[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 03814213.9

[45] 授权公告日 2008 年 4 月 23 日

[11] 授权公告号 CN 100383693C

[22] 申请日 2003.5.15 [21] 申请号 03814213.9

[30] 优先权

[32] 2002.6.18 [33] US [31] 10/177,626

[86] 国际申请 PCT/US2003/015359 2003.5.15

[87] 国际公布 WO2003/107151 英 2003.12.24

[85] 进入国家阶段日期 2004.12.17

[73] 专利权人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 E·布里克尔

[56] 参考文献

EP0422757A 1991.4.17

EP0892521A2 1999.1.20

CN1186580A 1998.7.1

EP0869636A2 1998.10.7

APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C. SCHNEIER,47.52,NY: JOHN WILEY & SONS, US. 1996

APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C. SCHNEIER,56.65,NY: JOHN WILEY & SONS, US. 1996

APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C. SCHNEIER B,28.33,176.177,216.217,461.473,518.522,NY: JOHN WILEY & SONS, US. 1996

审查员 唐楹琰

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 程天正 王 勇

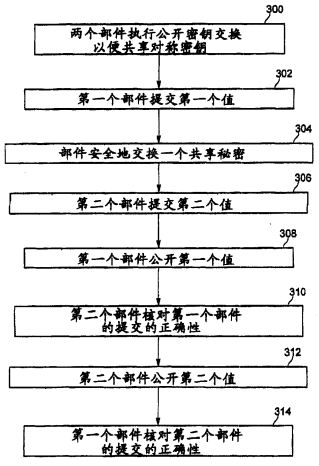
权利要求书 3 页 说明书 13 页 附图 6 页

[54] 发明名称

用于安全地交换对称密钥的系统和方法

[57] 摘要

一种密钥交换协议可以在一个系统的部件之间被执行，诸如在被一台 PC(或者其它计算机系统)执行的计算机程序和一个外围设备之间被执行。 诸如键盘和鼠标的具有用户输入能力和十分有限的显示能力的外围设备，可以被用于确认在所述系统部件之间的密钥交换，这只需要用户输入少量输入数据(例如，键击或鼠标点击)。 在没有对所述系统的可用性的负面影响的情况下，部件之间的安全性可以被增强。 本发明的实施方案有助于阻止“中间人”攻击，其中一个攻击者控制位于某些通信系统部件之间的一个系统部件。



1. 一种在一个系统的第一个和第二个部件之间安全地交换对称密钥的方法，包括:

通过所述第一个部件产生一个非对称密钥对、第一个现时、第二个现时以及第一个散列值，该散列值是根据所述第一个现时、第二个现时以及所述非对称密钥对的公开密钥产生的散列值;

通过第一个部件发送第一个命令、所述第一个散列值、以及所述第一个部件的公开密钥到所述第二个部件;

通过所述第二个部件产生所述对称密钥，使用所述第一个部件的公开密钥加密所述对称密钥，并且响应于接收所述第一个命令，发送所述被加密的对称密钥到所述第一个部件;

通过第一个部件导致所述第一个现时的显示;

通过第二个部件接受被显示的第一个现时的输入;

通过第二个部件产生第三个现时，用所述对称密钥加密所述第三个现时，并根据所述输入到第二个部件的第一个现时、所述第三个现时以及所述被加密的第三个现时产生第二个散列值，并且发送所述第二个散列值到第一个部件;

通过第一个部件发送第二个现时到第二个部件;

通过第二个部件检验根据所述输入到第二个部件的第一个现时、第二个现时以及第一个部件的公开密钥产生的散列值是否匹配于从第一个部件接收的第一个散列值;

当所述散列值匹配时，通过第二个部件启动第二个信任指示器；以及

当所述散列值不匹配时，通过第二个部件启动第三个信任指示器。

2. 如权利要求 1 中所述的方法，还包括:

通过第二个部件发送所述第三个现时到第一个部件；以及

通过第一个部件检验根据第一个现时、第三个现时以及被加密的第三个现时产生的散列值是否匹配于从第二个部件接收的第二个散列值。

3. 如权利要求 1 中所述的方法，其中，所述第二个部件包括一个键盘，所述第一个现时包括随机被产生的第一个数量的字符，该字符代表所述键盘上的键。

4. 如权利要求 1 中所述的方法，其中，所述第二个现时包括预先确定数量的随机被产生的比特。

5. 如权利要求 1 中所述的方法，其中，所述第一个命令包括一个“重置学习”命令，以便使第二个部件进入一种“学习”模式，由此，当第二个部件处于“学习”模式中时，被第二个部件接收的输入数据不被转发到第一个部件。

6. 如权利要求 1 中所述的方法，还包括在接收所述第一个命令之后，在第二个部件上启动第一个信任指示器。

7. 如权利要求 2 中所述的方法，还包括第一个部件显示一个消息，它指示当根据第一个现时、第三个现时以及被加密的第三个现时产生的散列值匹配于从第二个部件接收的第二个散列值时，在所述第一个和第二个部件之间启用安全通信。

8. 如权利要求 2 中所述的方法，还包括第一个部件显示一个消息，它指示当根据第一个现时、第三个现时以及被加密的第三个现时产生的散列值不匹配于从第二个部件接收的第二个散列值时，在所述第一个和第二个部件之间的安全通信被禁止。

9. 一种在处理器和外围设备之间安全地交换对称密钥的系统，包括:

一个处理器，它被配置产生非对称密钥对、第一个现时、第二个现时以及第一个散列值，该散列值是根据所述第一个现时、所述第二个现时以及所述非对称密钥对的公开密钥产生的散列值，并且发送第一个命令、所述第一个散列值、以及所述处理器的公开密钥;

一个外围设备，它被耦合到所述处理器并且被配置来接收第一个命令、第一个散列值、以及所述处理器的公开密钥，并产生一个对称密钥，使用所述处理器的公开密钥来加密所述对称密钥，并且响应于接收第一个命令，发送所述被加密的对称密钥到所述处理器;

其中，所述处理器还被配置通过所述处理器导致显示第一个现时，

并且所述外围设备还被配置接受所述被显示的第一个现时的输入，产生第三个现时，用所述对称密钥加密所述第三个现时，根据所述输入到外围设备的第一个现时、第三个现时以及被加密的第三个现时产生第二个散列值，并且发送所述第二个散列值到所述处理器；并且

其中，所述处理器还被配置发送第二个现时到外围设备；所述外围设备包括第二个信任指示器和第三个信任指示器，并且还被配置检验根据所述输入到外围设备的第一个现时、第二个现时以及处理器的公开密钥产生的散列值是否匹配于从处理器接收的第一个散列值，当所述散列值匹配时，启动第二个信任指示器；而当所述散列值不匹配时，启动第三个信任指示器。

10. 如权利要求 9 中所述的系统，其中，所述外围设备还被配置发送第三个现时到所述处理器；所述处理器还被配置检验根据第一个现时、第三个现时以及被加密的第三个现时产生的散列值是否匹配于从外围设备接收的第二个散列值。

