[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510087314.0

[45] 授权公告日 2008 年 10 月 8 日

[11] 授权公告号 CN 100424611C

[22] 申请日 2005.7.28
[21] 申请号 200510087314.0
[73] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 叶航军 周 涛 谢伟凯 林国辉 戈 弋
[56] 参考文献
CN1567267A 2005.1.19
WO03/098868A1 2003.11.27
WO2005/017756A1 2005.2.24
审查员 梁小容

[74] 专利代理机构 北京市中咨律师事务所
代理人 于 静 李 峥

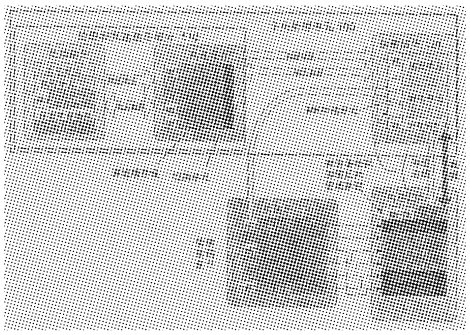
权利要求书 5 页 说明书 8 页 附图 1 页

[54] 发明名称

用于处理加密软件的方法和中央处理单元

[57] 摘要

本发明提供了一种用于处理至少一个已加密软件的中央处理单元，包括处理和高速缓存部分；保密部分，包括：存储有所述设备密钥的设备密钥存储单元；多个用于存储管理密钥的管理密钥存储单元，每一管理密钥存储单元具有相对应的管理密钥索引；解密单元，用于使用所述设备密钥对加密后的管理密钥进行解密，以便获取管理密钥，将管理密钥存储到一管理密钥存储单元中，并将与该管理密钥存储单元相应的管理密钥索引输出，所述用于与所述已加密软件部分相关联；其中，所述解密单元还用于根据所述 MKI 调用相应的管理密钥，对已加密软件部分进行解密，并将解密得到的软件代码和/或数据直接传递给所述处理和高速缓存部分。



1. 一种用于处理至少一个已加密软件的中央处理单元，其中，所述已加密的软件至少包括一个已加密软件部分，该已加密软件部分已被使用一管理密钥MK进行了加密，该管理密钥已被一设备密钥DK加密为加密后的管理密钥，所述中央处理单元包括:

处理和高速缓存部分;

保密部分，包括：存储有所述设备密钥的设备密钥存储单元;多个用于存储管理密钥的管理密钥存储单元，每一管理密钥存储单元具有相对应的管理密钥索引MKI；以及解密单元;

其中，所述解密单元，用于使用所述设备密钥对加密后的管理密钥进行解密，以便获取管理密钥，将管理密钥存储到一管理密钥存储单元中，并将与该管理密钥存储单元相应的管理密钥索引 MKI 输出，所述MKI用于与所述已加密软件部分相关联;

其中，所述解密单元还用于根据所述MKI调用相应的管理密钥，对已加密软件部分进行解密，并将解密得到的软件代码和/或数据直接传递给所述处理和高速缓存部分。

2. 根据权利要求1所述的中央处理单元，其中所述解密单元将解密得到的软件代码和/或数据连同相应的MKI一起直接传递给所述处理和高速缓存部分，所述处理和高速缓存部分根据 MKI 对解密得到的软件代码和/或数据进行处理。

3. 根据权利要求2所述的中央处理单元，其中，所述处理和高速缓存部分进一步将处理后的软件代码和/或数据连同相应的MKI传给保密部分；所述保密部分进一步包括一加密单元，用于根据 MKI 调用相应的管理密钥对所述处理后的软件代码和/或数据进行再次

加密，并将再次加密后的软件代码和/或数据连同 MKI 输出。

4. 根据权利要求 1-3 中任一项所述的中央处理单元，进一步配置为用于处理多个已加密软件，每个已加密软件是用不同的管理密钥分别加密的，所述不同的管理密钥已分别用所述设备密钥加密为多个加密后的管理密钥，

所述解密单元，进一步用于使用所述设备密钥分别对多个加密后的管理密钥进行解密，以便获取多个管理密钥，将多个管理密钥存储到多个管理密钥存储单元中，并将与该多个管理密钥存储单元相应的多个管理密钥索引 MKI 输出，所述多个 MKI 用于分别与相应的所述多个已加密软件相关联。

