(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 1909421 B
(45)授权公告日 2010.09.29

(21)申请号 200610109209.7

(22)申请日 2006.08.01

(30)优先权数据
2005-223084 2005.08.01 JP

(73)专利权人 索尼株式会社
地址 日本东京都

(72)发明人 杉山寿伸

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

(51)Int.Cl.
*H04B 10/10*(2006.01)
*H04L 9/00*(2006.01)

(56)对比文件
WO 01/80463 A2,2001.10.25, 说明书第3页第5段至第5页第4段,附图1－5.
JP 特开2004-320708 A,2004.11.11, 全文.
CN 1327680 A,2001.12.19, 说明书第2页第2段至第6页第4段.
CN 1458749 A,2003.11.26, 全文.
CN 1249584 A,2000.04.05, 说明书第2页第3段至第4页第3段,附图1－2.

审查员 袁堃

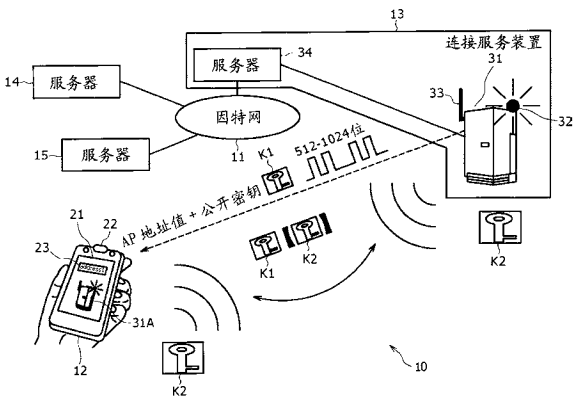
权利要求书 2 页 说明书 12 页 附图 16 页

(54)发明名称

信息处理系统、信息处理装置和方法

(57)摘要

本发明提供一种信息处理系统、信息处理装置和方法。该信息处理系统用于:通过从光源发出的光线的变化,公开分发第一密钥;从光源发出的光线中提取第一密钥;利用所提取的第一密钥对第二密钥进行加密,以通过近距离通信发送加密后的第二密钥;接收加密后的第二密钥,并对接收到的第二密钥进行解密;以及利用第二密钥作为公共密钥传输信息。




CN 1909421 B

1. 一种信息处理系统，其由因特网、客户端、连接服务装置和服务器组成，

所述连接服务装置包括：

分发部件，用于通过从光源发出的光线的变化，公开分发第一密钥；以及

接收部件，用于接收利用所分发的第一密钥加密后的信息，

所述接收部件具有解密部件，该解密部件用于接收作为利用第一密钥加密后的信息的第二密钥，并对接收到的第二密钥进行解密以获得公共密钥，

布置在接入点上的所述分发部件将所述第一密钥公开分发给所述客户端，

所述客户端的控制块包括：

接收部件，用于接收从所述光源公开发出的变化光线；

读取部件，用于从接收到的光线中读取所述第一密钥；

发送部件，用于利用读取的所述第一密钥对所述第二密钥进行加密，以通过近距离通信发送加密后的所述第二密钥；以及

传输部件，用于利用所述第二密钥作为公共密钥传输信息。

2. 一种用于信息处理系统的信息处理方法，所述信息处理系统由因特网、客户端、连接服务装置和服务器组成，所述信息处理方法包括以下步骤：

通过从接入点中的光源发出的光线的变化，公开分发第一密钥；

从所述光源发出的所述光线中提取所述第一密钥；

利用所述提取的第一密钥对第二密钥进行加密，以通过近距离通信发送所述加密后的第二密钥；

接收所述加密后的第二密钥并对所述接收到的第二密钥进行解密；以及

利用所述第二密钥作为公共密钥传输信息。

3. 一种连接服务装置，包括：

分发部件，用于通过从光源发出的光线的变化，公开分发第一密钥；以及

接收部件，用于接收利用所分发的第一密钥加密后的信息，

所述接收部件具有解密部件，该解密部件用于接收作为利用第一密钥加密后的信息的第二密钥，并对接收到的第二密钥进行解密以获得公共密钥，

布置在接入点上的所述分发部件将所述第一密钥公开分发给客户端。

4. 根据权利要求 3 所述的连接服务装置，其特征在于，所述分发部件分发作为所述第一密钥的由认证机构发出的公开密钥。

5. 根据权利要求 3 所述的连接服务装置，其特征在于，所述分发部件分发作为所述第一密钥的由认证机构发出的公开密钥，并将表示所述认证机构的认证的信息显示在所述接入点上。

6. 根据权利要求 3 所述的连接服务装置，其特征在于，所述分发部件还通过从所述光源发出的光线的变化，分发地址值。

7. 根据权利要求 3 所述的连接服务装置，其特征在于，所述光源为用于照明与要被提供的信息有关的物体的照明设备。

8. 根据权利要求 7 所述的连接服务装置，其特征在于，所述接入点在电力线上发送用于控制所述照明设备的闪烁的信号。

9. 根据权利要求 3 所述的连接服务装置，其特征在于，所述光源是发出可见光和红外

光中的至少一种的发光二极管。

10. 一种用于连接服务装置的信息处理方法，所述信息处理方法包括以下步骤：

通过从接入点中的光源发出的光线的变化，分发第一密钥；

接收用分发的所述第一密钥加密后的信息，

其中，所述连接服务装置包括：分发部件，用于通过从光源发出的光线的变化，公开分发第一密钥；以及接收部件，用于接收利用所分发的第一密钥加密后的信息，所述接收部件具有解密部件，该解密部件用于接收作为利用第一密钥加密后的信息的第二密钥，并对接收到的第二密钥进行解密以获得公共密钥，布置在接入点上的所述分发部件将所述第一密钥公开分发给客户端。

11. 一种客户端，所述客户端的控制块包括：

接收部件，用于接收从接入点中的光源公开发出的变化光线；

读取部件，用于从接收到的光线中读取第一密钥；

发送部件，用于用读取的所述第一密钥对第二密钥进行加密，以通过近距离通信发送加密后的所述第二密钥；以及

传输部件，用于利用所述第二密钥作为公共密钥传输信息。

12. 根据权利要求 11 所述的客户端，其特征在于，所述读取部件还从接收到的光线中读取地址值。

13. 根据权利要求 12 所述的客户端，其特征在于，还包括：

显示部件，用于显示与所述地址值相对应的符号；以及

判断部件，用于判断是否选择所述符号。

14. 一种用于客户端的信息处理方法，所述信息处理方法包括以下步骤：

接收从接入点中的光源公开发出的变化光线；

从接收到的光线中读取第一密钥；

利用读取的所述第一密钥对第二密钥进行加密，以通过近距离通信发送加密后的所述第二密钥；以及

利用所述第二密钥作为公共密钥传输信息，

其中，所述客户端的控制块包括：接收部件，用于接收从接入点中的光源公开发出的变化光线；读取部件，用于从接收到的光线中读取第一密钥；发送部件，用于用读取的所述第一密钥对第二密钥进行加密，以通过近距离通信发送加密后的所述第二密钥；以及传输部件，用于利用所述第二密钥作为公共密钥传输信息。

# 信息处理系统、信息处理装置和方法

## 技术领域

[0001] 本发明涉及一种信息处理系统、信息处理装置和方法、计算机程序以及记录介质，尤其涉及一种能够迅速、自由且安全地传输信息的信息处理系统、信息处理装置和方法、计算机程序以及记录介质。

## 背景技术

[0002] 近年来，当个人计算机用户离开家或办公室时，可以利用越来越多的接入点 (access point) 以使他们能够访问因特网。提出了一种在远离家或办公室布置的用户通过其访问因特网的各接入点通过使用口令和用户 ID 执行认证的方法（参考“802.11High-Speed Wireless LAN Textbook”，334 和 335 页）。

[0003] 下面参考图 1 说明通过使用口令和用户 ID 认证接入点的操作。在图 1 所示的系统中，通过无线电执行客户端 1 和接入点 2 之间的通信，以有线方式执行接入点 2 和认证服务器 3 之间的通信。

[0004] 在通过远离家或办公室的接入点访问因特网之前，每个用户必须进行注册以获得口令和用户 ID。然后，在步骤 S1，客户端 1 向接入点 2 发送连接请求。

[0005] 在步骤 S21，接入点 2 从客户端 1 接收该连接请求，在步骤 S22 将接收到的连接请求发送给认证服务器 3。在步骤 S51，认证服务器 3 接收该连接请求，判断现在是否可以进行对该请求的应答。在步骤 S52，认证服务器 3 向接入点 2 输出与该判断相对应的连接应答。接入点 2 在步骤 S23 接收该连接应答，在步骤 S24 将接收到的连接应答发送给客户端 1。在步骤 S2，客户端 1 接收该连接应答。

[0006] 在步骤 S53，认证服务器 3 向接入点 2 发送由未示出的认证机构 (certification body) 预先公布的公开密钥 (public key) 和证书。在步骤 S25，接入点 2 接收这些公开密钥和证书。在步骤 S26，接入点 2 将接收到的公开密钥和证书发送给客户端 1。在步骤 S3，客户端 1 接收从接入点 2 提供的公开密钥和证书。

[0007] 该证书包括规格版本、序列号、公开密钥所有者和公开密钥等明文 (plaintext) 数据、以及基于这些数据的数字签名。客户端 1 可以将通过用该公开密钥对该数字签名进行解密获得的内容与已经获得的明文规格版本、序列号、公开密钥所有者和公开密钥进行比较，以确认其所接收到的公开密钥和证书是从真正的认证服务器即由认证机构认证的管理员接收的公开密钥和证书。因此，客户端可以通过该认证服务器安全地连接到因特网。

[0008] 在步骤 S4，客户端 1 生成用于与认证服务器 3 发送和接收信息的公共密钥的加密密钥，通过从接入点 2 接收的公开密钥对所生成的加密密钥进行加密，并将加密后的加密密钥发送给接入点 2。在步骤 S27，接入点 2 接收该加密密钥。在步骤 S28，接入点 2 将接收到的加密密钥发送给认证服务器 3。在步骤 S54，认证服务器 3 接收该加密密钥，通过与公开密钥相对应的私人密钥 (private key) 对接收到的加密密钥进行解密，并使用解密后的加密密钥作为公共密钥。

[0009] 另一方面，在步骤 S5，客户端 1 通过加密密钥对用户 ID 进行加密，并将加密后的用

户 ID 发送给接入点 2。在步骤 S6，客户端 1 通过加密密钥对口令进行加密，并将加密后的口令发送给接入点 2。在步骤 S29，接入点 2 接收该用户 ID，并在步骤 S31 接收该口令。在步骤 S30，接入点 2 将该用户 ID 发送给认证服务器 3，并在步骤 S32，将该口令发送给认证服务器 3。在步骤 S55，认证服务器 3 接收该用户 ID，并在步骤 S56 接收该口令。认证服务器 3 通过在步骤 S54 中接收到的加密密钥对接收到的用户 ID 和口令进行解密，从而确认该用户 ID 和口令是注册用户所拥有的用户 ID 和口令。

[0010] 如果通过用户 ID 和口令发现客户端 1 是认证过的用户，则在步骤 S7 客户端 1 完成通过接入点 2 与认证服务器 3 的连接过程，在步骤 S57 认证服务器 3 完成通过接入点 2 与客户端 1 的连接过程。随后，客户端 1 可以通过接入点 2 和认证服务器 3 连接到因特网以从因特网获得各种服务。

[0011] 因为在许多地方布置了接入点 2，所以用户可以在需要时通过接入点 2 和认证服务器 3 连接到因特网以接收各种服务的提供。

## 发明内容

[0012] 然而，相关技术需要每个用户预先进行注册以获得用以利用接入点连接到因特网的 ID 和口令。因此，对于服务提供者来说，难以迅速且无限制地提供信息，这也使得用户难以迅速且无限制地获得信息。

[0013] 为了克服上述问题，可以跳过用户 ID 和口令的预先注册以及证书的使用，但是以有可能变成无线 LAN 网页仿冒 (phishing) 的受害者为代价。更具体地，报告了如下情况：试图进行网页仿冒的人在接入点的服务范围内发出未授权的无线电波，使接收到该无线电波的用户客户端显示伪造网页，从而如果该用户点击所显示的伪造网页上的任何地方，则使该客户端自动下载计算机病毒。

[0014] 因此，本发明提出了上述和其它与相关技术有关的问题，并通过迅速且无限制地发送和接收信息来解决所提出的问题。

[0015] 在实现本发明时并根据其一个实施例，提供一种信息处理系统和方法。该信息处理系统和方法通过从光源发出的光线的变化，公开分发第一密钥；从所述光源发出的所述光线中提取所述第一密钥；利用所述提取的第一密钥对第二密钥进行加密，以通过近距离通信发送所述加密后的第二密钥；接收所述加密后的第二密钥并对所述接收到的第二密钥进行解密；以及利用所述第二密钥作为公共密钥传输信息。

[0016] 在本发明的上述实施例中，基于从光源发出的光线的变化公开分发第一密钥，并从接收到的光线中提取第一密钥。利用所提取的第一密钥对第二密钥进行加密，以通过近距离通信发送加密后的第二密钥。接收加密后的第二密钥并对其进行解密以作为公共密钥进行传输。

[0017] 在实现本发明时并根据其另一实施例，提供一种信息处理装置。该信息处理装置具有：分发部件，用于通过从光源发出的光线的变化，公开分发第一密钥；以及接收部件，用于接收用所述分发的第一密钥加密后的信息。

[0018] 在上述信息处理装置中，分发部件可以分发作为第一密钥的由认证机构发出的公开密钥。

[0019] 在上述信息处理装置中，接收部件可以具有解密部件，该解密部件用于接收作为

用所述第一密钥加密后的信息的第二密钥，并对所述接收到的第二密钥进行解密以获得公共密钥。

[0020] 在上述信息处理装置中，布置在接入点上的所述分发部件可将所述第一密钥公开分发给客户端；以及布置在所述接入点上的所述接收部件可通过近距离通信接收从所述客户端发送的所述第二密钥。