11. 如权利要求 9 中所述的系统，其中，所述外围设备包括第一个信任指示器并且还被配置在接收第一个命令之后启动所述第一个信任指示器。

12. 如权利要求 10 中所述的系统，其中，所述外围设备包括一个键盘，所述信任指示器包括彩色发光二极管。

13. 如权利要求 10 中所述的系统，其中，所述外围设备包括一个键盘，所述第一个现时包括随机被产生的第一个数量的字符，该字符代表所述键盘上的键。

14. 如权利要求 10 中所述的系统，其中，所述外围设备包括一个键盘，所述信任指示器包括可闻音。

15. 如权利要求10中所述的系统，其中，所述外围设备还包括一个非易失性存储器用于存储所述对称密钥。

用于安全地交换对称密钥的系统和方法

技术领域

本发明总地涉及计算机安全性，并且特别涉及在计算机部件之间建立共享加密密钥。

背景技术

一种诸如个人电脑（PC）、工作站、服务器、主机等等的计算机系统，可以包括多个不同的部件。所述系统的一些部件可以是被该系统用于与用户或者另一个系统通信的外围设备。例如，键盘和鼠标通常被用户用于把数据输入到系统中。显示器可以被用于给用户显示信息。网络接口设备可以被用于通过网络把所述计算机系统连接到其它计算机系统或者设备。

一些系统部件可以使用称作“即插即用”协议的协议被耦合到其它部件。例如，通过使用通用串行总线（USB），一个系统可以允许多个外围设备被连接到该系统。当一个新的外围设备被连接到该系统时，系统检测并且识别最近被增加的部件。这种方案一般依靠至少一个主机控制器设备（称为用于使用 USB 的系统的 USB 主机控制器）来控制和监控被连接的外围设备到所述系统的接入。

有时，可能希望不同的系统部件彼此安全地通信。在一些系统中，这可以通过使用众所周知的加密方法来完成。然而，当先于进行安全通信而在系统部件之间交换密钥时，可能会出现困难。通常，交换密钥的动作可能容易受到“中间人”攻击。换句话说，攻击者可以在两个通信部件之间插入一个未被授权的部件或程序，以便截取一个或多个被交换的密钥。攻击者还可能在所述部件之间的通信流中替换其它信息。

在使用 USB 主机控制器的系统中，攻击者在“中间人”攻击期间能够控制 USB 主机控制器并且使在所述系统中的外围设备和处理器之间的安全通信失效。

在一个基于证书的密钥交换协议中，每一方接收另一方公开密钥的证书。随后每一方核对另一方的证书。在这个情况中为系统部件使用这个协议将要求每个外围设备（或者其它系统部件）具有被存储在其上的唯一的公开/专用密钥对。这将增加外围设备的制造成本。此外，为确保证书未被废除，在所述协议被使用时，所述计算机系统将必须是“联机”状态并且通信地被耦合到另一台存储证书废除信息的网络计算机。这可能存在可用性问题。

在一个基于拇指指纹的密钥交换协议中，每一方产生一个公开/专用密钥对并且通过一个安全的信道（例如，“带外”信道）交换公开密钥的散列。在这个情况中，当使用这个协议用于外围设备发送它的公开密钥的散列到处理器时，没有技巧。如果所述处理器将导致它的公开密钥的完整散列显示，则用户可以用外围设备（诸如键盘）输入它，但是这至少将进行27次随机的键击（当使用称为安全散列算法（SHA-1）的众所周知的散列算法时）。此外，处理器将无法知道外围设备已经接收了正确的公开密钥（而不是“中间人”攻击者插入的非法公开密钥）。因此，如果有这种攻击，所述外围设备将知道用户输入的散列与外围设备从处理器接收的公开密钥的散列不匹配，但是处理器不知道这点。解决这个问题的传统方法

是为第二方（所述外围设备）产生一个公开密钥，发送它到第一方（所述处理器），并且随后让双方比较它们的散列。因为所述外围设备无法显示所述外围设备的散列，所以在这种情况下所述方法是行不通的。

因此，需要一种在系统部件之间交换密钥的更好的方法。

发明内容

一种在一个系统的第一个和第二个部件之间安全地交换对称密钥的方法，包括：通过所述第一个部件产生一个非对称密钥对、第一个现时、第二个现时以及第一个散列值，该散列值是根据所述第一个现时、第二个现时以及所述非对称密钥对的公开密钥产生的散列值；通过第一个部件发送第一个命令、所述第一个散列值、以及所述第一个部件的公开密钥到所述第二个部件；通过所述第二个部件产生所述对称密钥，使用所述第一个部

部件的公开密钥加密所述对称密钥，并且响应于接收所述第一个命令，发送所述被加密的对称密钥到所述第一个部件；通过第一个部件导致所述第一个现时的显示；通过第二个部件接受被显示的第一个现时的输入；通过第二个部件产生第三个现时，用所述对称密钥加密所述第三个现时，并根据所述输入到第二个部件的第一个现时、所述第三个现时以及所述被加密的第三个现时产生第二个散列值，并且发送所述第二个散列值到第一个部件；通过第一个部件发送第二个现时到第二个部件；通过第二个部件检验根据所述输入到第二个部件的第一个现时、第二个现时以及第一个部件的公开密钥产生的散列值是否匹配于从第一个部件接收的第一个散列值；当所述散列值匹配时，通过第二个部件启动第二个信任指示器；以及当所述散列值不匹配时，通过第二个部件启动第三个信任指示器。

一种在处理器和外围设备之间安全地交换对称密钥的系统，包括：一个处理器，它被配置产生非对称密钥对、第一个现时、第二个现时以及第一个散列值，该散列值是根据所述第一个现时、所述第二个现时以及所述非对称密钥对的公开密钥产生的散列值，并且发送第一个命令、所述第一个散列值、以及所述处理器的公开密钥；一个外围设备，它被耦合到所述处理器并且被配置来接收第一个命令、第一个散列值、以及所述处理器的公开密钥，并产生一个对称密钥，使用所述处理器的公开密钥来加密所述对称密钥，并且响应于接收第一个命令，发送所述被加密的对称密钥到所述处理器；其中，所述处理器还被配置通过所述处理器导致显示第一个现时，并且所述外围设备还被配置接受所述被显示的第一个现时的输入，产生第三个现时，用所述对称密钥加密所述第三个现时，根据所述输入到外围设备的第一个现时、第三个现时以及被加密的第三个现时产生第二个散列值，并且发送所述第二个散列值到所述处理器；并且，其中，所述处理器还被配置发送第二个现时到外围设备；所述外围设备包括第二个信任指示器和第三个信任指示器，并且还被配置检验根据所述输入到外围设备的第一个现时、第二个现时以及处理器的公开密钥产生的散列值是否匹配于从处理器接收的第一个散列值，当所述散列值匹配时，启动第二个信任指示器；而当所述散列值不匹配时，启动第三个信任指示器。