5. 根据权利要求 4 所述的中央处理单元，其中所述解密单元根据预定的策略为多个管理密钥分配多个管理密钥存储单元及 MKI，所述处理和高速缓存部分进一步根据该预定的策略对解密得到的软件代码和/或数据进行处理。

6. 根据权利要求 5 所述的中央处理单元，其中，所述预定的策略包括：对于与一 MKI 相关联的代码和/或数据只允许具有相同 MKI 的代码进行读写；或者对于与一 MKI 相关联的代码和/或数据，根据预定的策略而允许具有不同 MKI 的代码进行读写。

7. 根据权利要求 5 所述的中央处理单元，其中，所述处理和高速缓存部分进一步包括保密寄存器组，所述预定的策略包括：对于保密寄存器组内存储的与一MKI相关联的代码和/或数据只允许具有相同 MKI 的代码进行读写；或者对于保密寄存器组内存储的与一 MKI 相关联的代码和/或数据，根据预定的策略而允许具有不同 MKI 的代

码进行读写。

8.一种利用中央处理单元处理至少一个已被加密的软件的方法，其中所述中央处理单元包括处理和高速缓存部分以及保密部分，该保密部分包括解密单元、存储有设备密钥的设备密钥存储单元、多个用于存储管理密钥的管理密钥存储单元，每一管理密钥存储单元具有一相对应的管理密钥索引 MKI,所述已被加密的软件已被使用一管理密钥进行了加密，该管理密钥已被所述设备密钥加密为加密后的管理密钥，所述方法包括:

将与所述已被加密的软件相应的用设备密钥加密后的管理密钥读取到所述保密部分之中;

解密单元使用所述设备密钥对加密后的管理密钥进行解密，以便获取管理密钥;

将所述管理密钥存储到管理密钥存储单元中，并获取该管理密钥在所述管理密钥存储单元中的管理密钥索引 MKI;

将该 MKI 与所述已被加密的软件相关联;

根据所述 MKI 取出相应的管理密钥，并利用所述管理密钥在所述解密单元内解密所述已被加密的软件;

将解密得到的软件代码和/或数据直接传递给处理和高速缓存部分，并利用所述处理和高速缓存部分处理解密后的软件。

9. 根据权利要求 8 所述的方法，其中所述解密单元将解密得到的软件代码和/或数据连同相应的MKI一起直接传递给所述处理和高速缓存部分，所述处理和高速缓存部分根据 MKI 对解密得到的软件代码和/或数据进行处理。

10. 根据权利要求 9 所述的方法，其中，所述处理和高速缓存

部分进一步将处理后的软件代码和/或数据连同相应的MKI传给保密部分；所述保密部分进一步包括一加密单元，该加密单元根据 MKI 调用相应的管理密钥对所述处理后的软件代码和/或数据进行再次加密，并将再次加密后的软件代码和/或数据连同 MKI 输出。

11. 根据权利要求 8-10 中任一项所述的方法，进一步用于处理多个已加密软件，每个已加密软件是用不同的管理密钥分别加密的，所述不同的管理密钥已分别用所述设备密钥加密为多个加密后的管理密钥，所述方法进一步包括:

所述设备密钥使用所述解密单元对多个加密后的管理密钥进行解密，以便获取多个管理密钥，将多个管理密钥存储到多个管理密钥存储单元中，并将与该多个管理密钥存储单元相应的多个管理密钥索引 MKI 输出，所述多个 MKI 用于与相应的所述多个已加密软件相关联。

12. 根据权利要求 11 所述的方法，其中所述解密单元根据预定的策略为多个管理密钥分配多个管理密钥存储单元及 MKI，所述处理和高速缓存部分进一步根据该预定的策略对解密得到的软件代码和/或数据进行处理。

13. 根据权利要求 12 所述的方法，其中，所述预定的策略包括对于与一MKI相关联的代码和/或数据只允许具有相同MKI的代码进行读写；或者对于与一 MKI 相关联的代码和/或数据，根据预定的策略而允许具有不同 MKI 的代码进行读写。

