

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 9/30 (2006.01)

H04K 1/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 00817630.2

[45] 授权公告日 2007 年 4 月 18 日

[11] 授权公告号 CN 1311657C

[22] 申请日 2000.12.19 [21] 申请号 00817630.2

[30] 优先权

[32] 1999.12.23 [33] FI [31] 19992778

[86] 国际申请 PCT/FI2000/001112 2000.12.19

[87] 国际公布 WO2001/048963 英 2001.7.5

[85] 进入国家阶段日期 2002.6.21

[73] 专利权人 塞特克有限公司

地址 芬兰万塔

[72] 发明人 劳雷·帕特罗 泰穆·阿西凯宁

坚尼·兰特拉

[56] 参考文献

US5867577 1999.7.2

US5974148 1999.10.26

US5623637 1997.4.22

US4935962 1990.6.19

审查员 何怀燕

[74] 专利代理机构 北京三友知识产权代理有限公司

代理人 李 辉

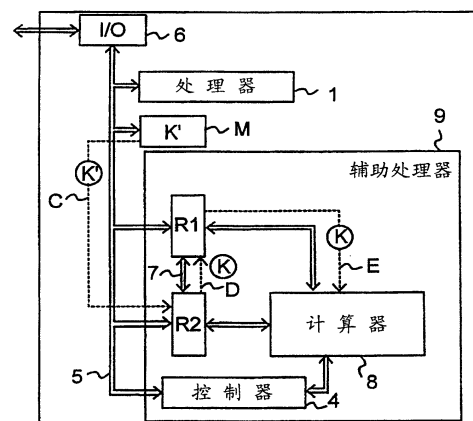
权利要求书 2 页 说明书 7 页 附图 3 页

[54] 发明名称

处理密钥的方法和装置

[57] 摘要

本发明涉及一种装置，该装置包括：一个控制该装置运行的处理器(1)；一个通过一条总线(5)与处理器(1)相连的存储器(M)；以及通过所述总线(5)与处理器(1)和存储器(M)相连的辅助处理器(9)，以便在密钥(K)的基础上产生响应。为了使外来的攻击者更难找到密钥，所述密钥(K)编码后(K')存储在所述存储器(M)中。辅助处理器(9)的计算装置(8)包括根据数据寄存器(R2)中的编码密钥(K')计算出密钥(K)的解码函数，计算装置(8)的一个计算函数取出该解码密钥(K)以便产生所述响应。



1. 一种处理一个装置中的密钥的方法，该装置包括一个存储器、一个处理器和一个通过一条总线与存储器相连的辅助处理器，该方法包括：

为密钥编码并将编码密钥存储在所述存储器中；

在一个输入、所述密钥和一个预定的计算函数的基础上，辅助处理器产生一个响应， 其特征在于包括以下步骤：

将所述输入发送给辅助处理器的数据寄存器；

从存储器重新得到所述编码密钥，并通过所述总线将其提供给辅助处理器的数据寄存器，以及

作为辅助处理器的内部操作，通过预定的解码函数对数据寄存器中存储的编码密钥解码，将解码的密钥通过辅助处理器的内部总线提供给辅助存储器的钥匙寄存器，并从钥匙寄存器重新得到所述密钥，用来基于所述数据寄存器中的所述输入、所述钥匙寄存器中的所述解码的密钥、和所述辅助处理器的所述预定的计算函数产生所述响应。

2. 根据权利要求1所述的方法，其特征在于：

将对编码密钥解码所必需的第二密钥存储在辅助处理器中； 以及

重新得到辅助处理器的解码函数所用的所述第二密钥，并且利用所述解码函数和第二密钥对编码密钥解码。

3. 一种装置，包括：

控制该装置运行的处理器（1）；

通过总线（5）与处理器（1）相连的存储器（M）； 和

通过所述总线（5）与处理器（1）和存储器（M）相连的辅助处理器（9，9'），辅助处理器包括：计算装置（8，8'），用来在密钥（K），预定的计算函数和通过所述总线（5）发送到辅助处理器（9，9'）的输入的基础上产生响应；以及通过所述总线（5）传送所述响应的装置，其特征在于：

