

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200780051188.0

[51] Int. Cl.
G06F 21/00 (2006.01)
H04L 9/00 (2006.01)

[43] 公开日 2010 年 1 月 13 日

[11] 公开号 CN 101627390A

[22] 申请日 2007.12.4

[21] 申请号 200780051188.0

[30] 优先权

[32] 2006.12.14 [33] US [31] 11/638,405

[86] 国际申请 PCT/FI2007/050658 2007.12.4

[87] 国际公布 WO2008/071836 英 2008.6.19

[85] 进入国家阶段日期 2009.8.11

[71] 申请人 诺基亚公司

地址 芬兰埃斯波

[72] 发明人 J-E·埃克贝里 L·帕特洛

[74] 专利代理机构 北京市中咨律师事务所

代理人 杨晓光 杨博

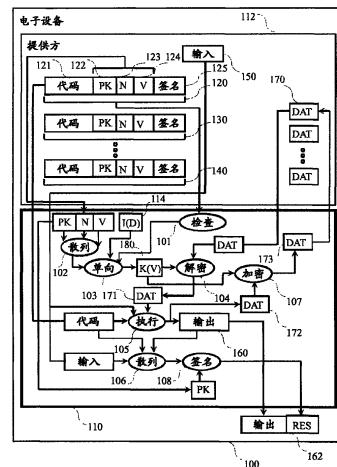
权利要求书 4 页 说明书 11 页 附图 5 页

[54] 发明名称

用于程序状态数据在电子设备中的安全存储
的方法

[57] 摘要

本发明涉及一种方法，在所述方法中，程序信息被获取到电子设备(100)中的执行环境(110)。所述程序信息至少包括程序代码(121)。所述程序信息和特定于设备的秘密值(114)的密钥被计算。所述密钥被用于在所述执行环境(110)中解密特定于程序的状态数据(170)，以及在所述执行后加密已修改状态数据。



1. 一种方法，包括：

将程序信息获取到包含在电子设备中的执行环境，所述程序信息至少包括程序代码；

计算特定于所述电子设备的秘密值和所述程序信息的至少一部分的机密性密钥；以及

用所述机密性密钥作为密钥对第一数据部分应用密码操作，所述第一数据部分包括到所述程序代码的第一输入数据部分或来自所述程序代码的第一输出数据部分，所述密码操作包括解密和加密中的至少一个。

2. 根据权利要求 1 所述的方法，所述方法进一步包括：

在所述执行环境中用第二输入数据部分和所述第一输入数据部分执行所述程序代码以产生第二输出数据部分；

计算所述第二输入数据部分、所述第二输出数据部分和所述程序信息的第二散列；以及

用第二私钥加密所述第二散列以产生结果签名，所述第二私钥关联于所述执行环境。

3. 根据权利要求 1 或 2 所述的方法，所述方法进一步包括：

将所述程序信息获取到网络节点；

在所述网络节点中产生第二输入数据部分；

将所述程序信息和所述第二输入数据部分提供给所述电子设备；

将来自所述电子设备的第二输出数据部分获取到所述网络节点；以及

在所述网络节点中验证所述结果签名，以确定包括在所述程序信息中的程序代码已在所述电子设备中被执行。

4. 根据权利要求 3 所述的方法，所述方法进一步包括：

所述网络节点从所述第二输出数据部分提取控制信息；

所述网络节点用所述控制信息控制设备。

5. 根据前述权利要求 1 - 4 中任一个所述的方法，所述方法进一步包

括：

在所述程序信息中提供对于所述执行环境的程序代码、第一公钥、程序名称、版本号和签名；

用关联于第一私钥的所述第一公钥检查所述签名；

至少由所述第一公钥、所述程序名称和所述版本号计算第一散列；

将所述第一输入信息部分提供给所述执行环境以用于所述程序代码的执行；

使用单向函数从所述第一散列和特定于所述电子设备的所述秘密值计算机密性密钥；

用所述机密性密钥解密所述第一输入信息部分；

在所述执行环境中修改所述第一信息部分；以及

使用所述机密性密钥加密所述第一输出信息部分。

6. 根据权利要求 5 所述的方法，所述方法进一步包括：

获取所述程序代码；

为所述程序代码提供所述第二公钥、所述程序名称和所述版本号以产生第二数据对象；以及

用所述第一公钥签名所述第二数据对象以获得所述签名。

7. 根据权利要求 5 所述的方法，其中，所述第一输入数据部分包括关联于所述程序代码的状态信息。

8. 根据前述权利要求 1-7 中任一个所述的方法，其中，所述机密性密钥是对称密钥。

9. 根据前述权利要求 1-8 中任一个所述的方法，其中，所述执行环境是移动节点中的安全环境。

10. 一种电子设备，包括：

执行环境，其被配置为：获取程序信息，所述程序信息至少包括程序代码；计算特定于所述电子设备的秘密值和所述程序信息的至少一部分的机密性密钥；以及，用所述机密性密钥作为密钥对第一数据部分应用密码操作，所述密码操作包括到所述程序代码的第一输入数据部分或来自所述

程序代码的第一输出数据部分，所述密码操作包括解密和加密中的至少一个。

11. 根据权利要求 10 所述的电子设备，所述电子设备进一步包括：

所述执行环境被配置为：在所述执行环境中用第二输入数据部分和所述第一输入数据部分执行所述程序代码以产生第二输出数据部分；计算所述第二输入数据部分、所述第二输出数据部分和所述程序信息的第二散列；以及，用第二私钥加密所述第二散列以产生结果签名，所述第二私钥关联于所述执行环境。

12. 根据权利要求 10 或 11 所述的电子设备，所述电子设备进一步包括：

提供方实体，其被配置为，在所述程序信息中提供对于所述执行环境的程序代码、第一公钥、程序名称、版本号和签名；将所述第一输入信息部分提供给所述执行环境以用于所述程序代码的执行；

所述执行环境被配置为：用关联于第一私钥的第一公钥检查所述签名；至少由所述第一公钥、所述程序名称和所述版本号计算第一散列；使用单向函数从所述第一散列和特定于所述电子设备的所述秘密值计算机密性密钥；使用所述机密性密钥解密所述第一输入信息部分；在所述执行环境中修改所述第一信息部分；以及，使用所述机密性密钥加密所述第一输出信息部分。