14. 根据权利要求 12 所述的方法，其中，所述处理和高速缓存部分进一步包括保密寄存器组，所述预定的策略包括：对于保密寄

存器组内存储的与一 MKI 相关联的代码和/或数据只允许具有相同 MKI 的代码进行读写;或者对于保密寄存器组内存储的与一 MKI 相关联的代码和/或数据,根据预定的策略而允许具有不同 MKI 的代码进行读写。

用于处理加密软件的方法和中央处理单元

技术领域

本发明涉及信息安全技术，尤其涉及用于处理加密软件的方法和中央处理单元。

背景技术

一般，防篡改技术用于保护在非安全环境中的设备免受修改或破坏，这些修改或破坏经常通过物理的或其它攻击方式来进行。对于软件，防篡改技术用于防止恶意的用户通过分析或篡改，而从软件中提取机密信息，例如密钥、专用算法等等。主要的应用情景是在保护包括敏感数据和/或代码的软件内容。

大多数传统的防止篡改软件的技术是基于软件的方法。这些方法通过将软件的敏感数据和/或代码进行加密，来增加恶意用户获取机密的难度。但是，在软件加密的方法中，全部加密的数据和/或代码最终必须使用软件例程解密后将明文（plain form）存储到内存中，然后再提供给CPU。因此，恶意的用户可以通过截取软件的明文来获取信息。

还有几种基于硬件的方法来实现防止篡改软件，但是均要基于专有结构并作为协处理器来实现。其中，一种典型的结构是将一单独的处理器、易失性存储器（如RAM）、非易失性存储器（如闪存）以及保密引擎（cryptographic engine）封装到一起，作为一个协处理器与主计算机通过外部总线进行通信。这种结构适于特定用途的软件，如ATM软件。但是，因为在这种硬件结构中，受保护的程序必须在协处理器上运行，而不是在CPU上运行，因此运行、开发、实施和分发软件都受到限制，很难开发通用的防篡改的软件。

发明内容

鉴于已有技术的不足，本发明所要解决的问题之一是提供一种改进的中央处理单元 CPU，其中解密后的数据和/或代码直接被 CPU 处理。

本发明提供了一种用于处理至少一个已加密软件的中央处理单元，其中，所述已加密的软件至少包括一个已加密软件部分，该已加密软件部分已被使用一管理密钥 MK 进行了加密，该管理密钥已被一设备密钥 DK 加密为加密后的管理密钥，所述中央处理单元包括：处理和高速缓存部分；保密部分，包括：存储有所述设备密钥的设备密钥存储单元；多个用于存储管理密钥的管理密钥存储单元，每一管理密钥存储单元具有一相对应的管理密钥索引 MKI；解密单元，用于使用所述设备密钥对加密后的管理密钥进行解密，以便获取管理密钥，将管理密钥存储到一管理密钥存储单元中，并将与该管理密钥存储单元相应的管理密钥索引 MKI 输出，所述 MKI 用于与所述已加密软件部分相关联；其中，所述解密单元还用于根据所述 MKI 调用相应的管理密钥，对已加密软件部分进行解密，并将解密得到的软件代码和/或数据直接传递给所述处理和高速缓存部分。

本发明还提供了一种利用中央处理单元处理至少一个已被加密的软件的方法，其中所述中央处理单元包括处理和高速缓存部分以及保密部分，该保密部分包括解密单元、存储有设备密钥的设备密钥存储单元、用于存储管理密钥的管理密钥存储单元，每一管理密钥存储单元具有一相对应的管理密钥索引 MKI，所述已被加密的软件已被使用一管理密钥进行了加密，该管理密钥已被所述设备密钥加密为加密后的管理密钥，所述方法包括：将与所述软件相应的用设备密钥加密后的管理密钥读取到所述保密部分之中；解密单元使用所述设备密钥对加密后的管理密钥进行解密，以便获取管理密钥；将所述管理密钥存储到管理密钥存储单元中，并获取该管理密钥在所述管理密钥存储单元中的管理密钥索引 MKI；将该 MKI 与所述被加密的软件相关联；根据所述 MKI 取出相应的管理密钥，并利用所述管理密钥在所述解密单元内解密所述软件；将解密得到的软件代码和/