附图说明

通过下列本发明附图的详细描述，本发明的特点和优点将变得显而易见，其中：

图 1 是一个根据本发明的一个实施方案的系统的示意图；

图 2 和 3 是根据本发明的一个实施方案表示在系统部件之间建立共享加密密钥的流程图；

图 4 和 5 是根据本发明的另一个实施方案表示在系统部件之间建立共享加密密钥的流程图；以及

图 6 是一个本发明的另一个实施方案的流程图。

具体实施方式

本发明的一个实施方案是一个密钥交换协议，它可以在一个系统的部件之间，诸如在正被 PC（或其它计算机系统）的处理器执行的计算机程序和外围设备之间被执行。在本发明的实施方案中，诸如键盘或者鼠标的具有用户输入能力和十分有限的显示能力的外围设备，可以被用于确认在所述系统部件之间密钥的交换，这只需要用户输入少量输入数据（例如，键击或鼠标点击）。根据本发明，在没有对所述系统可用性的负面影响的情况下，部件之间的安全性可以被增强。本发明的实施方案不要求外围设备的任何唯一性，用户只需要输入几个输入数据，并且如果在所述密钥交换协议期间所述外围设备没有接收其它部件（诸如处理器）的正确公开密钥，则所述处理器可以检测这种情况。本发明的实施方案有助于阻止“中间人‘攻击，其中，攻击者控制位于某些通信系统部件之间的一个系统部件。

在说明书中提及本发明的“一个实施方案”或者“实施方案”意味着连同该实施方案被描述的特殊的特点、结构或特征被包括在本发明的至少一个实施方案中。因此，贯穿说明书的不同位置出现的短语“在一个实施方案中”不必全部指同一个实施方案。

图 1 是根据本发明的一个实施方案的系统的高级示意图。系统 10 包括诸如处理器 12 和存储器 14 的各种众所周知的部件。为了清楚，其它部件在图 1 中未被显示。使用一个桥接器/存储器控制器 16，处理器 12 和存储

器 14 可以被通信地耦合。所述桥接器/存储器控制器可以被耦合到图形控制器 18。所述图形控制器在显示器 20 上控制显示数据的输出。在一个实施方案中，在所述处理器、图形控制器和显示器之间的通信包括一条受托信道，这样，对手或攻击者不能读取或修改在显示器上被显示的数据。桥接器/存储器控制器 16 可以被耦合到被表示为线 22 的一条或多条总线。一个通信地被耦合到一条或多条总线的设备可以是总线主机控制器 24。当所述总线之一是通用串行总线（USB）时，所述总线主机控制器可以是一个 USB 主机控制器。

当使用一条 USB 时，多个设备可以被耦合到该总线。例如，诸如键盘 26 和鼠标 28 的用户输入设备可以被包括在所述系统中用于提供输入数据。虽然在图 1 中显示了键盘和鼠标，但是设想本发明也可以适合其它外围设备的使用。在本发明的实施方案中，被用于安全地与其它系统部件通信的输入设备包括至少一个信任指示器。例如，键盘 26 可以包括至少一个信任指示器 30，并且鼠标 28 可以包括至少一个信任指示器 32。在一个实施方案中，所述至少一个信任指示器包括多个彩色发光二极管（LED）。在一个实施方案中，具有三种明显的颜色（诸如琥珀色、绿色和红色）的 LED 可以被用于代表三种不同的状态。下面将解释说明不同的颜色和状态的操作意义。在其它的实施方案中，指示外围设备当前状态的其它方法可以被用来代替彩色 LED，诸如在一个液晶显示器（LCD）上的多可闻音、符号，或者其它明显的指示器。

在本发明的实施方案中，外围设备（例如，键盘和/或鼠标）不必根据预置的唯一的密钥或数值被制造。然而，根据本发明的实施方案的外围设备必须包括用于不对称密码术、对称密码术和散列函数的能力。具有随机数发生器和非易失性存储器的外围设备增强了用户的经验，但不是必要的。

在图 1 的高级示意图中被描述的系统中，可能希望在正被所述处理器执行的程序和诸如键盘 26 的外围设备之间的通信是安全的。用于这种安全通信的一种机制是通过使用已知的对称密码方法来加密和解密在所述部件之间被通信的数据。在这种通信开始之前，一个对称密钥必须在所述部件

之间被交换。如图 1 中所示，在所述外围设备和处理器之间的通信路径包括所述总线主机控制器。然而，作为“中间人”攻击的一部分，攻击者可以控制所述总线主机控制器，并且可能随后能够读取和/或修改总线业务量。所述攻击者在所述总线上传输期间能够读取对称密钥并且解密在所述总线上的后来的业务量。

非对称公开密钥密码术可以被用于在所述交换期间保护所述对称密钥。第一个部件可以使用第二个部件的公开密钥来加密一个对称密钥并且发送所述被加密的对称密钥到第二个部件。第二个部件随后能够使用第二个部件的专用密钥来解密被加密的对称密钥。为了以这种方法使用非对称密钥以便在所述对称密钥传输上消除可能的攻击，最初，第二个部件（例如，处理器）的公开密钥必须被安全地传输到第一个部件（例如，外围设备）。如果所述公开密钥在这个通信路径上使用典型的方法被传输，则攻击者在没有被检测的情况下可以用一个非法的公开密钥来截取和代替所述公开密钥。为阻止这种行为，本发明实施方案的密钥交换协议可以被用于最初在所述部件之间建立安全通信。

图 2 和 3 是根据本发明的一个实施方案表示在系统部件之间建立共享加密密钥的流程图。在所示的实施方案中，讨论了在处理器 12 和外围设备（诸如键盘 26 或鼠标 28）之间的通信，不过，这种方法可以被应用于在其它系统部件之间的通信。在框 100，所述处理器根据已知的非对称密码术技术产生一个专用/公开密钥对。注意，在此属于所述处理器的动作可以通过被所述处理器执行的计算机程序被实现。而且，属于所述外围设备的动作可以通过驻留在所述外围设备中的电路、固件和/或软件的任何组合被实现。所述处理器把所述密钥对存储在存储器中用于稍后使用。在框 102，所述处理器产生一个短现时（nonce）（SN）和一个长现时（LN）。一个现时可以是一个由随机数发生器随机产生的比特序列。在一个实施方案中，所述短现时可以包括四个或更多的字符，每个字符包括至少六个比特。当所述外围设备是一个键盘时，每个字符可以代表键盘上的任何键。在其它的实施方案中，其它数量的比特可以被用于所述短现时。在一个实施方案中，所述长现时可以包括随机被产生的 160 个比特。在其它的实施方案中，其

它数量随机被产生的比特可以被用于所述长现时。在框104，所述处理器通过应用一种散列算法，使用所述短现时、长现时以及在框 100 中被产生的公开密钥产生第一个散列值作为输入信号。在一个实施方案中，SHA-1 散列算法可以被使用，不过，在其它的实施方案中，其它的散列算法也可以被使用（例如，MD5、等等）。