13. 根据权利要求 12 所述的电子设备，所述电子设备进一步包括：

所述提供方实体，其被配置为：获取所述程序代码；为所述程序代码提供所述第二公钥、所述程序名称和所述版本号以产生第二数据对象；以及，用所述第一公钥签名所述第二数据对象以获得所述第一数据对象。

14. 根据前述权利要求 10 - 13 中任一个所述的电子设备，其中，所述第一输入数据部分包括关联于所述程序代码的状态信息。

15. 根据前述权利要求 10 - 14 中任一个所述的电子设备，其中，所述机密性密钥是对称密钥。

16. 根据前述权利要求 10 - 15 中任一个所述的电子设备，其中，所述

执行环境是移动节点中的安全环境。

17. 一种电子设备，包括：

用于获取程序信息的装置，所述程序信息至少包括程序代码；

用于计算特定于所述电子设备的秘密值和所述程序信息的至少一部分的机密性密钥的装置；

用于以所述机密性密钥作为密钥对第一数据部分应用密码操作的装置，所述第一数据部分包括到所述程序代码的第一输入数据部分或来自所述程序代码的第一输出数据部分，所述密码操作包括解密和加密中的至少一个。

18. 一种包含在计算机可读介质中的计算机程序，所述计算机程序包括用于控制处理器执行包括以下的方法的代码：

获取程序信息，所述程序信息至少包括程序代码；

计算特定于所述电子设备的秘密值和所述程序信息的至少一部分的机密性密钥；

以所述机密性密钥作为密钥对第一数据部分应用密码操作，所述第一数据部分包括到所述程序代码的第一输入数据部分或来自所述程序代码的第一输出数据部分，所述密码操作包括解密和加密中的至少一个。

19. 根据权利要求 18 所述的计算机程序，其中，所述计算机可读介质是可移除存储卡。

20. 根据权利要求 18 所述的计算机程序，其中，所述计算机可读介质是磁或光盘或全息存储器。

用于程序状态数据在电子设备中的安全存储的方法

技术领域

本发明涉及电子设备安全。特别地，本发明涉及一种用于程序状态数据在电子设备中的安全存储的方法。

背景技术

在其中所有计算机程序和应用都是操作的潜在目标的世界中，对用户来说有必要能够确信无疑他们正在使用的程序保持与最初被安装或下载时一样。存在这样的风险：程序被用具有类似观感但收集并泄漏信息（例如向互联网）的程序代替。软件和数字媒体厂商还认识到未授权分发和产品篡改中涉及的风险。所述风险在计算机程序被用于控制现实资源的情况下尤为突出。

越来越多移动设备和计算设备被配备了可信任环境，即安全的程序执行环境。所述可信任环境被用于运行应用，该应用处理设备专用或输入的秘密（secret）。所述可信任环境中的数据可以被用于实现数字版权管理和复制保护。

然而，现有可信任环境中的问题是，程序和数据与可信任环境的所有者协作地被存储、更新和读取。所述所有者可以是设备制造商、业务提供商（xSP）或网络运营商。添加的任何新特征和程序需要来自可信任环境的所有者的验证。能够拥有这样的解决方案将是有益的，所述解决方案使第三方能够利用可信任环境来为过剩的可信任第三方程序提供基础。

发明内容

本发明涉及一种方法，包括：将程序信息获取到包括在电子设备中的

执行环境，所述程序信息至少包括程序代码；计算特定于所述电子设备的秘密值和所述程序信息的至少一部分的机密性密钥；以及，以所述机密性密钥作为密钥对第一数据部分应用密码操作，所述第一数据部分包括到所述程序代码的第一输入数据部分或来自所述程序代码的第一输出数据部分，所述密码操作包括解密和加密中的至少一个。

本发明还涉及一种电子设备，所述电子设备包括执行环境，所述执行环境被配置为：获取程序信息，所述程序信息至少包括程序代码；计算特定于所述电子设备的秘密值和所述程序信息的至少一部分的机密性密钥；以及，以所述机密性密钥作为密钥对第一数据部分应用密码操作，所述第一数据部分包括到所述程序代码的第一输入数据部分或来自所述程序代码的第一输出数据部分，所述密码操作包括解密和加密中的至少一个。

本发明还涉及一种电子设备，所述电子设备包括：用于获取程序信息的装置，所述程序信息至少包括程序代码；用于计算特定于所述电子设备的秘密值和所述程序信息的至少一部分的机密性密钥的装置；用于以所述机密性密钥作为密钥对第一数据部分应用密码操作的装置，其中，所述第一数据部分包括到所述程序代码的第一输入数据部分或来自所述程序代码的第一输出数据部分，所述密码操作包括解密和加密中的至少一个。

本发明还涉及一种计算机程序，所述计算机程序包括当在数据处理系统上执行时适于实施以下步骤的代码：获取程序信息，所述程序信息至少包括程序代码；计算特定于所述电子设备的秘密值和所述程序信息的至少一部分的机密性密钥；以所述机密性密钥作为密钥对第一数据部分应用密码操作，所述第一数据部分包括到所述程序代码的第一输入数据部分或来自所述程序代码的第一输出数据部分，所述密码操作包括解密和加密中的至少一个。

在本发明的一个实施例中，从特定于所述电子设备的主秘密值(master secret value)获得特定于所述电子设备的所述秘密值。通过在所述执行环境中多样化所述主秘密值来获得用于在所述机密性密钥的计算中使用的秘密值。例如，可以通过计算所述程序信息(例如所述程序代码)的散列以

及将所述散列连接到所述主秘密值来实施所述多样化。因此，所述执行环境以所述连接的散列和主秘密值作为自变量（argument）来计算单向函数（one-way function）并获得已多样化的秘密值，即，特定于所述电子设备的秘密值。

在本发明的一个实施例中，所述电子设备中的执行环境被配置为，在所述执行环境中以第二输入数据部分和所述第一输入数据部分执行所述程序代码以产生第二输出数据部分。所述执行环境计算所述第二输入数据部分、所述第二输出数据部分和所述程序信息的第二散列。因此，所述执行环境用第二私钥来加密所述第二散列以产生结果签名，其中，所述第二私钥关联于所述执行环境。