或数据直接传递给处理和高速缓存部分，并利用所述处理和高速缓存部分处理所述软件。

附图说明

图1示出了根据本发明一实施例的方框图。

具体实施方式

下面结合附图对本发明的具体实施方式进行详细说明。

图 1 示出了根据本发明一实施例的方框图。其中，根据本发明的中央处理单元 100 用于处理至少一个已加密软件。所述已加密的软件至少包括一个已加密软件部分。如图 1 中的内存 130 内存储的软件，该软件包括多个已加密的部分和多个未加密的部分。其中加密页面所存储的是软件的已加密部分，而普通页面存储的是软件的未加密部分。该已加密软件部分已被使用一管理密钥 MK 进行了加密。该管理密钥已被与该中央处理单元相应的设备密钥加密为加密后的管理密钥,如图中所示的设备密钥加密的管理密钥 MK-DK。

所述中央处理单元 100 包括处理和高速缓存部分 110 以及保密部分（Cryptographic Unit）120。

该保密部分 120 包括设备密钥（DK）存储单元，其中存储有与所述中央处理单元相对应的设备密钥 DK；多个用于存储管理密钥 MK 的管理密钥（MK）存储单元，每一管理密钥存储单元具有相对应的管理密钥索引 MKI；解密单元，用于使用所述设备密钥对加密后的管理密钥进行解密，以便获取管理密钥，将管理密钥存储到一管理密钥存储单元中，并将与该管理密钥存储单元相应的管理密钥索引 MKI 输出，所述 MKI 用于与所述已加密软件部分相关联。其中，所述解密单元还用于根据所述 MKI 调用相应的管理密钥，对已加密软件部分进行解密，并将解密得到的软件代码和/或数据直接传递给所述处理和高速缓存部分。

此外，根据需要，每一管理密钥存储单元可以有一个或多个管理密钥

索引 MKI 相对应。

对于所要处理的软件，首先将与所述软件相应的用设备密钥加密后的管理密钥读 MK-DK 取到所述保密部分 120 之中。然后，使用所述设备密钥 DK 对加密后的管理密钥 MK-DK 进行解密，以便获取管理密钥 MK。

将所述管理密钥 MK 存储到管理密钥（MK）存储单元中，并获取该管理密钥在所述管理密钥存储单元中的管理密钥索引号 MKI。其中，每一管理密钥存储单元具有一相对应的管理密钥索引 MKI。然后，将该 MKI 与所述被加密的软件部分相关联。

这样，当中央处理单元需要处理与 MKI 相关联的已加密软件部分的时候，就可以根据所述 MKI 取出相应的管理密钥。并利用所述管理密钥在所述解密单元内解密所述已加密的软件部分。将解密得到的软件代码和/或数据直接传递给处理和高速缓存部分，并利用所述处理和高速缓存部分处理所述软件。

在本发明中，受保护的代码和/或数据从来不会被软件例程解密并存储到用户可以访问的存储装置中，如内存、硬盘等。相反，根据本发明的硬件解密单元嵌入到中央处理单元 CPU 之中，对加密的代码和/或数据进行解密并直接提供给 CPU。由于用户无法访问到受保护内容的明文代码和/或数据（plain code/data），例如明文形式的数据和或代码不会出现在用户可访问的存储装置中，这样，有效地避免了恶意用户截取这些信息。

根据下文所述的一些预定的策略，可以进一步限制为仅仅允许被授权的代码对受保护的内容进行存取。这样就进一步防止了恶意的用户通过一些未授权的方式截取受保护的信息。而已有的保护方法，尤其是基于软件的保护方法对此却很难实现。

对于需要处理的部分已加密的软件，如图 1 所示,在内存中可以以页面的方式来进行存储。已加密的部分和未加密的部分分别使用加密的页面和普通页面来存储。还可以生成一页面表 150，将加密的页面和普通页面的页面地址与解密得到的管理密钥 MK 的索引 MKI 相关联。这样，CPU 就可以将加密后的软件部分与未加密的软件部分，根据 MKI 来区别对待。

本领域的技术人员容易理解，还可以利用其它方法，来将 MKI 与加密的软件部分相关联，例如为加密的软件部分添加一标题来指示其对应的 MKI。对于使用该 CPU 处理多个已加密软件的情况，可以将它们各自的 MK 对应的 MKI 与这些软件分别相关联。