在框 106，所述处理器发送第一个命令、第一个散列值和所述处理器的公开密钥到所述外围设备。这个数据可以在一个或多个单独的传送中被发送到所述外围设备。假定对手能够选择防止这些数据传送到所述外围设备，或者修改它们。在此被描述的剩余的动作通常假定所述数据传送发生（尽管它们可能被攻击者修改）。在一个实施方案中，所述第一个命令可以被称为“重置学习”命令。所述外围设备（诸如键盘 26 或鼠标 28）收到这个命令，使所述外围设备进入一种“学习”模式并且激活驻留在所述外围设备中的信任指示器 30 的一部分。对于所述系统用户，所述信任指示器充当所述外围设备处于“学习”模式的明显的符号。

在一个实施方案中，所述信任指示器可以是一个彩色 LED。被选择的 LED 颜色（诸如琥珀色 LED）可以被照亮以便指示用户所述外围设备现在处于“学习”模式或状态。在所述“学习”模式中，所述外围设备执行在此被描述的密钥交换协议，并且除了在剩余的协议中指出的之外，直到所述协议被完成，不转发任何由用户输入的输入数据到总线主机控制器 24。注意，所述外围设备包括软件、固件和/或电路用于接收第一个命令、解释该命令并且启动信任指示器用于用户感知。

在框 108，响应于接收“重置学习”命令，所述外围设备产生一个对称密钥（被用作用于随后通信的会话密钥），使用所述处理器的公开密钥（在框 106 中被接收的）加密所述对称密钥，并且发送被加密的对称密钥到所述处理器。所述对称密钥的产生可能在所述外围设备中需要一个随机数发生器。在这个框期间，可以有一个通过控制所述总线主机控制器作为一个“中间人”来操作的攻击者。假定，该攻击者能够选择防止所述被加密的对称密钥的数据传送到所述处理器，或者修改它。剩余动作假定所述数据传送发生（尽管它可能被修改）。在一个实施方案中，所述对称密钥

可以是一个具有128个比特的高级加密标准（AES）密钥，不过其它不同类型和长度的对称密钥也可以被使用。

在框110，一旦所述处理器接收了被加密的对称密钥，则处理器12导致在显示器20上使用一些形式的受托输出显示所述短现时和可能的指令。在框112，用户看到所述短现时和被启动的信任指示器的显示。例如，在显示器上的正文可以指示用户被启动的信任指示器的意义以及根据被显示的短现时做什么。此时，所述信任指示器仍然为所述外围设备指示“学习”模式或状态。根据所述短现时和被启动的信任指示器的显示，用户使用所述外围设备输入所述短现时。例如，用户可以注意琥珀色LED被照亮，并且按照显示器上的指令输入所述短现时。当所述外围设备是一个键盘时，用户键入所述短现时。当所述外围设备是一个鼠标时，用户可以按照方向操作鼠标指向显示屏的某些区域和/或以符合于所述短现时的顺序按压一次或多次鼠标按钮。本领域的技术人员将认识到其它的输入机制也可以被使用。因为所述外围设备是在“学习”模式中，所以它不转发用户的输入数据到所述总线主机控制器。

在框114，所述外围设备产生一个外围设备现时（PN）并且用所述对称密钥加密所述外围设备现时来构成加密（PN）。所述外围设备现时可以是任何随机被产生的值。这可以在所述外围设备中通过随机数发生器被完成，或者它可以通过要求用户输入随机的键击（当所述外围设备是一个键盘时）一小段时间被完成。对于鼠标，随机数可以通过要求用户移动一会儿鼠标并且捕获关于鼠标移动的输入数据被产生。在图3上的框116，处理会通过连接器A而继续。在框116，所述外围设备通过应用一种散列算法，使用所述短现时（在框112被从用户接收的）、外围设备现时、和加密（PN）来产生第二个散列值作为输入参数。在一个实施方案中，SHA-1散列算法可以被使用。在框118，所述外围设备发送第二个散列值到所述处理器。注意，在消除这个方案的努力中，攻击者（例如，所述“中间人”）将必须在看到所述短现时之前提交所述第二个散列值。

下一步，在框120，处理器在接收第二个散列值之后发送所述长现时到外围设备。在各种实施方案中，框114和120的实现可以按所示的顺序

或者相反的顺序被执行。此时，所述外围设备已经从处理器接收了长现时和处理器的公开密钥，并且从用户接收了短现时。在框122，所述外围设备检验所述短现时、长现时以及处理器公开密钥的散列是否匹配于被所述处理器发送到外围设备的第一个散列值（在框106）。相同的散列算法必须被使用。例如，如果SHA-1散列算法在框104被使用，则随后SHA-1散列算法必须在框122被使用。

如果从所述处理器被接收的第一个散列值等于所述外围设备计算的散列值，则随后所述外围设备被保证所述外围设备实际上接收了所述处理器的合法公开密钥。当所述散列值匹配时，在框124，所述外围设备启动信任指示器来指示第二种模式或状态（例如，“OK”状态）。例如，所述外围设备可以照亮一个绿色LED，指示用户处理正在以一种被授权的方式进行并且来自所述设备的输入可以被信任。如果所述散列值不匹配，则随后所述外围设备知道它没有从所述处理器接收可信的公开密钥。在框124，所述外围设备随后可以启动所述信任指示器来指示第三种模式或状态（例如，错误状态）。例如，所述外围设备可以照亮一个红色LED，指示用户一些未被授权的活动已经发生并且在系统部件之间的通信是不安全的。在其中只有两种颜色的LED被使用的另一个实施方案中，当一个错误被检测到时，可以使琥珀色灯闪亮。错误处理操作随后可以在所述系统中被启动。

此时，所述外围设备知道它是否已经从所述处理器接收了可信的公开密钥，但是处理器不知道外围设备是否接收了正确的密钥。因此，在框126，外围设备发送在框114被产生的所述外围设备现时到处理器。在框128，所述处理器计算在框102被产生的短现时、在框126被从所述外围设备接收的外围设备现时以及加密（PN）（由所述处理器通过用所述对称密钥加密所述外围设备现时被建立，通过使用所述处理器的专用密钥解密在框108被接收的被加密的对称密钥，所述处理器可以得到所述对称密钥）的散列值。如果在框106中SHA-1散列算法被使用，则随后所述处理器在框128中使用SHA-1算法。所述处理器把被计算的散列值和在框118被从所述外围设备接收的第二个散列值比较。如果所述散列值匹配，则随后处理器知道外围设备接收了所述处理器的公开密钥并且进而安全通信被启动。在一

个实施方案中，所述处理器可以在显示器上显示一个密钥交换完成消息以便通知用户安全通信现在被启动。如果所述散列值不匹配，则错误处理可以被启动和/或安全通信被禁止。例如，所述处理器可以拒绝从所述外围设备接受任何受托输入数据。此外，一个警告消息可以被输出到显示器，通知用户来自所述外围设备的输入不能被信任。

