

[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 200810085689.7

[43] 公开日 2008 年 12 月 10 日

[51] Int. Cl.

H04L 29/06 (2006.01)

G05B 19/418 (2006.01)

[11] 公开号 CN 101321165A

[22] 申请日 2008.1.25

[21] 申请号 200810085689.7

[30] 优先权

[32] 2007. 1. 26 [33] US [31] 11/627,477

[71] 申请人 洛克威尔自动控制技术股份有限公司

地址 美国俄亥俄州

[72] 发明人 J·C·小维尔金森

T·J·加斯帕 M·D·卡兰

N·L·小普鲁托 G·B·舒尔茨

J·A·米科 K·M·塔姆巴斯科

J·M·维索基

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 陈 炜

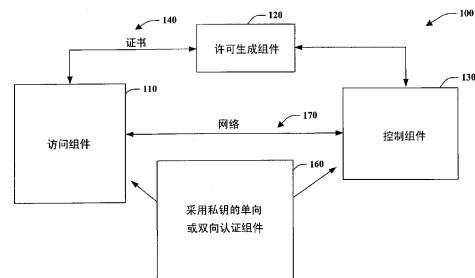
权利要求书 3 页 说明书 13 页 附图 10 页

[54] 发明名称

嵌入式系统中许可的认证

[57] 摘要

提供一种工业自动化系统。这包括至少一种由第三方授予以准许访问工业控制组件的部分的许可组件。部分基于私钥交换的至少一个协议组件帮助认证和对工业控制组件的部分的访问。



1、一种工业自动化系统，包括：

至少一个许可组件，它被许可生成组件（LGC）授予准许访问工业控制组件的部分；以及

至少一个协议组件，其部分基于非对称密钥交换以帮助认证和对所述工业控制组件的部分的访问。

2、如权利要求1所述的系统，其特征在于，所述非对称密钥交换与私钥组件相关联。

3、如权利要求1所述的系统，其特征在于，所述非对称密钥交换与公钥组件相关联。

4、如权利要求1所述的系统，其特征在于，所述许可组件是数字证书。

5、如权利要求4所述的系统，其特征在于，数字证书包括至少一个报头部分、许可部分或属性部分。

6、如权利要求4所述的系统，其特征在于，所述数字证书包括公钥组件或数字签名组件。

7、如权利要求4所述的系统，其特征在于，所述数字证书包括证书长度、证书类型或证书版本组件。

8、如权利要求4所述的系统，其特征在于，所述数字证书包括许可计数、许可列表、许可密钥或许可实例。

9、如权利要求4所述的系统，其特征在于，所述数字证书包括属性类型、以及属性长度或属性数据组件。

10、如权利要求1所述的系统，其特征在于，还包括用以处理至少两个认证组件之间的消息交换的状态机。

11、如权利要求10所述的系统，其特征在于，所述状态机包括至少三个状态，具有初始状态、质询提交状态、等待会话提交状态或会话状态。

12、如权利要求1所述的系统，其特征在于，所述协议组件还包括序列数生成器或随机数生成器。

13、如权利要求12所述的系统，其特征在于，所述协议组件还包括用以帮助认证的随机数生成器。

14、如权利要求 1 所述的系统，其特征在于，所述协议组件还包括 SHA-1 组件、级联组件或随机数生成器。

15、如权利要求 1 所述的系统，其特征在于，所述协议组件还包括非对称加密或解密算法。

16、如权利要求 1 所述的系统，其特征在于，所述协议组件还包括质询组件、证书组件或响应组件。

17、一种其上存储有用以帮助工业自动化环境中的许可的数据结构的计算机可读介质，所述数据结构包括：

第一数据字段，用以指定来自客户端的证书，所述证书作为来自第三方的许可被发布；

第二数据字段，用以指定对所述客户端的响应；以及

第三数据字段，它部分地基于所述证书和所述响应来建立会话。

18、如权利要求 17 所述的计算机可读介质，其特征在于，还包括用于单向认证的设备质询字段。

19、如权利要求 17 所述的计算机可读介质，其特征在于，还包括质询提交字段。

20、如权利要求 17 所述的计算机可读介质，其特征在于，还包括质询响应字段。

21、如权利要求 17 所述的计算机可读介质，其特征在于，还包括用于双向认证的会话提交字段。

22、如权利要求 17 所述的计算机可读介质，其特征在于，还包括会话响应字段。

23、一种用于工业控制组件的许可方法，包括：

从至少一个第三方组件获得证书；

向至少一个其它设备发送所述证书；以及

采用私钥和所述证书来确定是否建立了许可授予。

24、如权利要求 23 所述的方法，其特征在于，还包括向所述设备发送客户端证书。

25、如权利要求 23 所述的方法，其特征在于，还包括响应于接收到证书，向客户端发送质询。

26、如权利要求 25 所述的方法，其特征在于，还包括发送对所述质询的响应。

27、如权利要求 26 所述的方法，其特征在于，还包括在至少两个设备之间建立会话。

28、如权利要求 23 所述的方法，其特征在于，还包括采用公钥来验证与所述数字

证书相关联的签名。

29、如权利要求 28 所述的方法，其特征在于，还包括在签名被确定为无效的情况下生成错误消息。

30、如权利要求 29 所述的方法，其特征在于，还包括在至少一个验证程序之后交换随机数。

31、一种用于工业控制环境的许可系统，包括：

用于从至少一个第三方获得许可的装置；

用于在接收到所述许可之后通过工业控制网络传送证书的装置；以及

用于基于所述证书和所述许可来协商可信会话的装置。

嵌入式系统中许可的认证

相关申请的交叉引用

本申请是2006年9月29日提交的标题为 ALARM/EVENT ENCRYPTION IN AN INDUSTRIAL ENVIRONMENT（工业环境中的警报/事件加密）的美国专利申请序列 No.11/537,413 的部分继续申请，其全部内容通过引用包含于此。

技术领域

本主题发明通常涉及工业控制系统，尤其涉及提供一种采用许可组件作为加密认证和许可过程的部分的工业控制系统的认证协议。

背景

长久以来已经操作在紧密控制的工厂网络中的工业控制器是多个控制器和相关的模块通信。这些低层控制元件通常与从控制器聚集数据以及帮助管理企业的日常活动的高层计算系统或服务器通信。然而最近几年，控制系统已经迅速地成为适于向例如 Internet 的全球网络开放这些系统的 Ethernet 通信。虽然这有利于控制系统通过这样的全球网络通信，但是也出现了其它的问题，例如怎样保护敏感控制系统及其上存储的相关知识产权免受讹误，或者更糟糕的网络攻击（cyber attack）。直到现在，已经采用各种方法来认证需要通过公共网络向控制系统通信的网络用户。这些方法常常给控制系统施加负担来要求其不仅仅认证各个用户，还需要负责确定哪个用户被允许访问控制系统的哪个部分。

控制器提供了其中资源仅仅限于例如确定和认证谁或什么应该访问控制器的活动的嵌入式方法。通常，控制器或控制系统一般需要哪些限制的处理和存储能力来用于自动化制造操作。在授权访问在控制器（或控制组件）中所包含的有价值知识产权之前的尝试是采用外部服务器来检查特定设备或软件组件是否被许可这些访问。已采用专用于一个用户、公司或产品的协议以获得后续控制器访问（例如密码），而不在过程中使用的更多安全方案。

概要

以下给出了简单的概要以便提供对在此所述的某些方面的基本理解。该概要既不是广泛的概述，也非旨在标识关键/重要元件，或者刻划在此所述的各个方面的范围。唯一目的是以简单的形式给出某些概念作为对稍后给出的更详细描述的前序。

提供一种许可协议来在工业控制组件和寻求访问该工业控制组件的其它组件之间实现加密认证。例如设备或软件的寻求访问控制器的组件采用许可生成组件来寻求电子证书，这是对于该设备已经适当被许可来访问控制器的证明。可以使用许可证书来提供这种证明，其中例如私钥的加密组件可用于来证明希望访问控制系统的组件是该许可的可信持有者。可以提供单向或双向认证协议，随后对访问设备或软件授予从控制系统访问。通过采用许可生成组件来确定是否已经维护了适当的许可协定、控制器资源是否可以被保存。而且，由于加密技术已经被用作获得许可之后的认证过程的一部分，增加了优于现有系统的安全性。因此，提供了一种结构框架来保护在控制组件中的知识产权，其中框架确定了与控制组件通信的模块是被适当地许可的模块。因此，被许可的模块由于身份是已知的而可使用其它功能。

为了完成前述及相关目标，这里结合以下描述和附图描述了特定示例性方面。这些方面表示可被实现的各种方式，所有这些都被预期包含于此。当结合附图考虑以下详细描述时，其它优点和新颖特征将变得很明显。