所述密钥（K）在编码后（K'）存储在所述存储器（M）中；

所述辅助处理器(9, 9')包括: 通过所述总线(5)从存储器(M)接收所述编码密钥(K')的数据寄存器(R2);

辅助处理器(9, 9')的计算装置(8, 8')从数据寄存器(R2)中的编码密钥(K')计算密钥(K); 以及

辅助处理器(9, 9')包括钥匙寄存器(R1)和内部总线(7), 辅助处理器(9, 9')通过内部总线(7)将密钥(K)存储在所述钥匙寄存器(R1)中, 计算装置(8, 8')的计算函数从密钥寄存器(R1)重新得到所述密钥(K)以便产生所述响应。

4. 根据权利要求3所述的装置, 其特征在于: 所述装置是一张智能卡, 其对提供给智能卡的与验证有关的输入产生所述响应。

5. 根据权利要求3或4所述的装置, 其特征在于: 所述辅助处理器(9')包括第二钥匙寄存器(R3), 其中存储着对编码密钥(K')解码所必需的第二密钥(K2), 以及

计算装置(8')的解码函数从第二钥匙寄存器(R3)重新得到所述第二密钥(K2), 以便计算出从编码密钥(K')产生响应所必需的密钥(K)。

处理密钥的方法和装置

技术领域

本发明涉及密钥的处理，使得外来攻击者无法找到某装置的密钥。本发明主要涉及用来验证某装置（如智能卡）的密钥处理。但要注意：尽管本发明主要结合智能卡及验证操作进行描述，本发明仍可用于其它方面。

背景技术

已知智能卡的验证通常以请求-响应过程为基础。智能卡在验证中所用的智能卡专用密钥被存储在智能卡的存储器中。与验证有关的验证装置将一个输入发送给智能卡。智能卡在输入、密钥和预定的验证函数的基础上计算响应，并把响应提供给验证装置。智能卡和验证函数所用的密钥还对于验证装置是已知的，或者还对于例如与验证装置通信的验证中心是已知的。因此，验证装置或验证中心能够进行与智能卡相似的运算操作，在这种情况下，智能卡应该对发送来的输入产生的响应被通知给验证装置。如果验证装置从智能卡接收到的响应是正确的，验证装置确定智能卡的验证已经成功。与已知的智能卡有关，验证操作也可与上述的操作相反。此时，智能卡验证外部装置，这就意味着输入从智能卡传送到外部装置，接着，响应从外部装置传送到智能卡。这样，由智能卡验证已经接收到对其产生的输入的正确响应。

包括密钥的装置是先前已知的，它包括：控制装置运行的处理器；通过总线与处理器相连的存储器；以及通过所述总线与存储器和处理器相连的辅助处理器。在这些已知的装置中，密钥存储在存储器中。但是，由装置中的辅助处理器进行产生响应所必需的运算操作，这意味着为了产生响应，必需通过上述

的总线经处理器将密钥由存储器传输给辅助处理器。将密钥通过总线从存储器传输给辅助处理器的过程有可能为外来攻击者提供有助于找到密钥的信息。如果外来攻击者成功地找到密钥，这就意味着攻击者通过制作另一个使用与原始装置相同的密钥的装置，能够克隆该装置。

发明内容

本发明的目的之一就是要消除上述的问题，并提供一种使外来攻击者更难找到某装置的密钥的解决方法。该目的通过本发明中处理一个装置中的密钥的方法得以实现，所述装置包括存储器、处理器和通过总线与存储器相连的辅助处理器；所述方法包括：为密钥编码并将编码密钥存储在所述存储器中；由辅助处理器在一个输入、所述密钥和一个预定的计算函数的基础上产生一个响应。本发明的方法的特征在于包括以下一些步骤：将所述输入发送给辅助处理器的数据寄存器；从存储器中取出所述编码密钥并通过所述总线将其传送给辅助处理器的数据寄存器；以及作为辅助处理器的内部操作，通过预定的解码函数对数据寄存器中存储的编码密钥解码，将解码的密钥通过辅助处理器的内部总线提供给辅助存储器的钥匙寄存器，并从钥匙寄存器重新得到所述密钥，用来基于所述数据寄存器中的所述输入、所述钥匙寄存器中的所述解码的密钥和所述辅助处理器的所述预定的计算函数产生所述响应。