如果所述外围设备包括一个非易失性存储器，则上述方法只需要被执行一次，并且随后所述对称密钥可以被永久地存储在所述外围设备中以及所述处理器可接入的存储器中。在一个实施方案中，所述对称密钥可以被用于加密和解密后来在系统部件之间的通信。在另一个实施方案中，所述对称密钥可以被用于加密新的会话密钥，它们随后被用于实际被加密的在所述外围设备和处理器之间的通信。在会话密钥已经被产生之后，所述外围设备可以建立一个专用/公开密钥对，用所述对称密钥加密所述公开密钥和一个机器鉴别码（MAC），并且发送所述被加密的公开密钥和MAC到处理器。随后，如果所述外围设备包括一个非易失性存储器，则所述外围设备的专用密钥可以被永久地存储在所述外围设备中，并且所述外围设备的公开密钥可以被存储在所述处理器可接入的存储器中。

虽然在此已经描述了一个特殊的动作顺序，但是在各种实施方案中，不同的动作可以被以不同的顺序执行来达到相同的结果。

在其它实施方案中，可以对上述协议进行各种改变。例如，在框 104 的动作和在框 122 中的检验在框 108 之后可以被一个新框代替，其中，所述处理器使用被接收的对称密钥产生所述短现时、长现时以及所述长现时的加密的散列值，并且在框 122 中的检验将是根据这个被修订的散列值的检验。在这个实施方案中，被所述处理器和外围设备执行的检验可以是相同的。

当所述外围设备是一个鼠标时，困难可能跟着而来。因为由所述处理器产生的短现时和由用户使用鼠标输入的现时可能不完全相同，这是因为鼠标在按钮的范围内，而不是一个确切的位置被点击，在框 122 处理器可以连同长现时一起发送它的短现时的版本，并且在框 126 鼠标可以发送它的短现时版本到所述处理器，并且每一步将检验它们是结束的。

假定被使用的散列算法是可信赖的，攻击者在攻击本方法中能够采用的最佳方法是尽力猜测所述短现时。当使用 SHA-1 散列算法时，战胜本方法的机会是 2^（6*v）分之一，其中 v 是短现时中的字符数，并且假定每个字符有 6 个比特。因此，当在所述短现时中只有 4 个字符被使用时，战胜本方法的机会是 1600 万分之一。使用四个字符作为短现时为本发明提供了好的安全性，而且需要用户把很少的字符数输入到系统中，这样在可用性上有很小的影响。

在另一个实施方案中，交换对称密钥的方法可以根据众所周知的迪非-海尔曼（Diffie-Hellman）方法。根据迪非-海尔曼方法，所述对称密钥根据在所述协议期间被发送的消息被产生。在迪非-海尔曼方法被用于产生共享对称密钥之后，所述处理器和外围设备将确定它们具有相同的对称密钥。图 4 和 5 说明这个实施方案。

在图 4 中所示的协议中，在框 208，所述处理器构成对所述短现时、长现时和共享对称密钥的提交，其中，在外围设备已经接收了被散列值之后，处理器不能改变这些值，因此所述处理器已经“提交”这些值。通过公开在所述提交中的秘密信息，处理器对外围设备开放所述提交。因为外围设备已经具有所述共享对称密钥，所述外围设备只需要获得所述短现时和长现时的值。通过不能被任何对手观察的安全方法这个步骤的一部分可以被进行。这在框 210 和 212 进行。所述长现时在框 220 被揭示。这使外围设备确定所述处理器具有相同的对称密钥。相反地，在所述处理器已经完全开放处理器的值之前所述外围设备能够提交一个值。这在框 214、216、218 被进行。如在框 226 中所示，所述外围设备随后开放这个提交。这使处理器确定所述外围设备具有相同的对称密钥。

这个更普通协议的一个实施方案在图 6 中被描述。在框 300，通过一个诸如迪非-海尔曼密钥交换的过程或者使用一种公开密钥加密算法，所述第一个部件和第二个部件交换一个共享秘密（例如，一个对称密钥）。在框 302，第一个部件给第二个部件提交第一个值，诸如在框 202、206 和 208 中被描述的机制。在框 304，所述部件通过诸如在框 204 的机制安全地交换一个共享秘密。在框 308，第一个部件通过诸如在框 210、212 和 220 中的

机制公开所述第一个值。在框 310，第二个部件通过诸如在框 222 中的机制核对第一个部件的提交的正确性。这个实施方案也可以包括所述第二个部件的相反的提交和公开。在框 306 中，第二个部件通过诸如在框 214、216 和 218 中被使用的机制提交第二个值。注意，如果这个相反的提交被使用，则它对于第二个提交在所述第一个部件已经揭示它的提交之前出现是重要的。在框 312 中，第二个部件通过诸如在框 226 中被使用的机制公开第二个值。在框 314，第一个部件通过诸如在框 228 中被描述的机制核对所述提交和所述提交的公开的正确性。

如上面描述的，本发明的实施方案在一个处理器和一个外围设备之间建立了一个共享加密密钥，即使其中有一个攻击者控制所述总线主机控制器。所述密钥交换协议具有一个优点，即，在所述外围设备上它不要求任何唯一性，用户只需要输入几个输入选择（例如，键击），并且如果所述外围设备未接收正确的处理器公开密钥，则处理器将知道该结果。

在此被描述的技术未被限于任何特殊的硬件或软件配置；它们可以在任何计算或处理环境中发现适用性。该技术可以在硬件、软件或两者的组合中被实现。所述技术可以在诸如移动或固定计算机、便携计算机、个人数字助理、机顶盒、蜂窝电话和寻呼机、以及其它电子设备的可编程机器上执行的程序中被实现，每个机器包括一个处理器、一个所述处理器可以读取的存储媒体（包括易失性和非易失性存储器和/或存储单元）、至少一个输入设备、以及一个或多个输出设备。程序代码被应用于使用所述输入设备输入的数据以便执行所描述的功能并且产生输出信息。所述输出信息可以被应用于一个或多个输出设备。本领域的普通技术人员之一可以理解本发明可以用包括多处理机系统、小型计算机、主计算机等等的各种计算机系统配置被实践。本发明也可以在分布式计算环境中被实践，在所述环境中，任务可以用通过通信网络被链接的远程处理设备被执行。

每个程序可以在一个高级过程或面向对象程序设计语言中被实现以便与处理系统通信。然而，如果希望，程序也可以在汇编或机器语言中被实现。总之，所述语言可以被编译或者解释。

程序指令可以被用于促使根据所述指令被编程的一个通用或专用处理

系统执行在此被描述的操作。可替代地，所述操作可以通过包括用于执行所述操作的硬布线逻辑的特定硬件部件被执行，或者通过被编程的计算机部件和定制的硬件部件的任何组合被执行。在此被描述的方法可以被提供作为一种计算机程序产品，它可以包括具有被存储在其上的指令的机器可读取的媒体，这些指令可以被用于编程处理系统或者其它电子设备以便执行该方法。在此被使用的术语“机器可读取的媒体”应该包括能够存储或编码用于被所述机器执行的一系列指令并且导致所述机器执行在此被描述的任何一个方法的任何媒体。术语“机器可访问的媒体”因此包括，但是不限于，固态存储器、光和磁盘、以及编码一个数据信号的载体。而且，在现有技术中，用采用一个动作或者导致一个结果的种种形式（例如，程序、过程、进理、应用、模块、逻辑等等）谈到软件是常见的。这些表达式仅仅是陈述处理系统导致处理器执行产生一个结果的动作的软件执行的简略方式。