通过 MKI 将管理密钥与加密的软件部分相关联，还使得根据本发明的中央处理单元可以用于处理多个加密的软件，或多个包括加密部分的软件。

根据本发明的另一方面，其中所述解密单元还可以将解密得到的软件代码和/或数据连同相应的 MKI 一起直接传递给所述处理和高速缓存部分，所述处理和高速缓存部分根据 MKI 对解密得到的软件代码和/或数据进行处理。

根据上述 CPU 和方法，所述处理和高速缓存部分还可以进一步将处理后的软件代码和/或数据连同相应的 MKI 传给保密部分；所述保密部分进一步包括一加密单元，用于根据 MKI 调用相应的管理密钥对所述处理后的软件代码和/或数据进行再次加密，并将再次加密后的软件代码和/或数据连同 MKI 输出。

根据本发明的上述 CPU 和方法，所述中央处理单元进一步配置为用于处理多个已加密软件，每个已加密软件是用不同的管理密钥分别加密的，所述不同的管理密钥已分别用所述设备密钥加密为多个加密后的管理密钥。所述解密单元，进一步用于使用所述设备密钥分别对多个加密后的管理密钥进行解密，以便获取多个管理密钥，将多个管理密钥存储到多个管理密钥存储单元中，并将与该多个管理密钥存储单元相应的多个管理密钥索引 MKI 输出，所述多个 MKI 用于分别与相应的所述多个已加密软件相关联。这样，同一软件的加密部分或同一已加密的软件与同一 MKI 相关联，或者使用相同 MK 加密后的多个软件相关联的 MKI 相同。

根据本发明的上述 CPU 和方法，其中所述解密单元根据预定的策略为多个管理密钥分配多个管理密钥存储单元及 MKI，所述处理和高速缓存部分进一步根据预定的策略对解密得到的软件代码和/或数据进行处理。其

中，所述预定的策略包括：对于与一 MKI 相关联的代码和/或数据只允许具有相同 MKI 的代码进行读写；或者对于与一 MKI 相关联的代码和/或数据，根据预定的策略而允许具有不同 MKI 的代码进行读写。例如，MKI 的取值在某一范围内的代码之间，允许相互读写。但是，可以允许不具有或不同 MKI 的代码与具有 MKI 的代码之间相互调用。

其中，与一 MKI 相关联的代码和/或数据，可以选自与 MKI 相关联的未解密的代码和/或数据、与 MKI 相关联的解密得到的代码和/或数据、和/或对具有该 MKI 的代码和/或数据进行中间处理而得到的代码和/或数据。与 MKI 相关联的代码和/或数据可以仅在解密前保持其 MKI 指示。作为优选方案，与 MKI 相关联的代码和/或数据还可以在高速缓存中保持其 MKI 指示，或者在中央处理单元的各个部分中均保持代码和/或数据的 MKI 指示。

根据本发明的上述 CPU 和方法，其中，所述处理和高速缓存部分进一步包括保密寄存器组，所述预定的策略包括对于保密寄存器组内存储的与一 MKI 相关联的代码和/或数据只允许具有相同 MKI 的代码进行读写。或者对于保密寄存器组内存储的与一 MKI 相关联的代码和/或数据，根据预定的策略而允许具有不同 MKI 的代码进行读写，如其 MKI 取值在某一范围内的代码可以进行读写。

根据 CPU 的具体要求，图 1 中所示的处理和高速缓存部分可以包括处理部分和高速缓存部分。其中，所述高速缓存部分可以包括控制单元、高速缓存线及相应的 MKI 指示部分；而处理部分可以包括执行单元、当前指令寄存器及其相应的 MKI 存储部分，保密寄存器组、寄存器（根据需要寄存器可以具有或不具有相应的 MKI 指示或存储部分）以及其它单元。本领域的技术人员容易理解，根据本发明以及 CPU 的其它具体要求，该处理和高速缓存部分还可以使用其它配置，而不脱离本发明。例如，在处理部分和高速缓存部分也可以不使用 MKI 和保密寄存器组。这时，可以依靠保密部分的隔离作用来保护加密的软件。