本发明的目的还通过一种装置得以实现，该装置包括：控制该装置运行的处理器；通过总线与处理器相连的存储器；以及通过所述总线与处理器和存储器相连的辅助处理器，所述辅助处理器包括：在一个密钥、一个预定的计算函数和通过所述总线发送给辅助处理器的一个输入的基础上产生响应的计算装置；以及通过所述总线传送所述响应的装置。本发明的装置的特征为：所述密钥在编码后存储在所述存储器中，所述辅助处理器包括通过所述总线从存储器接收所述编码密钥的数据寄存器，辅助处理器的计算装置从数据寄存器中的编码密钥计算出密钥，并且辅助处理器包括钥匙寄存器和内部总线，辅助处理器

通过内部总线将密钥存储在所述密钥寄存器中，计算装置的计算函数从所述密钥寄存器取出所述密钥，以产生所述响应。

本发明的基础思想为：当将存储器与辅助处理器相连的装置总线内传输的密钥决不会是未编码的密钥时，外来攻击者找到密钥的难度将会更大。这样，外来攻击者通过监视总线通信将会一无所获。根据本发明，密钥在被编码后存储在存储器中。密钥通过总线从存储器以编码的形式传送给辅助处理器。外来攻击者不知道密钥是如何被编码的，这就是为什么攻击者并不会因找到编码密钥而受益。

在编码密钥被传送给辅助处理器之后，编码密钥被解码，即，由编码钥匙产生密钥，并通过辅助处理器内的内部总线被传送给辅助寄存器的外部钥匙寄存器。这样，就没有必要在辅助处理器外以未编码的形式处理密钥。本发明的解决方法的最大优点为：外来攻击者找到装置的密钥的难度更大。

附图说明

在下文中将以举例方式结合附图对本发明进行更详细的说明，其中：

图 1 为已知的智能卡；

图 2 为本发明装置的第一优选实施例；

图 3 为本发明装置的第二优选实施例；以及

图 4 为本发明方法的第一优选实施例的流程图。

具体实施方式

图 1 为已知的智能卡。图 1 的智能卡包括：通过总线 5 互连的处理器 1，存储器 M 和辅助处理器 2。连接电路 6 与总线相连，智能卡通过它的总线 5 通过电路 6 与外部装置相连。与验证有关，外部装置发送的一个输入通过总线 5 被发送给辅助处理器 2。在接收该输入后，辅助处理器 2 通过该输入、密钥 K 和预定的验证算法产生一个响应。该响应通过总线 5 和连接电路 6 从辅助处理

器发送给外部装置。

为了验证智能卡，密钥 K 被存储在它的存储器 M 中，并通过总线 5 取出到辅助处理器的钥匙寄存器 $R1$ 中（箭头 A）。与验证有关，输入从外部装置通过总线 5 被发送给辅助处理器的数据寄存器 $R2$ 。辅助处理器 2 的计算器 3 从钥匙寄存器 $R1$ 中取出钥匙 K （箭头 B）并从数据寄存器 $R2$ 取出输入，之后，计算器在预定的验证函数的基础上计算响应，接着，辅助处理器将响应提供给数据寄存器 $R2$ 。响应从数据寄存器 $R2$ 通过总线 5 被传送给外部装置。

上述的智能卡的最大缺点就是处理密钥的方法。密钥 K 是智能卡专用的，即为每张智能卡存储一个唯一的密钥。因此，只有一张智能卡对提供给一个特定智能卡的与验证有关的输入产生预定的响应。密钥通过总线 5 从存储器传送给辅助处理器的事实为外来攻击者提供了找到密钥的机会。如果攻击者成功地找到密钥，这就意味着外来攻击者能够（至少在理论上）制作另一张使用与原始智能卡相同的密钥的智能卡（克隆卡）。

图 2 为本发明装置的第一优选实施例。在下文中，假设图 2 中的装置是一张智能卡，并且，智能卡的密钥专用于验证。

图 2 中的智能卡包括：存储器 M ，如 EEPROM，其中存储了经过编码的密钥 K' 。实际中，可以例如通过应用预定的编码函数 f 在密钥 K 的基础上计算编码密钥 K' 来对密钥编码，即 $K' = f(K)$ 。

