(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101044491 B
(45)授权公告日 2010.04.14

(21)申请号 200580035981.2

(22)申请日 2005.12.28

(30)优先权数据
11/287,886 2005.11.28 US

(85)PCT申请进入国家阶段日
2007.04.20

(86)PCT申请的申请数据
PCT/JP2005/024268 2005.12.28

(87)PCT申请的公布数据
WO2007/060752 EN 2007.05.31

(73)专利权人 松下电工株式会社
地址 日本大阪

(72)发明人 布赖恩特·伊斯特汉

(74)专利代理机构 北京林达刘知识产权代理事务所 11277
代理人 刘新宇 权鲜枝

(51)Int.Cl.
G06F 21/24(2006.01)

(56)对比文件
US 5745576 A,1998.04.28, 说明书第1栏第13－54行,第5栏第10－45行,第6栏第18行－第9栏第41行,第10栏第15－31行、附图1－6.
US 6711263 B1,2004.03.23, 第6栏第7－52行,第8栏第12－34行.
EP 0387599 A2,1990.09.19, 第6栏第38行－第8栏第31行,第11栏第9－31行.
US 2003/0044020 A1,2003.03.06, 第5,13－14, 39－48段.
US 5144664 A,1992.09.01, 全文.
WO 99/21094 A2,1999.04.29, 第14页第1－19行,第16页第12行－第18页第21行.
Stephen R. Hanna.Configuring Security Parameters in Small Devices.IETF Standard-Working-Draft
draft-hanna-zeroconf-seccfg-00.txt.2002, 第1-4节.

审查员 杜军

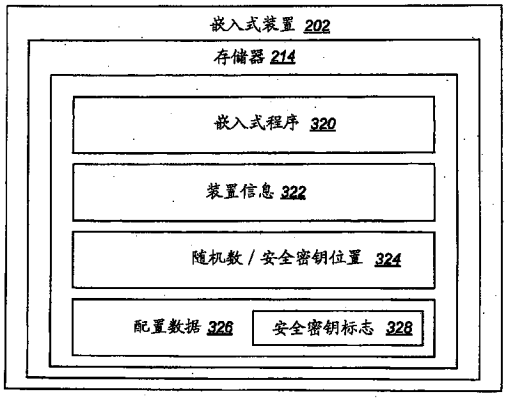
权利要求书 1 页 说明书 11 页 附图 8 页

(54)发明名称

便于对嵌入式装置发布安全密钥的系统和方法

(57)摘要

嵌入式装置上的嵌入式程序判断是否对嵌入式装置分配了安全密钥。如果没有分配安全密钥，则嵌入式程序使用由嵌入式装置的厂商提供的、存储在嵌入式装置的存储器中的随机数来获得嵌入式装置的安全密钥。将安全密钥存储在嵌入式装置的存储器中。安全密钥用于建立与其它装置的安全连接。



CN 101044491 B

1. 一种便于对嵌入式装置发布安全密钥的方法，所述方法由所述嵌入式装置上的嵌入式程序来实现，所述方法包括：

判断是否已经对所述嵌入式装置分配了安全密钥，其中判断是否分配了安全密钥包括：判断存储在所述嵌入式装置的配置数据中的安全密钥标志的值；

如果没有分配所述安全密钥：

使用由所述嵌入式装置的厂商提供的、存储在所述嵌入式装置的存储器中的随机数来获得所述嵌入式装置的所述安全密钥；

将所述安全密钥写入到所述嵌入式装置的所述存储器中，并覆盖所述随机数，以此存储所述安全密钥，并且将所述安全密钥标志的值改变为表示已经对所述嵌入式装置分配了安全密钥的情形；

保存所述安全密钥，使用所述安全密钥来建立与其它装置的安全连接；以及

判断是否需要改变安全密钥，在不需要改变安全密钥的情况下，继续使用所述安全密钥来建立安全连接，

在判断为需要改变安全密钥的情况下，

停止使用所述安全密钥来建立安全连接，并且将所述安全密钥标志的值改变为表示没有对所述嵌入式装置分配安全密钥的情形，

随后，将所述安全密钥用作新的随机数来获取新的安全密钥。

便于对嵌入式装置发布安全密钥的系统和方法

技术领域

[0001] 本发明一般地涉及嵌入式装置。更具体地说，本发明涉及便于对嵌入式装置发布安全密钥的系统和方法。

背景技术

[0002] 计算机和通信技术持续以快速的步伐前进。实际上，计算机和通信技术涉及人们日常生活的很多方面。例如，现今消费者正在使用的很多装置，在装置的内部具有小型计算机。这些小型计算机具有不同的大小和精密度。这些小型计算机包括从一个微型控制器到全功能的完整计算机系统的每一种。例如，这些小型计算机可能是例如微型控制器的单片计算机、例如控制器的单板型计算机、例如 IBM-PC 兼容机的典型台式计算机等。

[0003] 计算机一般具有一个或多个在计算机核心的处理器。处理器通常与不同的外部输入和输出相互连接，用来管理特定计算机或装置。例如，可以将自动调温器中的处理器连接到用于选择温度设置的按钮、连接到暖炉或空调以改变温度、连接到温度传感器以读取当前温度并将其显示在显示器上。

[0004] 很多电器、装置等包括一个或多个小型计算机。例如，自动调温器、暖炉、空调系统、电冰箱、电话、打字机、汽车、自动售货机、及很多不同种类的工业设备，现在一般在其内部具有小型计算机或处理器。计算机软件使这些计算机的处理器运行并指示处理器如何执行某个任务。例如，在自动调温器上运行的计算机软件可以在达到特定温度时使空调停止运行，或可以在需要时打开加热器。

[0005] 通常将作为装置、电器、工具等的一部分的这些种类的小型计算机称为嵌入式装置或嵌入式系统。（这里，术语“嵌入式装置”和“嵌入式系统”可互换使用。）嵌入式系统通常指作为更大系统的一部分的计算机硬件和软件。嵌入式系统可以不具有例如键盘、鼠标、和 / 或监视器的典型的输入和输出装置。通常，在每个嵌入式系统的核心，是一个或多个处理器。

[0006] 照明系统可以包含嵌入式系统。嵌入式系统可以用于监视并控制照明系统的效果。例如，嵌入式系统可以提供调暗照明系统内灯的亮度的控制。作为选择，嵌入式系统可以提供增加灯的亮度的控制。嵌入式系统可以对照明系统内的各灯提供启动特定的照明模式的控制。可以将嵌入式系统连接到照明系统内的各开关。这些嵌入式系统可以指示开关对各灯或整个照明系统通电或断电。类似地，可以将嵌入式系统连接到照明系统内的各灯。通过嵌入式系统可以控制每一个独立的灯的亮度或电源状态。

[0007] 安全系统也可以包含嵌入式系统。嵌入式系统可以用来控制组成安全系统的各安全传感器。例如，嵌入式系统可以提供对每个安全传感器自动通电的控制。可以将嵌入式系统连接到各安全传感器中的每一个。例如，可以将嵌入式系统连接到运动传感器。如果检测到运动，则嵌入式系统可以自动给独立的运动传感器通电，并提供启动运动传感器的控制。启动运动传感器可以包括提供给位于运动传感器内的 LED 通电、从运动传感器的输出端口输出警报等指令。嵌入式系统还可以连接到监视门的传感器。当门被打开或关闭时，嵌入

式系统可以对监视门的传感器提供指令以使其启动。类似地，可以将嵌入式系统连接到监视窗户的传感器。如果窗户被打开或关闭，则嵌入式系统可以提供启动监视窗户的传感器的指令。

[0008] 一些嵌入式系统还可以用来控制例如蜂窝式电话的无线产品。嵌入式系统可以提供给蜂窝式电话的LED显示器通电的指令。嵌入式系统还可以启动蜂窝式电话内的音频扬声器从而向用户提供关于蜂窝式电话的音频通知。

[0009] 家用电器也可以包含嵌入式系统。家用电器可以包括在传统厨房中通常使用的电器，例如，炉、电冰箱、微波炉等。家用电器还可以包括与用户的健康和舒适相关的电器。例如，按摩躺椅可以包含嵌入式系统。嵌入式系统可以根据用户的偏好提供使椅子的背部自动倾斜的指令。嵌入式系统还可以根据用户的偏好提供启动在椅子内引起躺椅内的振动的振动组件的指令。

[0010] 在家庭中通常备有的附加产品也可以包含嵌入式系统。例如，可以将嵌入式系统用在厕所内以控制用来补充储水箱中的水的水平位置。可以将嵌入式系统用在喷射式浴缸内以控制空气的流出。

[0011] 嵌入式装置可能为各种原因建立到其它电子装置的连接。例如：一个组织可能希望使关于其嵌入式装置的数据对特定的远程客户端可用。然而，组织希望使远程客户端可以使用的数据中的一些可能比较敏感，即不打算公开。该数据可能涉及嵌入式装置本身的操作。例如，数据可能显示以下信息：嵌入式装置是否打开，其是否正确地校准，操作循环是否正确地完成等。作为选择，或另外，该数据可能涉及嵌入式装置操作之外的事情。例如，数据可能包括：与嵌入式装置的用户相对应的用户标识符，由嵌入式装置取得的测定，由嵌入式装置产生的警报等。