[0021] 在上述信息处理装置中，所述分发部件可以分发作为所述第一密钥的由认证机构发出的所述公开密钥，并将表示所述认证机构的认证的信息显示在所述接入点上。

[0022] 在上述信息处理装置中，所述分发部件还可以通过从所述光源发出的光线的变化，分发地址值。

[0023] 在上述信息处理装置中，所述光源可以是用于照明与要被提供的信息有关的物体的照明设备。

[0024] 在上述信息处理装置中，所述接入点可以在电力线上发送用于控制所述照明设备的闪烁的信号。

[0025] 在上述信息处理装置中，所述光源可以是发出可见光和红外光中的至少一种的发光二极管。

[0026] 在实现本发明时并根据其另一实施例，提供一种信息处理方法、程序和存储该程序的记录介质。这些方法和程序各具有以下步骤：通过从光源发出的光线的变化，分发第一密钥；以及接收用所述分发的第一密钥加密后的信息。

[0027] 在本发明的上述实施例中，基于从光源发出的光线的变化，公开分发密钥，并接收用所分发的密钥加密后的信息。

[0028] 在实现本发明时和根据其又一实施例，提供一种信息处理装置。该信息处理装置具有：接收部件，用于接收从光源公开发出的变化光线；读取部件，用于从接收到的光线中读取第一密钥；发送部件，用于用所述读取的第一密钥对第二密钥进行加密，以通过近距离通信发送所述加密后的第二密钥；以及传输部件，用于利用所述第二密钥作为公共密钥传输信息。

[0029] 在上述信息处理装置中，所述读取部件还可以从接收到的光线中读取地址值。

[0030] 上述信息处理装置还可以具有：显示部件，用于显示与所述地址值相对应的符号；以及判断部件，用于判断是否选择所述符号。

[0031] 在实现本发明时和根据其不同的实施例，提供一种信息处理方法、程序和存储该程序的记录介质。这些方法和程序各具有以下步骤：接收从光源公开发出的变化光线；从接收到的光线中读取第一密钥；利用所述读取的第一密钥对第二密钥进行加密，以通过近距离通信发送所述加密后的第二密钥；以及利用所述第二密钥作为公共密钥传输信息。

[0032] 在本发明的上述实施例中，接收从光源公开发出的变化光线；从接收到的光线中读取第一密钥；利用所读取的第一密钥对第二密钥进行加密，以通过近距离通信对其进行传输；以及利用第二密钥作为公共密钥传输信息。

[0033] 如上所述并根据本发明的实施例，可以发送和接收信息。特别地，根据本发明的实施例，可以迅速、无限制和安全地发送和接收信息。

## 附图说明

[0034] 图 1 是示出相关技术接入点的操作的流程图；

[0035] 图 2 是示出作为本发明一个实施例实施的信息提供系统的典型结构的示意图；

[0036] 图 3 是示出客户端的典型结构的框图；

[0037] 图 4 是示出接入点的典型结构的框图；

[0038] 图 5 是示出服务器的典型结构的框图；

[0039] 图 6 是示出客户端的控制块的典型功能结构的框图；

[0040] 图 7 是示出接入点的控制块的典型功能结构的框图；

[0041] 图 8 是示出服务器的控制块的典型功能结构的框图；

[0042] 图 9 是示出图 2 所示的信息提供系统的操作的流程图；

[0043] 图 10 是示出客户端的处理的流程图；

[0044] 图 11 是示出接入点的操作的流程图；

[0045] 图 12 是示出服务器的操作的流程图；

[0046] 图 13 是示出曼彻斯特编码 (Manchester encoding) 中的“0”和“1”的图；

[0047] 图 14 是示出数据编码序列的例子的图；

[0048] 图 15 是示出认证机构的符号的例子显示的透视图；

[0049] 图 16 是示出本发明另一实施例的典型结构的示意图；

[0050] 图 17 是示出图 16 所示的实施例的处理的流程图；

[0051] 图 18 是示出客户端的处理的流程图；

[0052] 图 19 是示出接入点的处理的流程图；

[0053] 图 20 是示出服务器的处理的流程图；以及

[0054] 图 21 是示出个人计算机的典型结构的框图。

## 具体实施方式

[0055] 将参考附图利用例子更详细地说明本发明。在此说明的发明和其实施例具有以下的相互关系。其说明旨在证实如下事实：在此说明支持在此所述的本发明的实施例。因此，如果存在如下任何实施例：尽管在优选实施例的说明中对其进行了说明，但是在此并未将其作为对应于本发明进行说明，这并不意味着这样的实施例不对应于本发明。相反，如果在此对作为对应于本发明的任何实施例进行说明，这并不意味着这样的实施例不对应于除本发明以外的其它发明。

[0056] 本发明的一个实施例是信息处理系统（例如，图 2 所示的信息提供系统 10）或信息处理方法（例如，图 2 所示的信息提供系统 10 的信息处理方法），其通过从光源（例如，图 2 所示的 LED 32）发出的光线的变化公开分发（例如，图 11 所示的步骤 S42 和图 19 所示的步骤 S147）第一密钥（例如，图 2 所示的公开密钥 K1），从光源发出的光线中提取（例如，图 10 所示的步骤 S12 和图 18 所示的步骤 S108）该第一密钥，利用所提取的第一密钥对第二密钥（例如，图 2 所示的加密密钥 K2）进行加密，从而以近距离通信发送（例如，图 10 所示的步骤 S19 和图 18 所示的步骤 S110）加密后的第二密钥，接收加密后的第二密钥且对接收到的第二密钥进行解密（例如，图 12 所示的步骤 S78 和图 20 所示的步骤 S178），并利用该第二密钥作为公共密钥传输（例如，图 10 所示的步骤 S20、图 18 所示的步骤 S111、图

12 所示的步骤 S79 和图 20 所示的步骤 S179) 信息。

[0057] 本发明的另一实施例是信息处理装置（例如，图 2 所示的连接服务装置 13)。该信息处理装置具有：分发部件（例如，图 7 所示的发送器块 122，用于执行图 11 所示的步骤 S42 和图 19 所示的步骤 S147 的处理），用于通过从光源（例如，图 2 所示的 LED 32) 发出的光线的变化公开分发第一密钥（例如，图 2 所示的公开密钥 K1)；以及接收部件（例如，图 7 所示的接收器块 121，用于执行图 11 所示的步骤 S47 和图 19 所示的步骤 S148 的处理），用于接收利用所分发的第一密钥加密后的信息（例如，图 2 所示的加密密钥 K2)。

[0058] 上述分发部件可以分发作为第一密钥的由认证机构发出的公开密钥（例如，图 2 所示的公开密钥 K1)。

[0059] 上述接收部件可具有解密部件（图 8 所示的解密块 144，用于执行图 12 所示的步骤 S78 和图 20 所示的步骤 S178 的处理），该解密部件用于接收作为利用第一密钥加密后的信息的第二密钥（例如，图 2 所示的加密密钥 K2)，并对接收到的第二密钥进行解密以获得公共密钥。

[0060] 被布置在接入点（例如，图 2 所示的接入点 31) 上的上述分发部件可以将第一密钥公开分发（例如，图 11 所示的步骤 S42 和图 19 所示的步骤 S147 的处理）给客户端（例如，图 2 所示的客户端 12)，而被布置在该接入点上的接收部件可以接收（例如，图 11 所示的步骤 S47 和图 19 所示的步骤 S148 的处理）通过近距离通信从客户端发送的第二密钥。

[0061] 上述分发部件可以分发作为第一密钥的由认证机构发出的公开密钥（例如，图 2 所示的公开密钥 K1)，并将表示通过认证机构的认证的信息（例如，显示在图 15 所示的通知块 171 上的通知）显示在接入点上。

[0062] 上述分发部件还可以通过从光源发出的光线的变化分发（例如，图 11 所示的步骤 S42 和图 19 所示的步骤 S141 的处理）地址值。

[0063] 上述光源可以是用于照明与要提供的信息相关的物体（例如，图 16 所示的海报 204 和 205) 的照明设备（例如，图 16 所示的照明设备 202 和 203)。

[0064] 上述接入点可以在电力线（例如，图 16 所示的电力线 201) 上发送用于控制照明设备的闪烁的信号。

[0065] 上述光源可以是发出可见光和红外光中的至少一种的发光二极管（例如，图 2 所示的 LED 32)。

[0066] 本发明的又一实施例是一种信息处理方法（例如，用于图 2 所示的连接服务装置 13 的信息处理方法）、程序和存储该程序的记录介质。这些方法和程序均具有以下步骤：通过从光源（图 2 所示的 LED 32) 发出的光线的变化分发（例如，图 11 所示的步骤 S42 和图 19 所示的步骤 S147 的处理）第一密钥（例如，图 2 所示的公开密钥 K1)；以及接收（例如，图 11 所示的步骤 S47 和图 19 所示的步骤 S148 的处理）利用所分发的第一密钥加密后的信息（例如，图 2 所示的加密密钥 K2)。

[0067] 本发明的不同实施例是一种信息处理装置。该信息处理装置具有：接收部件（例如，图 6 所示的成像块 101，用于执行图 10 所示的步骤 S11 和图 18 所示的步骤 S101 的处理），用于接收从光源公开发出的变化光线；读取部件（例如，图 6 所示的读取块 102，用于执行图 10 所示的步骤 S12 和图 18 所示的步骤 S108 的处理），用于从接收到的光线中读取第一密钥（例如，图 2 所示的公开密钥 K1)；发送部件（例如，图 6 所示的发送器块 107，用于执行图 10 所示的步骤 S19 和图 18 所示的步骤 S110 的处理），用于利用所读取的第一密钥

对第二密钥（例如，图 2 所示的加密密钥 K2）进行加密以通过近距离通信发送加密后的第二密钥；以及传输部件（例如，图 6 所示的传输处理块 108，用于执行图 10 所示的步骤 S20 和图 18 所示的步骤 S111 的处理），用于利用第二密钥作为公共密钥传输信息。

[0068] 上述读取部件还可以从接收到的光线中读取（例如，图 10 所示的步骤 S12 和图 18 所示的步骤 S102 的处理）地址值。

[0069] 上述信息处理装置还可以具有：显示部件（例如，图 6 所示的显示块 103），用于显示与该地址值相对应的符号（例如，图 2 所示的图标 23）；以及判断部件（例如，图 6 所示的判断块 104，用于执行图 10 所示的步骤 S14 和图 18 所示的步骤 S104 的处理），用于判断是否选择该符号。

[0070] 本发明的另一不同实施例是一种信息处理方法、程序和存储该程序的记录介质。这些方法和程序均具有以下步骤：接收（例如，图 10 所示的步骤 S11 和图 18 所示的步骤 S101 的处理）从光源公开发出的变化光线；从接收到的光线中读取（例如，图 10 所示的步骤 S12 和图 18 所示的步骤 S108 的处理）第一密钥（例如，图 2 所示的公开密钥 K1）；利用所读取的第一密钥对第二密钥（例如，图 2 所示的加密密钥 K2）进行加密，以通过近距离通信发送（例如，图 10 所示的步骤 S19 和图 18 所示的步骤 S110 的处理）加密过的第二密钥；以及利用该第二密钥作为公共密钥传输（例如，图 10 所示步骤 S20 和图 18 所示步骤 S111 的处理）信息。

[0071] 下面将参考附图说明本发明的实施例。

[0072] 参考图 2，其示出作为以本发明的一个实施例实施的信息处理系统的信息提供系统的典型结构。信息提供系统 10 由因特网 11、客户端 12、连接服务装置 13、以及服务器 14 和 15 组成。参考图 2，仅示出了一个客户端 12。对于一个接入点 31，可连接多个客户端 12。可以将所需数量的接入点 31 以分布式方式布置在所需的地方。

[0073] 作为 PDS(Personal Digital Assistant，个人数字助理）的客户端 12 具有 LCD(Liquid Crystal Display，液晶显示器）21。LCD 21 有时显示所需的图像。客户端 12 的照相机 22 拍摄被摄体的照片，并将所拍摄的照片显示在 LCD 21 上。

[0074] 连接服务装置 13 由接入点 31 和服务器 34 组成。接入点 31 具有通过闪烁光线（可见红外光）发送光信号的 LED(Light EmittingDilde，发光二极管）32 和在无线近距离通信中使用的天线 33。接入点 31 和服务器 34 以有线或无线方式相互连接。服务器 34 还与因特网 11 连接。因特网 11 还与提供各种信息的服务器 14 和 15 连接。

[0075] 应该注意，客户端 12 与接入点 31 之间的近距离通信可以由以下任何一个支持，例如：标准 IEEE(Institute of Electrical andElectronic Engineers，电气与电子工程师协会）802.11b/a/g、UWB(Ultra Wide Band，超宽频）、蓝牙 (Bluetooth，注册商标）、以及 ZigBee。在此所用术语“近距离通信”是指在可以接收由光线变化所生成的信号并可对该信号进行解码的距离范围内所执行的通信。更具体地，近距离通信是指在几米到几十米的距离范围内所执行的无线通信。

[0076] 尽管后面将参考图 9 和 11 详细说明操作，但是接入点 31 的 LED32 通过闪烁光线发送接入点 31 的地址和公开密钥 K1。与相应的私人密钥一起通过预定的认证机构将该公开密钥 K1 发给连接服务装置 13 的管理员，或者通过接入点公司唯一地生成该公开密钥 K1。客户端 12 利用照相机 22 拍摄该接入点 31 的图像，并将所拍摄的图像显示在 LCD 21 上。用

户指定表示存在发出公开密钥K1的接入点的图标23，从而执行接入点选择。在从接收到的图像中提取公开密钥K1时，客户端12对由客户端12生成的加密密钥K2进行加密，并通过无线电波（即，近距离通信）将加密后的加密密钥发送给接入点31。

[0077] 接入点31将由公开密钥K1加密后的加密密钥K2传输给服务器34。因此，服务器34可以与客户端12共享加密密钥K2作为公共密钥，并当在服务器与客户端之间传输信息时使用该共享的密钥。

[0078] 参考图3，其示出了客户端12的典型结构。与照相机22相对应的成像块51拍摄被摄体的图像，并输出相应的图像信号。图像处理块52处理从成像块51接收到的图像信号，并将处理后的图像信号输出给显示块53，从而显示处理信号。显示块53对应于LCD 21。

[0079] 基于例如微型计算机的控制块55控制成像块51、图像处理块52、显示块53以及其它块的操作。由开关、按钮和其它控件组成的输入块54将与用户在输入块54上进行的操作相对应的信号输出给控制块55。通信块56执行与接入点31的无线电通信。