在本发明的一个实施例中，所述程序信息被获取到被配置为与所述电子设备通信的网络节点。所述网络节点产生第二输入数据部分。所述网络节点将所述程序信息和所述第二输入数据部分提供到所述电子设备。所述网络节点从所述电子设备获取第二输出数据部分，并且验证结果签名以确定包括在所述程序信息中的程序代码已经在所述电子设备中被执行。

在本发明的一个实施例中，所述网络节点从所述第二输出数据部分提取控制信息，并且用所述控制信息控制设备。所述设备可以连接到所述网络节点。所述设备例如可以是安全设备，例如锁系统或报警系统。

在本发明的一个实施例中，所述电子设备中的提供方实体在所述程序信息中提供对于所述执行环境的程序代码、第一公钥、程序名称、版本号和签名。所述执行环境用关联于第一私钥的所述第一公钥检查所述签名。所述执行环境至少从所述第一公钥、所述程序名称和所述版本号计算第一散列。所述提供方实体将所述第一输入信息部分提供给所述执行环境以用于所述程序代码的执行。所述执行环境使用单向函数从特定于所述电子设备的所述秘密值和所述第一散列计算机密性密钥。所述执行环境用所述机密性密钥解密所述第一输入信息部分，并且修改所述第一信息部分。最后，所述执行环境用所述机密性密钥加密所述第一输出信息部分。

在本发明的一个实施例中，所述提供方实体被配置为：获取所述程序

代码；向所述程序代码提供所述第一公钥、所述程序名称和所述版本号以产生第二数据对象；以及用所述第一公钥签名所述第二数据对象以获取所述签名。这些任务还可以在与所述电子设备通信的网络节点中提供。

在本发明的一个实施例中，所述第一输入数据部分包括关联于所述程序代码的状态信息。

在本发明的一个实施例中，所述机密性密钥是对称密钥。在本发明的一个实施例中，所述机密性密钥是私钥和公钥对，并且用所述私钥进行加密以及用所述公钥来进行解密，或反之亦然。

在本发明的一个实施例中，所述执行环境是移动节点中的安全环境。

在本发明的一个实施例中，所述执行环境是安全环境，例如移动节点。

在本发明的一个实施例中，所述移动节点是移动通信系统中的移动台。

在本发明的一个实施例中，所述移动节点包括移动台或一般而言的移动终端。在本发明的一个实施例中，所述移动通信系统包括全球移动通信系统（GSM）网络和通用移动电话系统（UMTS）网络中的至少一个。在本发明的一个实施例中，所述系统包括无线局域网（WLAN）。在本发明的一个实施例中，所述系统还包括微波接入全球互通（WiMAX）网络。在本发明的一个实施例中，所述移动节点例如可以是具有用于支持不同接入类型的双模或多模功能的 UMTS 移动台或 GSM 移动台。

在本发明的一个实施例中，所述计算机程序被存储在计算机可读介质中。所述计算机可读介质可以是可移除存储卡、磁盘、全息存储器、光盘或磁带。

在本发明的一个实施例中，程序信息被获取到所述电子设备中的执行环境。所述程序信息至少包括程序代码。所述程序信息和设备特定的秘密值的密钥被计算。所述密钥被用于在所述执行环境中解密程序特定的状态数据以用于所述程序代码执行。所述密钥在执行之后被用于加密已修改状态数据。

以上描述的本发明的实施例可以相互任意组合地被使用。所述实施例中的几个可以被合并到一起以构成本发明的进一步实施例。本发明所涉及

的一种方法、系统、电子设备或计算机程序可以包括以上描述的本发明的实施例中的至少一个。

本发明的好处涉及对于被提供给执行环境的程序代码的改进的安全性和安全应用的软件开发中改进的灵活性。

附图说明

为提供对本发明的进一步理解而被包括并且构成本说明书的一部分的附图示例性示出了本发明的实施例，并且与说明书一起有助于阐明本发明的原理。在附图中：

图 1 是示例性示出包括本发明的一个实施例中的安全执行环境的电子设备的框图；

图 2 是示例性示出包括本发明的一个实施例中的由程序代码计算散列的安全执行环境的电子设备的框图；

图 3 是示例性示出本发明的一个实施例中的对远程设备的安全控制的框图；

图 4 是示例性示出本发明的一个实施例中的用于安全程序执行的方法的流程图；以及

图 5 是示例性示出本发明的一个实施例中的电子设备的框图。

具体实施方式

现在将详细参考本发明的实施例，其中，所述实施例的示例在附图中被示例性示出。

图 1 是示例性示出包括本发明的一个实施例中的安全执行环境的电子设备的框图。在图 1 中存在电子设备 100。电子设备 100 包括安全执行环境 110 和提供方实体 112。在本发明的一个实施例中，提供方实体 112 与电子设备 100 分离，并且在远程节点（未示出）中执行。在提供方实体 112 中存储了至少一个程序记录，例如程序记录 120、130 和 140。程序记录 120 包括计算机程序代码 121、公钥 122（PK）、程序名称 123（N）、程序版

本 124 (V) 和该程序的数字签名 125。程序记录可以较长期地存储在电子设备 100 中，或者可以仅在该程序记录即将在安全执行环境中被执行之前的时刻被接收到网络 100。在提供方实体 112 中还存在输入数据 150 和程序记录状态 170 (DAT)。提供方实体 112 可以为至少一个程序记录存储程序状态。

图 1 中的起始点是提供方实体 112 提供程序记录 120 以用于在安全执行环境 110 中的执行。提供方实体 112 向程序代码 121 附加公钥 122、该程序的名称和该程序的版本号 124 以产生已附加的程序代码。因此，提供方实体 112 使用对应于公钥 122 的第一私钥对所述已附加的程序代码进行数字签名，并且进一步将由此产生的签名附加到所述已附加的程序代码以产生程序记录 120。已附加程序代码的数字签名例如包括对已附加程序代码的消息摘要的计算以及使用私钥对所述消息摘要进行加密以得到签名。提供方实体向安全执行环境 110 提供程序记录 120、程序代码 121 的输入数据 150 和程序记录状态 170 以用于程序代码 121 的执行。提供方实体 112 还或者作为程序记录 120 的一部分或者作为单独的数据向安全执行环境 110 提供公钥 122、程序名称 123 和版本号 124。在本发明的一个实施例中，提供方实体 112 位于不同于电子设备 100 的网络节点中。