本发明将保密部分（cryptographic unit）和其它保护单元嵌入到 CPU 之内，而不是将与保护程序执行的全部单元集成到协处理器之中。这样，就保留了 CPU 和计算机的原有结构，并且该原有结构对于包括操作系统和应用的传统软件是透明的，传统软件不会察觉到该基于硬件的防篡改特性。使用操作系统来支持这种防篡改特性，如操作系统在对软件进行存储时，将加密的部分与未加密的部分分别存储。这样就容易实现将 MKI 与加密的部分相关联。应用就很容易实现防篡改并同时保持原有的工作、开发、实施以及分发方式。

如上文所述，传统的基于软件的防篡改方法，是对软件的敏感数据和或代码进行加密，以增加进行非法侦听或截取的难度。而传统的基于硬件的防篡改方法，是将与防篡改的全部相关部件都集成到一个单独的协处理器中，并在其中运行受保护的软件。

在本发明之中，将保密部分和其它保护单元嵌入到 CPU 之内，并利用 MKI 来进行管理。图 1 展示了根据本发明一实施例的结构。保密部分被设置在 CPU 之内，在 CPU 数据流的最外侧。一般可以设置在高速缓存和外部数据总线之间。

受保护的软件部分(数据和或代码)，在 CPU 以外存储时，总是处于已被加密状态。当 CPU 读到加密后的内容时，解密单元将该内容解密为 CPU 能够识别的明文。当 CPU 要将内容写回内存或存储装置的加密部分时，在将该内容送出 CPU 之前，加密单元将该内容加密。在本发明中，保护内容的基本原则包括：受保护的内容（数据和或代码）在 CPU 之外时，总是处于加密状态；对于受保护内容的访问权限，局限于得到授权的代码。

图 1 示出了根据本发明的一实施例的加密 CPU。该加密 CPU 具有以下特征。

1. 每个加密 CPU 内都存储有被分配的一个或多个设备密钥（DK），用于有条件地授权访问受保护的软件。

2. 软件受保护的部分被管理密钥（MK）加密。一般情况下，MK 与 DK 不同，以便于密钥的分发。在应用被分发时，可以随机地为每个应用生成 MK。

3. 如果选定了与 DK 不同的 MK，使用选定的 DK 加密 MK，并将 MK 与应用一起或分别分发。通常，广播加密技术，例如 媒体密钥块（Media Key Block (MKB)）技术，和简单 PKI（Public Key Infrastructure 公开密钥机制）技术可以用于管理密钥的分发。

4. CPU 的保密部分（cryptographic unit）可以保存用于运行全部应用的内部 MK 列表。

5. 与受保护的应用一起分发的 MK，可以用适当的 DK 解密出来，内部 MK 列表的可用项目被分配用于存储应用 MK。在加载应用之前，通常可以由操作系统调用 CPU 来完成该过程，并且在内部 MK 列表中的 MK 索引（MKI）被返回给操作系统。

6. 该 MKI 用于创建用于执行受保护应用的数据结构。通常，操作系统可以使用相应的 MKI 适当地创建页面表。

7. 上述加密单元和解密单元根据相关的 MKI 访问受保护的部分。

8. 对于受保护内容的访问权限如读写全线，被限制为访问被授权的代码。一个典型的选择是限制为：仅仅具有相同 MKI 的来自受保护部分的代码可以读写受保护的内容。未授权的代码只能访问加密的受保护内容

9. 一个特别的保密寄存器组（secret register set）可以用于实施特定的访问策略限制寄存器的使用。一个典型的访问策略是限制为：仅仅具有相同 MKI 的代码可以读写具有相同 MKI 的寄存器值；其它的代码只能读写加密后的寄存器值（可以被 MKI 对应的 MK 加密）。

10. 操作系统在进行任务切换的时候需要将任务的当前寄存器组的内容保存到存储器，并从存储器加载待执行的任务的寄存器组。如果是保密寄存器组，存储器里的保存值都是加密后的值。