为了给辅助处理器 9 的计算器 8 提供与验证有关的密钥，编码密钥 K' 通过总线 5 从存储器 M 取出到数据寄存器 $R2$ （箭头 C）。计算器 8 能够从数据寄存器 $R2$ 重新得到编码密钥 K' ，并且能够应用编码函数 f 的逆函数 f' 计算密钥 K ，即 $K = f'(K')$ 。在运算之后，辅助处理器将密钥 K 提供给数据寄存器 $R2$ 。为了足够安全地处理密钥，上述的编码函数 f 及其逆函数应该是外来攻击者无法获得的秘密函数。

根据本发明，辅助处理器 5 包括：内部总线 7，该总线使得辅助处理器能够将计算出的密钥 K 从数据寄存器 $R2$ 传送到钥匙寄存器 $R1$ （箭头 D）。这样就

不必通过智能卡的总线 5 传输密钥 K，优点就在于使外来攻击者找到密钥的难度增大。

计算器 8 能够以与图 1 的智能卡相似的方式从钥匙寄存器 R1 重新得到与验证有关的密钥 K。

根据本发明，可以用一个新的密钥替换智能卡的密钥来改变它。然后，外部装置将新的密钥提供给智能卡。新的密钥在被提供给智能卡时可以被编码。接着，经过编码的新密钥通过总线 5 被提供给辅助处理器的数据寄存器 R2。在这之前（例如，当智能卡与外部装置相连时），辅助处理器所用的密钥 K 已经被存储在其钥匙寄存器中。辅助处理器的控制器 4 也接到处理器 1 的通知：新的编码密钥被存储在它的数据寄存器 R2 中。随后，辅助处理器先把新密钥当作一个与验证有关的输入来处理。接着，辅助处理器用钥匙寄存器中的密钥和辅助处理器所用的验证函数为新密钥解码。当找到新密钥时，辅助处理器用编码函数 f 为其编码，之后，新的经过编码的密钥从辅助处理器发送给存储器 M，在存储器 M 中代替先前经过编码的密钥。

图 3 为依据本发明待验证的装置的第二优选实施例。在下文中，假设图 3 中待验证的装置是一张智能卡。

图 3 中的智能卡与图 2 中的大致相同，即，图 3 中的智能卡的辅助处理器 9' 还包括内部总线 7，通过总线 7 密钥 K 被从数据寄存器 R2 发送给钥匙寄存器 R1。但是，图 3 中的实施例与图 2 中的不同之处在于：图 3 的实施例中，辅助处理器 9' 包括一个附加寄存器，即，一个第二钥匙寄存器 R3。第二密钥 K2 存储在第二钥匙寄存器中。计算器 8' 用密钥 K2 来计算验证中所用的密钥 K。

为了能够进行验证，从存储器 M 中重新得到编码密钥 K'。用存储在第二钥匙寄存器 R3 中的第二密钥 K2 和预定的编码函数显式地为钥匙编码。编码密钥 K' 通过总线 5 被提供给数据寄存器 R2（箭头 C）。接着，计算器 8' 利用编码密钥 K'、第二密钥 K2 和所述预定编码函数的逆函数计算密钥 K，并且辅助处理器将密钥 K 提供给数据寄存器 R2。密钥 K 通过总线 7 从数据寄存器 R2 被发

送给钥匙寄存器 R1 (箭头 D), 计算器 8' 可以从钥匙寄存器 R1 重新得到该与验证有关的钥匙 (箭头 E)。

与图 2 中的实施例相比, 图 3 中的实施例的优点在于: 计算器用来从编码密钥 K' 计算密钥 K 的函数, 即解码函数, 可以是公开的。换句话说, 外来的攻击者不能利用他/她所知道的在计算密钥 K 中采用的函数, 因为外来的攻击者不知道第二钥匙寄存器 R3 内的第二密钥 K2。因此, 即使外来攻击者既了解编码密钥 K' 又了解上述的函数, 他/她仍不能找到验证中所用的密钥 K。

图 3 中的实施例还使得不同用途的几个编码密钥能够存储在存储器 M 中。所有的这些编码密钥的解码使第二钥匙寄存器 R3 中的第二密钥 K2 成为必要。从而辅助处理器 9' 可以如上所述在给定的时间对所需密钥解码并储存在钥匙寄存器中。