在安全执行环境 110 中，检查功能块 101 例如通过解密签名 125 并将已解密签名与使用安全执行环境 110 中的已附加程序代码重复计算出的消息摘要匹配，来验证程序记录 120 中的签名 125 是否是实际上使用对应于公钥 122 的私钥产生的。基于检查功能块 101 的成功，安全执行环境 110 由公钥 122、程序名称 123 和版本号 124 计算散列函数 102。散列函数 102 的结果被作为输入与电子设备 100 的唯一设备秘密 114 一起提供给单向功能块 103。单向功能块 103 产生特定于程序记录的密钥 180。密钥 180 可以是对称密钥。密钥 180 被用于在解密功能块 104 中解密程序记录状态 170 以产生已解密程序记录状态 171。基于解密功能块 104 的完成，执行功能块 105 可以使用输入数据 150 和已解密程序记录状态 171 来执行程序代码 121。已解密程序记录状态 171 包括在程序代码 121 的不同执行之间传送的

信息。在程序代码 121 在执行功能块 105 中的执行期间，来自程序代码 121 的输出被收集作为输出 160，并且被更改的程序记录状态被认为是已修改的程序记录状态 172。在执行功能块 105 完成之后，输入 150、程序代码 121 和输出 160 在散列功能块 106 中被散列以产生第二散列结果。该第二散列结果在签名功能块 108 中被使用第二私钥 116 加密以产生结果签名 162 (RES)。私钥 116 可以与可信任公钥相关。可以通过任何方式来形成信任关系，例如经由来自第三方的证书或经由设备的物理所有权。结果签名 162 提供这样的证明：即，输出 160 是使用拥有第二私钥 116 的安全执行环境中程序代码 121 中的输入 150 产生的。可以使用关联于第二私钥 116 的公钥来验证结果签名。第二私钥 116 可以关联于安全环境 110 和电子设备 100 或者安全环境 110 的所有者。已修改程序记录状态 172 被提供给加密功能块 107，该加密功能块 107 使用密钥 180 来加密已修改程序记录状态 172 以产生新的已加密程序记录状态 173。新的已加密程序记录状态 173 被提供给提供方实体 112 以便于直到程序记录 120 被重复提供用于执行之前的存储。

图 2 是示例性示出电子设备的框图，其包括本发明的一个实施例中的从程序代码计算散列的安全执行环境。在图 2 中存在电子设备 200。电子设备 200 包括安全执行环境 210 和提供方实体 212。在本发明的一个实施例中，提供方实体 212 与电子设备 200 分离，并且在远程节点（未示出）中执行。在提供方实体 212 中存储了至少一个程序记录，例如程序记录 220、230 和 240。程序记录 220 至少包括计算机程序代码 221。在提供方实体 212 中还存在输入数据 250 和程序记录状态 270。提供方实体 212 可以为至少一个程序记录存储程序状态。

图 2 中的起始点是提供方实体 212，其提供程序记录 220 以用于在安全执行环境 210 中的执行。提供方实体向安全执行环境 210 提供程序记录 220、程序代码 221 的输入数据 250 和程序记录状态 270 以用于程序代码 221 的执行。在本发明的一个实施例中，提供方实体 212 位于不同于电子设备 200 的网络节点中。

安全执行环境 210 从程序代码 221 的至少一部分计算散列函数 201。散列函数 201 的结果被作为输入与电子设备 200 的唯一设备秘密 214 一起提供给单向功能块 202。单向功能块 202 产生特定于程序记录的密钥 280。密钥 280 可以是对称密钥。密钥 280 被用于在解密功能块 203 中解密程序记录状态 270 以产生已解密程序记录状态 271。基于解密功能块 203 的完成，执行功能块 204 可以使用输入数据 250 和已解密程序记录状态 271 来执行程序代码 221。已解密程序记录状态 271 包括在程序代码 221 的不同执行之间传送的信息。在程序代码 221 在执行功能块 204 中的执行期间，来自程序代码 221 的输出被收集作为输出 260，以及被更改的程序记录状态被认为是已修改程序记录状态 272。在执行功能块 204 完成之后，输入 250、程序代码 221 和输出 260 在散列功能块 205 中被散列，以产生第二散列结果。该第二散列结果在签名功能块 207 中被使用可与公钥证书相关的第二私钥 216 加密以产生结果签名 262。结果签名 262 提供这样的证明：即，输出 260 是使用拥有第二私钥 216 的安全执行环境中程序代码 221 中的输入 250 产生的。可以使用关联于第二私钥 216 的公钥来验证结果签名。第二私钥 216 可以关联于安全执行环境 210 和电子设备 200 或者安全执行环境 210 的所有者。已修改程序记录状态 272 被提供给加密功能块 206，该加密功能块 206 使用密钥 280 来加密已修改程序记录状态 272 以产生新的已加密程序记录状态 273。新的已加密程序记录状态 273 被提供给提供方实体 212 以便于直到程序记录 220 被重复提供用于执行之前的存储。

图 3 是示例性示出本发明的一个实施例中的远程设备的安全控制的框图。在图 3 中存在包括移动节点 360、移动网络 370 (MN) 和互联网 380 的通信系统 350。移动节点 360 的内部功能块用框 362 示例性示出。移动节点 360 包括通信实体 363、安全执行环境 364 和提供方实体 365。图 3 中的起始点是移动节点 360 想要向远程客户端 382 发出控制请求。远程客户端 382 例如控制对现实资源提供接入的设备。现实资源例如可以是住宅或车辆。如用箭头 301 所示，移动节点 360 向远程客户端 382 发送初始消息。该初始消息例如包括现时 (nonce) 即非重复的随机字符串、关联于移