[0012] 嵌入式装置也可以允许这些远程客户端来控制嵌入式系统的动作。例如：校准中发现的问题可以远程进行调整，来代替派人到嵌入式系统的位置。作为选择，或另外，嵌入式系统可以允许以与本地改变极为相同的方式远程地改变系统的动作。一个例子是远程锁门。这种远程控制不限于本地可执行的功能，在很多情况下可以超出本地的能力。一个例子是没有本地接口，但允许远程控制其动作的传感器。

[0013] 考虑到前述情况，由用于嵌入式装置和其它装置或客户端之间的安全连接的改进的机构可以得到益处。在这里公开了一些用于提高该连接的安全性水平的示例性系统和方法。

发明内容

[0014] 公开了一种便于对嵌入式装置发布安全密钥的方法。方法由嵌入式装置上的嵌入式程序来实现。方法包括：判断是否已经对嵌入式装置分配了安全密钥，其中判断是否分配了安全密钥包括：判断存储在所述嵌入式装置的配置数据中的安全密钥标志的值；如果没有分配所述安全密钥：使用由所述嵌入式装置的厂商提供的、存储在所述嵌入式装置的存储器中的随机数来获得所述嵌入式装置的所述安全密钥；将所述安全密钥写入到所述嵌入式装置的所述存储器中，并覆盖所述随机数，以此存储所述安全密钥，并且将所述安全密钥标志的值改变为表示已经对所述嵌入式装置分配了安全密钥的情形；保存所述安全密钥，使用所述安全密钥来建立与其它装置的安全连接；以及判断是否需要改变安全密钥，在不

需要改变安全密钥的情况下，继续使用所述安全密钥来建立安全连接，在判断为需要改变安全密钥的情况下，停止使用所述安全密钥来建立安全连接，并且将所述安全密钥标志的值改变为表示没有对所述嵌入式装置分配安全密钥的情形，随后，将所述安全密钥用作新的随机数来获取新的安全密钥。

[0015] 公开了一种用于实现便于安全密钥发布的方法的嵌入式装置。嵌入式装置包括：处理器；与处理器进行电子通信的存储器；存储在存储器中的指令。该指令可以执行来实现以下方法，方法包括：判断是否已经对所述嵌入式装置分配了安全密钥，其中判断是否分配了安全密钥包括：判断存储在所述嵌入式装置的配置数据中的安全密钥标志的值；如果没有分配所述安全密钥：使用由所述嵌入式装置的厂商提供的、存储在所述嵌入式装置的所述存储器中的随机数来获得所述嵌入式装置的所述安全密钥；将所述安全密钥写入到所述嵌入式装置的所述存储器中，并覆盖所述随机数，以此存储所述安全密钥，并且将所述安全密钥标志的值改变为表示已经对所述嵌入式装置分配了安全密钥的情形；保存所述安全密钥，使用所述安全密钥来建立与其它装置的安全连接；以及判断是否需要改变安全密钥，在不需要改变安全密钥的情况下，继续使用所述安全密钥来建立安全连接，在判断为需要改变安全密钥的情况下，停止使用所述安全密钥来建立安全连接，并且将所述安全密钥标志的值改变为表示没有对所述嵌入式装置分配安全密钥的情形，随后，将所述安全密钥用作新的随机数来获取新的安全密钥。

[0016] 公开了一种用于制造便于安全密钥发布的嵌入式装置的方法。该方法包括：提供嵌入式装置的存储器；指定嵌入式装置的存储器中用于存储随机数的位置；产生随机数；将随机数存储在嵌入式装置的存储器的指定位置；提供嵌入式程序，将所述嵌入式程序存储在所述嵌入式装置的所述存储器中，所述嵌入式程序用于判断是否已经对所述嵌入式装置分配了安全密钥，其中判断是否分配了安全密钥包括：判断存储在所述嵌入式装置的配置数据中的安全密钥标志的值；如果没有分配所述安全密钥：使用由所述嵌入式装置的厂商提供的、存储在所述嵌入式装置的所述存储器的所述制定位置中的随机数来获得所述嵌入式装置的所述安全密钥；将所述安全密钥写入到所述嵌入式装置的所述存储器中，并覆盖所述随机数，以此存储所述安全密钥，并且将所述安全密钥标志的值改变为表示已经对所述嵌入式装置分配了安全密钥的情形；保存所述安全密钥，使用所述安全密钥来建立与其它装置的安全连接；以及判断是否需要改变安全密钥，在不需要改变安全密钥的情况下，继续使用所述安全密钥来建立安全连接，在判断为需要改变安全密钥的情况下，停止使用所述安全密钥来建立安全连接，并且将所述安全密钥标志的值改变为表示没有对所述嵌入式装置分配安全密钥的情形，随后，将所述安全密钥用作新的随机数来获取新的安全密钥。

附图说明

[0017] 根据以下结合附图的说明和所附权利要求，本发明的示例实施例将变得更充分明显。应当理解，这些附图只说明示例实施例，因此不应考虑为是对发明范围的限制，通过使用下列附图，更具体和详细地说明本发明的示例实施例，其中：

[0018] 图 1 是示出根据实施例的便于对嵌入式装置发布安全密钥的系统的框图；

[0019] 图 2 是可以在根据实施例构造的嵌入式装置中使用的硬件组件的框图；

[0020] 图 3 是可以存储在根据实施例构造的嵌入式装置的存储器中的软件组件和 / 或数

据的框图；

[0021] 图 4 是示出嵌入式装置厂商可以如何制造根据实施例构造方便安全密钥发布的嵌入式装置的流程图；

[0022] 图 5 是示出根据实施例的便于安全密钥发布的嵌入式装置程序的运行的流程图；

[0023] 图 6 是根据另一个实施例的可以存储在嵌入式装置的存储器中的软件组件和 / 或数据的框图；

[0024] 图 7 示出可以在其中实现本系统和方法的示例性照明系统；

[0025] 图 8 示出可以在其中实现本系统和方法的示例性安全系统；以及

[0026] 图 9 示出可以在其中实现本系统和方法的示例性家庭控制器系统。

具体实施方式

[0027] 现在参考附图说明本发明的各种实施例，其中同样的附图标记表示相同或功能相似的元件。这里，如在图中一般性说明和示出的，本发明的实施例可以以很多种不同的结构来设置和设计。因此，以下对如图所示的本发明的若干示例实施例的更详细的说明，不像权利要求那样旨在限制本发明的范围，而仅仅是发明的实施例的代表。

[0028] 在这里专用的词“示例性”意味着“作为实施例、例子或图示”。在这里作为“示例性”说明的任何实施例不必解释为比其它实施例优选或有利。尽管在附图中呈现了实施例的多种方面，但除非特别指出，附图不必按比例画出。

[0029] 这里公开的实施例的很多特征可以作为计算机软件、电子硬件、或二者的结合来实现。为了清楚地说明硬件和软件的这种可互换性，一般根据各种组件的功能来对其进行说明。这种功能是以硬件实现还是以软件实现取决于具体应用和施加在整个系统上的设计限制。本领域的技术人员针对每个具体应用可以以不同的方式实现所述功能，但是这种实现决定不应被解释为脱离了本发明的范围。

[0030] 在所述功能作为计算机软件来实现的情况下，这种软件可以包括：位于存储器装置内和 / 或作为电信号通过系统总线或网络发送的任何种类的计算机指令或计算机可执行代码。实现与这里所述的组件相关的功能的软件可以包括单个指令或多个指令，可以将该软件分配到若干不同的代码段，不同的程序中，以及跨越几个存储器装置。

[0031] 现今使用两种典型的安全密钥发布手段。第一种是公用密钥，第二种是共享密钥。公用密钥加密经常依赖于随机数来完成密钥发布。共享密钥系统典型地需要将密钥分配到不同的需要知道密钥的各方的配置。为了使共享密钥系统更容易管理，有时使用密码或短语密码 (pass-phrase) 作为密钥。这些低熵密钥不是很安全，采用了很多方法使它们更安全。这些方法中的很多也需要随机数。

[0032] 当将该手段做成嵌入式程序时存在一些潜在问题。如上所示，嵌入式程序是使嵌入式装置的处理器运行并告诉处理器做什么来执行特定任务的计算机软件。嵌入式程序典型地不具有产生有效的随机数的能力。在密钥发布期间，使用性能较差的随机数产生器可能危急整个密钥，由此终生削弱装置的安全性。此外，因为嵌入式程序典型地具有受限的（或没有）用户接口能力来例如向嵌入式程序拷贝密钥文件，所以由于共享密钥的特性，嵌入式程序很难配置共享密钥。