[0080] 需要时加载在客户端12上的可移动介质57将客户端的操作所需的程序和数据提供给控制块55。

[0081] 参考图4，其示出了接入点31的典型结构。通过控制块72控制与LED 32相对应的发光块73，以通过改变光的水平输出信号（例如，该块输出光闪烁信号）。通信块71通过天线33执行与客户端12的无线通信。通信块71还执行与服务器34的通信。存储块74存储将被发送给客户端12的地址和公开密钥K1。

[0082] 例如，基于例如微型计算机的控制块72连接到可移动介质75。可移动介质75存储控制块72操作所需的程序和数据。

[0083] 参考图5，其示出了服务器34的典型结构。通信块81通过接入点31和因特网11执行与其它单元的通信。存储块82存储例如将被提供给接入点31的公开密钥。显示块83显示所需的图像和信息。基于例如微型计算机的控制块85控制服务器的其它块的操作。基于键盘、鼠标等的输入块84将与用户在输入块84上进行的操作相对应的信号提供给控制块85。

[0084] 需要时连接到服务器34的可移动介质86有时向服务器34提供程序和数据。

[0085] 客户端12的控制块55具有如图6所示的功能结构。尽管未示出，控制块55的各组成块可以与其它组成块发送和接收信号。其它控制块具有图7和8所示的结构。

[0086] 成像块101拍摄被摄体的图像。读取块102从所拍摄的图像中读取地址值和公开密钥。显示块103控制将图像显示在显示块53上。判断块104执行各种判断。请求块105请求连接接入点。读取块106读出加密密钥。发送器块107将由公开密钥加密后的加密密钥发送给接入点31。传输处理块108通过接入点31和服务器34与服务器14和15传输信息。

[0087] 参考图7，其示出了接入点31的控制块72的功能结构。接收器块121从服务器34接收公开密钥。发送器块122发送地址值和公开密钥，将连接请求发送给服务器34，并将连接应答发送给客户端12。另外，发送器块122将加密密钥发送给服务器34。判断块123执行各种判断。存储块124存储地址值和公开密钥。传输处理块125在客户端12与服务器34之间传输信息。

[0088] 参考图8，其示出了服务器34的控制块85的功能结构。发送器块141将公开密钥

发送给接入点 31，并将连接应答发送给接入点 31。接收器块 142 从接入点 31 接收连接应答。判断块 143 执行各种判断。解密块 144 利用私人密钥对加密密钥进行解密。传输处理块 145 在接入点 31 与服务器 14 和 15 之间传输信息。

[0089] 下面参考图 9 ～ 12 所示的流程图来说明当客户端 12 通过接入点 31 连接到服务器 34 以通过因特网 11 从服务器 14 和 15 获得所需要的信息时执行的处理。图 9 示出客户端 12、接入点 31 和服务器 34 的整体操作。图 10 示出客户端 12 的操作。图 11 示出接入点 31 的操作。图 12 示出服务器 34 的操作。

[0090] 在步骤 S71，服务器 34 的发送器块 141 将公开密钥发送给接入点。更具体地，通信块 81 从存储块 82 读取公开密钥，并将该公开密钥发送给接入点 31。

[0091] 在步骤 S41，接入点 31 的接收器块 121 接收该公开密钥。在步骤 S42，发送器块 122 将在步骤 S41 中接收到的公开密钥与地址值一起发送给客户端 12。

[0092] 更具体地，接入点 31 的控制块 72 通过控制发光块 73 将通信块 71 从服务器 34 接收到的公开密钥和从存储块 74 读取的预先存储的地址值（即，通过其访问接入点 31 的地址值）作为光闪烁信号来发送（或广播）。

[0093] 如图 13 所示对待发送的信号进行曼彻斯特编码。在曼彻斯特编码中，上升沿（表示从 LED 32 的关闭到其打开的状态转变）为“0”，下降沿（表示从 LED 32 的打开到其关闭的状态转变）为“1”。因此，例如如图 14 所示，发送例如“010011”等的数据编码序列作为光闪烁信号（显然，LED 32 的关闭状态不是必然意味着没有发光；即，仅在光的高与低水平之间存在显著差异，从而允许照片接收器端完全识别出该差异）。

[0094] 如上所述，通过使 LED 32 闪烁，接入点 31 始终广播接入点 31 的地址值和公开密钥（即，接入点 31 以公开方式分发接入点 31 的地址值和公开密钥）。

[0095] 然后，用户将客户端 12 的照相机 22 指向接入点 31 以进行访问，并操作输入块 54 给出拍摄接入点 31 的图像的命令以进行访问。此刻，成像块 101 执行步骤 S11 中的成像处理。更具体地，通过成像块 51 拍摄接入点 31 的图像，并通过图像处理块 52 处理结果图像信号，以将其输出并显示在显示块 53(LCD 21) 上。

[0096] 由于光线以直线方式行进，所以仅拍摄将照相机 22 所指向的接入点 31 的图像；因此，如果存在任何其它照相机 22 未指向的接入点，则不拍摄这些接入点的图像。因此，用户不可能从任何非期望的接入点接收光，从而使变成网页仿冒受害人的风险最小化。

[0097] 例如如图 15 所示，如果接入点公司使用从预定的认证机构发出的公开密钥，则将符号 172（图 15 的例子中的单词“Certification”）显示在接入点 31 的通知块 171 上，作为表示该接入点 31 由预定认证机构进行了认证的信息。除符号 172 以外，通知块 171 示出认证的日期例如“2005.6.28”和认证期满的日期例如“2006.6.27”。因此，用户可以从所显示的图像中检查符号 172 以及认证的日期和认证期满的日期，以识别出接入点 31 是适当认证的接入点。该配置还增强了该系统的安全性。

[0098] 在步骤 S12，读取块 102 通过分析由成像块 101 所拍摄的图像（即，对闪烁信号或曼彻斯特码进行解码），从该闪烁信号中读取（或提取）地址值和公开密钥。接着，在步骤 S13，显示块 103 将与在步骤 S12 中读取（或提取）的地址值相对应的符号的图标显示在 LCD 21 上。因此，例如如图 2 所示，将与接入点 31 相对应的地址“address 1”显示在接入点 31 的图像 31A 的附近，作为 LCD 21 上的图标 23。

[0099] 通过该地址（或图标），用户再次检查该接入点是用户所期望的接入点，并利用例如他的手指点击该图标，从而指定该接入点以进行访问。在步骤 S14，判断块 104 判断用户是否选择了该图标。如果发现没有选择该图标，则判断块 104 在步骤 S15 中判断用户是否已经指定了结束处理。如果发现未指定结束处理，则程序返回到步骤 S11 以重复上述从步骤 S11 开始的处理。即，直到点击选择图标 23 为止，重复步骤 S11 ～ 15 中的处理。

[0100] 如果用户点击了图标 23，则请求块 105 在步骤 S16 中请求连接接入点。即，在控制块 55 的控制下，通信块 56 以无线方式通过近距离通信，将连接请求信号发送给接入点 31。

[0101] 在步骤 S43，判断块 123 判断接入点 31 是否已经接收到连接请求。如果通过接收器块 121 还未接收到连接请求，则程序返回到步骤 S41 以重复上述从步骤 S41 开始的处理。

[0102] 如果在步骤 S43 发现接收器块 121 接收到了连接请求，则在步骤 S44，发送器块 122 将该连接请求传输给服务器。即，接入点 31 的通信块 71 将从客户端 12 接收到的连接请求发送给服务器 34。

[0103] 在服务器 34 中，判断块 143 在步骤 S72 中判断是否已经从接入点接收到了连接请求。如果发现未接收到该连接请求，则程序返回到步骤 S71 以重复上述步骤 S71 和 S72 的处理，直到接收到该连接请求为止。

[0104] 如果发现从接入点 31 接收到了连接请求，则判断块 143 在步骤 S73 中判断是否可以进行对该连接请求的应答。即，因为该接入点被太多的客户端请求接入，所以判断该应答是否困难。如果可以进行该应答，则发送器块 141 在步骤 S74 中将连接应答“OK”发送给接入点。如果在步骤 S73 中发现不可以进行该应答，则发送器块 141 在步骤 S75 中将连接应答“NG”发送给接入点。

[0105] 在步骤 S45，接入点 31 的判断块 123 判断是否已经从服务器 34 接收到了连接应答，并一直等待直到接收到该连接应答为止。如果发现从服务器 34 接收到了连接应答，则在步骤 S46，发送器块 122 将接收到的连接应答发送给访问客户端。

[0106] 客户端 12 的判断块 104 在步骤 S17 中判断是否有来自接入点的应答，并一直等待直到该应答来到为止。如果发现从接入点 31 接收到了应答，则读取块 106 在步骤 S18 中读取加密密钥。该加密密钥可以是已经生成的加密密钥或是需要时由读取块 106 生成的加密密钥。

[0107] 在步骤 S19，发送器块 107 利用公开密钥对在步骤 S18 中读取的加密密钥进行加密，并发送加密后的加密密钥。即，通过在步骤 S12 中读取的公开密钥对在步骤 S18 中读取的加密密钥进行加密，并将加密后的加密密钥发送给接入点 31。

[0108] 在步骤 S47，接入点 31 的判断块 123 判断是否已经接收到该加密密钥，并一直等待直到接收到该加密密钥为止。当接收到该加密密钥时，则在步骤 S48，发送器块 122 将在步骤 S47 中接收到的加密密钥发送给服务器 34。

[0109] 在步骤 S76，服务器 34 的判断块 143 判断是否已经接收到该加密密钥。如果发现未接收到该加密密钥，则在步骤 S77，判断块 143 判断是否已经到达超时。即，在步骤 S74 和 S75 中发送连接应答之后，判断预先设置的时间是否已经过去。如果发现预先设置的时间没有过去，则程序返回到步骤 S76 以重复上述从步骤 S76 开始的处理。如果发现预先设置的时间已经过去，则上述处理结束。

[0110] 如果在步骤 S76 中发现接收到了该加密密钥，则解密块 144 在步骤 S78 中利用私

人密钥对该加密密钥进行解密。即，利用与在步骤 S71 中发送的公开密钥相对应的私人密钥，对接收器块 142 在步骤 S76 中接收到的加密密钥进行解密。因此，在客户端 12 和服务器 34 之间共享该加密密钥作为公共密钥。

[0111] 因此，传输处理块 145 在步骤 S79 中、传输处理块 108 在步骤 S20 中和传输处理块 125 在步骤 S49 中均执行信息传输处理。更具体地，客户端 12 的传输处理块 108 在步骤 S20 中将所需的信息发送给接入点 31。接入点 31 的传输处理块 125 在步骤 S49 中将从客户端 12 所提供的信号传输给服务器 34。服务器 34 的传输处理块 145 基于通过接入点 31 从客户端 12 所提供的访问信息，例如通过因特网 11 访问服务器 14，从而在步骤 S79 中连接到服务器 14。

[0112] 在步骤 S79 中，通过因特网 11 在服务器 34 的传输处理块 145 上接收从服务器 14 发送的主页等数据，然后将该数据发送给接入点 31。接入点 31 的传输处理块 125 在步骤 S49 中从服务器 34 接收该数据时，将接收到的数据传输给客户端 12。在步骤 S20，客户端 12 的传输处理块 108 通过服务器 34 和接入点 31 将从服务器 14 接收到的数据输出到例如 LCD 21，从而将该数据显示在 LCD 21 上。

[0113] 如上所述，用户无需具有 ID 和口令，从而不必进行预先注册。在不进行预先注册的情况下，用户可以在需要时通过接入点 31 从服务器 34 访问因特网 11。因此，用户可以迅速且不受限制地在任何地方（在接入点 31 的附近）通过因特网 11 访问预定的服务器 14 和 15，从而获得所期望信息的提供。该结构还允许信息提供者在所期望的地方布置接入点，从而迅速且不受限制地提供信息。

[0114] 另外，使用从用户实际拍摄的闪烁 LED 32 的图像中检测到的地址值和公开密钥，使得难以通过拾取在隐蔽地方生成的未授权的无线电波而变成尝试无线 LAN 网页仿冒的受害者。因此，上述新结构允许信息的安全传输。此外，利用加密密钥 K2 对客户端 12 与服务器 34 之间通过接入点 31 的通信进行加密，从而确保安全性。

[0115] 应该注意，在上述结构中，组成连接服务装置 13 的接入点 31 和服务器 34 被布置在相互远离的位置；显而易见，还可以一体形成接入点 31 和服务器 34。

[0116] 在上述结构中，将用作光源的 LED 32 和接入点 31 一体布置。将光源和接入点 31 布置在分开的位置也是可行的。图 16 示出使用该布置的实施例。更具体地，在该实施例中，基于 LED 的照明设备 202 照明海报 204，基于 LED 的照明设备 203 照明海报 205。基于 LED 的照明设备 206 照明陈列各种产品项的陈列架 207。通过电力线 201 向照明设备 202、203 和 206 提供必要的电能。接入点 31 也连接到该电力线 201。接入点 31 通过电力线 201 控制照明设备 202、203 和 206，从而使这些设备闪烁。

[0117] 在图 16 所示的实施例中，海报 204 和 205 是由客户端 12 的照相机 22 拍摄的。因此，海报 204 的图像 204A 和海报 205 的图像 205A 与同其对应的图标 23-1 和 23-2 一起被显示在 LCD 21 上。用户用手指等选择这些图标中的一个。

[0118] 在这种情况下，照明设备 202 利用由照明设备 202 生成的闪烁信号，提供用于提供与海报 204 有关的信息的 URL(UniformResourse Locator，统一资源定位器）。照明设备 203 还利用由照明设备 203 生成的闪烁信号提供与海报 205 有关的 URL。照明设备 206 利用由照明设备 206 生成的闪烁信号，提供用于提供与显示在陈列架 207 上的产品有关的信息的 URL。

[0119] 图 17 ～ 20 示出又一实施例的操作。在该实施例中，当至少一个客户端 12 访问接入点 31 时，接入点 31 仅正常广播其地址，并发送公开密钥。其它处理与参考图 9 ～ 12 的上述处理基本相同。