动节点 360 的公共用户身份和用于该设备的指令。基于接收到该初始消息，如用箭头 302 所示，远程客户端 382 向移动节点 360 发送认证请求。该认证请求包括质疑，其中，所述质疑进一步包括至少所述现时。所述质疑被移动节点 360 和提供方实体 365 接收。提供方实体 365 基于例如发送者和消息 302 的类型选择程序记录。提供方实体 365 将所选择的程序记录和质疑提供给安全执行环境 364 进行处理。如关联于图 1 所阐明的，来自安全执行环境 364 的结果包括输入、输出和结果签名。如用箭头 303 所示，所述输出和签名被从移动节点 360 提供给远程客户端 382。基于使用关联于第二私钥的公钥验证该签名，远程客户端 382 根据在初始消息中获得的指令控制设备。

图 4 是示例性示出用于本发明的一个实施例中的安全程序执行的方法的流程图。

在步骤 400，程序代码被获取到包括在电子设备中的提供方实体。所述电子设备可以还包括安全执行环境。所述程序代码可以例如是机器代码、字节代码、中间语言、虚拟机器代码、源代码、其任意组合或可以在安全执行环境中被处理的任意程序代码。

在步骤 402，所述程序代码在提供方实体中被提供了第一公钥、程序名称和版本号。程序的名称、版本号和第一公钥可以被添加到所述程序代码的头部。程序名称、版本号和第一公钥还可以被附加到所述程序代码，或者被放置到不阻碍该程序代码的执行的程序代码部分。在本发明的一个实施例中，仅程序代码被提供给执行环境。

在步骤 404，在提供方实体中用关联于第一公钥的第一私钥对已提供 (furnished) 程序代码进行签名。已提供程序代码的数字签名例如包括：已提供程序代码的消息摘要的计算，以及使用私钥对所述消息摘要进行加密以产生签名。所述签名也被提供给程序代码。产生的最终已提供程序代码被称为程序记录。

在步骤 406，程序记录与已加密程序记录状态和输入数据一起被从提供方实体提供给安全执行环境。该提供可包括程序记录向包括安全执行环

境的第二网络节点的发送，如果提供方实体和安全执行环境在不同节点中。程序记录和关联的输入数据和已加密程序记录状态可以被提供一个过程、功能块或方法调用或以若干部分来提供。输入数据部分可以被作为一个或几个自变量提供给任意数量的过程、部分、功能、模块、方法或等价计算机程序代码调用。

在步骤 408，安全执行环境检查签名是否可以，即，其使用关联于第一私钥的公钥来验证签名。如果签名不行，则方法在步骤 422 继续。签名验证不是强制的。

在步骤 410，安全执行环境从第一公钥、程序名称和可选地版本号的至少一部分计算散列值 H1。

在本发明的一个实施例中，仅从程序代码来计算散列值 H1。

在步骤 412，在安全执行环境中使用散列值 H1 和唯一设备秘密，以便在单向函数中计算密钥 K(V)。密钥 K(V)是特定于所处理的程序记录的密钥。密钥 K(V)可以是对称密钥或者公钥和私钥对。

在步骤 414，在安全执行环境中使用密钥 K(V)，以便解密从提供方实体获取的程序记录状态。程序记录状态在安全执行环境之外被以已加密格式维护以防止数据的篡改。

在步骤 416，来自程序记录的程序代码被在安全执行环境中执行，从而输入数据和程序记录状态被提供为对所述执行的输入。程序记录状态包括在程序代码的后续执行之间传送的信息。程序代码在安全执行环境中的执行提供输出数据。

在步骤 418，在程序代码的执行期间被修改的程序记录状态被在安全执行环境中用密钥 K(V)加密。已加密程序记录状态被向回提供给提供方实体进行存储。

在步骤 420，通过签名散列 H2 来在安全执行环境中计算结果签名，其中，通过用第二私钥对输入数据、输出数据和程序代码进行散列来获得散列 H2。结果签名与输出数据一起被从安全执行环境提供给提供方实体。

在步骤 422，安全执行环境向提供方实体发出错误。

在本发明的一个实施例中，安全执行环境负责程序记录状态的存储。

在本发明的一个实施例中，没有存储程序记录状态。

图 5 是示例性示出本发明的一个实施例中的电子设备的框图。

在图 5 中示出了电子设备 500。电子设备 500 包括处理器 510、辅存储器 520、主存储器 530、显示器 550 和用户接口 560。用户接口可以是例如键区（keypad）、键盘或控制杆或控制台。电子设备 500 还可以包括任意数量的其它处理器和任意数量的辅存储器单元。还可以存在具有单独地址空间的其它主存储器。电子设备 500 还包括网络接口 540。处理器 510 执行至少部分地存储在主存储器 530 中的多个软件实体。主存储器 530 包括通信实体 532、提供方实体 534 和安全执行环境 536。实体 534 和 536 可以在功能上类似于图 1 中的实体 110 和 112 以及图 2 中的实体 210 和 212。在本发明的一个实施例中，控制实体 535、536 和 537 的一部分被包括在电子设备 500 的操作系统中。

在图 5 中，电子设备 500 中的实体可以用多种方式来实现。其可以作为在电子设备的自带操作系统下被执行的进程来实现。所述实体可以作为单独的进程或线程来实现，或使得许多不同实体借助于一个进程或线程来实现。进程或线程可以是包括许多例程的程序块的实例，其中，所述例程即例如过程和函数。所述实体可以作为单独的计算机程序或作为包括实现所述实体的几个例程或函数的单一计算机程序来实现。所述程序块被存储在至少一个计算机可读介质中，例如存储器电路、存储卡、全息存储器、磁或光盘。一些实体可以作为链接到另一实体的程序模块来实现。图 5 中的实体还可以被存储在单独的存储器中，并且被单独的处理器执行，其中，所述单独的处理器例如经由电子设备中的消息总线或内部网络通信。这种消息总线的示例是外围部件互连（PCI）总线。所述内部网络可以是例如局域网。所述实体还可以部分上或整体上实现为硬件，例如 ASIC 或 FPGA。

对于本领域的技术人员显而易见，随着技术的进步，本发明的基本概念可以用各种方法来实现。本发明及其实施例由此不限于以上描述的示例；相反，其可以在权利要求的范围内改变。