以上结合优选法方案对本发明进行了详细的描述，但是可以理解，以上实施例仅用于说明而非限定本发明。本领域的技术人员可以对本发明的所示方案进行修改而不脱离本发明精神。

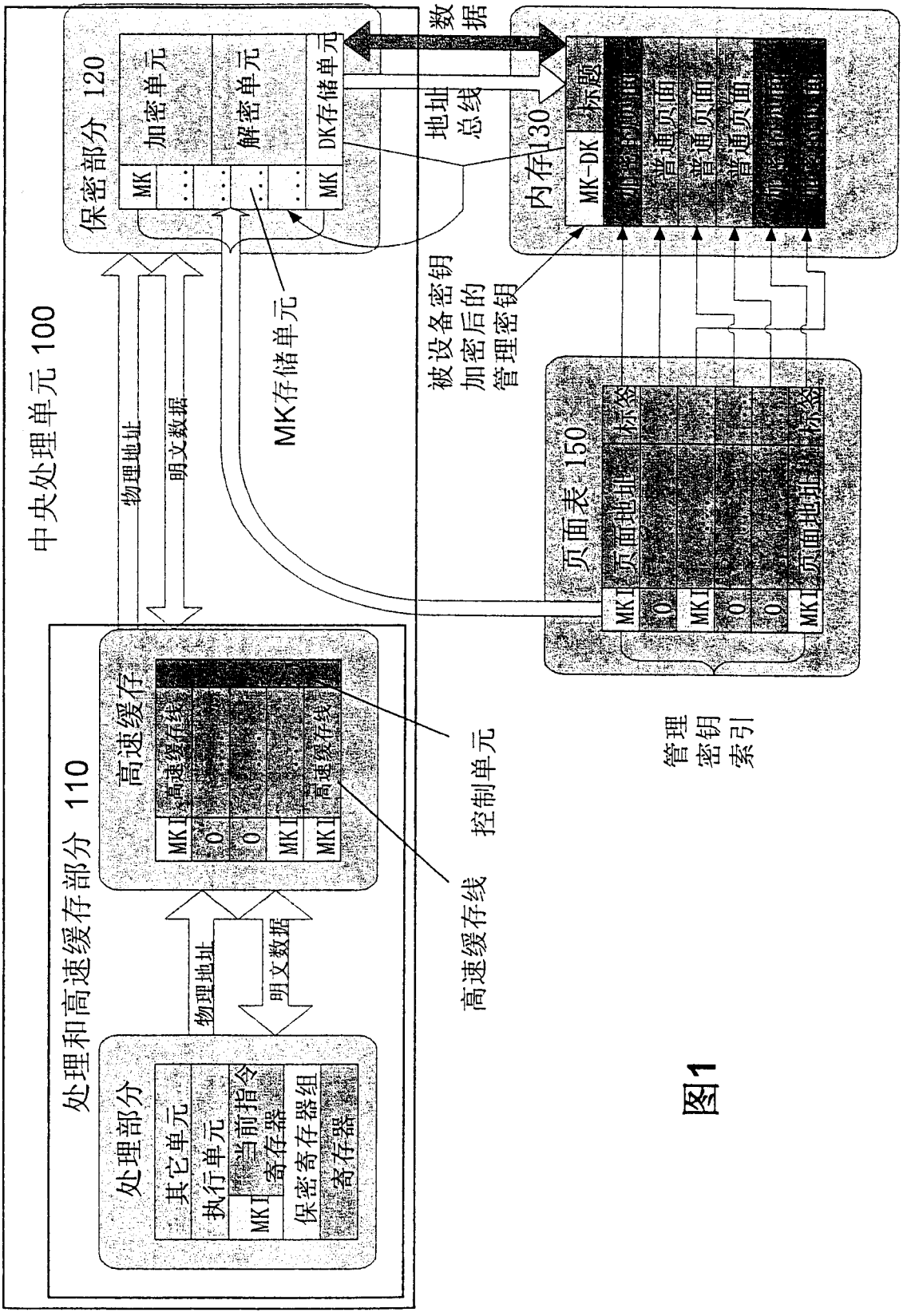

中央处理单元 100
处理和高速缓存部分 110
处理部分
其它单元
执行单元
MKI
当前指令寄存器
保密寄存器组
寄存器
高速缓存
MKI
高速缓存线
物理地址
明文数据
保密部分 120
MK
加密单元
解密单元
DK存储单元
MK存储单元
地址总线
数据
内存130
MK-DK
标题
普通页面
页面表 150
MKI
页面地址
标签
管理密钥索引
被设备密钥加密后的管理密钥
高速缓存线
控制单元

图1