[0120] 更具体地，在与图 12 所示的步骤 S71 ～ S79 相对应的步骤 S171 ～ S179 的处理当中，在图 20 所示的实施例中向接入点发送连接应答的步骤 S173 和 S174 之后的步骤 S175 中，执行图 12 所示的步骤 S71 中所执行的将公开密钥发送给接入点的处理。其它处理与图 12 中所示的基本相同。

[0121] 在与图 11 所示的步骤 S41 ～ S49 相对应的图 19 所示的步骤 S141 ～ S150 的接入点的处理中，在图 11 所示的例子中的步骤 S41 中接收公开密钥。在图 19 所示的实施例中，在步骤 S145 中将连接应答发送给访问客户端后的步骤 S146 中，接收公开密钥。此外，在图 11 所示的步骤 S42 中发送地址值和公开密钥。而在图 19 所示的步骤 S141 中，发送地址值。如果在图 19 所示的步骤 S146 中发现接收到公开密钥，则在步骤 S147 中将公开密钥发送给客户端。其它处理与图 11 所示的基本相同。

[0122] 在与图 10 所示的步骤 S11 ～ S20 相对应的图 18 所示的步骤 S101 ～ S111 中的客户端 12 的处理中，在图 10 所示的步骤 S12 中读取地址值和公开密钥。而在图 18 所示的步骤 S102 中，读取地址值。如果在图 18 所示的步骤 S107 中发现从接入点接收到应答，则在步骤 S108，由成像块 101 接收（或成像）从接入点发送的光闪烁信号，并由读取块 102 从所接收到的信号中读取公开密钥。其它处理与图 10 所示的基本相同。

[0123] 图 17 所示的上述实施例提供了与图 9 所示的实施例基本相同的效果。

[0124] 在上述实施例中，以面方式执行光线的检测（即，通过照相机对光线进行成像）。可选地，可以以点方式执行该检测。例如，一个红外线接收器元件可以接收红外线以检测其水平的变化。在这种情况下，用户还可以确认布置红外线接收器块的方向，从而识别出哪个接入点正在发出正由该红外线接收器块接收的红外线。因此，该结构使得难以拾取从隐蔽地方发出的光，从而难以变成网页仿冒的受害者。

[0125] 参考图 21，其示出了利用软件执行上述处理序列的个人计算机的典型结构。CPU（中央处理单元）221 根据存储在 ROM（只读存储器）222 或存储块 228 中的程序和数据，执行各种处理操作。RAM（随机存取存储器）223 有时存储由 CPU 221 执行的程序和其所需的数据。CPU 221、ROM 222 和 RAM 223 利用总线 224 相互连接。

[0126] CPU 221 还通过总线 224 连接到输入 / 输出接口 225。输入 / 输出接口 225 与基于例如键盘、鼠标和麦克风的输入块 226、以及基于例如显示监视器和扬声器的输出块 227 连接。CPU 221 根据用户通过 226 输入的命令，执行各种处理操作。CPU 221 将处理结果输出给输出块 227。

[0127] 与输入 / 输出接口 225 连接的由例如硬盘驱动器形成的存储块 228 存储由 CPU 221 执行的程序和其所需的数据。通信块 229 通过因特网和局域网等网络与外部设备进行通信。可以通过通信块 229 获取程序以将其存储在存储块 228 中。

[0128] 当在与输入 / 输出接口 225 连接的驱动器 230 上装载磁盘、光盘、磁光盘或半导体存储器等可移动介质 231 时，驱动器 230 驱动可移动介质 231，从而从可移动介质 231 中获得程序和数据。将由此获得的程序和数据提供给存储块 228 以将其存储在存储块 228 中。

[0129] 上述处理操作序列可通过软件和硬件来执行。当通过软件执行上述处理操作序列

时，将组成该软件的程序安装在内置于专用硬件设备中的计算机中，或将其从网络或记录介质安装到例如其中可以安装用于执行各种功能的各种程序的通用个人计算机中。

[0130] 如图 21 所示，用于存储被安装在计算机上来执行的程序的程序记录介质由可移动介质 231、临时或永久存储程序的 ROM 222、或形成存储块 228 的硬盘驱动器组成，其中，可移动介质 231 是由磁盘（包括软盘）、光盘（包括 CD-ROM（光盘只读存储器））、DVD（数字通用光盘）、磁光盘、或半导体存储器组成的盒装媒体 (package media)。在需要时，通过路由器和调制解调器等提供接口的通信块 229，利用 LAN、因特网或数字卫星广播等有线或无线通信媒体，执行将程序存储在程序记录介质中。

[0131] 在此应该注意，用于说明在记录介质中所记录的各程序的步骤不仅包括以依时方式顺序执行的处理操作，而且还包括同时或分开执行的处理操作。

[0132] 还应该注意，在此所用的术语“系统”表示由多个组成单元构成的整个装置。

[0133] 尽管使用特定术语已经对本发明的优选实施例进行了说明，但是，这样的说明仅仅是示例性的目的，应该理解，在不脱离以下权利要求的精神或范围的情况下，可以做出改变和变化。

[0134] 本发明包含与 2005 年 8 月 1 日在日本专利局提交的日本专利申请 JP2005-223084 有关的主题，将其全部内容通过引用包含在此。

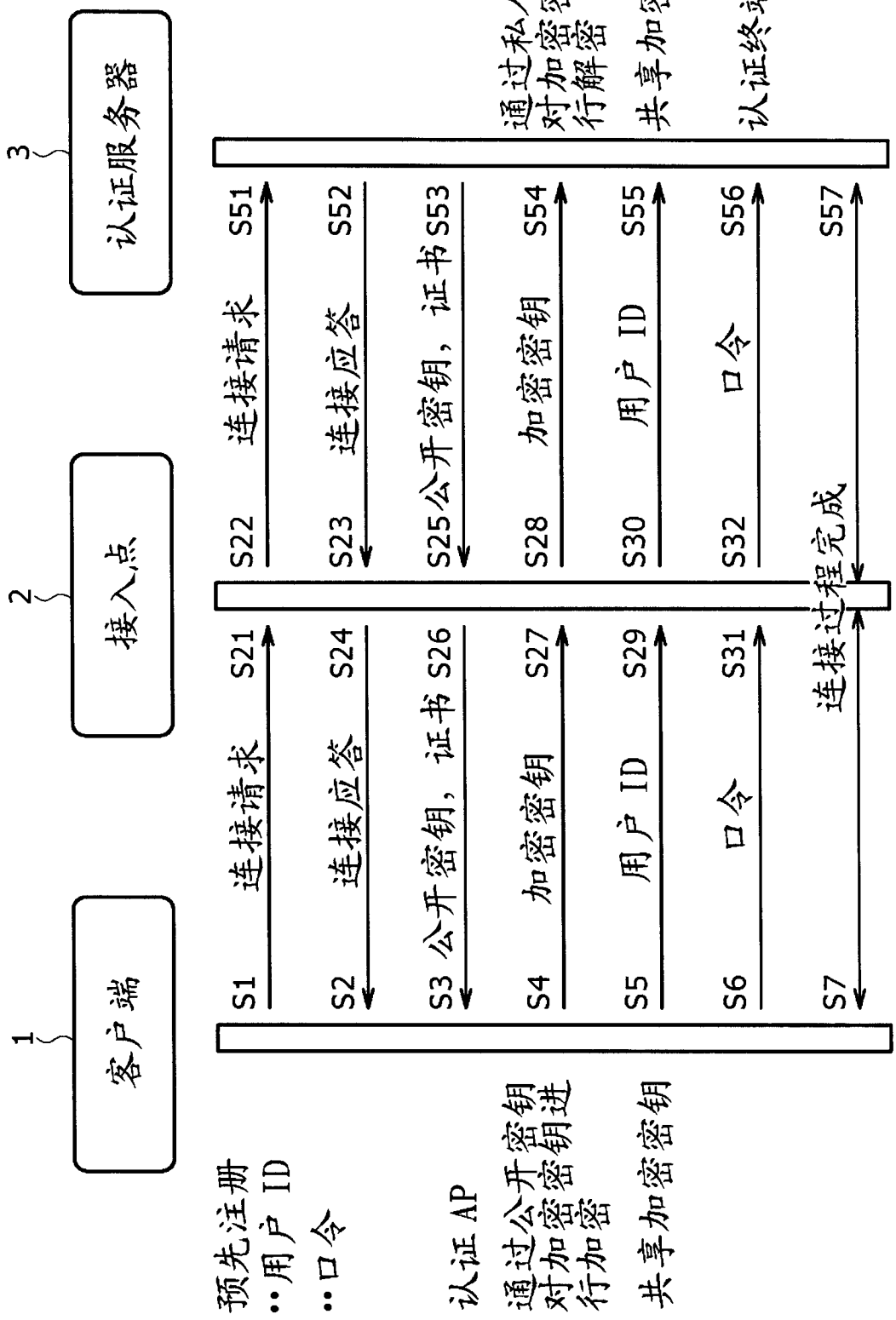

1
客户端
2
接入点
3
认证服务器
预先注册
••用户 ID
••口令
认证 AP
通过公开密钥
对加密密
行加密
共享加密密钥
S1 连接请求 S21
S2 连接应答 S24
S3 公开密钥，证书 S26
S4 加密密钥 S27
S5 用户 ID S29
S6 口令 S31
S7 连接过程完成
S22 连接请求 S51
S23 连接应答 S52
S25公开密钥，证书S53
S28 加密密钥 S54
S30 用户 ID S55
S32 口令 S56
S57
通过私人密钥
对加密密钥进
行解密密
共享加密密钥
认证终端

图 1

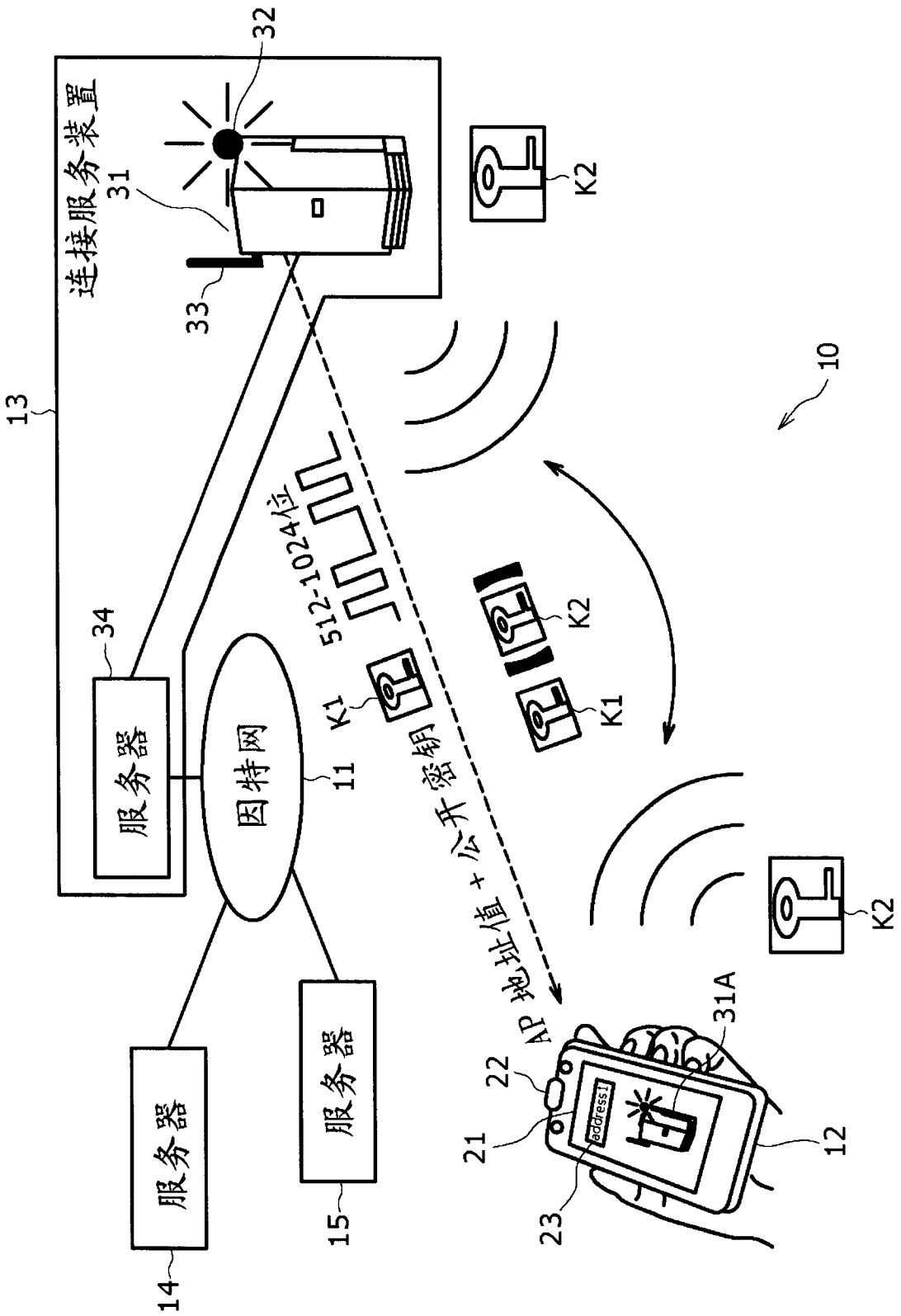

连接服务装置
32
31
33
13
34
服务器
因特网
11
服务器
15
服务器
14
512-1024位
K1
K2
K1
K2
K2
AP 地址值 + 公开密钥
10
31A
22
21
23
12
address1