[0033] 嵌入式装置可以大批量的生产，它们的初始程序和配置可以在该生产过程中写入

嵌入式装置中。典型地，将像序列号等一些装置特定信息写入可以由嵌入式程序访问的装置。虽然在该信息中可能包括共享密钥，但是如果在生产过程中写入密钥，可能出现信任和信息存储以及传输的问题。首先，一旦装置制造完成，厂商不想在存储密钥。其次，厂商将要把密钥给谁并不明确。第三，装置购买者可能不确信厂商没有将密钥有意或无意地泄露给第三方。

[0034] 对于嵌入式装置的安全密钥发布，还存在一些其它替代。例如，不具有产生随机数问题的膝上型电脑或其它计算机可以用来分配安全密钥。这种做法的缺点是需要使用计算机，而且秘密信息被发送到没有由计算机加密的嵌入式装置。另一个替代是为嵌入式装置增加产生随机数的能力。然而，这费用很高，而且可能需要特殊的硬件。因此，考虑到前述问题，存在对便于对嵌入式装置发布安全密钥的改进机构的需要。

[0035] 这里公开的实施例一般地涉及为嵌入式装置的安全密钥发布提供方便。根据实施例，嵌入式装置的厂商指定用于存储随机数的嵌入式装置的存储器中的位置。厂商还产生随机数，并将随机数存储在指定的存储位置。随后，在嵌入式装置运行期间，嵌入式装置上的嵌入式程序使用随机数来获得嵌入式装置的安全密钥。嵌入式程序将安全密钥存储在嵌入式装置的存储器中，并使用该安全密钥建立与其它装置的安全连接。

[0036] 当嵌入式程序获得安全密钥时，嵌入式程序可能将该安全密钥写入嵌入式装置的存储器并覆盖随机数。作为选择，厂商可以将安全密钥写入嵌入式装置的存储器中不包含随机数的分开的位置。

[0037] 有时，安全密钥不再适合建立安全连接。在这种情况下，嵌入式程序可以将安全密钥作为随后用来获得新的安全密钥的新的随机数。每次安全密钥不再适合建立安全连接且需要新的安全密钥时重复该循环。代替使用安全密钥本身作为新的随机数，可以将安全密钥与最近一次使用的随机数（如果其仍存储在存储器中）数学地相结合来产生新的随机数。

[0038] 图 1 是示出根据实施例的便于对嵌入式装置 102 发布安全密钥的系统 100 的框图。系统 100 包括计算机 104。计算机 104 可以是任何包括能够接收并处理数据的数字处理器的装置，例如微控制器、手持计算机、个人计算机、服务器、大型计算机、超级计算机和其任何变种或相关装置。尽管图 1 中示出单个计算机 104，但是实施例可以在具有多个计算机 104 的系统中实现。

[0039] 系统 100 还包括嵌入式装置 102。嵌入式装置 102 是一种可能不包括与典型桌上计算机相关联的全部相同的组件的计算装置。例如：一些嵌入式装置 102 不包括监视器，其它一些不包括键盘或鼠标，且一些嵌入式装置 102 既不包括监视器，也不包括键盘 / 鼠标。嵌入式装置 102 的例子包括：自动售货机、电话、门锁、温度传感器、电动机、开关、灯、打印机、传真机、冰箱、健康监视器、电梯 / 电动扶梯、复印机、扫描仪、制造设备、工业设备、计算机及其外围设备、安全系统、监视设备等。

[0040] 将关于图 2 更详细地说明嵌入式装置 102。尽管在图 1 中示出了单个嵌入式装置 102，但是实施例可以在具有多个嵌入式装置 102 的系统中实现。

[0041] 计算机 104 和嵌入式装置 102 通过网络 106 进行电子通信。这里使用的术语“网络”是指一系列节点通过通信路径互连的系统。节点是与其它节点通信的物理计算装置。节点的特定动作由其执行的应用程序或软件确定。网络节点上运行的应用程序通过实现协

议的软件模块互相通信，所述协议规定如何在网络上发送数据的规则。一些协议处理数据传送的定时、序列和错误检查。另一些更多地处理如何将数据格式化以及节点交换的命令和响应。一组一起工作的协议称为协议栈，其中每个协议作为栈中的一层设置在另一层顶上。协议栈的顶层由应用程序使用，中间层处理节点之间的数据传送组（包和帧），底层直接处理传送数据的网络硬件。

[0042] 物理网络由某种物理介质（例如，电线，光纤，空气）连接的节点组成。该物理连接有时可以称为链接。局限于两个节点的物理网络可以称为点对点，而可以支持两个以上节点的物理网络可以称为多址 (multiple-access)。多址网络上的每个节点具有用于将其与网络上的其它节点区分开的物理地址。

[0043] 可以将逻辑网络添加到物理网络上来指定唯一的节点组。逻辑网络中的每个节点具有通过协议映射到节点的物理地址的逻辑地址。子网络或子网是网络的物理上或逻辑上独立的一部分，由子网编号来区分。

[0044] 因为大多数物理网络事件已经具有很多定义好的实现，不需要定义新的物理层，所以大多数协议处理逻辑网络。逻辑网络还具有与物理网络隔离的优点，因此一般更有用。例如，TCP/IP 定义在逻辑网络的顶层 (IP)。IP 可以在很多物理网络上运行（以太网、串行、无线等）。这使得 TCP/IP 比仅将其定义在某个特定物理网络方面成为更通用的解决方案。

[0045] 图 2 是可以在根据实施例构造的嵌入式装置 202 中使用的硬件组件的框图。中央处理单元 (CPU)208 或处理器可以用于控制包括其通过总线 210 与 CPU 208 相连接的其它组件的嵌入式装置 202 的操作。CPU 208 可以实施为微处理器、微控制器、数字信号处理器或其它本领域已知的装置。CPU 208 基于存储器中存储的程序代码来进行逻辑和算术运算。在特定实施例中，存储器 214 可以是包括于 CPU 208 中的板上存储器。例如，微控制器经常包括一定量的板上存储器。

[0046] 嵌入式装置 202 还可以包括网络接口 212。网络接口 212 方便了嵌入式装置 202 和其它连接到网络 106 的装置之间的通信，网络 106 可以是寻呼网络、蜂窝网络、全球通信网络、因特网、计算机网络、电话网络等。网络接口 212 根据适用于网络 106 的标准协议操作。

[0047] 嵌入式装置 202 还可以包括存储器 214。存储器 214 可以包括用于存储临时数据的随机存取存储器 (RAM)。作为选择，或另外，存储器 214 可以包括用于存储例如固定代码和配置数据的较永久性数据的只读存储器 (ROM)。存储器 214 也可以实施为例如硬盘驱动器的磁性存储装置。存储器 214 可以是任何类型的能够存储电子信息的电子装置。

[0048] 嵌入式装置 202 还可以包括一个或多个为与其它装置进行通信提供方便的通信端口 216。嵌入式装置 202 还可以包括输入 / 输出装置 218，例如键盘、鼠标、操纵杆、触摸屏、监视器、扬声器、打印机等。

[0049] 当然，图 2 只示出嵌入式装置 202 的一种可能的配置。可以采用各种其它结构和组件。

[0050] 图 3 是可以存储在根据实施例的嵌入式装置 202 的存储器 214 中的软件组件和 / 或数据的框图。嵌入式程序 320 可以存储在存储器 214 中。嵌入式程序 320 是使嵌入式装置 202 的 CPU 208 运行，并告诉 CPU 208 做什么来执行特定任务的计算机软件。如下面将更详细说明的一样，嵌入式程序 320 可以用于为安全密钥和随机数共享提供方便。至少一

部分由嵌入式程序 320 提供的功能可能取决于嵌入式装置 202 的使用方法。

[0051] 装置特定信息 322(即,关于嵌入式装置 202 的信息)也可以存储在存储器 214 中。可以存储在存储器 214 中的装置特定信息 322 的一些例子包括 :序列号、嵌入式程序 320 的版本号、生产日期、用户名或其它用户特定信息等。至少一部分装置特定信息 322 可以在生产过程中由厂商存储在存储器 214 中。作为选择,或另外,至少一部分装置特定信息 322 可以包括嵌入式程序 320 运行期间存储在存储器 214 中的信息。

[0052] 包括在嵌入式装置 202 中的存储器 214 还可以包括指定来交替存储随机数和安全密钥的位置 324。该位置 324 在这里将被称为随机数 / 安全密钥位置 324。在制造嵌入式装置 202 的过程中的某个时刻,厂商最初地将随机数存储在随机数 / 安全密钥位置 324。在其后的某个时刻(典型地在厂商将嵌入式装置 202 提供给另一方后),使用随机数来获得安全密钥。然后将安全密钥写入随机数 / 安全密钥位置 324,取代随机数。以这种方式,可以使用随机数获得安全密钥,而不必要嵌入式装置 202 本身产生随机数。下面将进行更详细的说明。