图 3 的实施例还使得存储器 M 中存储的密钥 (或多个密钥) 能够如图 2 所述改变。另一方面, 很可能地, 存储在第二钥匙寄存器 R3 中的第二密钥几乎从来不需要改变, 因为只有智能卡“知道”第二密钥, 即, 没有外部装置需要知道第二密钥是什么。而且第二密钥从来不会在辅助处理器外传送, 所以外来攻击者不可能成功地找到第二密钥。

图 4 为本发明的方法的第一优选实施例的流程图。图 4 的流程图可以用于智能卡的验证, 如图 2 或图 3 描述的。

在框 10 中, 智能卡的密钥被预定的编码函数编码。在框 11 中, 编码密钥被存储在智能卡的存储器中。

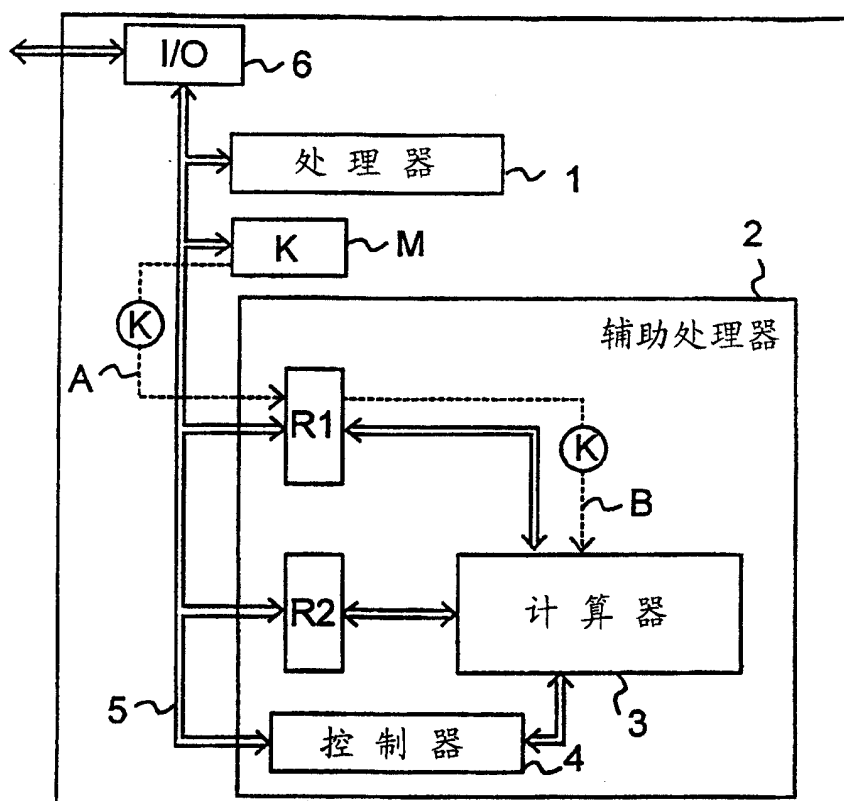
当智能卡与外部装置相连并且要验证智能卡时, 在框 12 中从存储器重新得到编码密钥, 编码密钥被传送给辅助处理器的数据寄存器。在框 13 中, 辅助处理器用编码函数的逆函数为编码密钥解码。接着, 经过解码的密钥, 即密钥, 通过辅助处理器的内部总线被传送给辅助处理器的钥匙寄存器。

在框 15 中, 智能卡从外部装置接收输入。输入通过智能卡的总线被传送给辅助处理器的数据寄存器。在框 16 中, 辅助处理器对智能卡接收的输入产

生一个响应。辅助处理器在预定的计算函数和存储在钥匙存储器中的密钥的基础上产生响应。辅助处理器将响应存储在它的数据寄存器中，响应从该寄存器通过智能卡的总线被发送给外部装置。

如上文所述，智能卡的密钥从来不需要提供给智能卡的总线，因为所有与处理密钥相关的步骤（框 13 至 16）都可以作为辅助处理器的内部操作完成。

应该了解的是，上文中的描述和相关附图只是用来说明本发明。对于熟悉本领域的人而言，很明显，在不偏离本发明所附权利要求的范围和实质的条件下，本发明可以以不同方式被改变和调整。