图 2

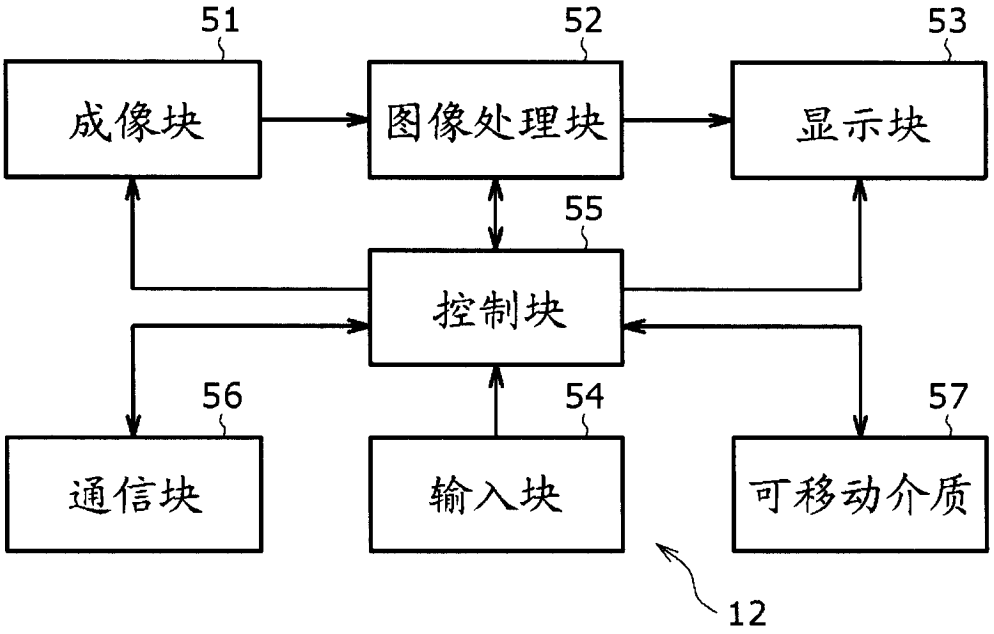

51
52
53
成像块
图像处理块
显示块
55
控制块
56
54
57
通信块
输入块
可移动介质
12

图 3

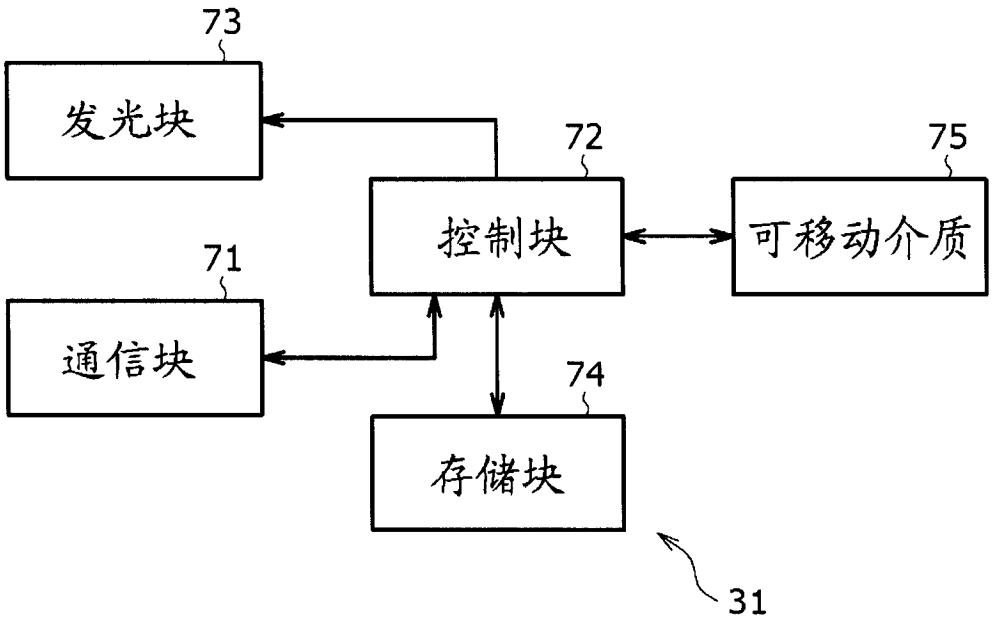

73
发光块
72
75
控制块
可移动介质
71
通信块
74
存储块
31

图 4

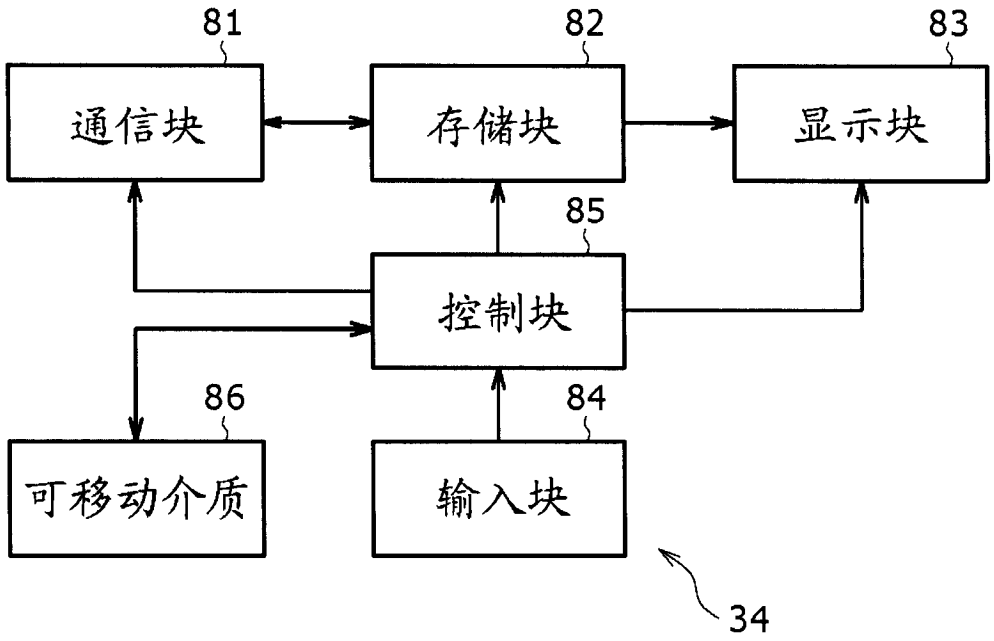

81
82
83
通信块
存储块
显示块
85
控制块
86
84
可移动介质
输入块
34

图 5

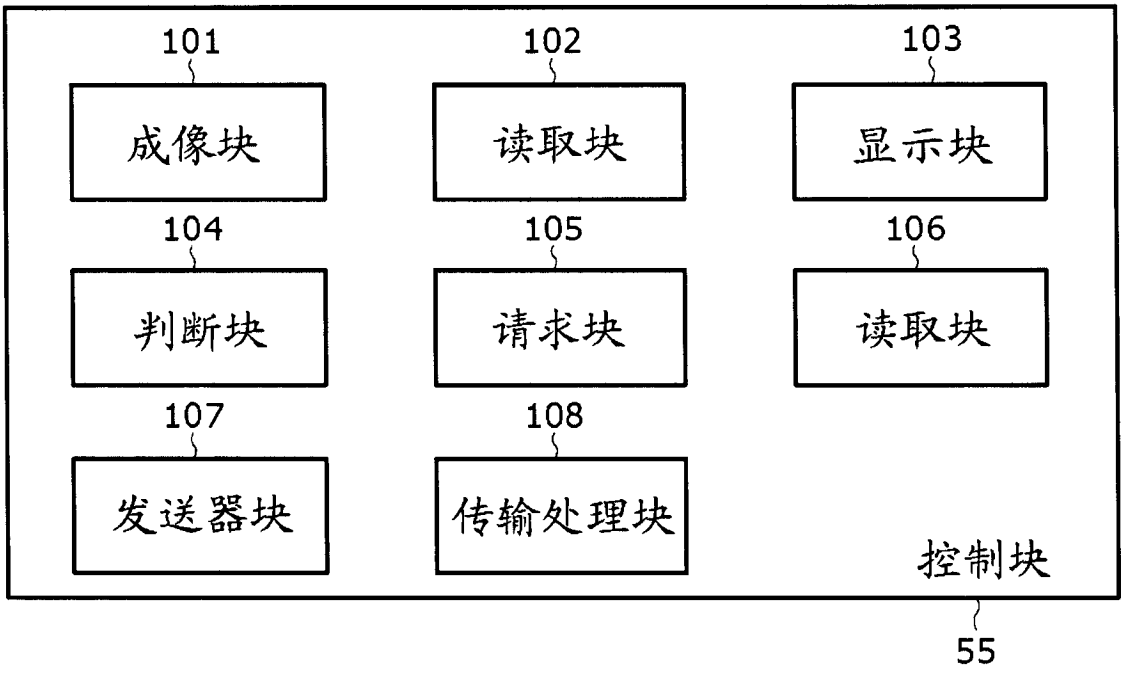

101
102
103
成像块
读取块
显示块
104
105
106
判断块
请求块
读取块
107
108
发送器块
传输处理块
控制块
55

图 6

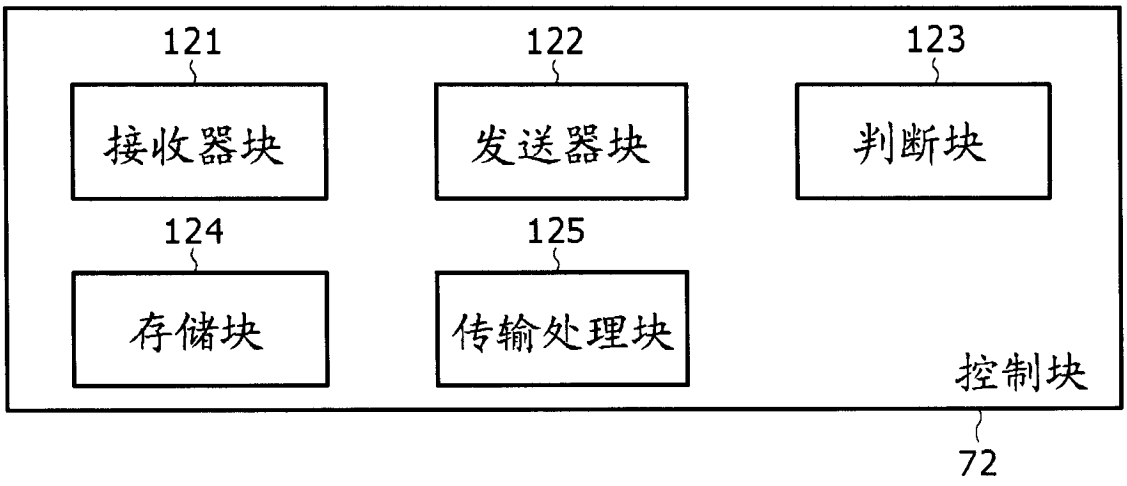

121
接收器块
122
发送器块
123
判断块
124
存储块
125
传输处理块
控制块
72

图 7

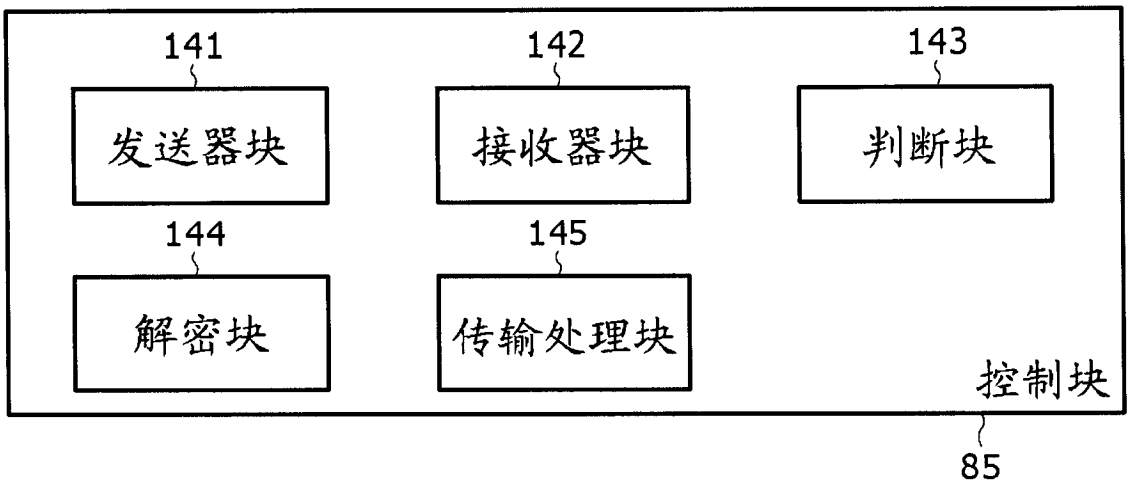

141
发送器块
142
接收器块
143
判断块
144
解密块
145
传输处理块
控制块
85

图 8

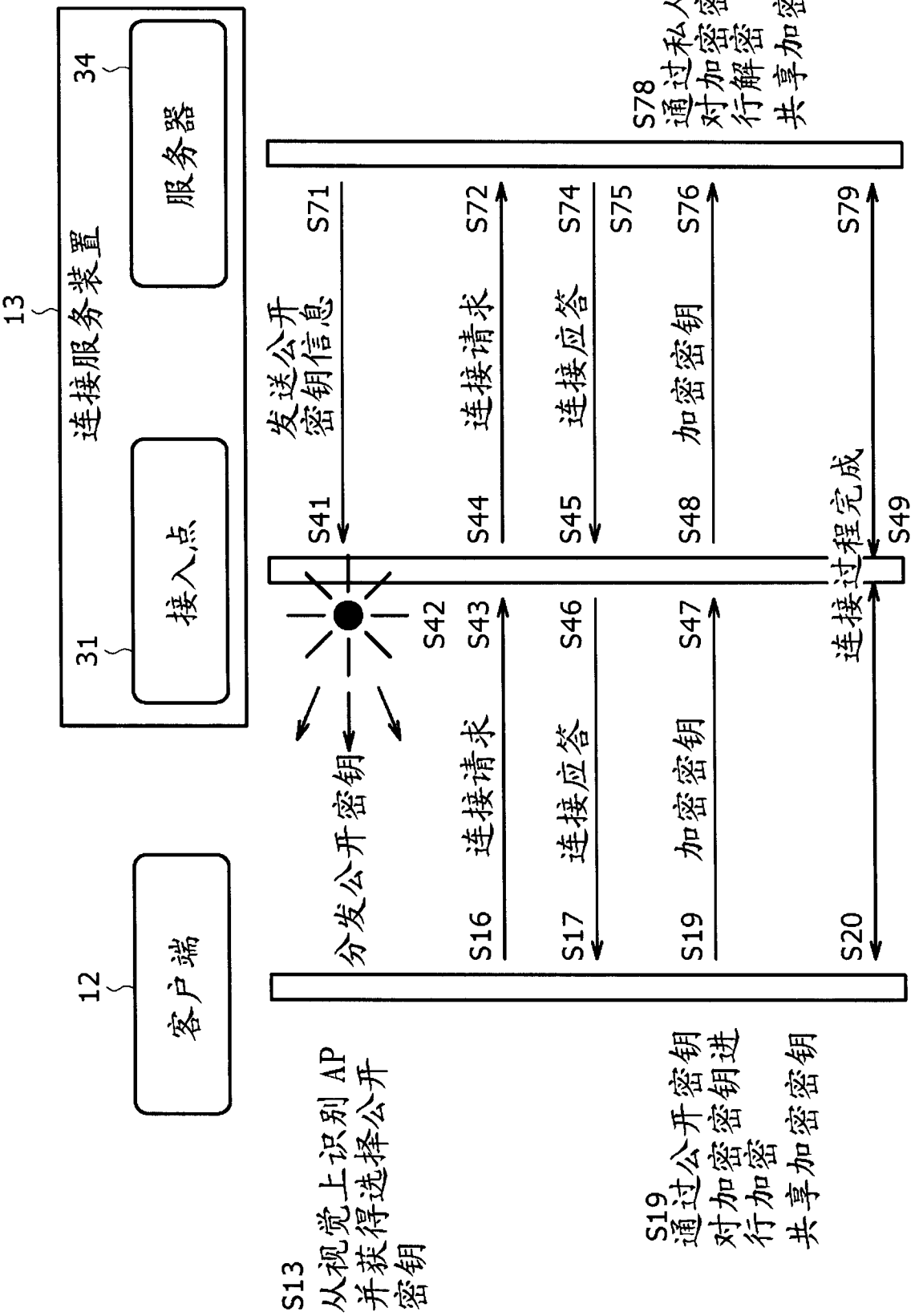

13
连接服务装置
31
接入点
34
服务器
12
客户端
S13
从视觉上识别 AP
并获得选择公开
密钥
分发公开密钥
S41
发送公开
密钥信息
S71
S42
S16
连接请求
S43
S44
连接请求
S72