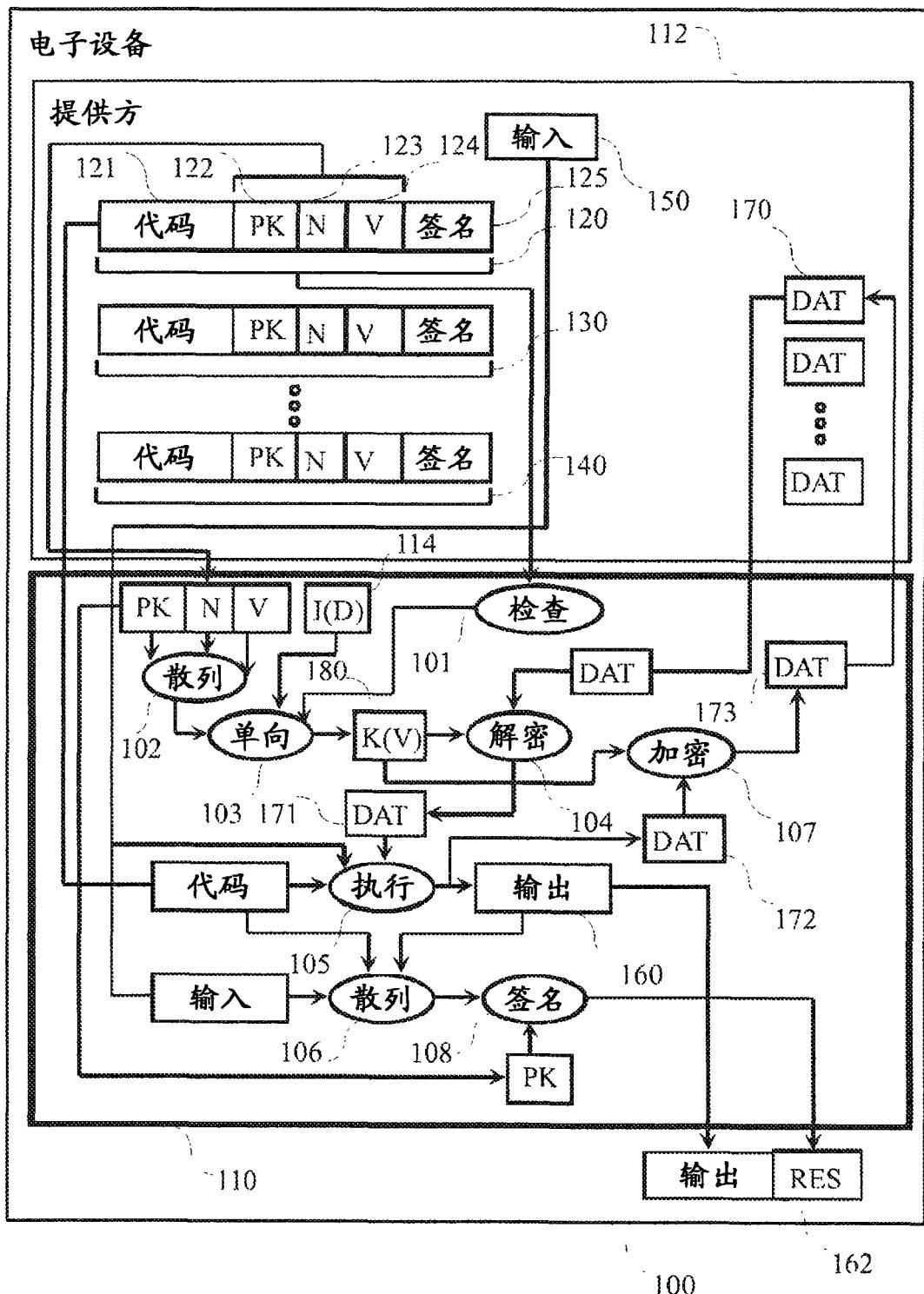


图 1

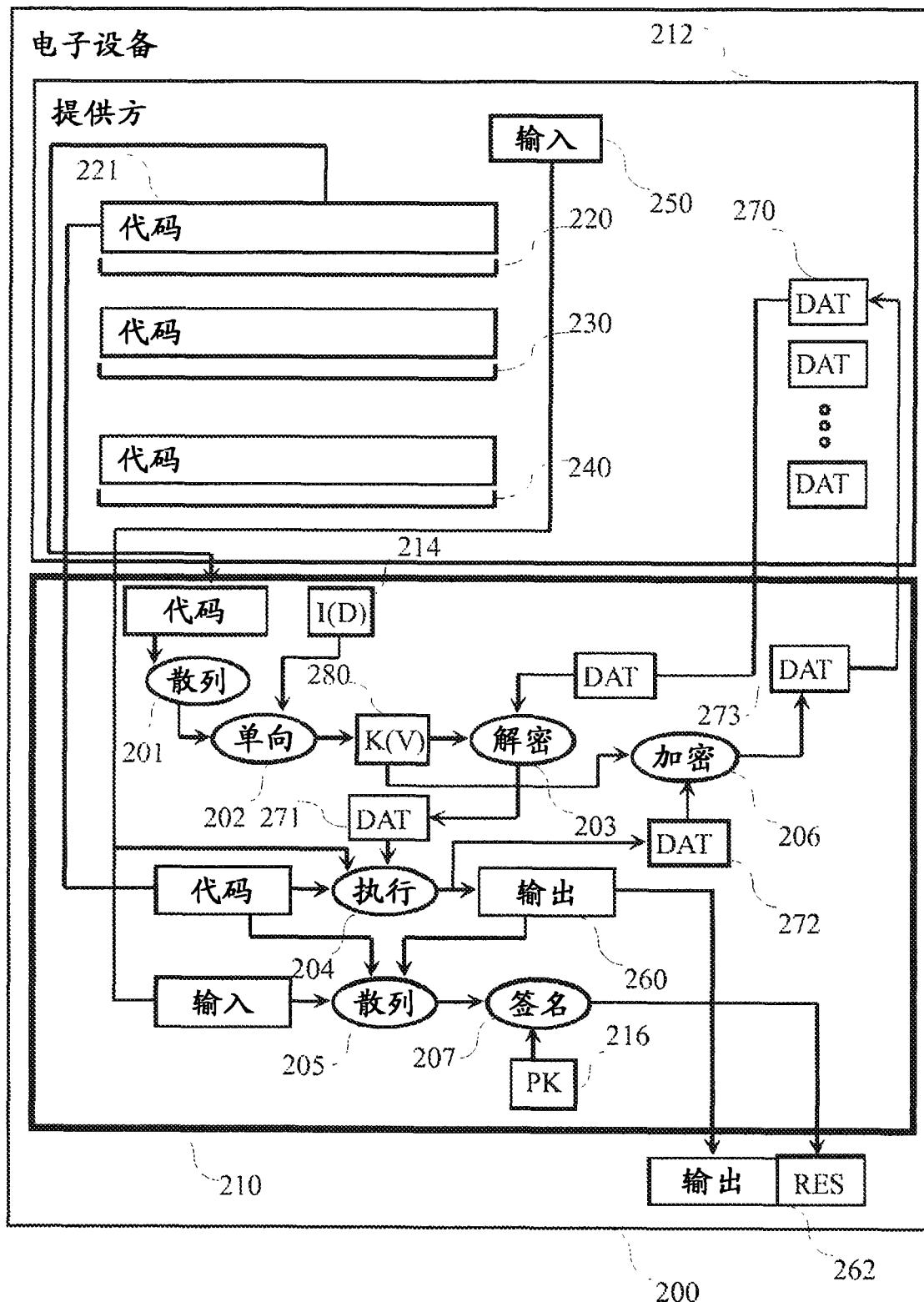