尽管已经参考说明性实施方案描述了本发明，但是这种描述并非限制性的。所述实施方案的各种修改，以及本发明的其它实施方案，对于本发明所属本领域的技术人员是显而易见的，它们属于本发明的精神和范围。

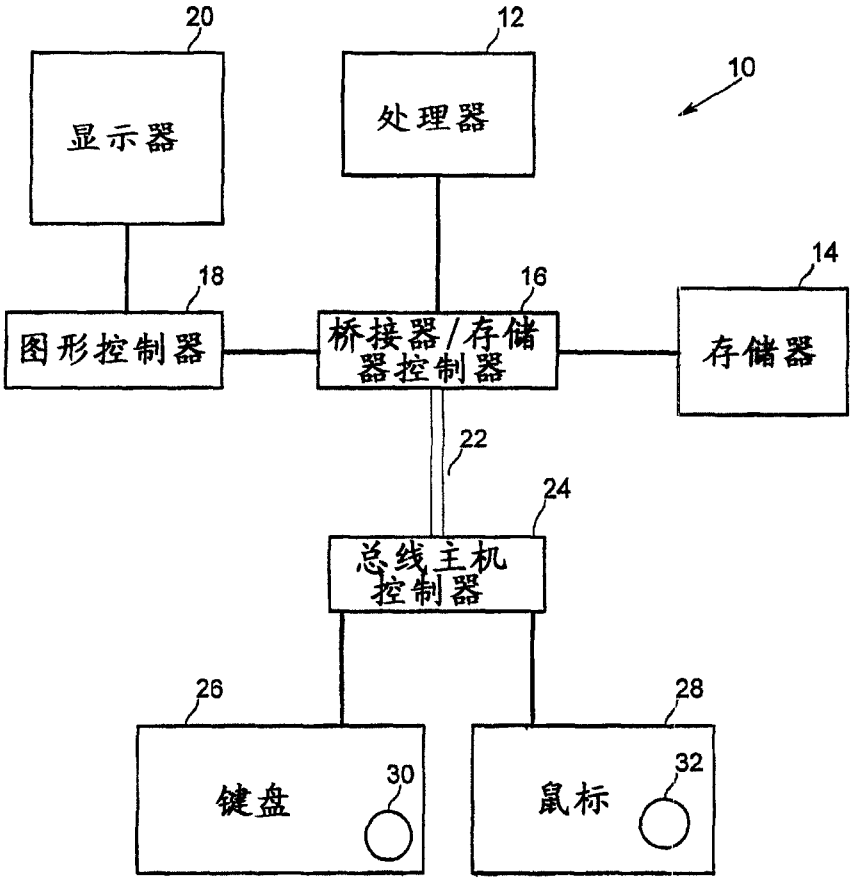

20
显示器
12
处理器
10
14
18
16
图形控制器
桥接器/存储器控制器
存储器
22
24
总线主机控制器
26
28
键盘
30
鼠标
32

图 1

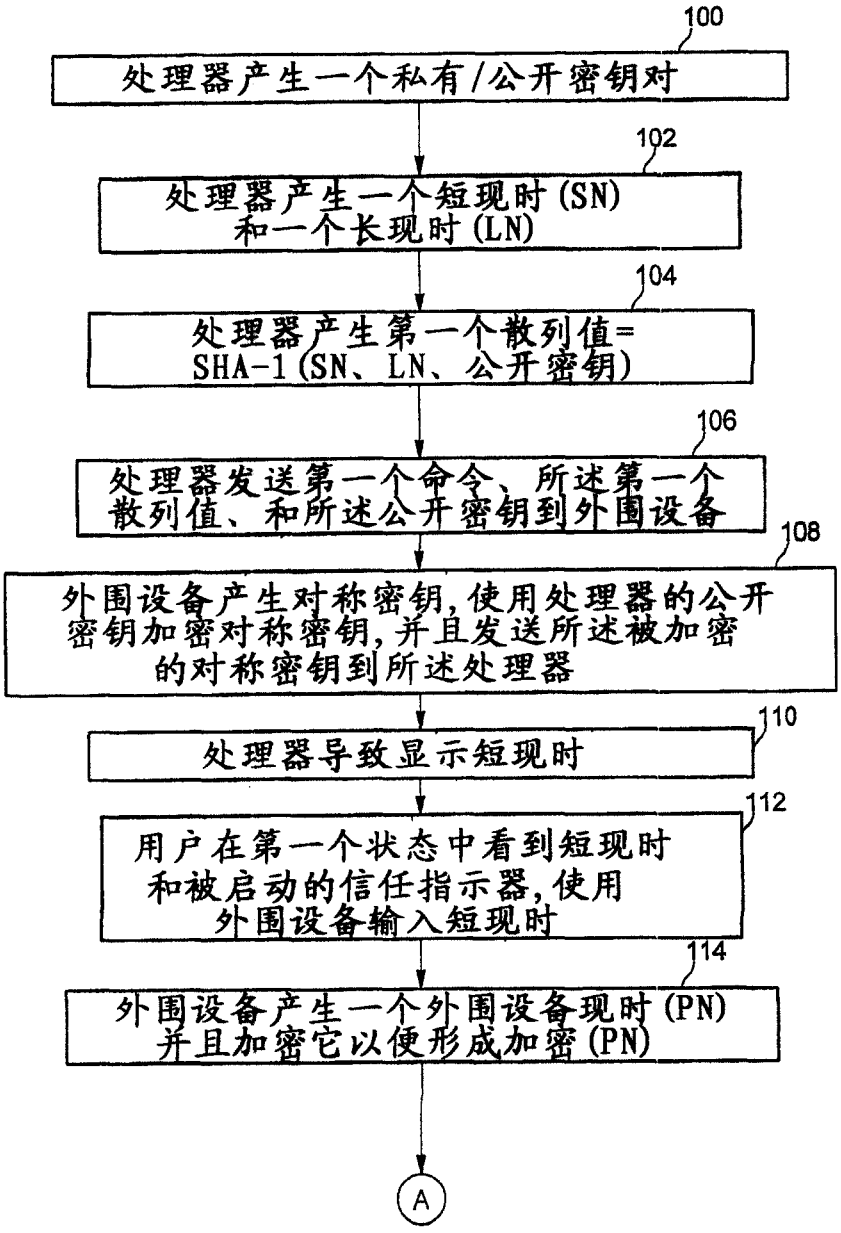

100
处理器产生一个私有/公开密钥对
102
处理器产生一个短现时(SN)
和一个长现时(LN)
104
处理器产生第一个散列值=
SHA-1(SN、LN、公开密钥)
106
处理器发送第一个命令、所述第一个
散列值、和所述公开密钥到外围设备
108
外围设备产生对称密钥,使用处理器的公开
密钥加密对称密钥,并且发送所述被加密
的对称密钥到所述处理器
110
处理器导致显示短现时
112
用户在第一个状态中看到短现时
和被启动的信任指示器,使用
外围设备输入短现时
114
外围设备产生一个外围设备现时(PN)
并且加密它以便形成加密(PN)
A