S17
连接应答
S46
S45
连接应答
S74
S75
S19
加密密钥
S47
S48
加密密钥
S76
S20
连接过程完成
S49
S78
通过私人密钥
对加密密钥进
行解密密
共享加密密钥
S19
通过公开密钥
对加密密钥进
行加密密
共享加密密钥

图 9

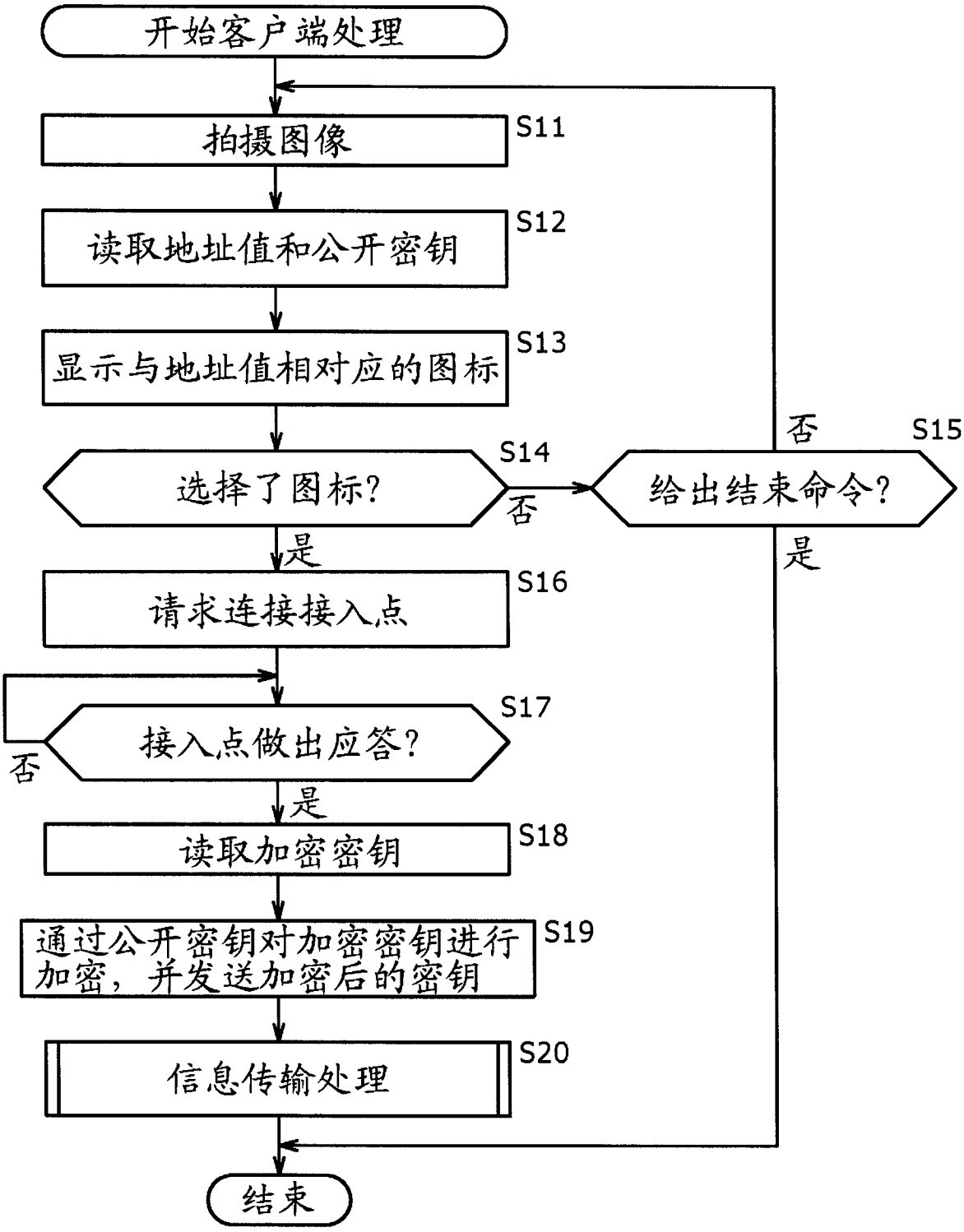

开始客户端处理
拍摄图像
S11
读取地址值和公开密钥
S12
显示与地址值相对应的图标
S13
选择了图标?
S14
否
给出结束命令?
S15
否
是
是
请求连接接入点
S16
接入点做出应答?
S17
否
是
读取加密密钥
S18
通过公开密钥对加密密钥进行加密，并发送加密后的密钥
S19
信息传输处理
S20
结束

图 10

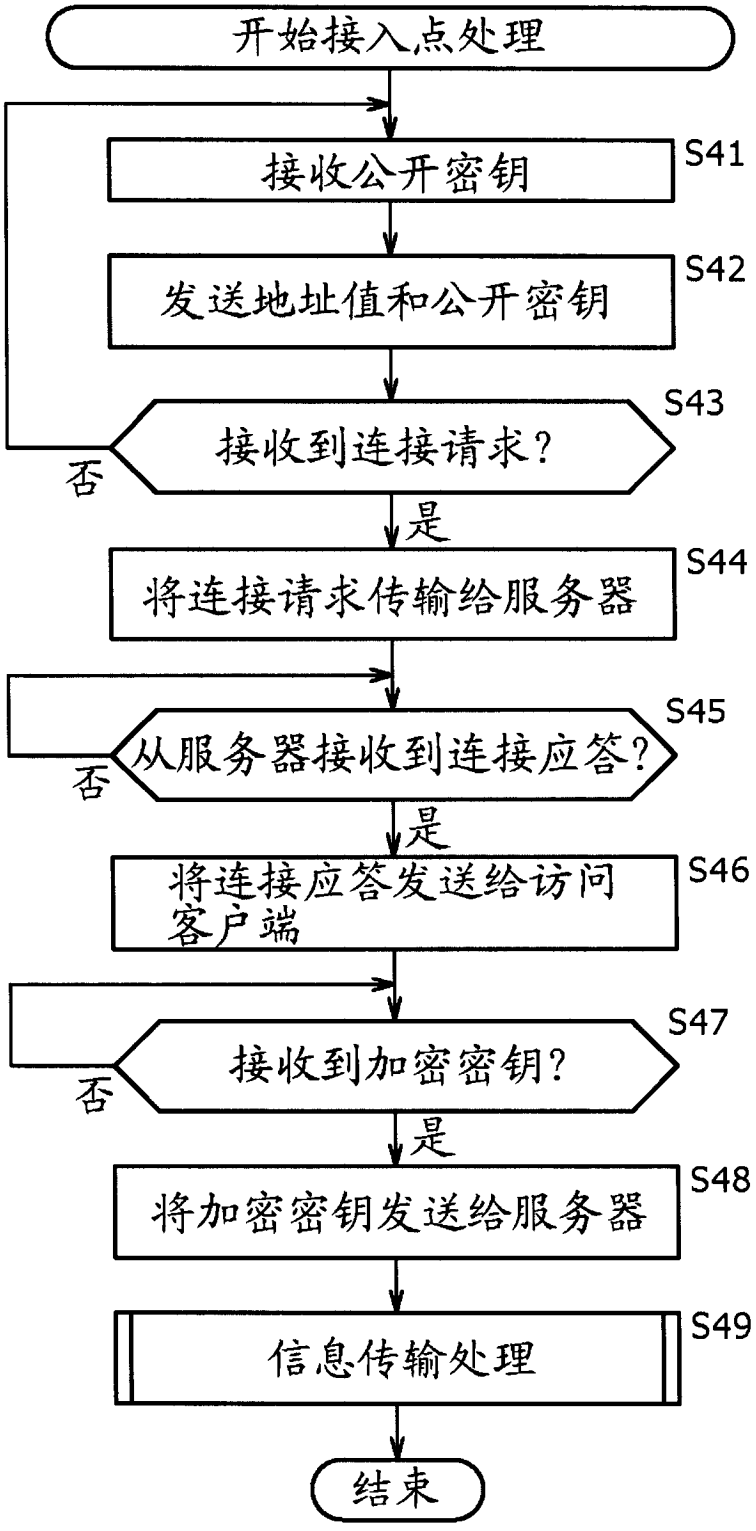

开始接入点处理
接收公开密钥
S41
发送地址值和公开密钥
S42
接收到连接请求?
S43
否
是
将连接请求传输给服务器
S44
从服务器接收到连接应答?
S45
否
是
将连接应答发送给访问客户端
S46
接收到加密密钥?
S47
否
是
将加密密钥发送给服务器
S48
信息传输处理
S49
结束

图 11

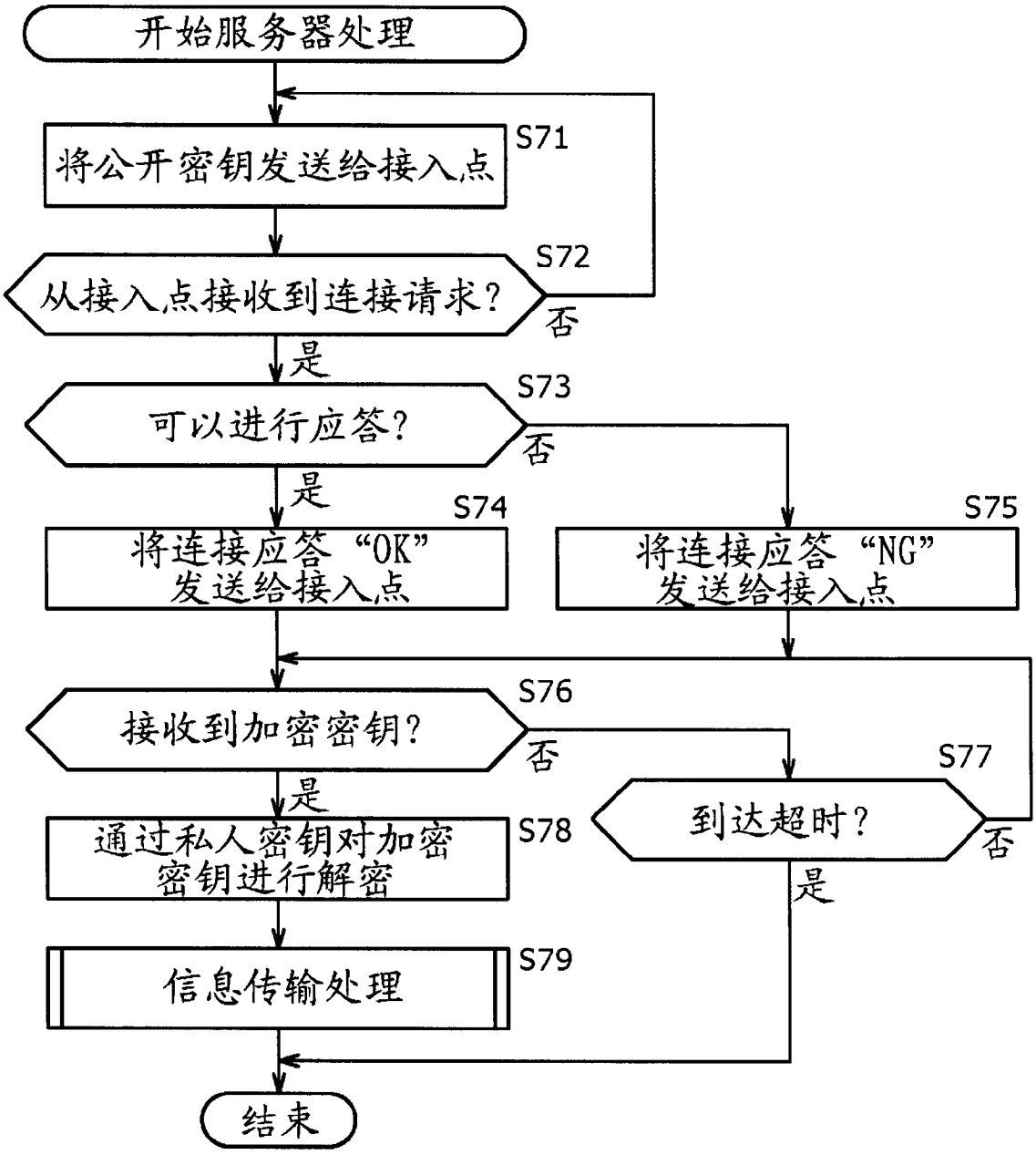

开始服务器处理
将公开密钥发送给接入点
S71
从接入点接收到连接请求?
S72
否
是
可以进行应答?
S73
否
是
将连接应答 "OK" 发送给接入点
S74
将连接应答 "NG" 发送给接入点
S75
接收到加密密钥?
S76
否
是
到达超时?
S77
否
是
通过私人密钥对加密密钥进行解密
S78
信息传输处理
S79
结束