图 2

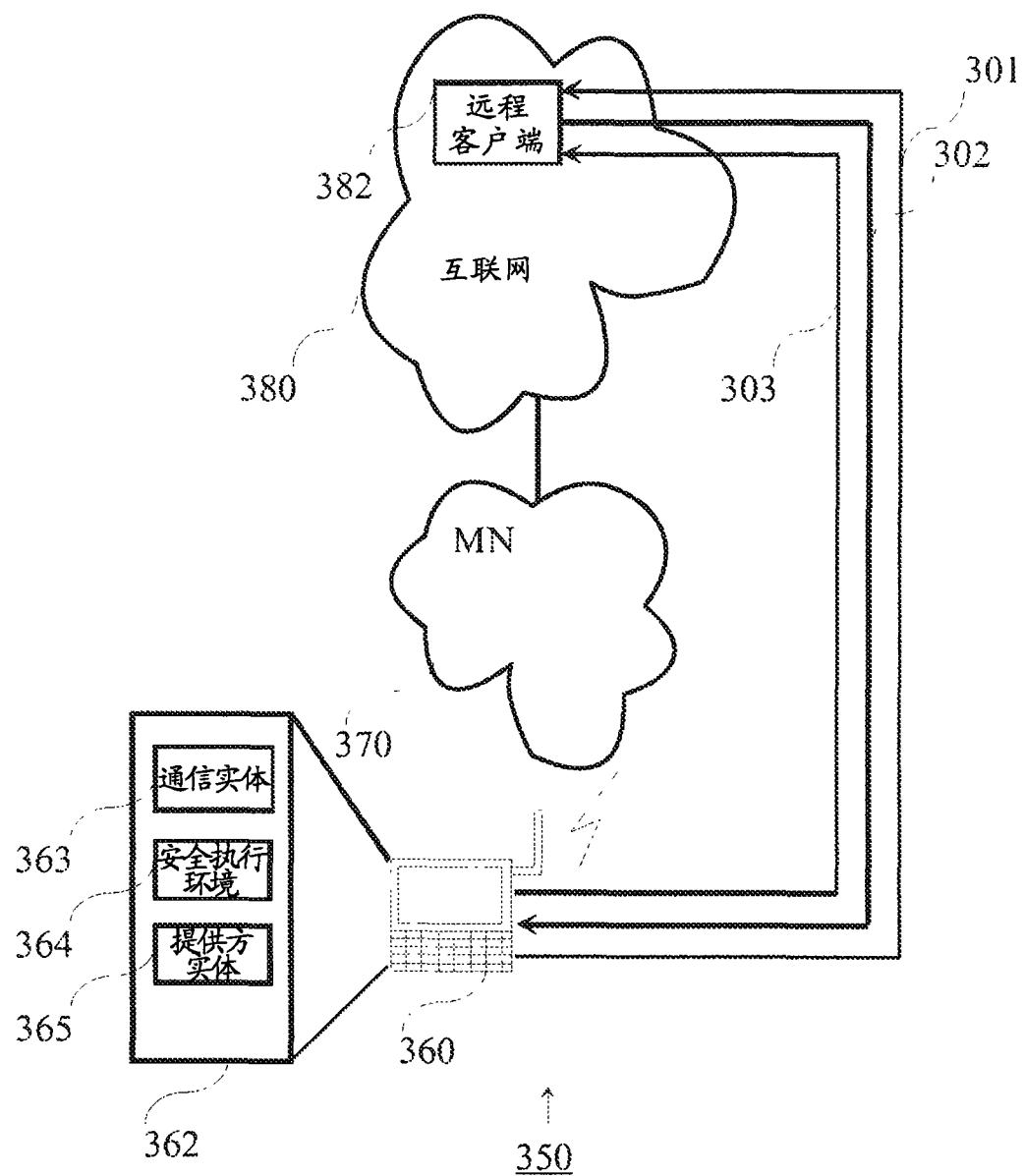


图 3