图 2

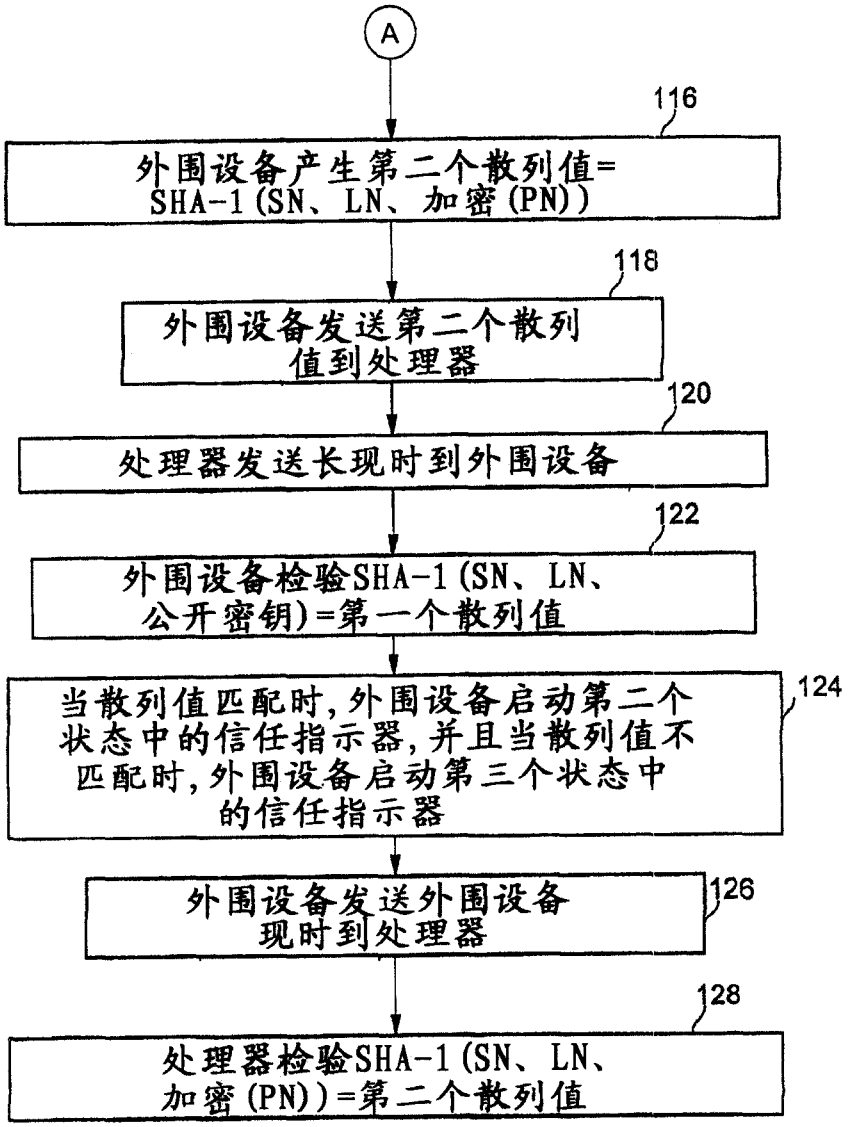

A
116
外围设备产生第二个散列值=
SHA-1(SN、LN、加密(PN))
118
外围设备发送第二个散列
值到处理器
120
处理器发送长现时到外围设备
122
外围设备检验SHA-1(SN、LN、
公开密钥)=第一个散列值
124
当散列值匹配时,外围设备启动第二个
状态中的信任指示器,并且当散列值不
匹配时,外围设备启动第三个状态中
的信任指示器
126
外围设备发送外围设备
现时到处理器
128
处理器检验SHA-1(SN、LN、
加密(PN))=第二个散列值

图 3

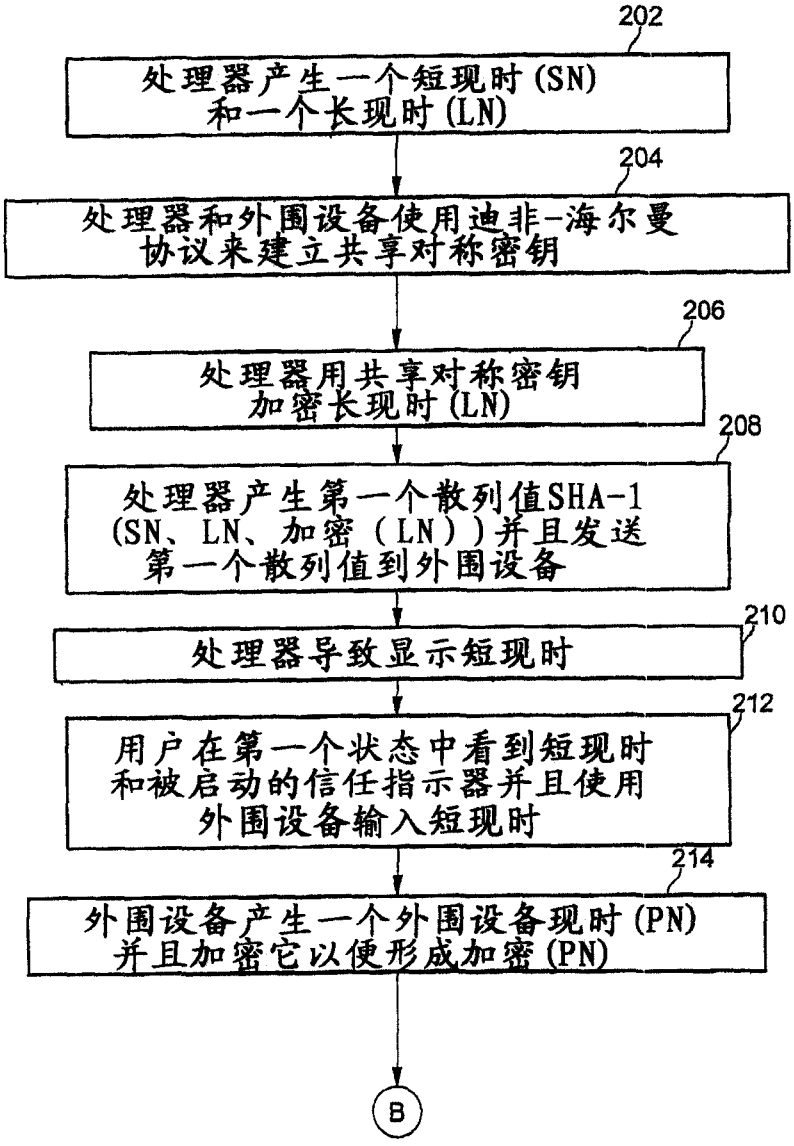

202
处理器产生一个短现时(SN)
和一个长现时(LN)
204
处理器和外围设备使用迪非-海尔曼
协议来建立共享对称密钥
206
处理器用共享对称密钥
加密长现时(LN)
208
处理器产生第一个散列值SHA-1
(SN、LN、加密(LN))并且发送
第一个散列值到外围设备
210
处理器导致显示短现时
212
用户在第一个状态中看到短现时
和被启动的信任指示器并且使用
外围设备输入短现时
214
外围设备产生一个外围设备现时(PN)
并且加密它以便形成加密(PN)
B