图 12

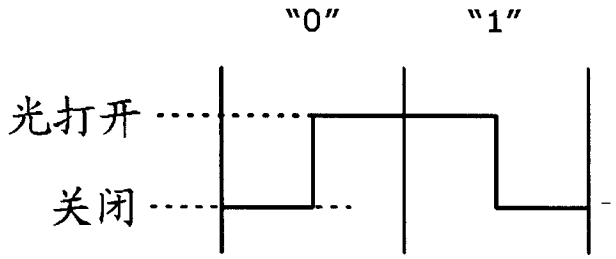

"0"
"1"
光打开
关闭

图 13

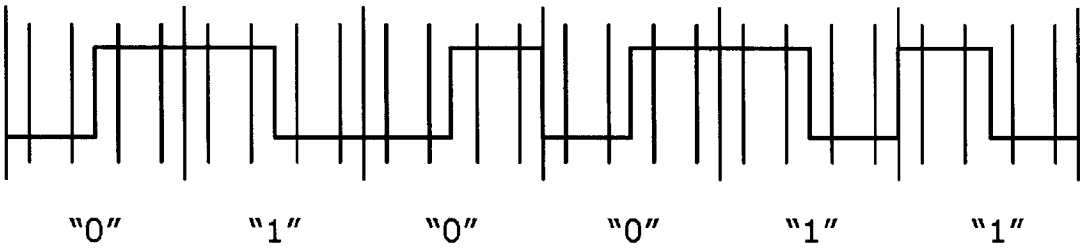

"0"
"1"
"0"
"0"
"1"
"1"

图 14

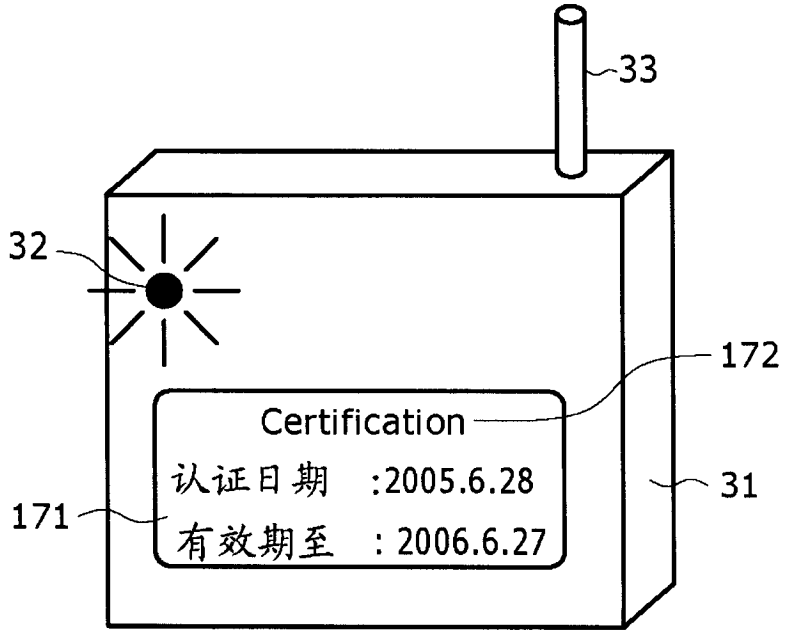

33
32
172
Certification
认证日期 :2005.6.28
有效期至 : 2006.6.27
171
31

图 15

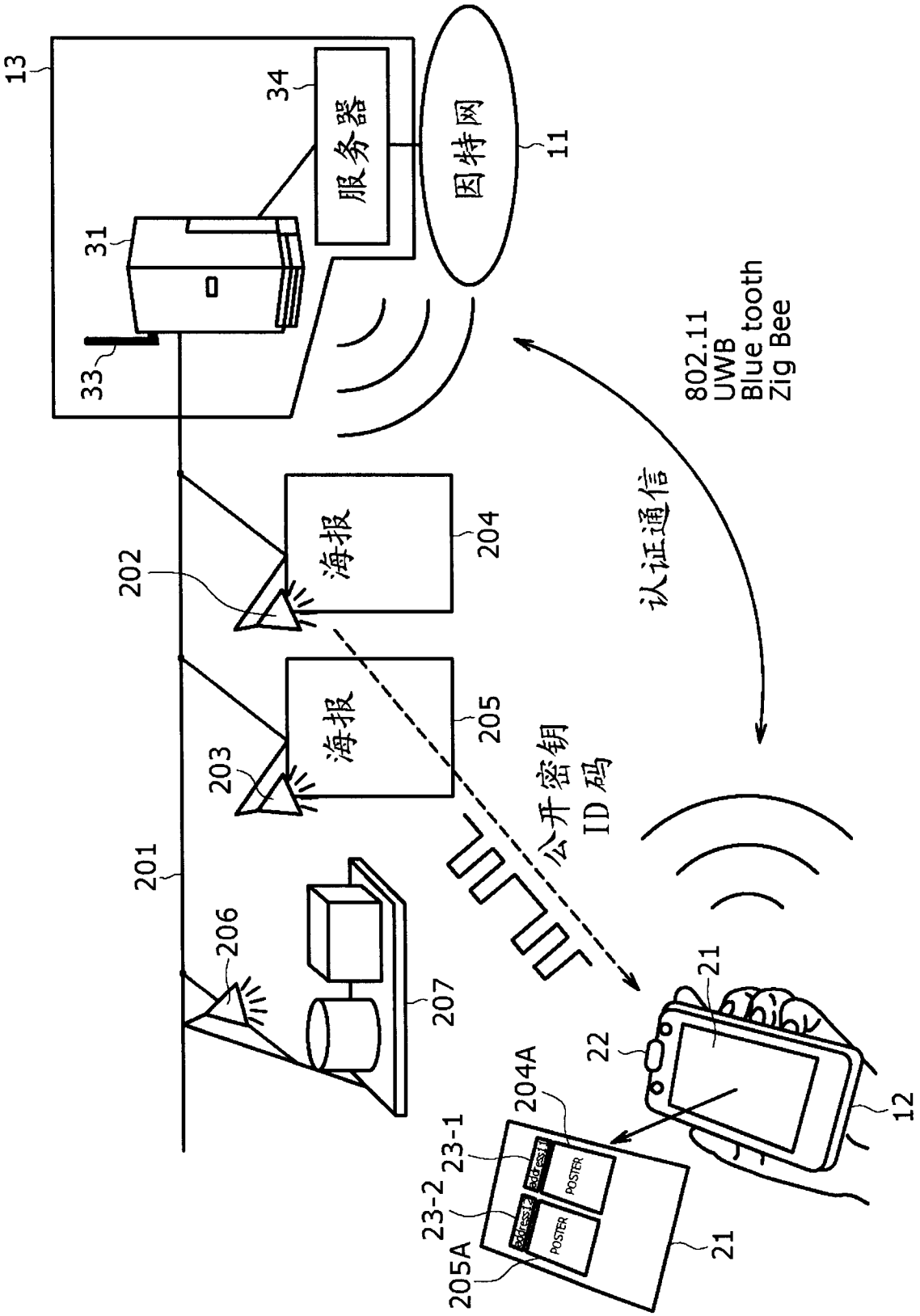

13
34
服务器
因特网
11
31
33
802.11
UWB
Blue tooth
Zig Bee
认证通信
202
海报
204
203
海报
205
公开密钥
ID 码
201
206
207
21
22
204A
12
23-1
23-2
205A
POSTER
POSTER
21

图 16

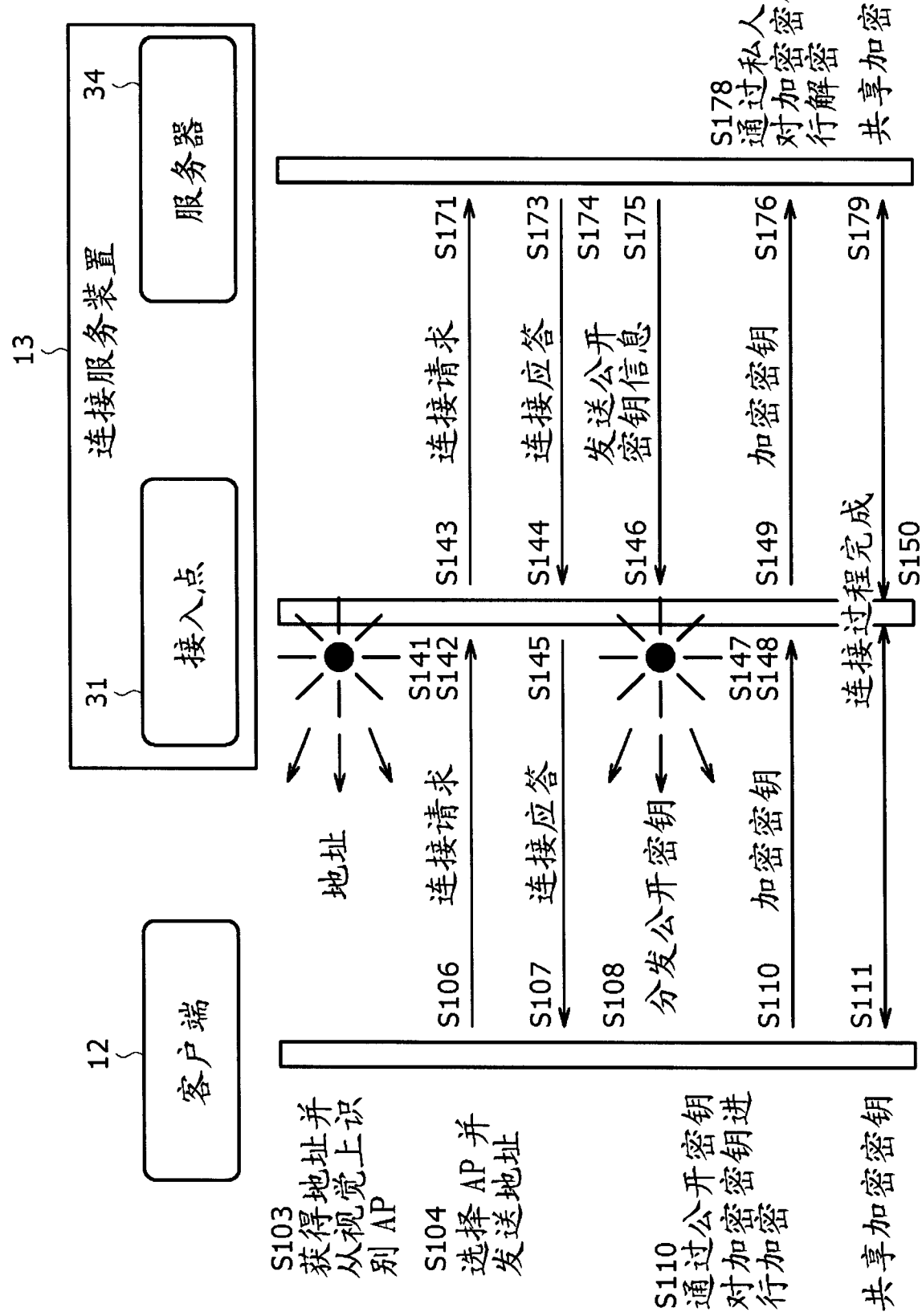

13
连接服务装置
31
接入点
34
服务器
12
客户端
地址
S141
S142
S143
连接请求
S171
S144
连接应答
S173
S145
S174
发送公开
密钥信息
S175
S146
S147
S148
S149
加密密钥
S176
S150
连接过程完成
S179
S106
连接请求
S107
连接应答
S108
分发公开密钥
S110
加密密钥
S111
S178
通过私人密钥进
行解密
共享加密密钥
S103
获得地址并
从视觉上识
别 AP
S104
选择 AP 并
发送地址
S110
通过公开密钥
对加密密钥进
行加密
共享加密密钥

图 17

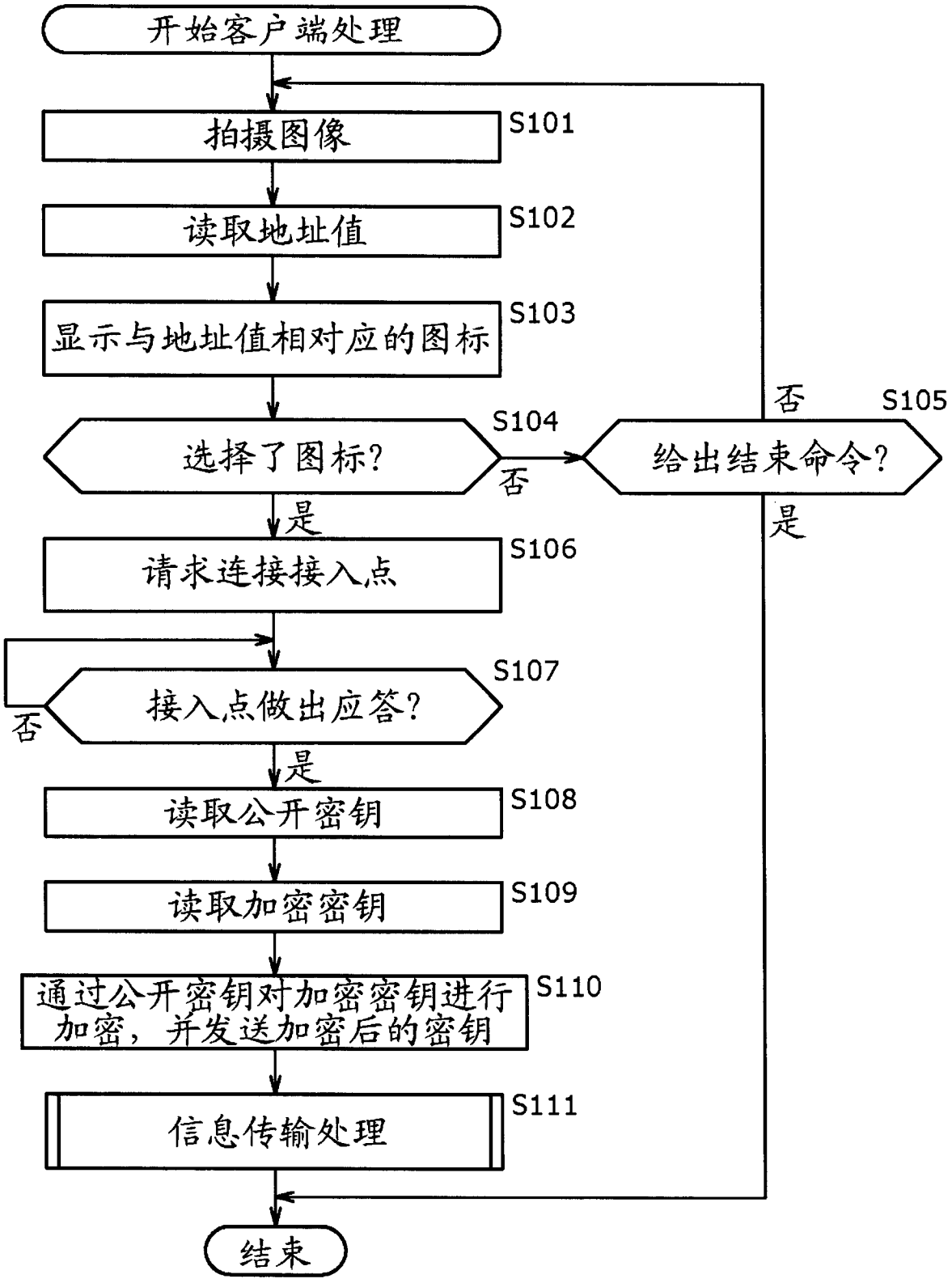

开始客户端处理
拍摄图像
S101
读取地址值
S102
显示与地址值相对应的图标
S103
选择了图标?
S104
否
给出结束命令?
S105
否
是
是
请求连接接入点
S106
接入点做出应答?
S107
否
是
读取公开密钥
S108
读取加密密钥
S109
通过公开密钥对加密密钥进行加密，并发送加密后的密钥
S110
信息传输处理
S111
结束