附图的简要说明

图 1 是示出了工业自动化系统的自动化许可的示意框图。

图 2 是示出了单向认证过程和许可协议的示图。

图 3-5 示出了采用相互认证协议的授权和许可交换。

图 6 示出了示例许可认证协议。

图 7 是示出了用以形成许可连接的随机数级联（nonce concatenation）示的图。

图 8 示出了消息交换的示例性状态图。

图 9 示出了示例性许可证书。

图 10 示出了简化的消息交换过程。

详细说明

提供了一种用于工业自动化系统的许可协议。一方面，提供了工业自动化系统。

这包括由第三方授权以允许访问工业控制组件的部分的至少一个许可组件。部分基于私钥交换的至少一个协议组件有助于认证和对部分工业控制组件的访问。可以提供单独认证或相互认证协议来支持对工业控制组件的预期访问。

注意：如本申请中所用的例如“组件”、“协议”、“证书”等术语旨在指计算机相关实体、或者硬件、硬件和软件的组合、软件或应用到工业控制的自动化系统的执行软件。例如，组件可以是但不限于：运行在处理器上的进程、处理器、对象、可执行文件、执行线程、程序和计算机。作为示例，运行在服务器上的应用和服务器都可以是组件。一个或多个组件可以驻留在执行的进程和/或线程中，且组件可以位于一个计算机上，和/或分布在两个或多个计算机、工业控制器和/或其间相互通信的模块之间。

开始参考图 1，系统 100 示出了工业自动化系统的自动许可。访问组件 110 与许可生成组件 (LGC) 组件 120 交互以接收对一个或多个控制组件 130 的许可权限。LGC 120 可以是由一企业操作的计算机，该企业向访问组件 110 出售权限以便访问控制组件 130 的全部或部分（例如，访问部分或存储器、访问警报、事件、程序、方法等的权限）。例如，LGC 120 可以是控制组件 130 的制造商、控制组件的所有者或者被认为适于生成许可的第三方。如所示，可以通过第三方组件 120 向访问组件 110 发布证书 140，其中根据认证组件 160 使用证书以通过网络（或多个网络）170 获得对控制组件 130 的访问。通常，认证组件 160 利用证书 140 和例如私钥的一个或多个安全协议以访问控制组件 130。如以下参照图 2 的更详细描述的，在 160 可以采用单向认证过程，而图 3-8 示出了相互认证过程的方面。

认证组件 160 可被两个或多个组件使用以通过网络 170 在这些组件之间进行认证，其中认证意味着建立基本上安全和可信的连接来交换数据。访问组件 110 可以采用一个或多个计算机、工业组件或通过网络 170 与例如由可编程逻辑控制器 (PLC) 130 表示（或以下所述的其它工厂组件）的一个或多个工业控制组件 130 通信的其它网络组件。注意：访问组件 110 也可以是实际上与控制组件 130 类似的其它控制组件。

在已经发布证书 140 后，认证组件 160 允许在工业控制组件 130 和访问组件 120 之间的认证。在一方面，由认证组件 160 提供采用部分基于一般不要求存在公钥基础结构的非对称密钥系统的单向或相互认证方案的密码认证协议。这样的协议能抵抗一般公知的攻击。这样，基于密码的认证协议提供了针对参与包括控制器、I/O 模块、工厂设备、计算机、服务器、客户端和/或其它网络组件的工业自动化网络 170 的未授权

应用和设备的技术壁垒。

现在在以下参考附图 2-9 讨论更详细方面之前讨论许可的一些基本方面。许可通常涉及两个或多个过程。首先，由 LGC120 向供应商（称为被许可方或访问组件）发布许可。第二，由被许可方创建的客户端实现应该包括在运行时提供和验证对许可认证的动作。

当被许可方从 LGC 120 获得许可时，至少两个制品的电子拷贝被接收并用在下述的许可认证协议中。这可以包括许可证书 140，该证书可以用来在 130 向受保护的硬件/软件证明存在已由 LGC 120 发布的有效许可。例如，LGC120 可以拥有一个或多个控制组件 130，并由此授予访问组件的许可。在 160 私钥可以由被许可方用来证明它们是许可证书 140 的可信持有者。

通常，许可证书 140 是一电子文档，它包含有关被许可方信息，例如他们拥有的许可类型、以及已被分配给被许可方并用来验证他们身份的公钥。许可证书 140 应该由 LGC120 进行数字签名，以使得组件 130 可以验证证书本身的可靠性。通常，被许可方将许可证书 140 嵌入在其客户端或访问组件 110 内。在运行时，客户端可将许可证书 140 下载到受保护的组件 130 以确定它们被许可哪些。

在客户端可以访问受保护设备或组件 130 的被许可特征之前，它将许可证书 140 的拷贝下载到设备。这向设备提供了关于希望访问其受保护特征的客户端或访问组件 110 的信息。当拥有证书 140 时，设备将其解码并验证其可靠性。它通过利用由第三方 120 提供的公钥验证证书中的数字签名来执行这个操作。如果这个完成了，设备可以作出以下断言：该证书是有效的，且未被篡改；并且该证书是由 LGC 120 原始发布的。

通常，存在由该设备或组件 130 在其可准许访问由证书 140 提供的特征并授权被许可方访问其之前执行的至少一个或多个断言。通常，在 110 组件 130 向客户端发回质询。为了成功地满足质询，客户端或访问组件 110 利用自身嵌入的私钥来解密会话密钥。为了证明设备或组件 130 成功地解密该会话密钥，它可以生成会话密钥的单向散列，并将它发送回该设备。如果该散列与设备自身的会话密钥的散列相匹配，则质询成功，并且该设备可以执行断言。如上所述，还可以提供如以下更加详细描述的双向认证方案。当客户端和访问组件 110 已经被成功证明该设备拥有与所提供的证书 140 相关的私钥时，该设备或组件 130 可以允许客户端访问由证书指定的许可特征。

如果任意的以下示例为真，则该设备或组件 130 可以拒绝对许可特征的访问：客

户端从不提供证书；证书验证不成功，例如，证书被篡改或者没有被第三方签名；客户端无法提供经解密的会话密钥的散列；客户端不具有与证书内的公钥相匹配的私钥；证书不准许访问客户端试图访问的特定特征；证书包含在过去的期满时间，或者在以后发生的有效时间；和/或证书中的公钥与设备的撤销列表中的密钥相匹配。

在进行前要注意，组件 110 可以包括例如服务器、客户端、通信模块、移动计算机、无线组件、控制组件等的能够通过网络 170 交互的各种计算机或网络组件。类似的，这里所用的术语 PLC 可以包括能够跨多个组件、系统和/或网络 170 共享的功能块。例如，一个或多个 PLC130 可以通过网络 170 与各种网络设备通信和协作。这可以包括基本上任意类型的控制、通信模块、计算机、I/O 设备、传感器、人机接口（HMI），它们通过包括控制、自动化和/或公共网络的网络 114 通信。

网络 170 可以包括公共网络，例如互联网、内联网和诸如包括 DeviceNet（设备网）和 ControlNet（控制网）的控制和信息协议（CIP）网络的自动化网络。其它网络包括以太网、DH/DH+、远程 I/O、现场总线、Modbus、Profibus、无线网络、串行协议等。另外，网络设备可以包括各种可行性（硬件和/或软件组件）。这些包括组件，例如具有虚拟局域网（VLAN）能力的交换机、LAN、WAN、代理、网关、路由器、防火墙、虚拟个人网络（VPN）设备、服务器、客户端、计算机、配置工具、监测工具和/或其它设备。

现在参考图 2，它示出了单向认证协议和过程。如上所述，附图 2-9 示出了相互认证协议和过程方面。然而，出于简要说明的目的，方法被示出并描述为一系列动作，应该理解和认同的是，该方法不限于动作的顺序，因为根据这里所示和所述的，某些动作可以按照不同的顺序发生和/或与其它动作并发进行。例如，本领域技术人员可以理解和认同，该方法可另外表示为例如状态表中的一系列相关状态或事件。此外，不是所有示出的动作都被要求来实现这里所述的方法。

参考图 2，并且在附图标记 210，提供了证书消息。通常，在访问设备 212 的受保护特征之前，在 210，客户端 214 向设备呈递自己的许可证书。其通过在 210 向设备发起证书消息来执行该操作。证书消息 210 将证书消息下载到设备。证书消息是一种逻辑消息，取决于证书文档的实际大小和传输能力，该消息可以是多个实际的物理消息。

一旦在 210 接收证书消息，设备 212 就解码该证书并对其进行处理。对于设备定位在证书内的每个委托人部分，试图标识和验证相关联授权的数字签名。对于简单许

可，通常应该是一个委托人部分（对于被许可方）和第三方的授权元素。第三方的数字签名应该参考委托人元素，且应该利用第三方公钥（嵌入在设备 212 内）来正确验证。如果委托人的数字签名正确的验证了，那么设备 212 可以假定证书的特定委托人部分是有效的、未经修改的和可信的。

在 220，可以由设备 212 发出质询消息。即使证书可以被证明是可信的，该设备应该仍确认客户端 214 与在证书中所标识的委托人相关。因此，在 220，设备准备质询消息以发送回客户端。为了准备质询消息，设备 212 应该创建例如随机会话密钥，尽管其它组件也是可以采用的。如果委托人具有定义了委托人的公钥的相关联密钥信息元素，则会话密钥利用所定义的密钥来加密。如果没有与委托人相关联的密钥，则会话密钥可被放置到未经加密的质询消息中。可以对证书中的每个委托人重复对会话密钥加密的过程。设备 212 能够自由地对每个委托人再使用同一会话密钥值，或者按需为每个委托人实例生成一个新的会话密钥值。该组经加密的会话密钥可以被发送回客户端作为针对其一即这是它所提供的证书的授权持有者一的质询。质询消息 220 是对证书消息 210 的逻辑响应。

