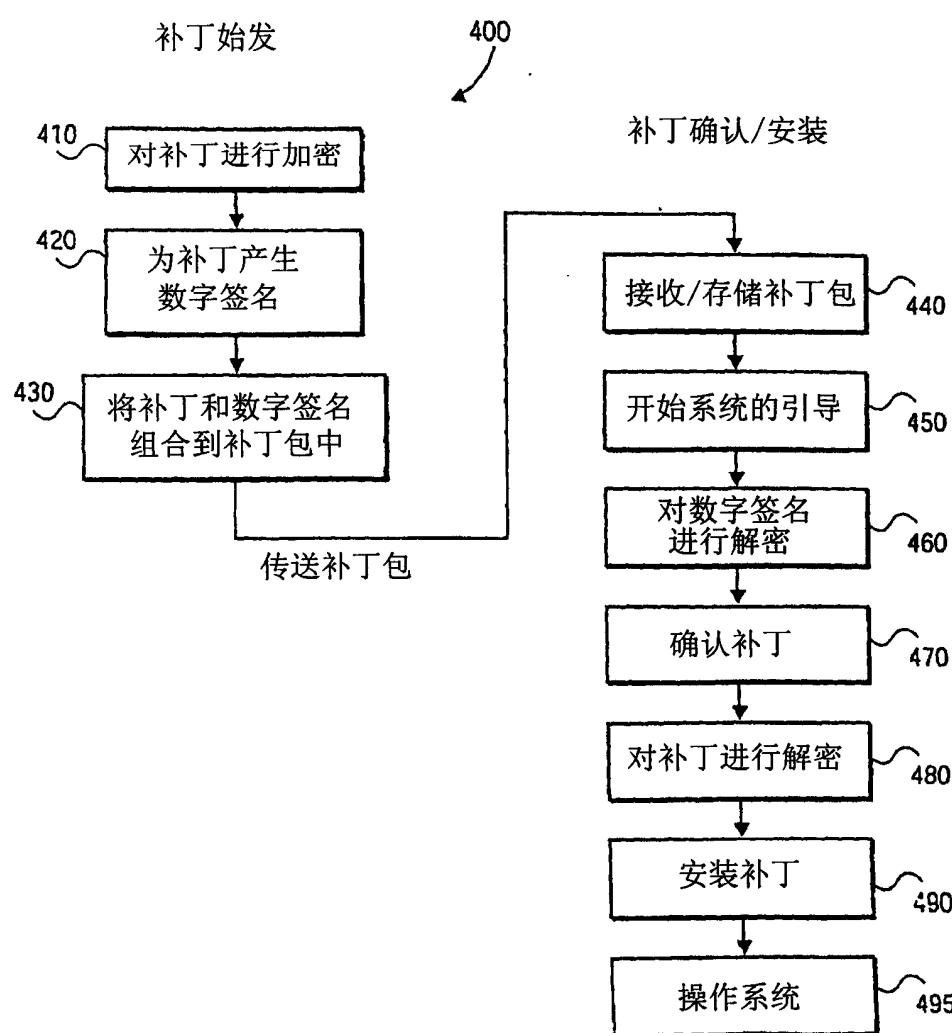


图 4

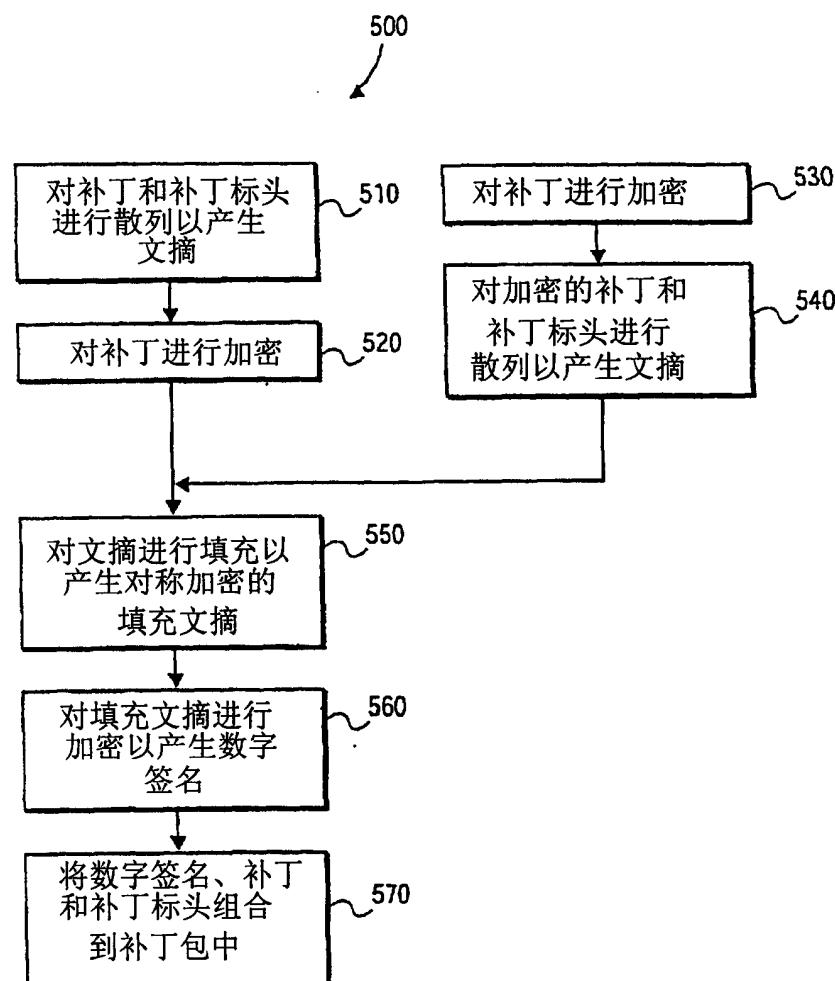