图 18

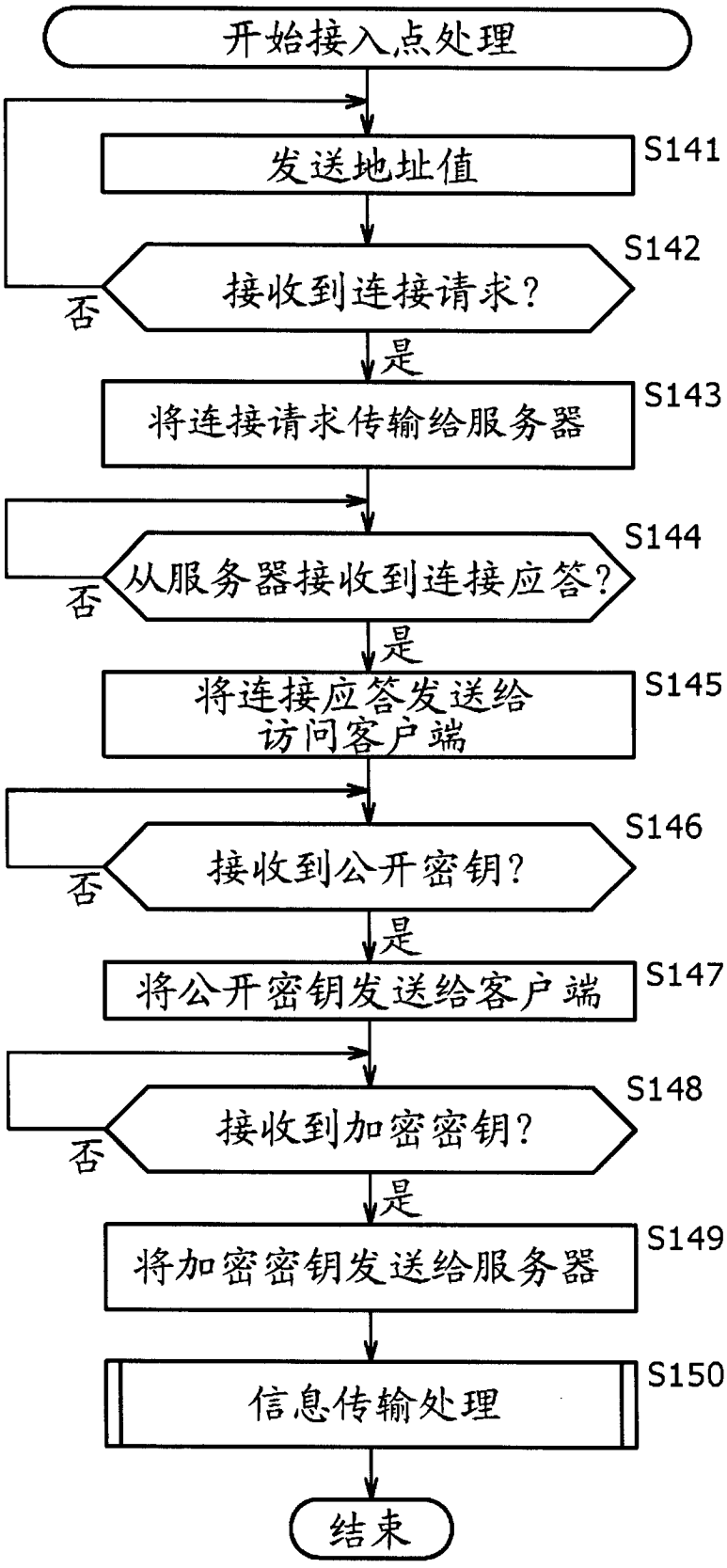

开始接入点处理
发送地址值
S141
接收到连接请求?
S142
否
是
将连接请求传输给服务器
S143
从服务器接收到连接应答?
S144
否
是
将连接应答发送给
访问客户端
S145
接收到公开密钥?
S146
否
是
将公开密钥发送给客户端
S147
接收到加密密钥?
S148
否
是
将加密密钥发送给服务器
S149
信息传输处理
S150
结束

图 19

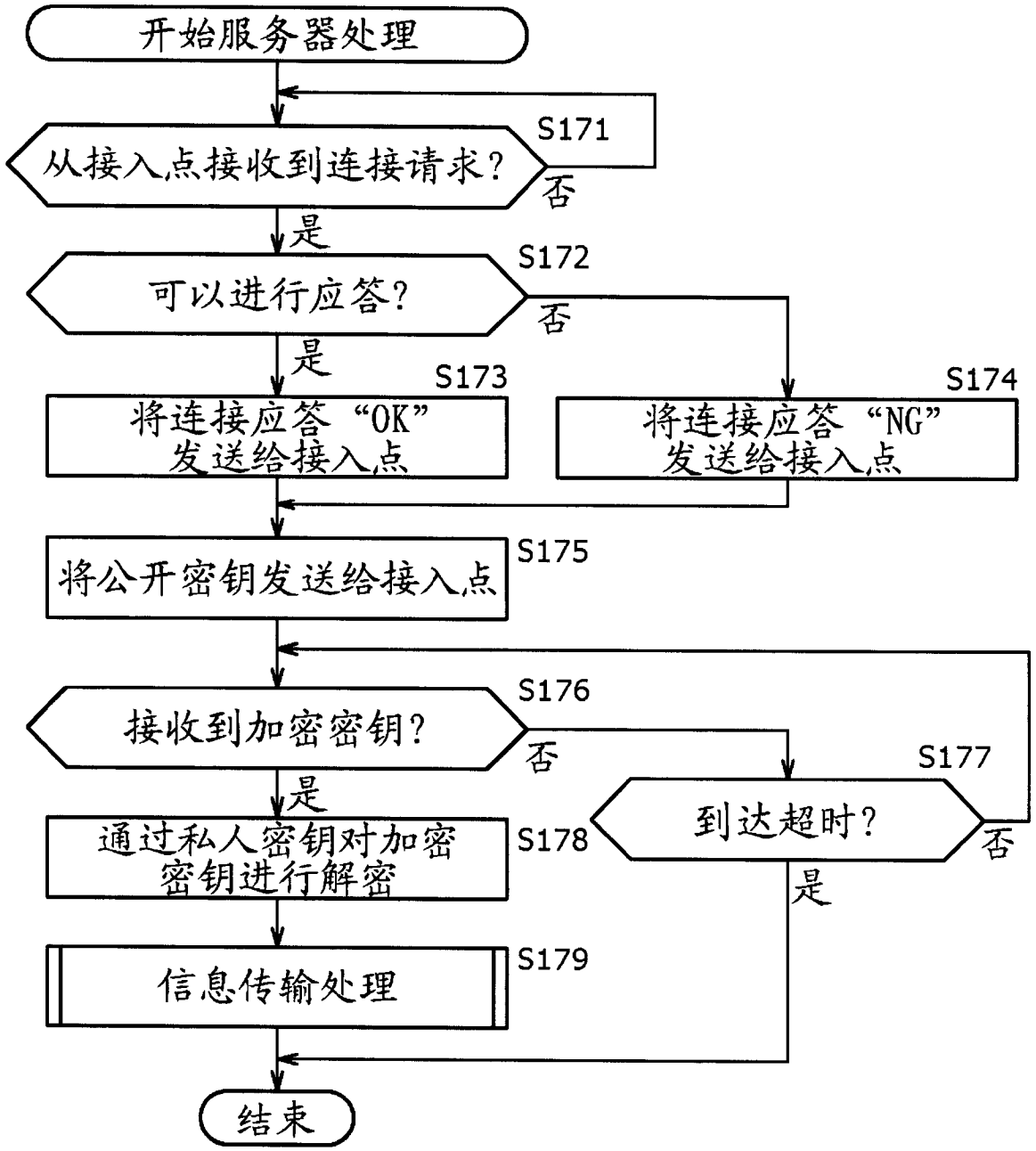

开始服务器处理
S171
从接入点接收到连接请求?
否
是
S172
可以进行应答?
否
是
S173
将连接应答“OK”
发送给接入点
S174
将连接应答“NG”
发送给接入点
S175
将公开密钥发送给接入点
S176
接收到加密密钥?
否
是
S177
到达超时?
否
是
S178
通过私人密钥对加密
密钥进行解密
S179
信息传输处理
结束

图 20

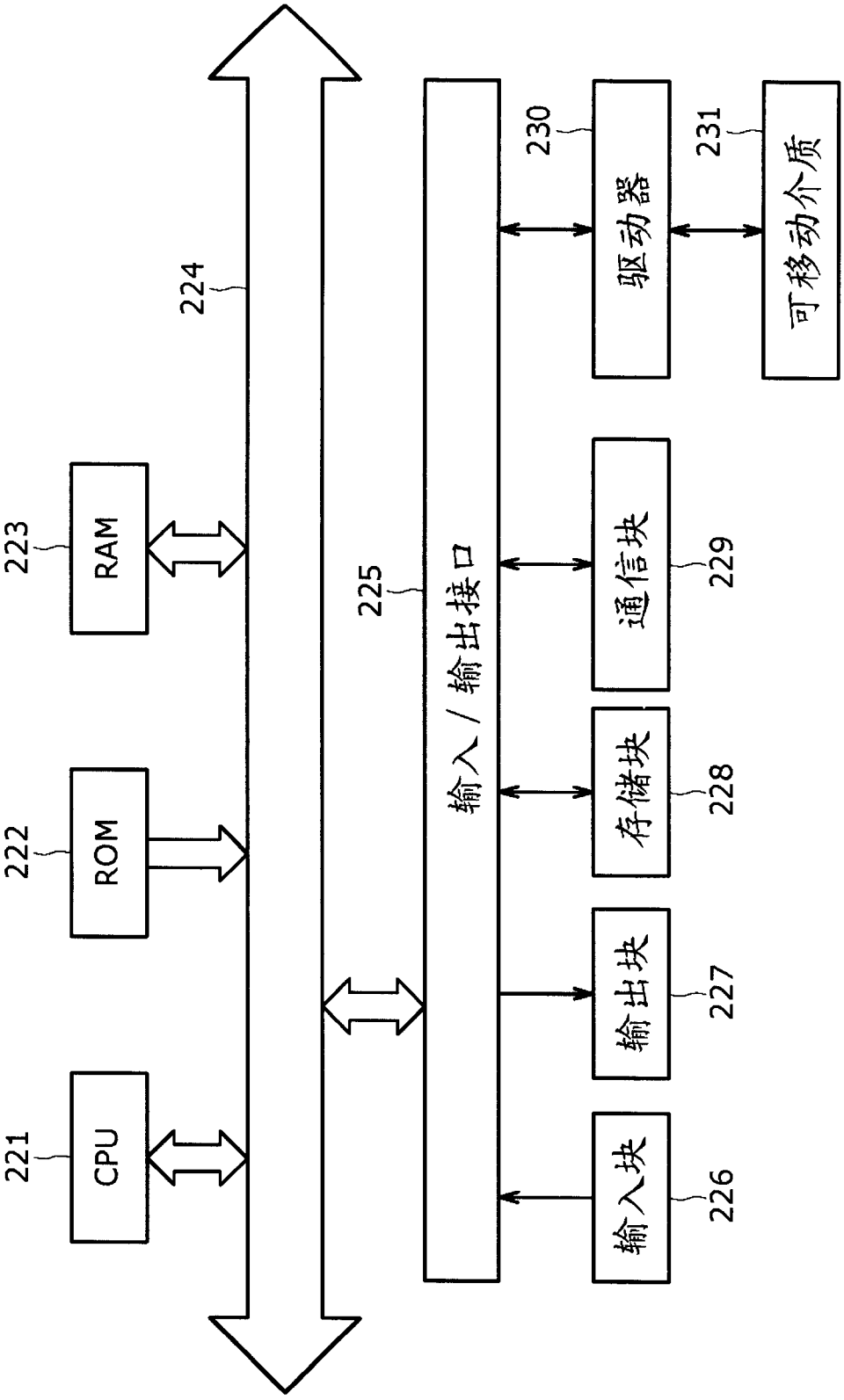

CPU
221
ROM
222
RAM
223
224
225
输入/输出接口
输入块
226
输出块
227
存储块
228
通信块
229
驱动器
230
可移动介质
231

图 21