前进到 230，可以由客户端 214 生成响应消息。为了满足质询 220 并向设备 212 证明客户端 214 被授权，在 230，它解码质询消息并生成匹配的响应消息。响应消息 230 是一种在质询消息 220 中采用每个经加密的会话密钥，并利用相关联委托人的私钥（客户端应当拥有）对其解密的内容。为了证明设备 212 可成功解码质询和会话密钥，客户端 214 生成每个会话密钥的单向散列，并将其发送给设备作为对质询的响应消息 230。

在 240，协议 200 的最后阶段是验证来自客户端的响应消息 230，并返回标识质询响应协商成功或失败的会话消息。这里，设备 212 从响应消息 230 得到散列会话密钥，并将其与已经执行的会话密钥的单向散列相比较。如果它们匹配，那么会话可以被成功建立。注意：成功建立会话意味着设备可以信任针对相应的委托人做出的断言。如果断言是许可断言，则客户端 214 可以被许可指定的特征。对于客户端 214 可以继续在某些会话上而非其它进行质询。该设备应该确保他们已经访问了其基于已成功建立的会话而具有权限的特征。

尽管上述协议 200 使用术语“会话密钥”来描述在客户端 214 和设备 212 之间定义的信息的共享部分，这个值本身并不表示在客户端和设备之间建立的通信会话。假定在客户端和设备之间的多数通信可以发生在连接的上下文中。与会话相关联的断言

可以被认为是有效的，只要保持相应的连接。如果连接丢失，客户端可能需要在许可协议 200 中通过在最新建立的连接上发出新的证书消息来重新建立他的权限。许可协议 200 不排除使用未连接的消息交换。在此情况中，“会话密钥”可以被用来在客户端 214 与设备 212 之间建立逻辑上下文。

转到图 3-5，示出了相互认证协议。在进行之前，提供一般的讨论。支持许可受保护服务的设备管理在许可交换和验证过程的实现中使用的多个电子制品。这可以包括用于企业或第三方的身份证书，该证书包括被用来标识发布到被许可方的有效许可证书的公钥。由第三方数字签名的和发布的身份证书可以被提供给硬件或软件。该证书包括硬件/软件组件的公钥。另一组件可以包括对应于在硬件身份证书中的公钥的硬件私钥。可以提供任选的撤销列表，该列表包括有关哪个在先授予的许可已经被第三方或企业实体撤销的信息。

设备应该保护所有的这些制品免受篡改。然而，它们其中的两个具有设备应该考虑的附加处理要求。设备私钥是不为其它实体所知的秘密数据。为此，设备应该设法保持设备的私钥被很好的隐藏和保护免受检查。撤销列表是一种在设备的使用期内不保持静态的数据。该设备应该具有允许升级撤销列表的某些手段。

当被许可方包括来自第三方的许可时，该被许可方应该接收在许可认证协议中使用的至少三个制品的电子拷贝。这可以包括包含公钥并被用于验证由设备或组件提供的证书的第三方的身份证书。可以提供可被用来向受保护硬件证明存在已由第三方发布的有效许可的许可证书。还可以采用可被许可者用来证明它们是许可证书的可信持有者的私钥。为了访问设备的许可受保护特征，被许可方和设备应该参与到交换和验证协议中，其中他们交换各自的证书并相互生成质询以响应。该协议可以采用至少三个双向交换以便实现如图 3-5 所示的目标。

继续到图 3，它示出了证书交换 300。客户端 310 通过向设备 320 发送自身证书来启动协议。这向设备 320 提供了有关客户端 310 的身份信息，因为证书包括客户端的公钥，并且允许访问的设备的服务。当拥有证书时，设备 320 对其解码并验证其完整性和可信性。设备 320 通过利用第三方的公钥验证在证书内的数字签名来执行此操作。它还对照它的撤销列表检查嵌入在客户端证书中的公钥。如果成功，设备可以作出以下断言：被许可方证书是有效的且未被篡改；被许可方证书是由第三方原始发布的；以及许可者证书可以被用来标识客户端被许可使用设备上的哪个服务。

如果成功，则设备 320 使用自己的身份证书作为响应，且客户端解码并验证设备

证书的完整性和可信性，并验证设备的公钥没有被撤回。如果成功，则该设备可以作出类似的一组判断，包括：设备证书是有效的且未被篡改；以及设备证书是由第三方原始发布的。

图4示出了质询交换过程400。在交换和验证证书后，双方（或多方）对相互之间所要求的有了理解，且设备420知晓客户端410断言其被许可的权限是什么；然而，他们不信任其他参与方是他们所呈递的证书的有效持有者。他们不做任何操作来认证其他参与方。建立那种信任是对于在图4和5所示的以下两个交换的一个可能的原因。

为了启动质询交换400，客户端410为设备420准备非确定性质询。该质询用设备的公钥加密，并由客户端数字签名。对该质询进行加密保证了仅仅具有正确私钥的设备可以成功响应该质询。作为响应，设备420解码质询，并准备其看似相似的质询返回给客户端。其对客户端的质询也包含由客户端的公钥加密并由设备数字签名的非确定性质询。通过数字签名该消息，客户端410和设备420具有保证该消息是由公钥的持有者产生的并且在过程中未被篡改的附加级。

为了减少往返行程的数量，设备对客户端410的质询包括其对客户端质询的响应。这种响应可以被包括在设备420发送回客户端410的数据的经加密的部分中。在此交换后，客户端可以作出至少不止一个断言，其中设备被认为是所呈递的设备证书的有效持有者。

转到图5，它示出了会话建立过程500。在这方面，设备520希望客户端510确实在上述证书交换期间呈递的许可证书的有效持有者的类似确信。为了完成许可交换，客户端510响应在前一交换中呈现的设备质询。当设备520已经确认了客户端成功地解释了其质询时，许可交换和验证完成。该设备现在能够进行关于客户端510的相应断言：客户端是所呈递的许可证书的有效持有者。

在这一点，设备可以允许客户端访问由证书指定的许可特征。如果以下的任一个为真，则该设备可以拒绝对许可特征的访问：客户端从不提供证书，或者该证书是不支持的格式；证书验证不成功；客户端510无法提供对其质询的响应；客户端不具有与证书中的公钥相匹配的私钥；证书不授予对客户端试图访问的特定特征的访问；证书包含在过去的期满时间，或者在以后发生的有效时间。该信息被包含在属性部分，且可以由知晓当前时间的设备使用；和/或证书中的许可信息与设备撤销列表中的信息相匹配。这可能表示尽管客户端具有有效许可和证书，但所授予的许可已经从被许可方撤销。

参考图 6，它示出了许可认证协议 600 的示例方面。可以提供协议 600 的以下成分：

在 610，级联是将字节串组合在一起的过程。在 620，SHA-1 是一加密散列函数，其采用任意长度的字节串（消息），并生成固定长度的字节串（例如，20 字节）。

在 630，随机数是来自没有可辨模式（discernible pattern）的序列的值。对于随机数的这个应用，希望随机数的源在统计上是随机的，且从非确定性原因导出。在 640，序列数是来自具有可辨模式的序列的值。如果序列数是基于时间模式的，那么使用表示“TIME_x”。在设备能够表示时间的范围内，时间值应该包括数据值和对分秒的时间粒度的表示（如果可以的话）。在 650，RSA 是非对称加密和解密算法。消息可以利用公共或私有密钥被转换为加密信息，使得可利用其它密钥将其转换回原始消息。在 660，数字签名是一种通过采用互补（complementary）算法来认证消息的方法。在 670，质询是用于认证及避免重放攻击的单次使用值（随机数）。在 680，证书是最小编码持有者的证书和公钥的数据块，且由证书发布授权机构进行数字签名。在 690，响应是标识会话建立协议的成功或失败的数据块。

现在转到图 7，示出了示例协议交换 700。交换 700 是在客户端 710 和设备 720 之间，但是也可涉及例如服务器或工业通信模块的其它组件。在 730，客户端 710 向设备 720 发出证书提交消息。该消息的一个目的是将客户端的证书下载到设备 720，并获得设备的证书。一旦接收到证书提交消息，设备 720 就解码该证书并处理它。处理证书涉及参照证书发布授权机构的设备知晓的公钥（具体是第三方的公钥）验证数字签名。如果验证了数字签名，那么设备 710 可以假定证书是有效的、未经修改的和可信的。如果证书有任何原因是无效的，错误响应可以被返回到客户端以代替 740 的证书响应消息。

在 740，设备 720 响应由客户端自己的证书发送的证书提交消息 730。该证书还应该由证书发布授权机构（第三方）数字签名。一旦接收到证书响应消息 740，客户端 710 就解码该证书并处理它，以验证该数字签名来确保证书是有效的、未经修改的和可信的。客户端还可以支持能够用来拒绝设备证书的撤销列表。