[0053] 配置数据 326 也可以设置在存储器 214 中。配置数据 326 可以包括安全密钥标志 328。安全密钥标志 328 示出存储在随机数 / 安全密钥位置 324 中的数据是对应于随机数还是安全密钥。在某些实施例中,安全密钥标志 328 具有两个可能的值。如果安全密钥标志 328 为第一个值(例如,“假”),则存储在随机数 / 安全密钥位置 324 的数据对应于随机数。如果安全密钥标志 328 为第二个值(例如 :“真”),则存储在随机数 / 安全密钥位置 324 的数据对应于安全密钥。嵌入式程序 320 可以查阅安全密钥标志 328 来判断是否要为嵌入式装置 202 来获得安全密钥。下面将更详细的说明。

[0054] 图 4 是示出嵌入式装置厂商可以如何制造根据实施例构造方便安全密钥发布的嵌入式装置 202 的流程图。根据方法 400,厂商可以指定随机数 / 安全密钥存储位置 324(402),即,嵌入式装置 202 的存储器 214 中、用于交替存储随机数和安全密钥的位置 324。

[0055] 在步骤 404 中,厂商产生随机数。随机数可以为任何希望的长度。典型地,越长的随机数对嵌入式装置 202 提供越高的安全性。在示例性实施例中,随机数为 32 字节。

[0056] 在步骤 406 中,厂商将步骤 404 中产生的随机数存储在随机数 / 安全密钥存储位置 324 中。在步骤 408 中,厂商设定安全密钥标志 328 的值以指出 :存储在随机数 / 安全密钥位置 324 中的数据对应于随机数。

[0057] 在步骤 410 中,厂商提供另一方使用的嵌入式装置 202。例如,最初的嵌入式装置所有者可能将嵌入式装置 202 卖给另一方。

[0058] 图 5 是示出根据实施例的便于对嵌入式装置 202 发布安全密钥的嵌入式装置程序 320 的运行的流程图。在步骤 502 中,开始嵌入式装置 202 的存储器 214 中的嵌入式程序 320。

[0059] 在步骤 504 中,嵌入式程序 320 判断安全密钥是否分配到了嵌入式装置 202。在某些实施例中,通过判断存储在配置数据 326 中的安全密钥标志 328 的值来进行是否分配了安全密钥的判断。如上所述,安全密钥标志 328 指出关于存储在随机数 / 安全密钥位置 324 中的数据是随机数还是安全密钥的信息。如果安全密钥标志 328 的值指出数据对应于安全密钥,则安全密钥分配到了嵌入式装置 202。然而,如果安全密钥标志 328 的值指出数

据对应于随机数，则安全密钥没有分配到嵌入式装置。

[0060] 如果判断为安全密钥没有分配到嵌入式装置 202，则在步骤 506 中，嵌入式程序 320 使用嵌入式装置 202 的存储器 214 的随机数 / 安全密钥位置 324 中的随机数来获得安全密钥。如上所示，该随机数可以由嵌入式装置 202 的厂商提供。根据这里公开的实施例，可以使用各种密钥发布方法。以安全远程密码 (SRP，Secure Remote Password) 协议为例，嵌入式程序 320 可以从用户请求低熵 (low-entropy) 密码。嵌入式程序 320 可以与厂商提供的随机数结合地使用该密码来用密钥产生器建立安全的连接。然后，嵌入式装置 202 可能需要使其身份通过的密钥。密钥产生器可以对嵌入式装置 202 配置密钥，并且通过安全的连接将该密钥发布到嵌入式装置 202。密钥产生器可以记住所分配的安全密钥以及嵌入式装置 202 的身份。

[0061] 尽管以 SRP 协议为例，但是实施例不局限于任何特定的密钥发布方法。在安全密钥发布过程中使用随机数的任何其它方法可以用在这里公开的实施例中。例如，可以使用公共 (public) 或私人 (private) 加密。

[0062] 在步骤 508 中，嵌入式程序 320 存储安全密钥。嵌入式程序 320 可以将安全密钥存储在嵌入式装置 202 的随机数 / 密钥位置 324 中，覆盖先前存储于那里的随机数。作为选择，如下面将更详细说明的，嵌入式程序 320 可以将安全密钥写到不包含随机数的存储位置，即，与存储随机数的存储位置分开的位置。在步骤 510 中，嵌入式程序 320 改变安全密钥标志 328 的值以指出已经对嵌入式装置 202 分配了安全密钥。

[0063] 如果在步骤 504 中判断为已经对嵌入式装置 202 分配了安全密钥，则方法 500 直接进行到步骤 512。在步骤 512 中，嵌入式程序 320 使用其分配的安全密钥来与其它装置建立安全连接。

[0064] 有时，可能希望对嵌入式装置 202 提供新的安全密钥。例如，可能重新部署嵌入式装置 202（例如，从一个所有者卖到另一个）。作为另一个例子，当前的安全密钥可能不再安全。

[0065] 在步骤 514 中，嵌入式程序 320 判断用户是否想要改变安全密钥。如果用户不想改变安全密钥，则嵌入式程序 320 可以继续使用安全密钥来建立安全连接 (512)。然而，如果在任何时刻想要对嵌入式装置 202 提供新的安全密钥，则嵌入式程序 320 可以停止使用安全密钥来建立与其它装置的安全连接。为了反映不再将随机数 / 安全密钥位置 324 中的数据用作安全密钥的情况，在步骤 516 中，将安全密钥标志 328 的值改变为指出没有对嵌入式装置 202 分配安全密钥。此时，随机数 / 安全密钥位置 324 中的数据本身还没有改变；更确切地说，当安全密钥标志 328 被改变时 (516)，嵌入式程序 320 简单地开始将该数据视为随机数而不是安全密钥。这起作用是因为安全密钥是秘密信息值，秘密信息的一般原则是它们理想地只是随机位模式。然后方法返回到步骤 504，然后在步骤 504 中，“新”随机数（先前的安全密钥）可以用来获得新的安全密钥。当每次希望为嵌入式装置 202 提供新的安全密钥时，可以重复该处理。

[0066] 图 6 是根据另一个实施例的可以存储在嵌入式装置 602 的存储器 614 中的软件组件和 / 或数据的框图。与先前说明的实施例相同，图 6 中所示的存储器 614 包括：嵌入式程序 620、装置特定信息 622 以及配置数据 626。此外，配置数据包括安全密钥标志 628。

[0067] 在图 3 所示实施例中，存储器 214 包括单个随机数 / 安全密钥位置 324。相反，在

图6所示实施例中，存储器614包括随机数用位置630，以及分开的安全密钥用位置632。在本文中，术语“分开的”简单地指随机数和安全密钥可以同时存储在嵌入式装置602的存储器614中。随机数位置630和安全密钥位置632可以互相邻接，或它们可以互相隔开。

[0068] 在所示实施例中，当将随机数用来获得安全密钥时，不必将所获得的安全密钥写到与随机数相同的存储位置。代替地，可以同时将随机数和安全密钥都存储在嵌入式装置602的存储器中。在该实施例中，当希望提供新的安全密钥时，可以结合当前随机数和当前安全密钥来产生新的随机数。然后，新的随机数可以用来获得新的安全密钥。

[0069] 除了以上所公开的技术，其它技术也可以用来获得嵌入式装置202的新安全密钥。例如，可以将来自厂商的原始随机数用作产生更长随机数的种子（即，随机位序列）。

[0070] 本系统和方法可以在若干情况下使用。图7示出实现本系统和方法的系统的一个实施例。图7是示出包括照明控制器系统708的照明系统700的一个实施例的框图。图7的照明系统700可以包含于家庭的各种房间中。如图所示，系统700包括房间A702、房间B704、以及房间C 706。尽管在图7中示出了三个房间，但是系统700可以在家庭、公寓、或其它环境的任何数量和种类的房间中实现。

[0071] 照明控制器系统708可以监视并控制系统700内的附加的嵌入式系统和组件。在一个实施例中，房间A 702和房间B 704分别包括开关组件714、718。开关组件714、718还可以包括次级嵌入式系统716、720。次级嵌入式系统716、720可以接收来自照明控制器系统708的指令。然后次级嵌入式系统716、720可以执行这些指令。指令可以包括对各种灯组件710、712、722和724的通电或断电。指令还可以包括调暗或增强各种灯组件710、712、722和724的亮度。指令可以进一步包括以各种模式设置灯组件710、712、722和724的亮度。次级嵌入式系统716、720便于照明控制器系统708监视并控制位于房间A 702和房间B 704中的每个灯组件710、712、722和724。

[0072] 照明控制器系统708还可以直接向所述房间C 706中的包括次级嵌入式系统728的灯组件726提供指令。照明控制器系统708可以指示次级嵌入式系统728来给独立的灯组件726断电或通电。类似地，从照明控制器系统708接收到的指令可以包括调暗或增强独立的灯组件726的亮度。

[0073] 照明控制器系统708还可以监视系统700内的独立的灯组件730和732，并直接向其提供指令。这些指令可以包括与前面所述的指令相似的指令。

[0074] 图8是实现本系统和本发明的方法的系统的又一实施例。图8是示出安全系统800的框图。在房间A 802、房间B 804、和房间C 806中实现所述实施例中的安全系统800。这些房间可以在家庭或其它封闭环境的界限内。系统800还可以在开放的环境中实现，其中房间A 802、B 804和C 806分别表示区域或边界。