现有技术

图 1

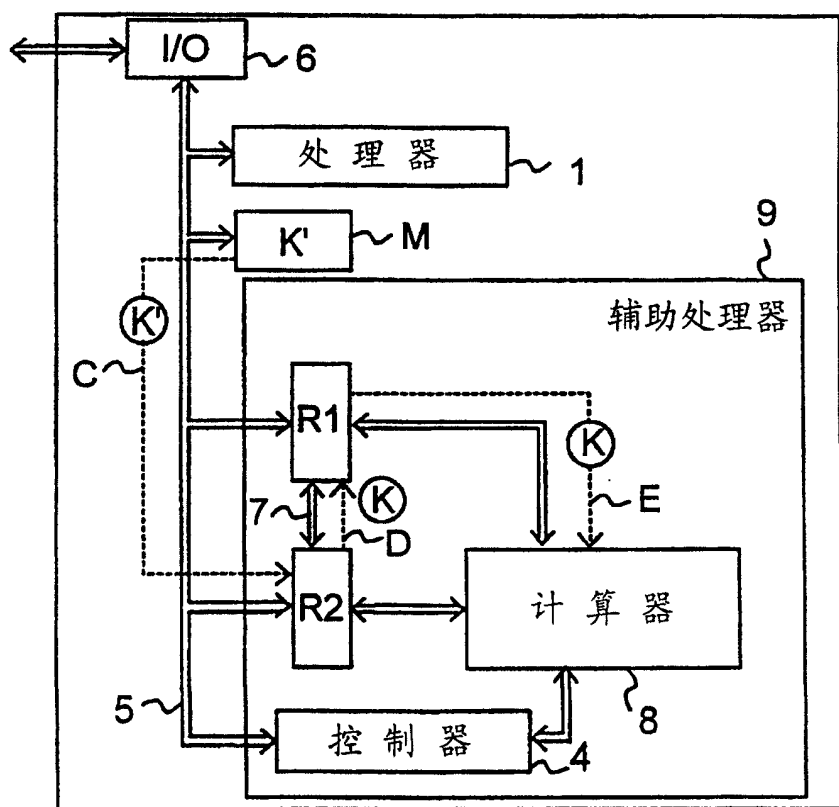


图 2