在 750，即使交换的证书可以证明是可信的，双方仍然确认另一方是证书内所标识的实际方。为此，客户端 710 在 750 向设备发起质询（以及设备会响应自己的质询返回给客户端）。如之前所示，质询可以由单次使用的一组值（随机数）组成。客户端 710 使用随机数生成器来产生随机字节序列，并接着用序列值和当前时间值级联它

们。一实现应该争取提供例如 16 字节的随机字节序列，例如，尽管最小实现可以使用与 4 字节长一样短的序列。该组字节接着使用 SHA-1 散列算法转换成固定长度的字节组。该 20 字节的序列可以被称为 CHALLENGEClient（质询客户端）值。

通过利用设备的公钥（从设备证书获得）加密该值并利用自己的私钥数字签名该结果，客户端 710 对设备形成质询消息 750。该质询消息 750 接着被提交给设备。为了响应质询，设备 720 验证消息的数字签名，通过利用自己的私钥解密消息数据来解码原始的 CHALLENGEClient 值。如果质询提交消息 750 是无效的（例如无效签名），则返回错误响应，而不是质询响应消息 760。

在 760，被发送回客户端 710 的质询响应消息有双重目的。它可以被用来开始客户端 710 的认证，以证明它是在证书提交消息 730 中被传送的 CERTClient 证书的有效持有者。同样，它还可以被用来回答客户端的质询。在此过程中，它证明客户端是在证书响应消息 740 中被传送的 CERTDevice 证书的有效持有者。

通常，设备 720 利用由客户端 710 用来生成其质询数据的同一算法来生成自己的 CHALLENGEDevice（质询设备）数据。它生成随机字节序列，并级联序列数和时间值，接着生成整个序列的 SHA-1 散列。CHALLENGEClient 和 CHALLENGEDevice 数据块可以被级联到一起成为接着利用客户端的公钥（从 CERTClient 证书获得）加密的 40 字节的数据块。该结果接着由设备 720 数字签名以证明自己的可靠性。

当客户端 710 接收响应消息 760 时，它验证数字签名并接着解密消息数据。当解密时，客户端 710 应该查找其原始发送到设备的 CHALLENGEClient 数据块。如果这个数据块与由客户端 710 发送的原始数据块相匹配，那么设备 720 已经在 760 成功地响应了的客户端的质询，且客户端 710 可以假定设备是在证书响应消息 740 中接收到的 CERTDevice 证书的有效持有者。如果质询响应消息 760 是无效的，客户端中断许可尝试，并不继续在 770 的会话提交消息。客户端 710 还应该查找由设备 720 产生的 CHALLENGEDevice 数据块。过程的最后步骤是为客户端 710 证明设备 720 其能够正确解码该值。

在 770，还需要被验证的剩余断言是客户端 710 是在初始质询提交消息 750 中提交的 CERTClient 证书的有效持有者。为此，客户端 710 采用在质询响应消息 760 中获得的 CHALLENGEDevice 数据，并利用设备的公钥对其加密、数字签名该消息、并把它发送回设备 720。当设备 720 接收到会话提交消息 770 时，它验证客户端 710 的数字签名，并接着解码该经加密的数据块。该设备 720 应该查找在质询响应消息 760 中

被发送到客户端的相同的 CHALLENGEDevice 字节序列。如果这是相同的字节组，那么客户端 710 已经成功的响应该质询，且设备 720 可以信任该客户端是在证书提交 730 中接收到的 CERTClient 证书的有效持有者。

在 780，过程 700 的最后步骤是为设备 720 向客户端 720 指示许可会话是否被成功建立。该设备 720 准备向客户端指示该设备是否允许会话的响应。该响应包括有关哪个许可被接收和哪个被拒绝的信息。它接着数字签名这个响应，并将其发送回该客户端作为会话响应消息。当这个消息 780 被客户端 710 接收到时，它可以验证该数字签名，并知晓是否已经访问许可受保护特征。有可能客户端 710 在一些会话上而非其它上继续质询。该设备 720 应该确保在它们成功建立的会话的上下文中客户端 710 已经访问了特征。

图 8 示出了消息交换的示例性状态图 800。尽管示出了四种状态，应该理解的，可以提供多于四种状态。状态图 800 包括四种状态，例如初始状态 810、等待质询提交状态 820、等待会话提交状态 830 和会话状态 840。如所示，对于进入相应状态而非初始状态 810 的转移包括接收到有效的客户端证书或发送有效的证书响应、接收到有效的质询或发送质询响应、和/或接收在设备的质询或发送会话响应。退出各自状态的原因包括无效签名、超时、错误检测、无效质询和/或会话关闭或超时。如可以理解的，可在相应状态中提供其它转移。

参考图 9，示出了示例证书 900。加密许可可以采用满足嵌入式环境需要的二进制证书 900。证书 900 可以被设计成在其表示上压缩，却在内容上是可表达的和可扩展的。证书的一般组织是三部分。证书报头部分 910 定义证书 900 的大小和格式版本。许可部分 920 是可变长度部分，定义了由证书授予的许可。属性部分 930 是可变长度部分，其可以包括多个有关证书 900 的附加属性。通常，具有在这个部分 930 中查找到的两个属性。“公钥” 940 定义与这个证书 900 的持有者相关联的公钥。“数字签名” 属性 950 为证书中先于其的所有数据提供验证。该证书报头部分 910 可以包括下表的成分：

名称	数据类型	描述
证书长度	UINT	以字节计的证书长度
证书	UINT	证书的格式类型。这个属性的唯一定义值是：0—“身份

类型		“证书”。它包括属性部分，但是不包括许可部分。证书的这个类型可以被用来表示授权的公钥而不意味任何许可。1—“许可证书”。它包括许可部分以及包含公钥和数字签名的属性部分。
证书版本	UNIT	证书的版本。初始设置成值 1。

许可部分 920 出现在被用于许可的任何证书中。它的目的是定义已经被授予许可证书 900 的有效持有者的许可组。该部分 920 是如下表定义的许可结构的计数组。

名称	数据类型	描述
许可计数	UINT	在许可列表中的成员数量
许可列表	结构数组:	许可列表是被授予证书的有效持有者的各个许可的数组。
许可密钥	UINT	特定授予许可的数字标识符。
许可实例	UINT	限定授予许可的特定实例的数值。由于授予的许可可被撤销和可能被恢复，撤销信息指定哪个许可的实例已经被撤销。

属性部分 930 包括提供有关证书的附加信息的一组类型化参数。属性部分 930 可以被设计成可扩充性，因为可随时间引入新的属性。在属性部分中的属性的数量并非预定的；其中实现应该解析属性部分到证书的长度。可在部分 930 中查找的主要属性 960 是公钥属性（与证书持有者的公钥通信）和数字签名（验证来自证书发布者的证书的可靠性）。该数字签名属性 950 可以被假定为证实在其之前的所有证书数据。这意味着它应该是在属性部分 930 中的最后的属性。