[0075] 系统800包括安全控制器系统808。安全控制器系统808监视系统800内的各种组件，并接收来自系统800内的各种组件的信息。例如，运动传感器814、818可以包括次级嵌入式系统816、820。当通过次级嵌入式系统816、820检测到运动时，运动传感器814、818可以监视运动的即时空间，并向安全控制器系统808报警。安全控制器系统808还可以向系统800内的各种组件提供指令。例如，安全控制器系统808可以向次级嵌入式系统816、820提供指令以对窗户传感器810、822和门传感器812、824通电或断电。在一个实施例中，当窗户传感器810、822检测到窗户的移动时，次级嵌入式系统816、820通知安全控制器系

统 808。类似地，当门传感器 812、824 检测到门的移动时，次级嵌入式系统 816、820 通知安全控制器系统 808。次级嵌入式系统 816、820 可以指示运动传感器 814、818 启动位于运动传感器 814、818 内的 LED（未视出）。

[0076] 安全控制器系统 808 还可以监视系统 800 内的各组件，并直接向其提供指令。例如，安全控制器系统 808 可以监视运动传感器 830 或窗户传感器 832，并向其提供通电或断电的指令。安全控制器系统 808 还可以指示运动传感器 830 和窗户传感器 832 启动传感器 830 和 832 内的 LED（未视出）或音频警报通知。

[0077] 组成系统 800 的每个独立的组件还可以包括次级嵌入式系统。例如，图 8 示出包括次级嵌入式系统 828 的门传感器 826。安全控制器系统 808 可以以与前面所述的方式相似的方式监视次级嵌入式系统 828 并向其提供指令。

[0078] 图 9 是说明家庭控制系统 900 的一个实施例的框图。家庭控制系统 900 包括家庭控制器 908，其便于监视例如照明系统 700、安全系统 800 等的各种系统。家庭控制系统 900 使得用户能够通过一个或多个嵌入式系统控制各种组件和系统。在一个实施例中，家庭控制器系统 908 以与前面联系图 7 和图 8 所述的方式相同的方式进行监视并提供信息。在所述实施例中，家庭控制器 908 通过次级嵌入式系统 920 向加热组件 924 提供指令。加热组件 924 可以包括在居住场所或办公室中通常备有的暖炉或其它加热装置。家庭控制器系统 908 可以通过次级嵌入式系统 920 提供对加热组件 924 通电或断电的指令。

[0079] 类似地，家庭控制器 908 可以监视家庭控制系统 900 内例如制冷组件 930 的组件并直接向其提供指令。制冷组件 930 可以包括在居住场所或办公室中通常备有的空调或其它制冷装置。中央家庭控制器 908 可以指示制冷组件 930 根据由中央嵌入式系统 908 收集的温度读数通电或断电。家庭控制系统 900 以与前面联系图 7 和图 8 所说明的方式相似的方式运行。

[0080] 可以使用各种不同的技术和方法表示信息和信号。例如，可以使用电压、电流、电磁波、磁场或粒子、光场或粒子、或其任意的组合来表示可能在以上说明中出现的数据、指令、命令、信息、信号、位、符号、以及码片 (chip)。

[0081] 结合在这里所公开的实施例所说明的各种说明性的逻辑块、模块、电路和算法步骤，可以实现为电子硬件、计算机软件、或二者的结合。为了清楚地说明硬件和软件的这种可交换性，以上主要根据各种说明性的组件、块、模块、电路和步骤的功能，对其进行了说明。这种功能是作为硬件实现还是作为软件实现取决于整个系统的特定应用和对整个系统所施加的设计限制。本领域的技术人员可以对于每个特定的应用以不同的方式实现所述功能，但是这种实现决定不应解释为脱离了本发明的范围。

[0082] 可以使用被设计为执行这里所述功能的通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC，application specificintegrated circuit)、现场可编程门阵列信号 (FPGA，fieldprogrammable gate array signal) 或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件、或其任意的组合，来实现或执行结合这里所公开的实施例所说明的各种说明性的逻辑块、模块和电路。通用处理器可以是微型处理器，但作为选择，处理器可以是任何传统的处理器、控制器、微型控制器、或状态机。处理器还可以实现为计算装置的结合，例如，DSP 和微型处理器的结合、多个微型处理器、与 DSP 核心结合的一个或多个微型处理器、或任何其它这样的配置。

[0083] 结合在这里所公开的实施例说明的方法或算法的步骤可以直接在硬件中、在由处理器执行的软件模块中、或在二者的结合中实现。软件模块可以存放于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动盘、CD-ROM、或本领域已知的任何其它形式的存储介质。示例存储介质连接到处理器使得处理器可以从存储介质读取信息，并向存储介质写入信息。作为选择，可以将存储介质集成到处理器。处理器和存储介质可以位于 ASIC 中。ASIC 可以位于用户终端中。作为选择，处理器和存储介质可以作为分离组件位于用户终端中。

[0084] 这里公开的方法包括用于实现所述方法的一个或多个步骤或动作。方法步骤和 / 或动作可以互相交换，而不脱离本发明的范围。换句话说，除非对于实施例的适当操作需要步骤或动作的特定顺序，可以改变指定步骤和 / 或动作的顺序和 / 或使用，而不脱离本发明的范围。

[0085] 尽管说明并描述了本发明的具体实施例和应用，但应该理解的是，本发明不局限于这里公开的精确的配置和组件。可以在这里公开的本发明的方法和系统的配置、操作、以及细节中做出对本领域的技术人员明显的各种变形、改变、和变化，而不脱离发明的精神和范围。