图 5

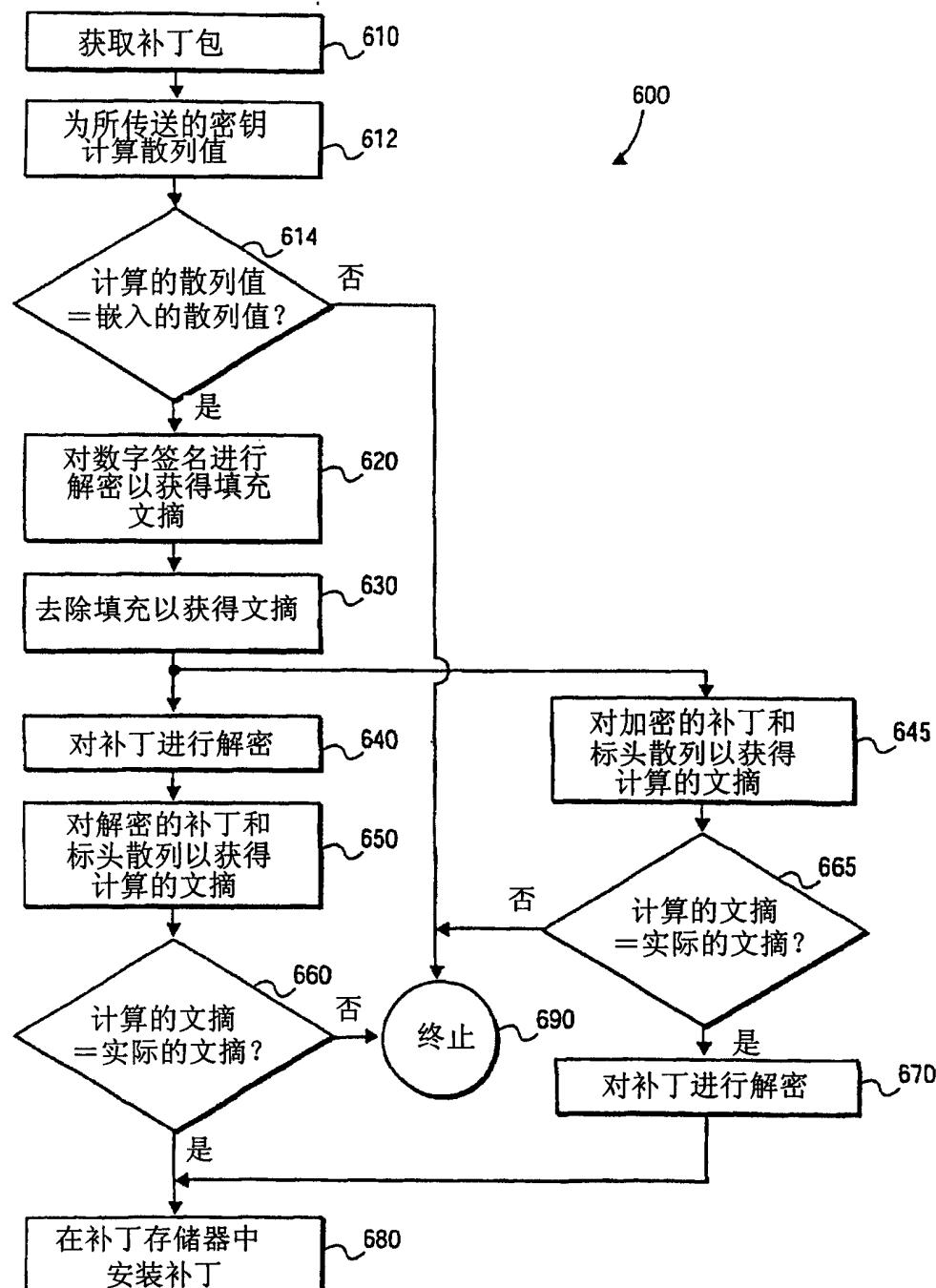


图 6