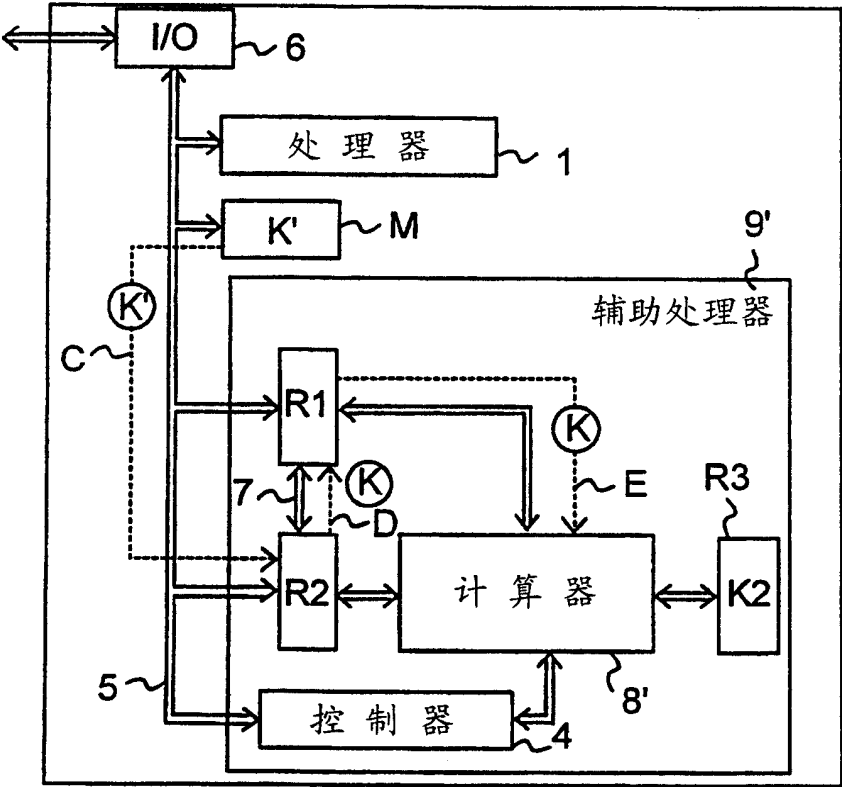


图 3

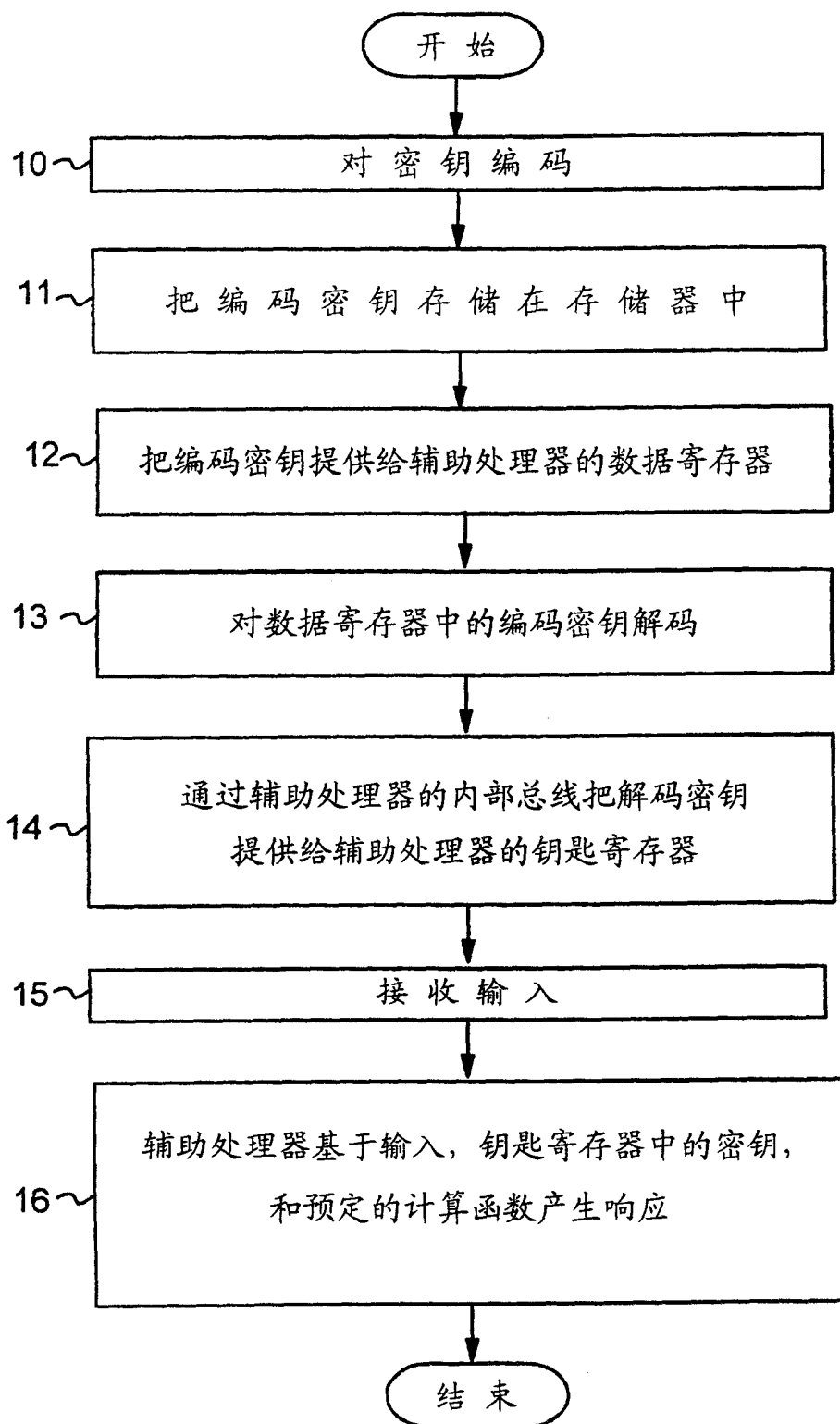


图 4