[0086] 产业应用性

[0087] 本发明可应用到嵌入式系统。

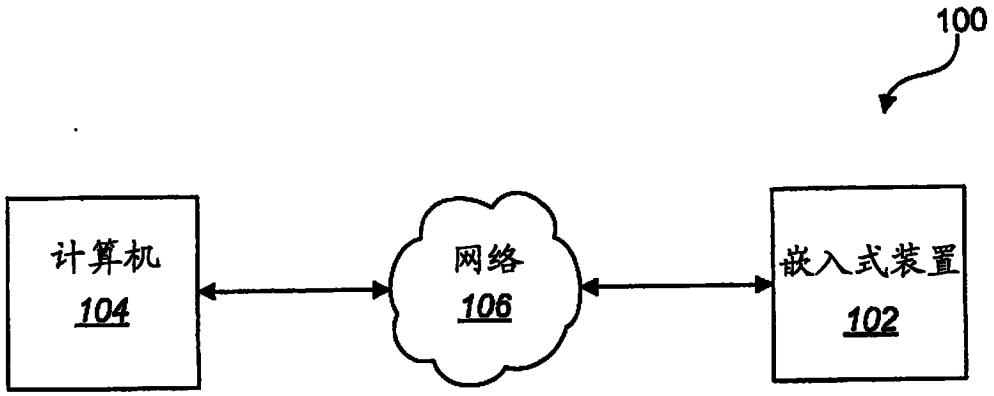

100
计算机
104
网络
106
嵌入式装置
102

图 1

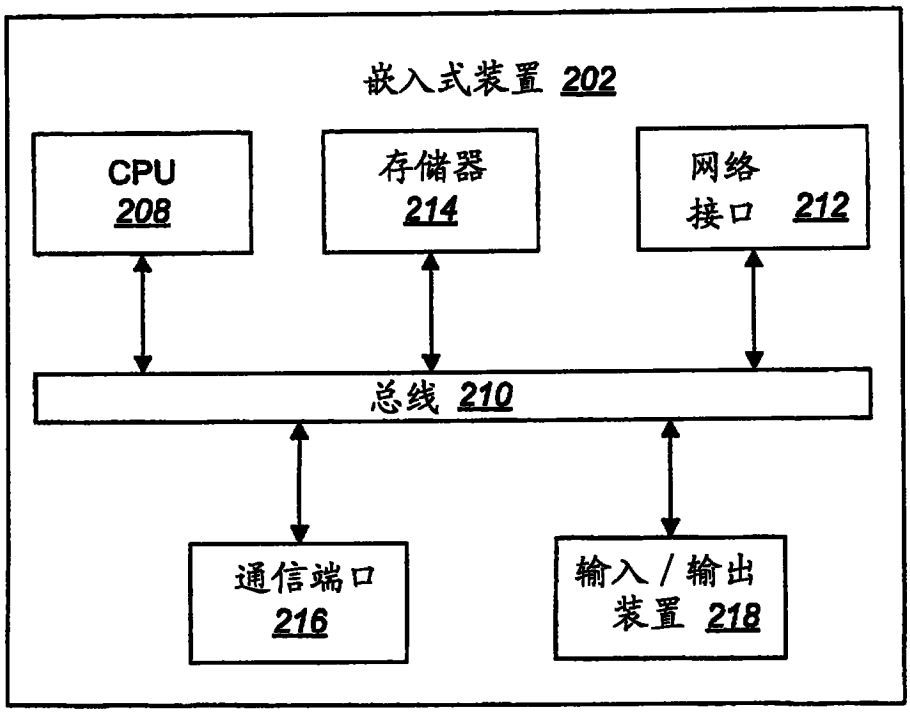

嵌入式装置 202
CPU
208
存储器
214
网络
接口 212
总线 210
通信端口
216
输入 / 输出
装置 218

图 2

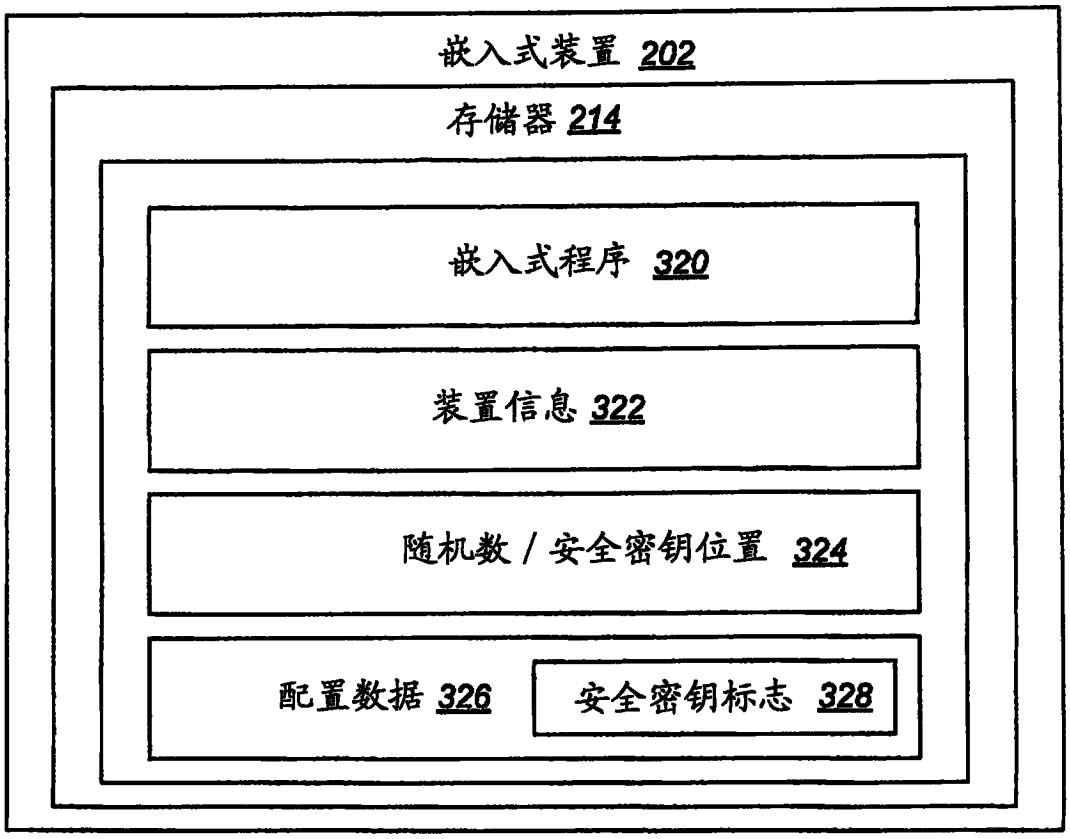

嵌入式装置 202
存储器 214
嵌入式程序 320
装置信息 322
随机数 / 安全密钥位置 324
配置数据 326
安全密钥标志 328

图 3

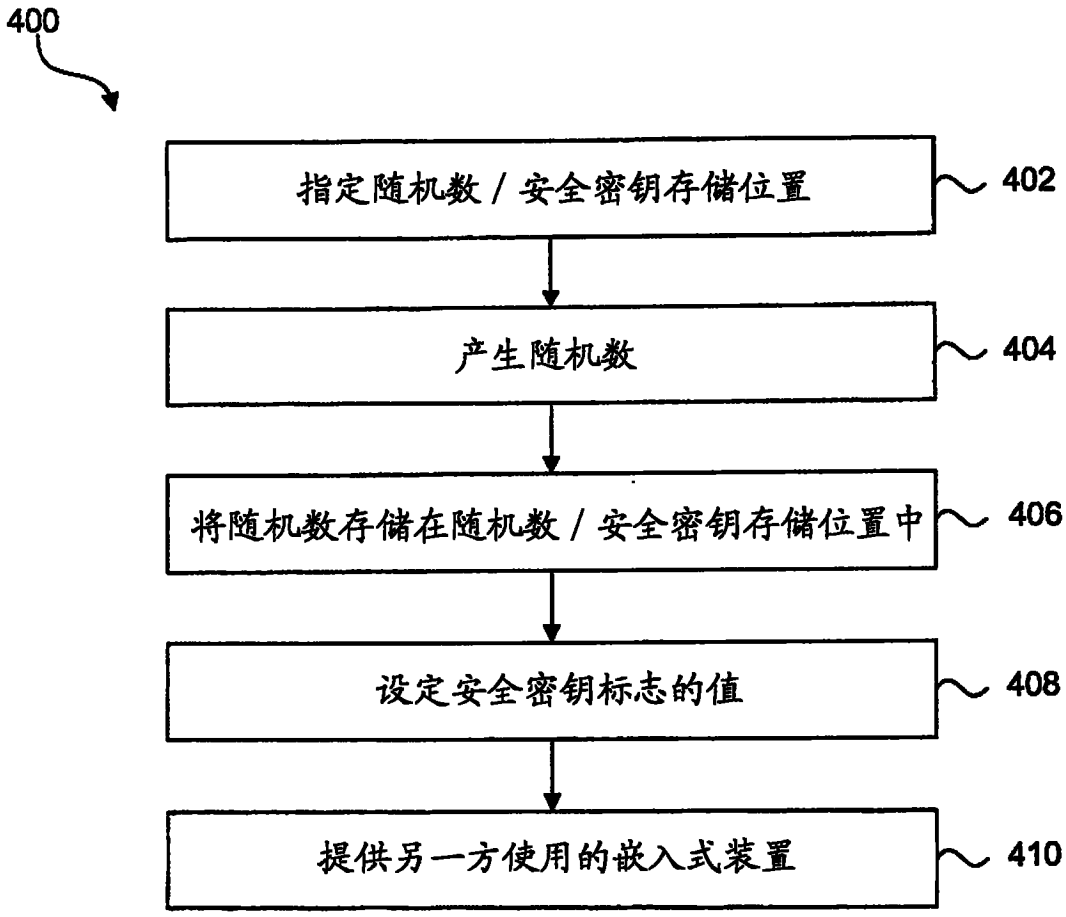

400
指定随机数 / 安全密钥存储位置
402
产生随机数
404
将随机数存储在随机数 / 安全密钥存储位置中
406
设定安全密钥标志的值
408
提供另一方使用的嵌入式装置
410