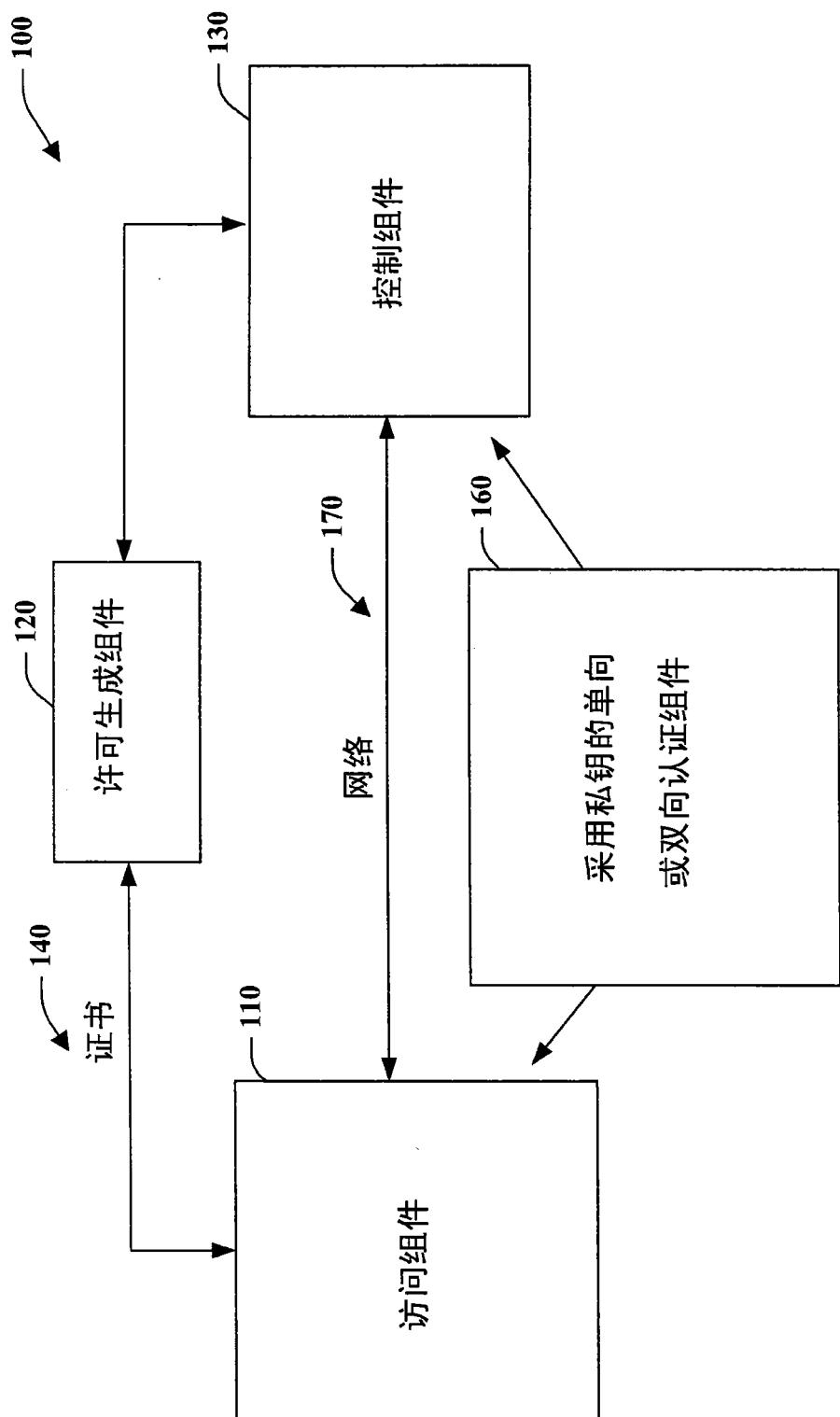
属性的格式可以如下表中定义：

名称	数据类型	描述
属性类型	UINT	证书的类型。属性类型可以利用允许实现知晓如何操作新的属性类型的信息来编码。如果实现可自由忽略不理解的属性类型，则属性类型的高位是零。如果确认实现应该

		理解属性的语义，则高位可以被设置为 1。如果实现在证书内遇到其不理解或不支持的属性类型，且高位被置位，那么证书验证过程应该失败。
属性长度	UINT	以字节计的属性长度。
属性数据	USINT 数组	与属性相关的数据值。这个数据的解释依赖于属性类型的类型。

附图 10 示出了简化的消息交换过程 1000。在简化的交换 1000 中，客户端 1010 向设备 1020 提交证书 1030。设备 1020 验证证书是否有效，从而该设备现在具有客户端的公钥。设备 1020 生成随机数（仅使用一次的数），其中随机数利用客户端的公钥被散列和加密，并在 1040 被作为质询的部分发送到客户端。客户端 1010 解密发送的数据、散列该数据、并作为响应 1050 发送回。设备 1020 比较客户端的响应和预期值，并且如果相等，则客户端被许可。在 1060，由设备 1020 发送指示会话已经建立的会话响应。

以上所述的包括各个示例性方面。当然，出于描述这些方面的目的，不可能描述组件的每个可预想的组合或方法，但是本领域普通技术人员可以认识到，许多其它组合和改变也是可能的。因此，这里所述的方面意味着包含落入所附权利要求的精神和范围内的所有这些变更、修改和变化。此外，术语“包括”被用在详细说明或权利要求中的范围内，此术语意味着以与术语“包含”相似的方式包括的，因为在权利要求中“包含”在使用时被解释为过渡词。