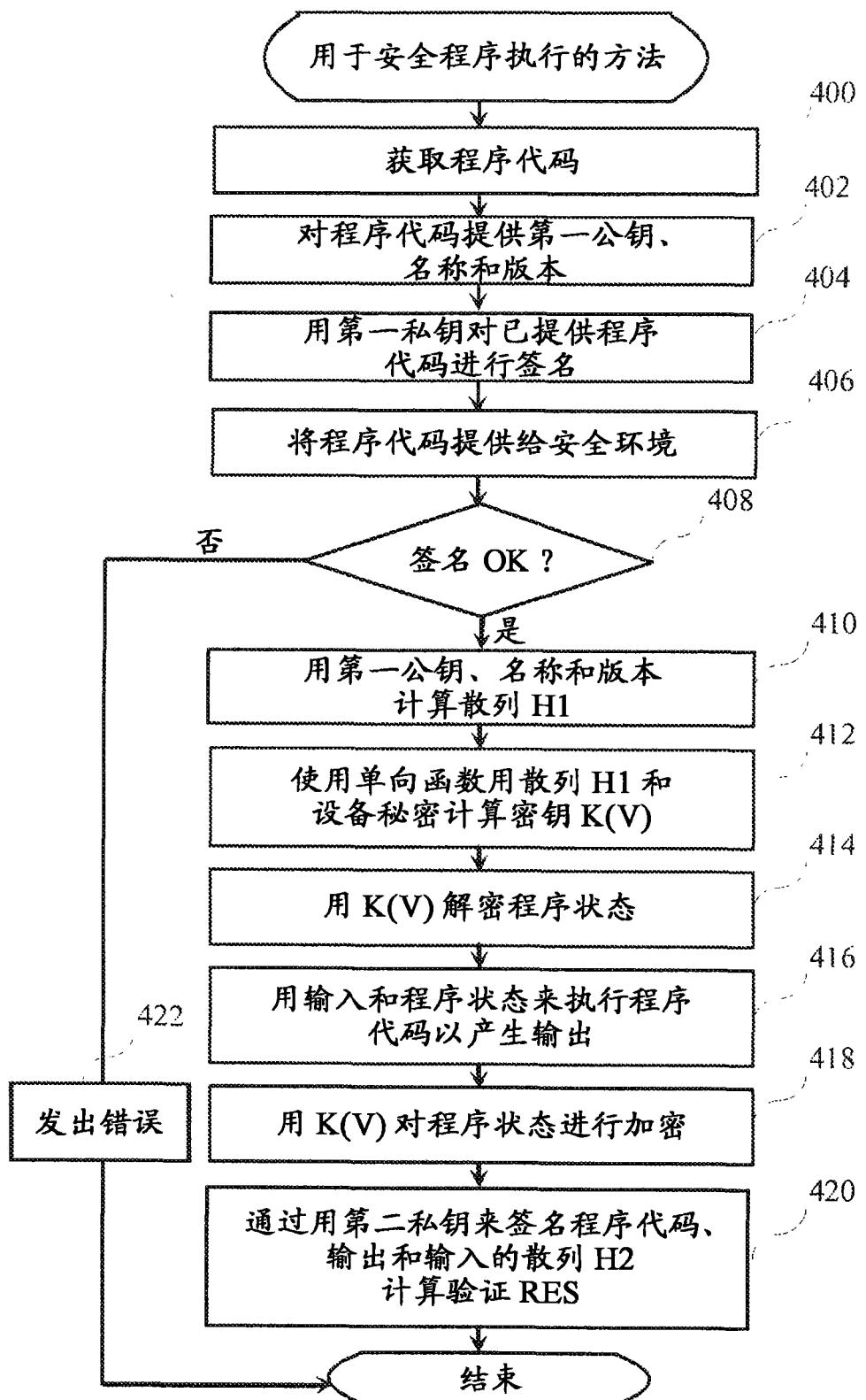


图 4

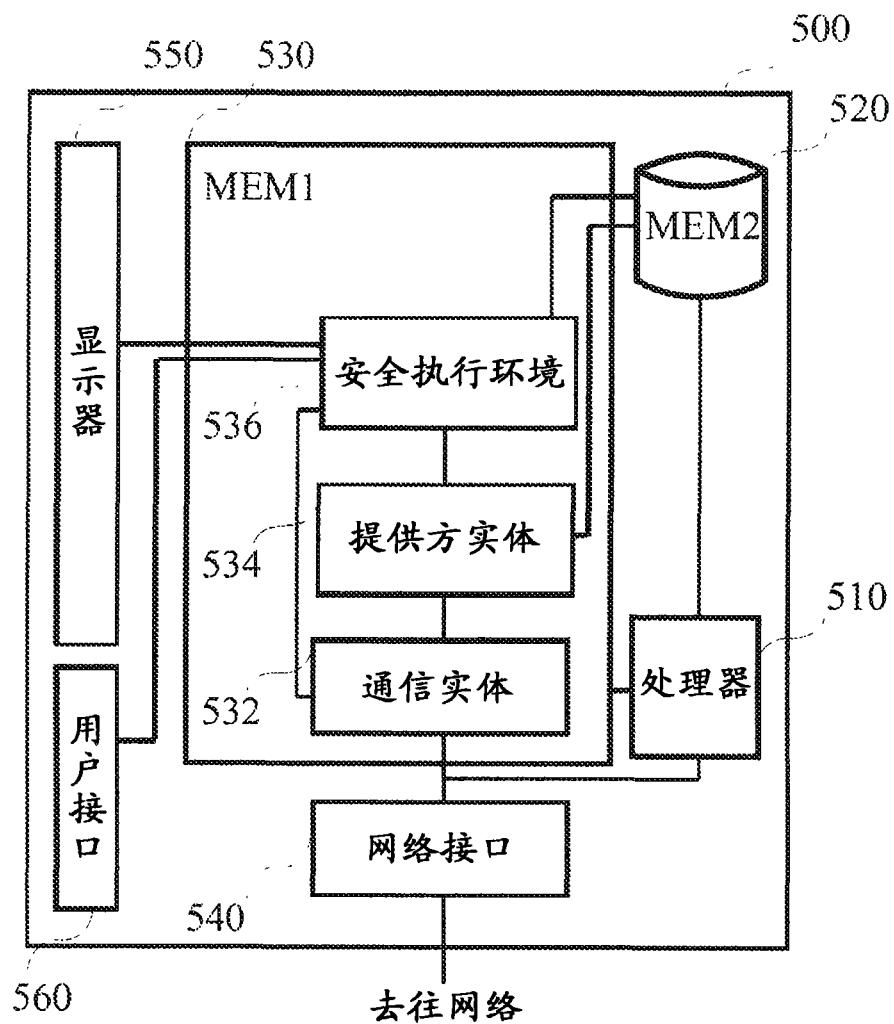


图 5