图 4

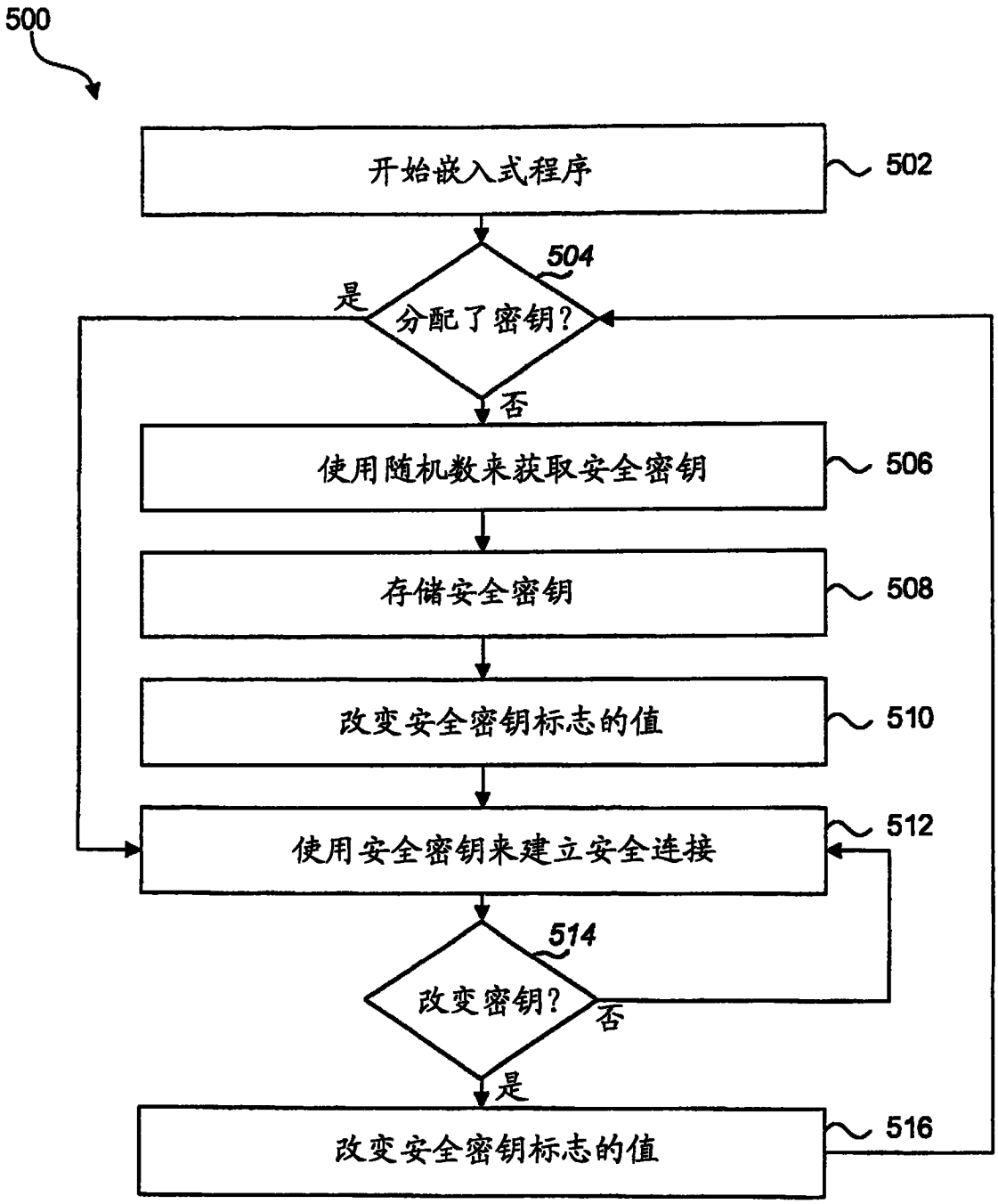

500
开始嵌入式程序
502
504
是
分配了密钥?
否
使用随机数来获取安全密钥
506
存储安全密钥
508
改变安全密钥标志的值
510
使用安全密钥来建立安全连接
512
514
改变密钥?
否
是
改变安全密钥标志的值
516

图 5

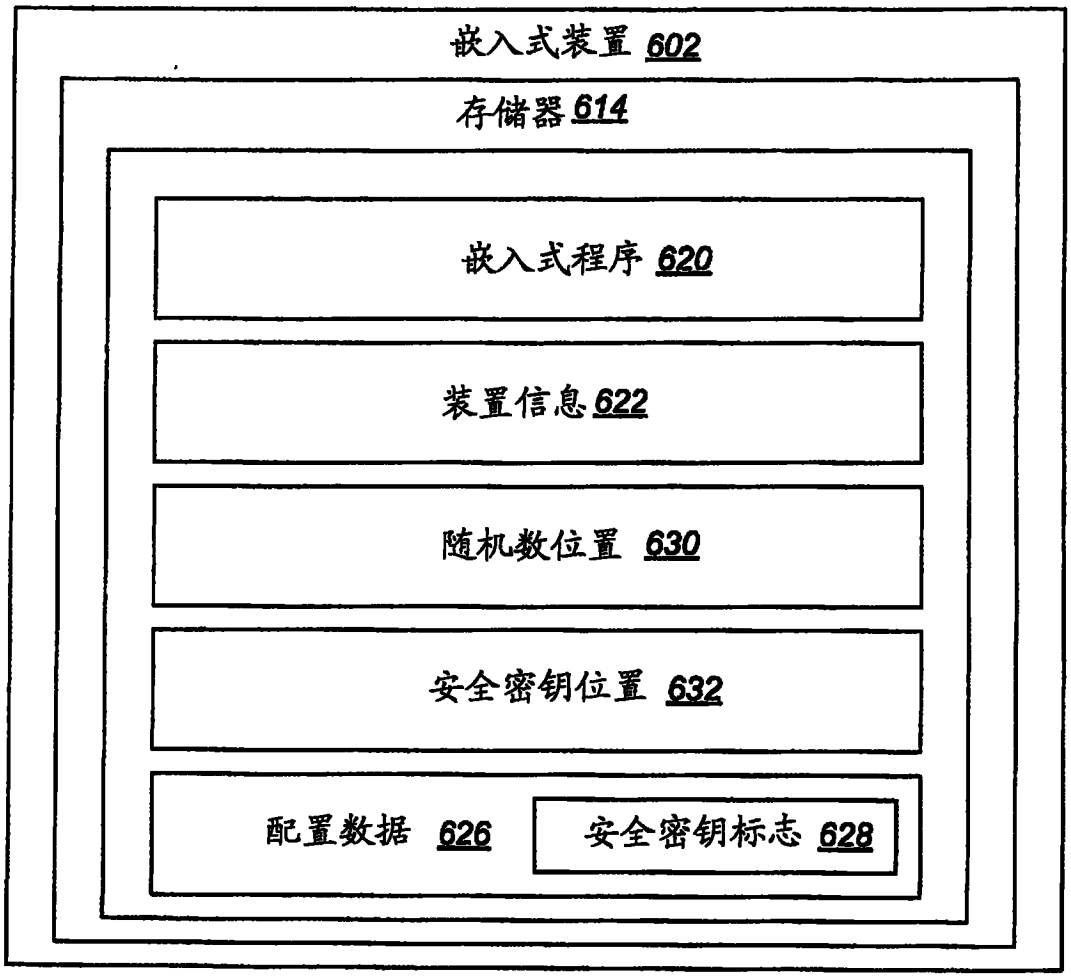

嵌入式装置 602
存储器 614
嵌入式程序 620
装置信息 622
随机数位置 630
安全密钥位置 632
配置数据 626
安全密钥标志 628

图 6

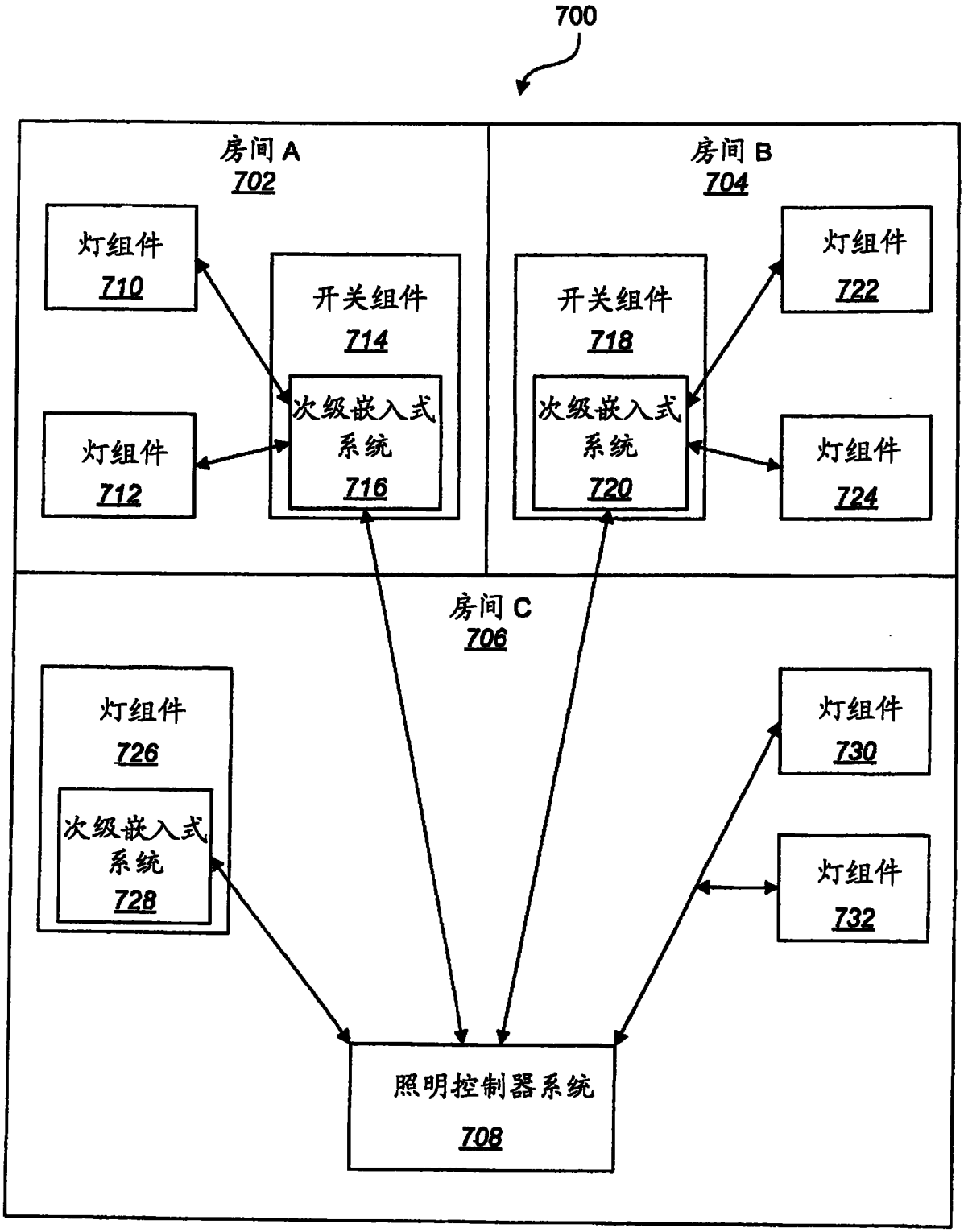

700
房间 A
702
灯组件
710
开关组件
714
次级嵌入式系统
716
灯组件
712
房间 B
704
灯组件
722
开关组件
718
次级嵌入式系统
720
灯组件
724
房间 C
706
灯组件
726
次级嵌入式系统
728
灯组件
730
灯组件
732
照明控制器系统
708