总 1

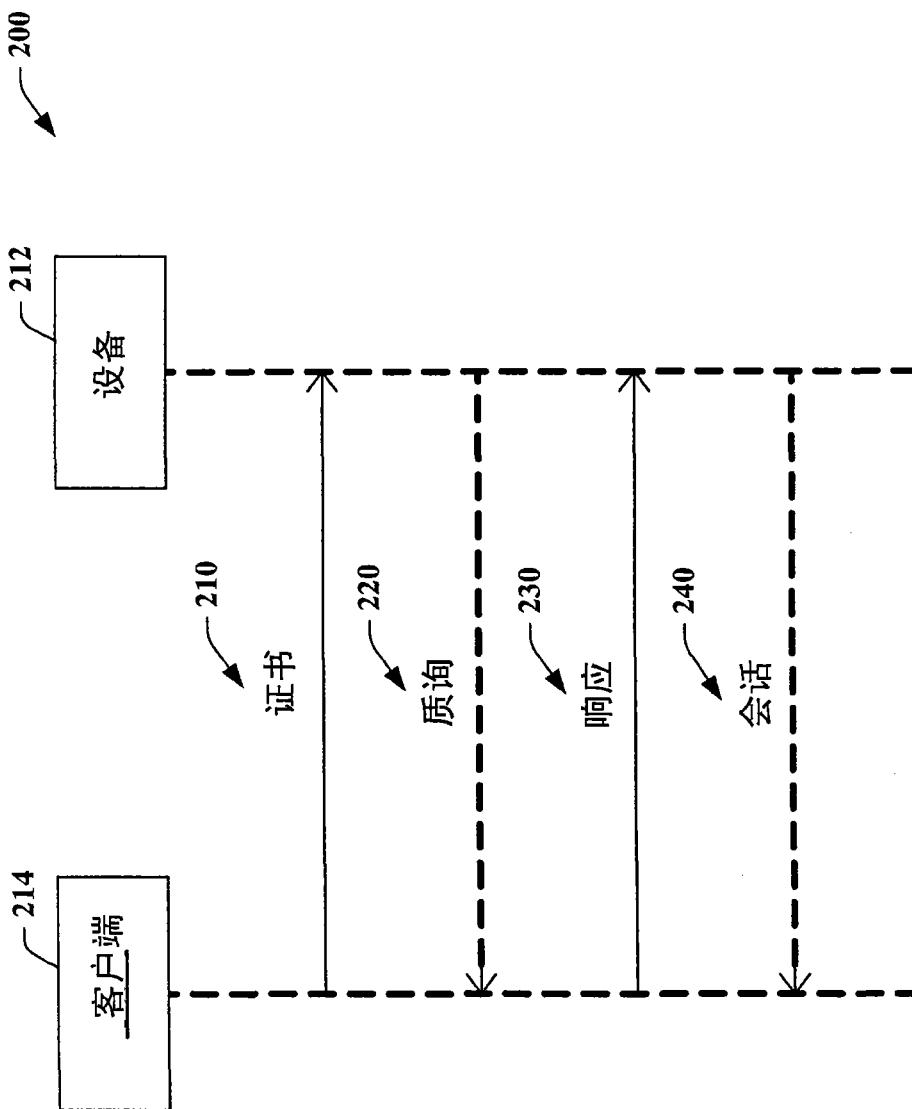


图 2

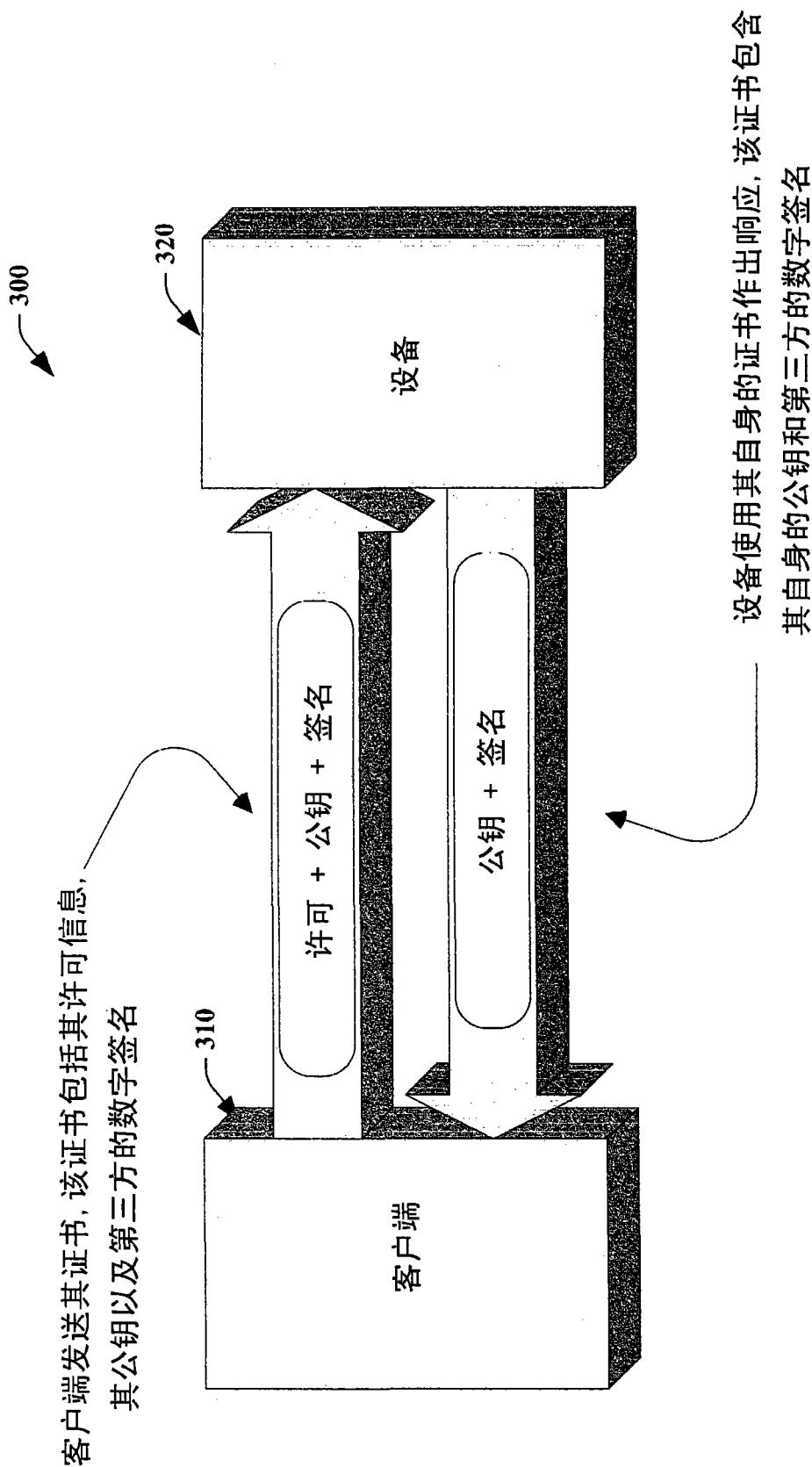
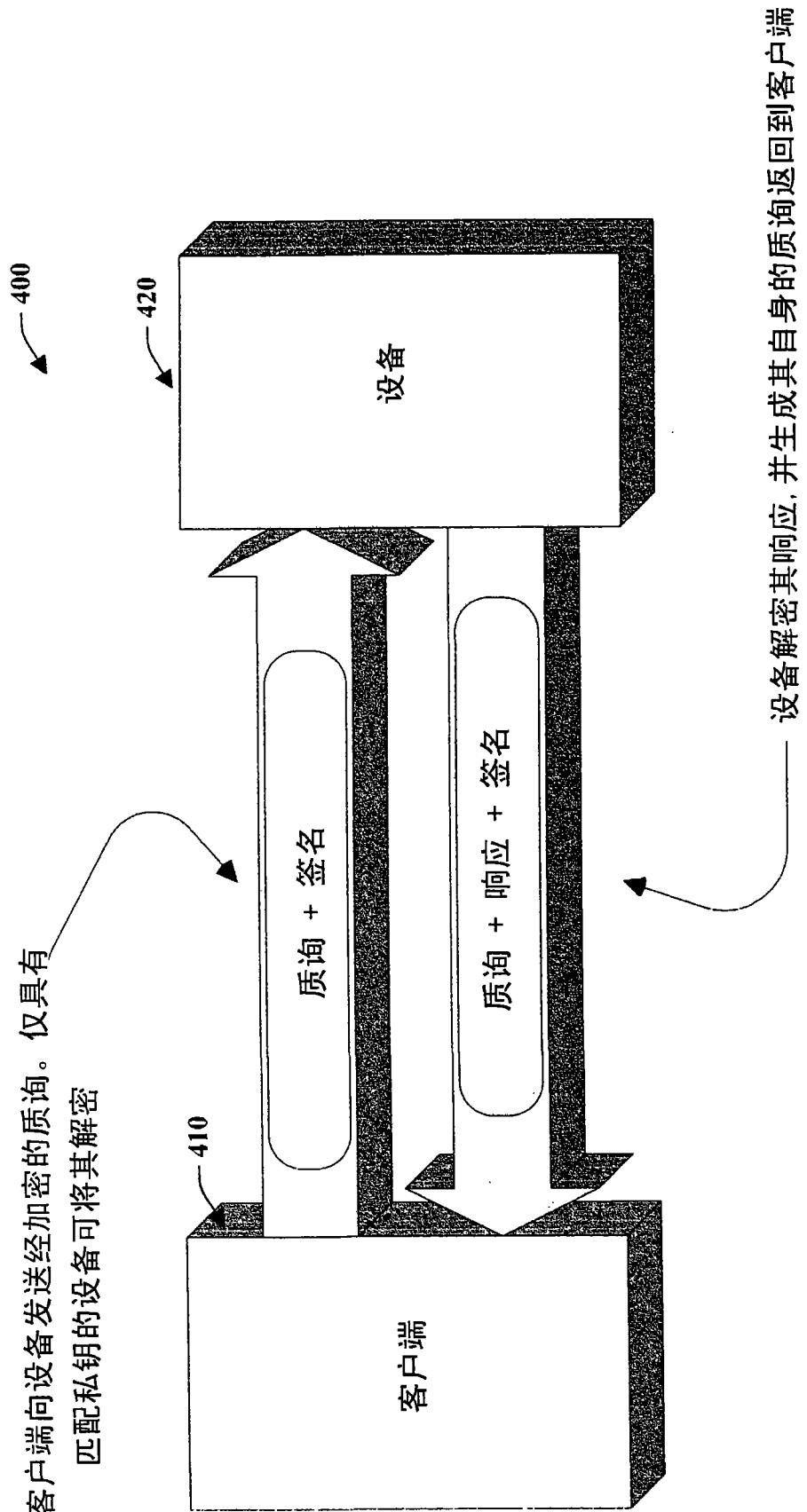