图 4

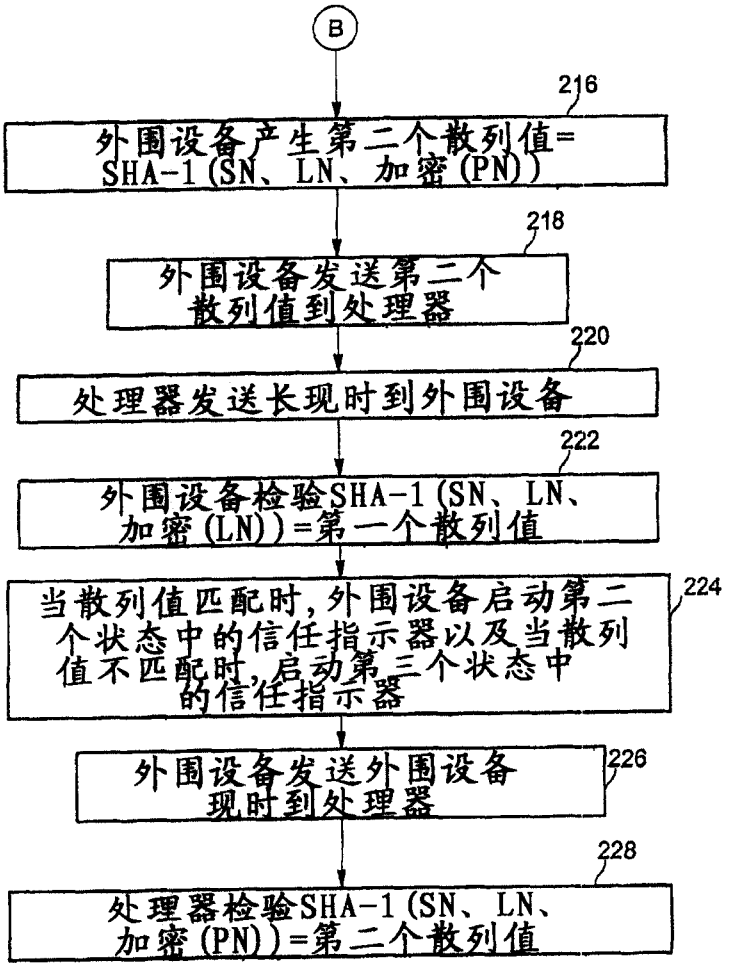

B
216
外围设备产生第二个散列值=
SHA-1(SN、LN、加密(PN))
218
外围设备发送第二个
散列值到处理器
220
处理器发送长现时到外围设备
222
外围设备检验SHA-1(SN、LN、
加密(LN))=第一个散列值
224
当散列值匹配时,外围设备启动第二
个状态中的信任指示器以及当散列
值不匹配时,启动第三个状态中
的信任指示器
226
外围设备发送外围设备
现时到处理器
228
处理器检验SHA-1(SN、LN、
加密(PN))=第二个散列值

图 5

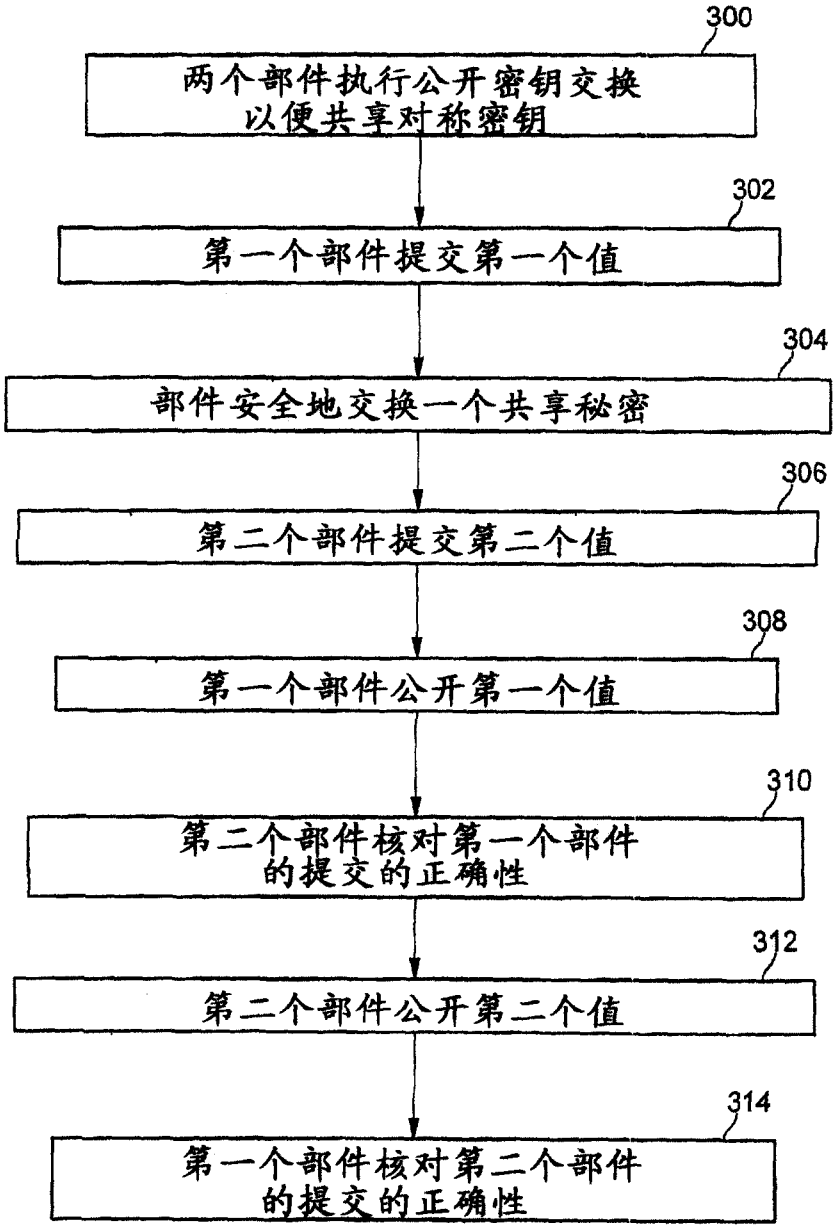

300
两个部件执行公开密钥交换
以便共享对称密钥
302
第一个部件提交第一个值
304
部件安全地交换一个共享秘密
306
第二个部件提交第二个值
308
第一个部件公开第一个值
310
第二个部件核对第一个部件
的提交的正确性
312
第二个部件公开第二个值
314
第一个部件核对第二个部件
的提交的正确性

图 6