图 7

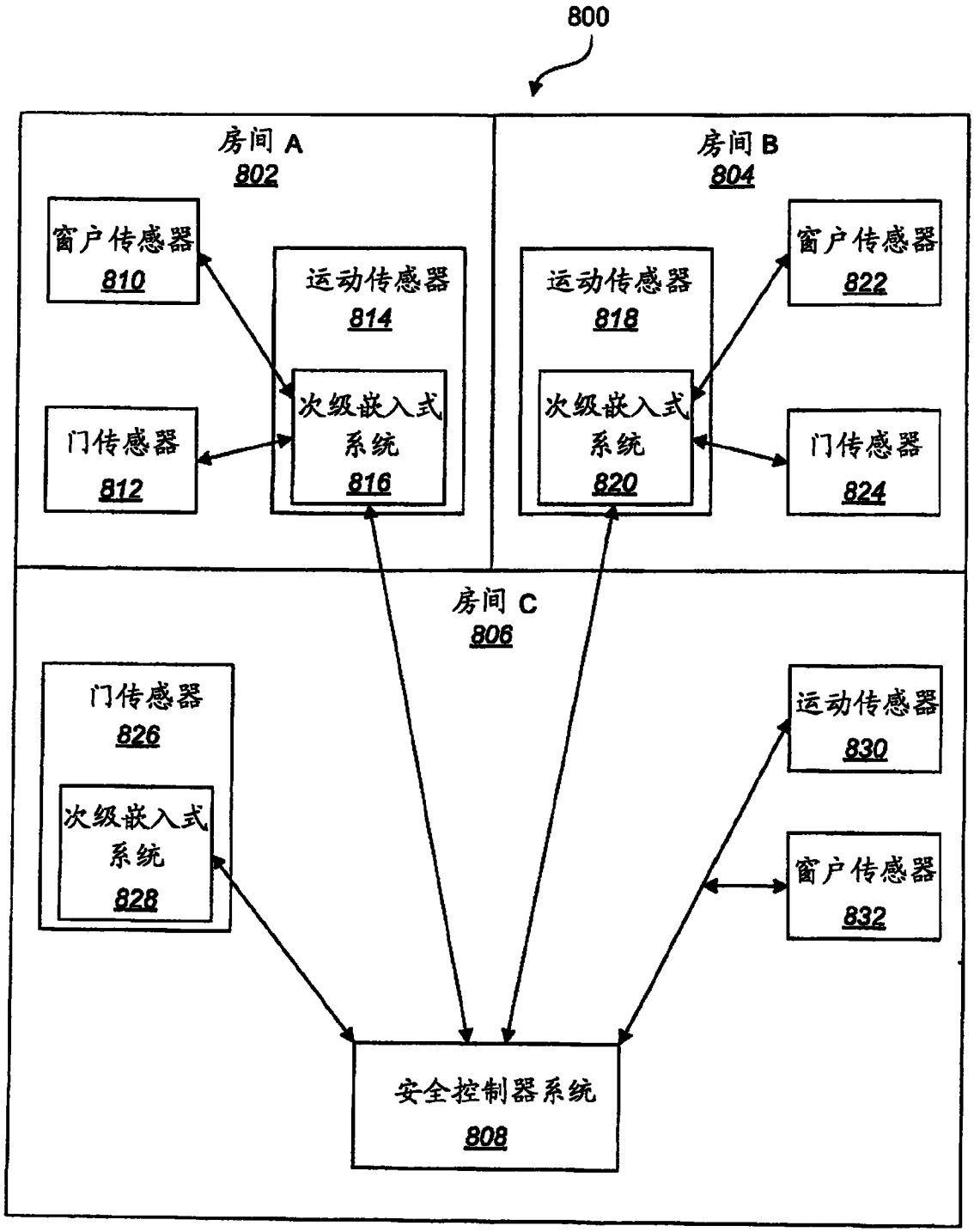

800
房间 A
802
房间 B
804
窗户传感器
810
运动传感器
814
次级嵌入式系统
816
门传感器
812
运动传感器
818
次级嵌入式系统
820
窗户传感器
822
门传感器
824
房间 C
806
门传感器
826
次级嵌入式系统
828
运动传感器
830
窗户传感器
832
安全控制器系统
808

图 8

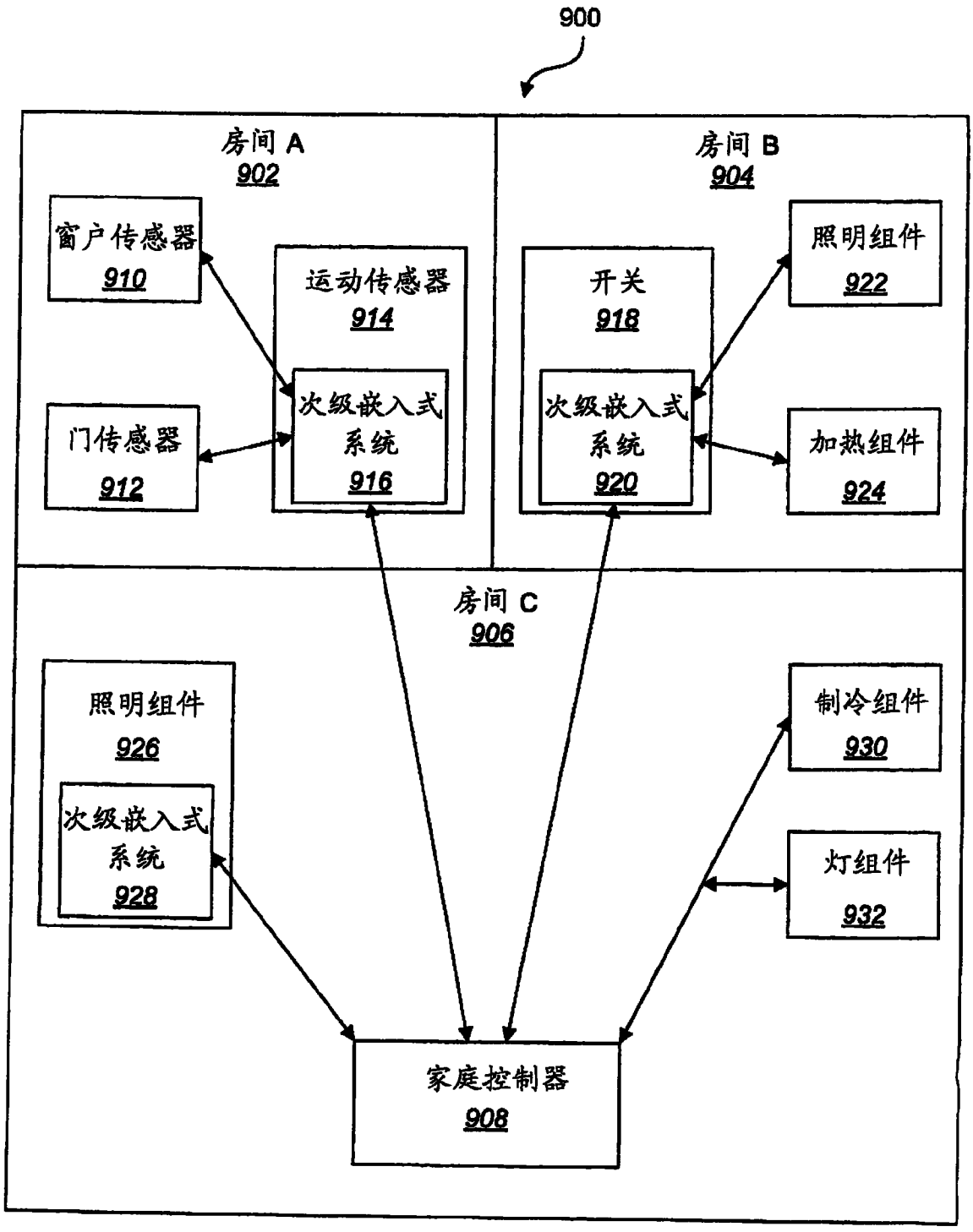

900
房间 A
902
窗户传感器
910
运动传感器
914
次级嵌入式系统
916
门传感器
912
房间 B
904
照明组件
922
开关
918
次级嵌入式系统
920
加热组件
924
房间 C
906
照明组件
926
次级嵌入式系统
928
制冷组件
930
灯组件
932
家庭控制器
908

图 9