图 3



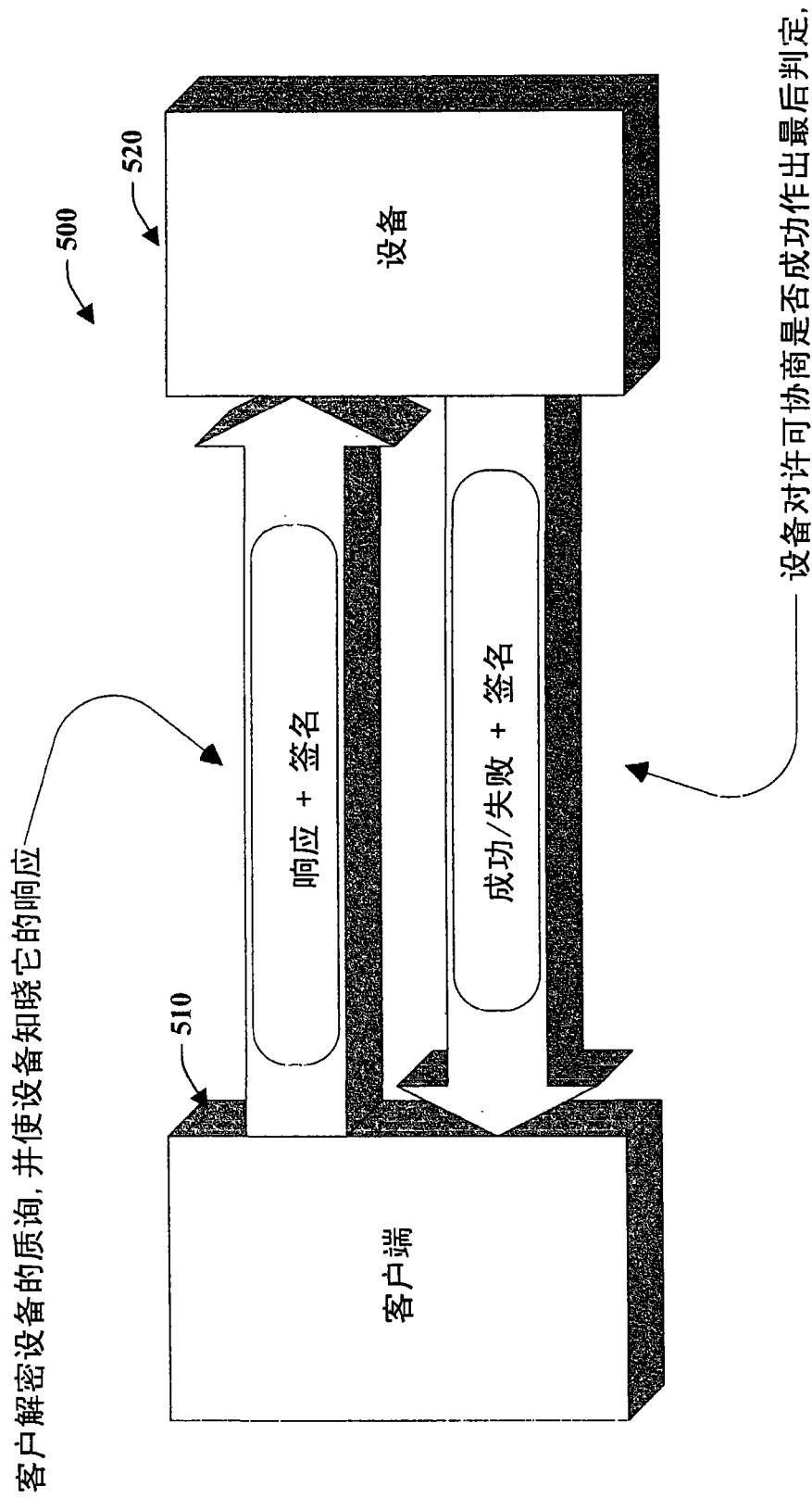


图 5

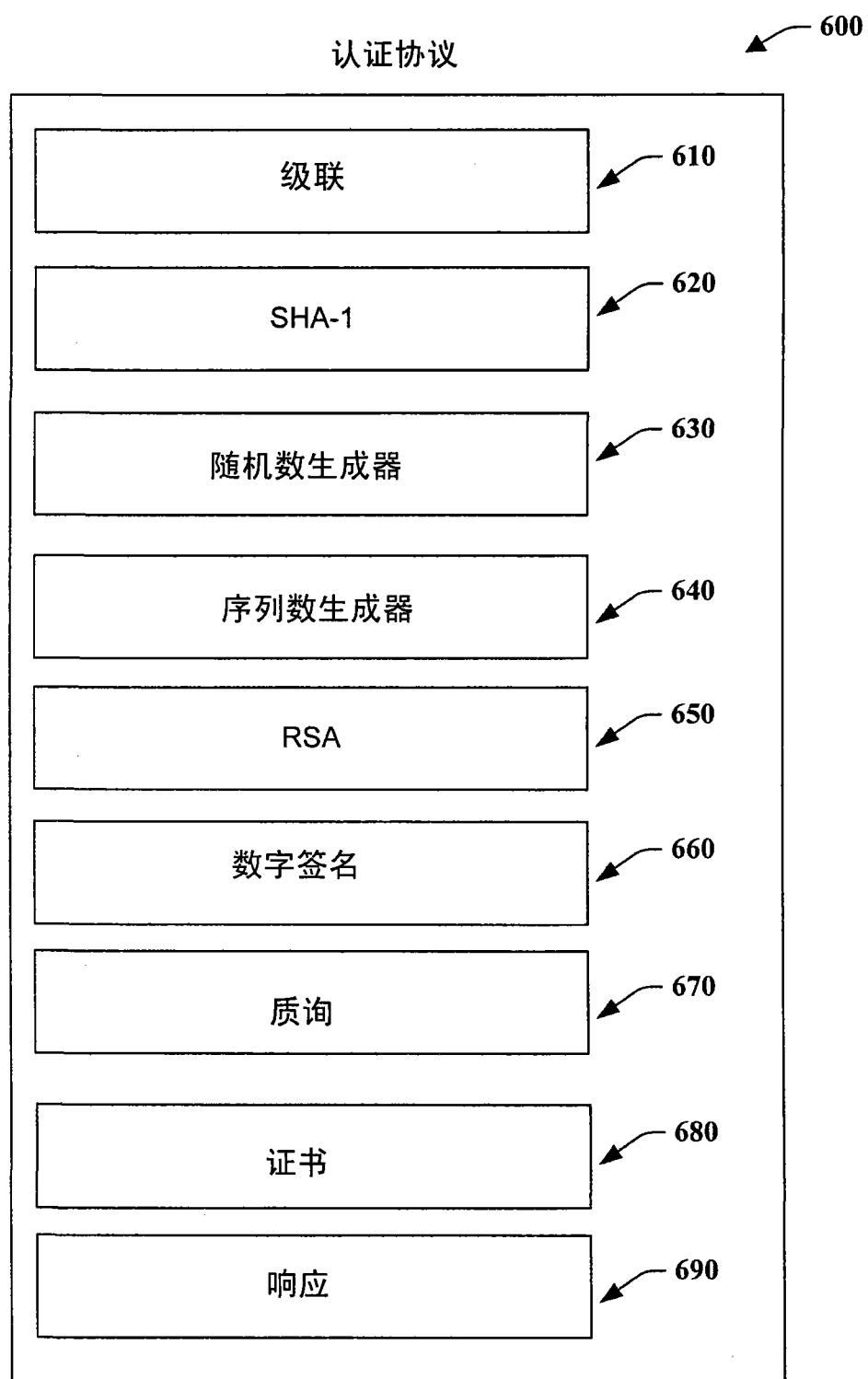


图 6

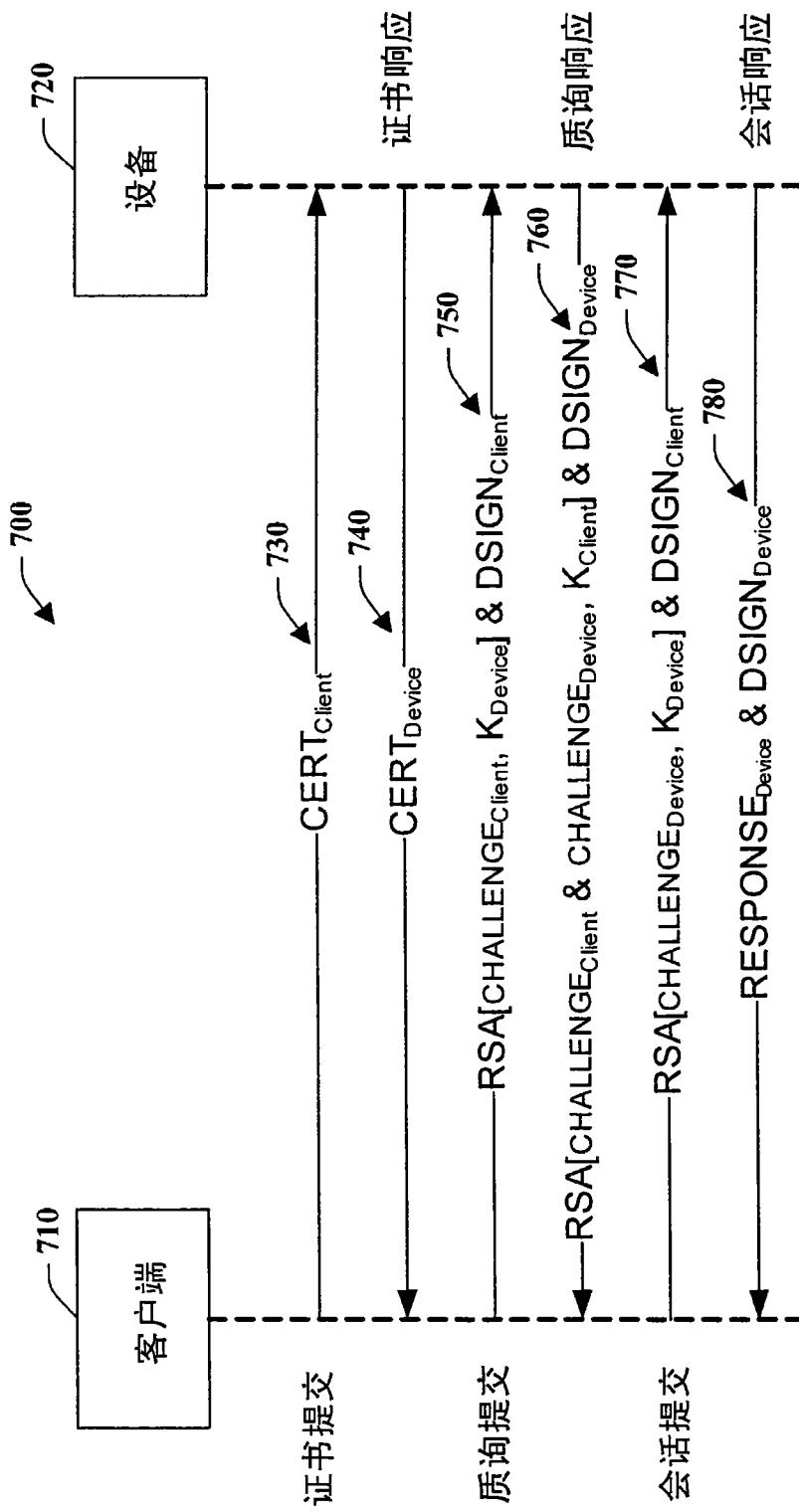


图 7

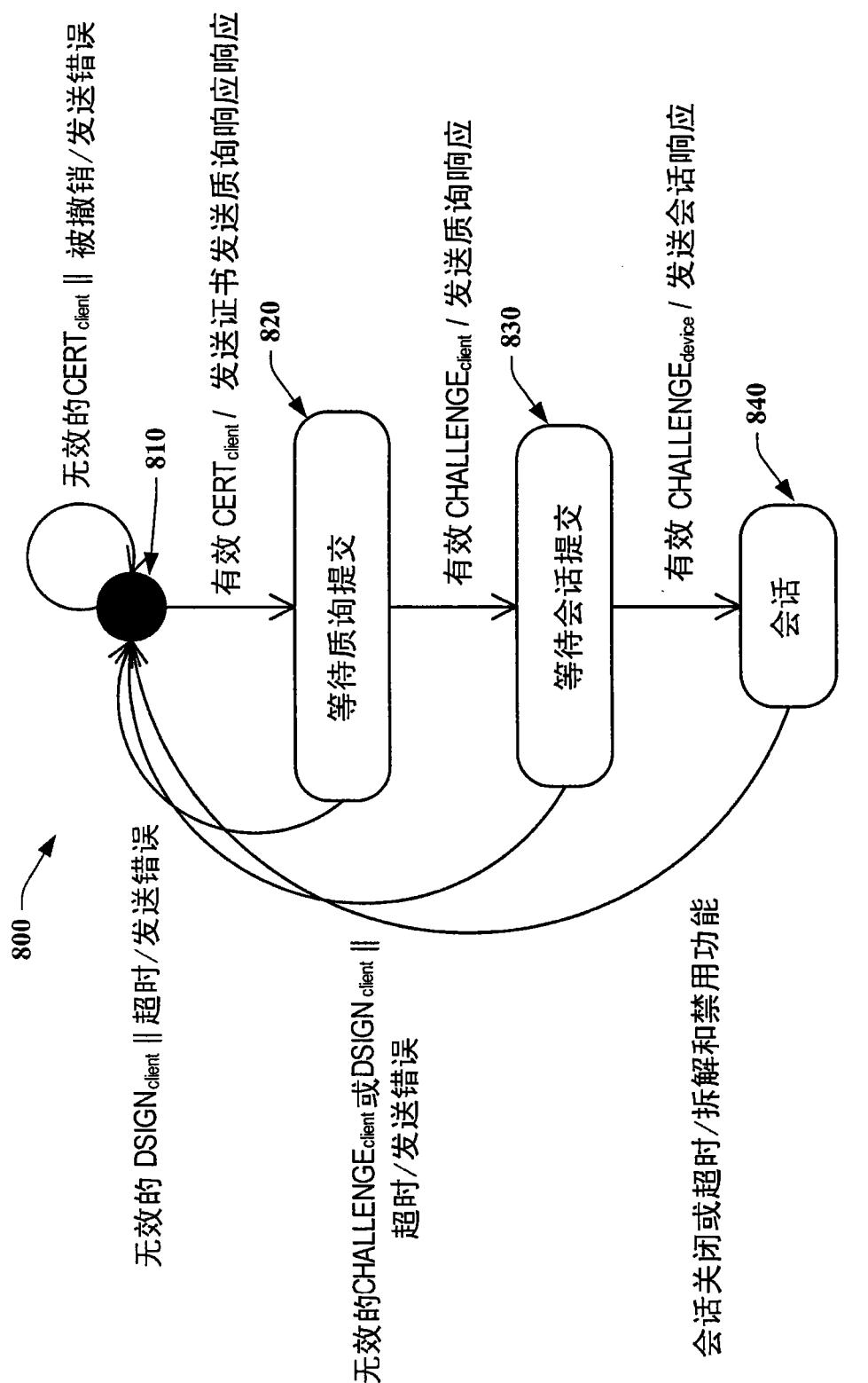
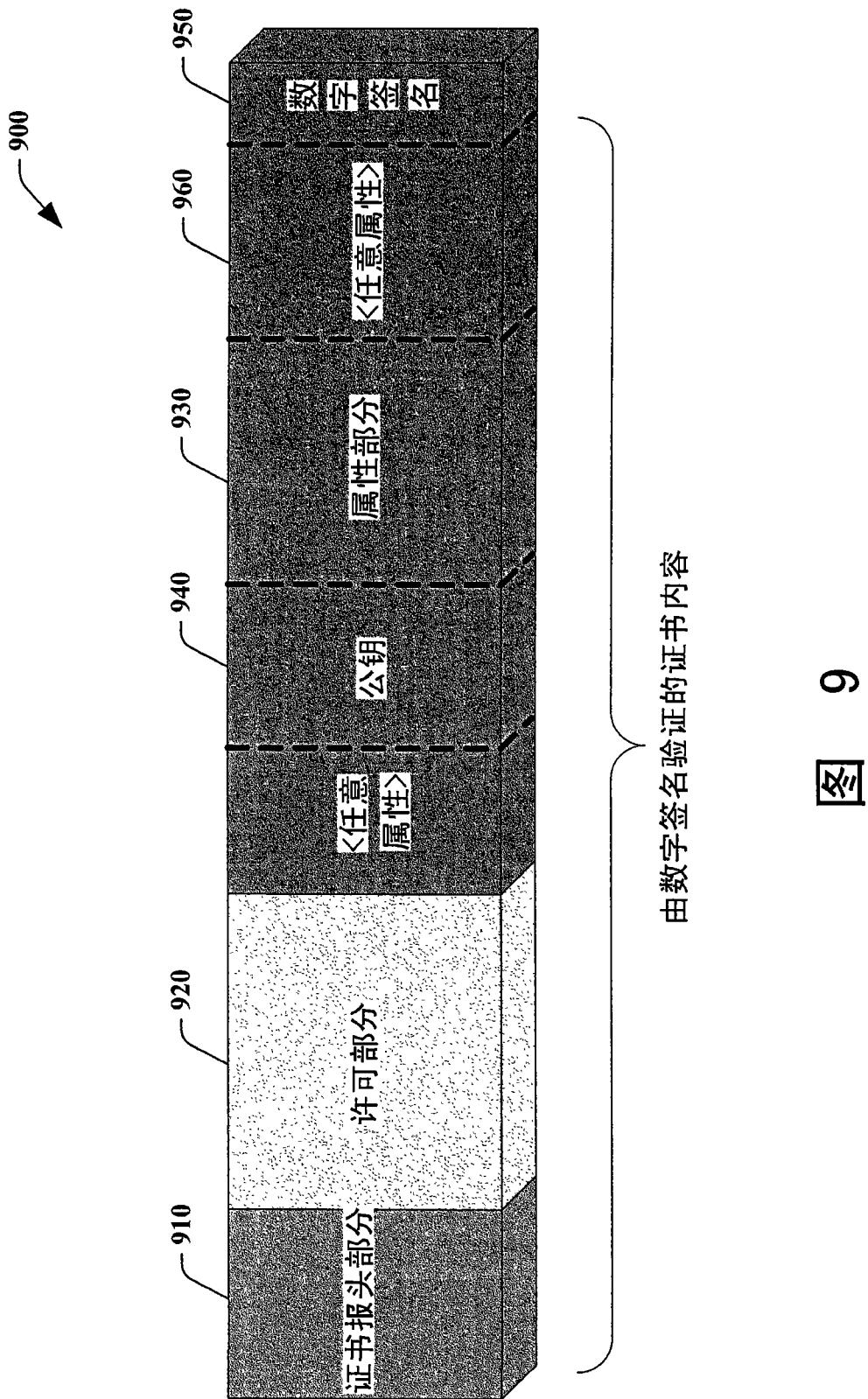


图 8



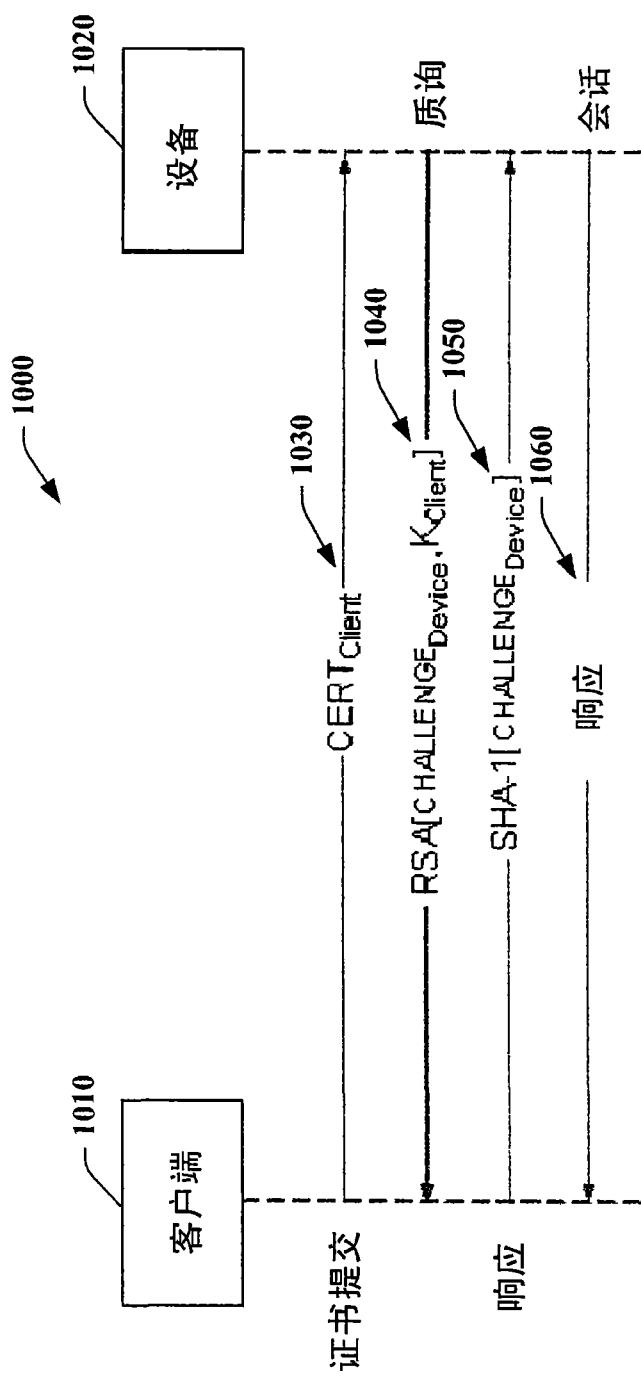


图 10