

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2023 年 6 月 29 日 (29.06.2023)



(10) 国际公布号
WO 2023/116239 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2022/130533

(22) 国际申请日: 2022 年 11 月 8 日 (08.11.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111590467.2 2021 年 12 月 23 日 (23.12.2021) CN

(71) 申请人: 深圳 TCL 新技术有限公司 (SHENZHEN TCL NEW TECHNOLOGY CO., LTD.) [CN/CN]; 中国广东省深圳市南山区西丽街道中山园路 1001 号国际 E 城 D4 栋 9 楼, Guangdong 518052 (CN)。

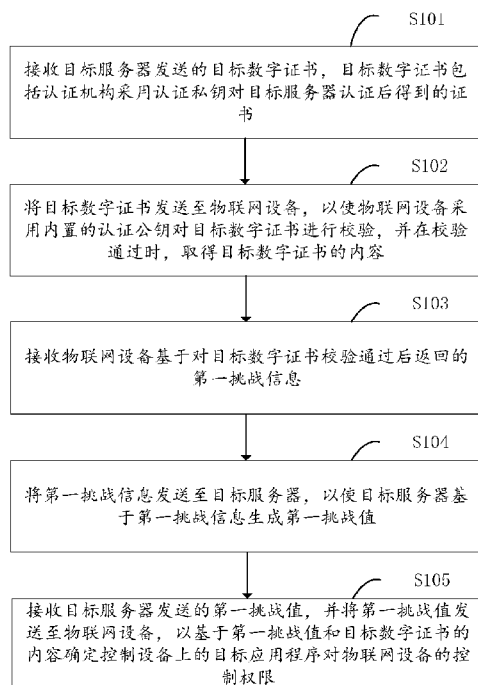
(72) 发明人: 李辉 (LI, Hui); 中国广东省深圳市南山区西丽街道中山园路 1001 号国际 E 城 D4 栋 9 楼, Guangdong 518052 (CN)。

(74) 代理人: 深圳紫藤知识产权代理有限公司 (PURPLEVINE INTELLECTUAL PROPERTY (SHENZHEN) CO., LTD.); 中国广东省深圳市南山区粤海街道大冲社区华润置地大厦 C 座 2901, Guangdong 518052 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN,

(54) Title: PERMISSION DETERMINATION METHOD AND APPARATUS, AND COMPUTER DEVICE AND COMPUTER-READABLE STORAGE MEDIUM

(54) 发明名称: 权限确定方法、装置、计算机设备和计算机可读存储介质



S101 Receive a target digital certificate, which is sent by a target server, wherein the target digital certificate comprises a certificate that is obtained after a certificate authority has certificated the target server by using a certification private key

S102 Send the target digital certificate to an Internet-of-Things device, such that the Internet-of-Things device checks the target digital certificate by using a certification public key that is set in the Internet-of-Things device, and then obtains the content of the target digital certificate when checking is passed

S103 Receive first challenge information that is returned by the Internet-of-Things device on the basis that the target digital certificate passes checking

S104 Send the first challenge information to the target server, such that the target server generates a first challenge value on the basis of the first challenge information

S105 Receive the first challenge value, which is sent by the target server, and send the first challenge value to the Internet-of-Things device, so as to determine, on the basis of the first challenge value and the content of the target digital certificate, a control permission of a target application on a control device with regard to the Internet-of-Things device

图 1

(57) Abstract: Disclosed in the embodiments of the present application are a permission determination method and apparatus, and a computer device and a computer-readable storage medium. In the embodiments of the present application, whether a target server can be trusted can be determined according to the content of a target digital certificate and a first challenge value that is sent by the target server, so as to determine whether a target application can be trusted, such that even if a target application on a control device is not an application corresponding to an Internet-of-Things device, the security of when the Internet-of Things device is controlled by means

MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE,
PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE,
SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW,
MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚
(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE,
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR,
HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO,
PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN,
TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

of the target application on the control device can be ensured.

(57) 摘要: 本申请实施例公开了一种权限确定方法、装置、计算机设备和计算机可读存储介质; 在本申请实施例中, 可以根据目标数字证书的内容和目标服务器发送的第一挑战值确定是否可以信任目标服务器, 从而确定是否可以信任目标应用程序, 进而使得即使控制设备上的目标应用程序不是物联网设备对应的应用程序, 通过控制设备上的目标应用程序控制物联网设备时也可以保证安全性。

权限确定方法、装置、计算机设备和计算机可读存储介质

[0001] 本申请要求申请日为2021年12月23日、申请号为202111590467.2、发明名称为“权限确定方法、装置、计算机设备和计算机可读存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及物联网设备技术领域，具体涉及一种权限确定方法、装置、计算机设备和计算机可读存储介质。

背景技术

[0003] 随着科学技术的发展，物联网（Internet of Things, IOT）设备的应用越来越广泛。

[0004] 目前，为了保证安全，一般是通过物联网设备的应用程序（Application）控制物联网设备，导致每增加一个物联网设备，用户需下载一个新的应用程序，比较麻烦。而如果通过其他应用程序控制物联网设备，无法保证安全性。

发明概述

技术问题

[0005] 通过其他应用程序控制物联网设备，无法保证安全性。

问题的解决方案

技术解决方案

[0006] 本申请实施例提供一种权限确定方法、装置、计算机设备和计算机可读存储介质，当通过其他应用程序控制物联网设备时也可以保证安全性。

[0007] 一种权限确定方法，应用于控制设备，包括：

[0008] 接收目标服务器发送的目标数字证书，上述目标数字证书包括认证机构采用认证私钥对上述目标服务器认证后得到的证书；

[0009] 将上述目标数字证书发送至物联网设备，以使上述物联网设备采用内置的认证

公钥对上述目标数字证书进行校验，并在校验通过时，取得上述目标数字证书的内容；

[0010] 接收上述物联网设备基于对上述目标数字证书校验通过后返回的第一挑战信息；

[0011] 将上述第一挑战信息发送至上述目标服务器，以使上述目标服务器基于上述第一挑战信息生成第一挑战值；

[0012] 接收上述目标服务器发送的上述第一挑战值，并将上述第一挑战值发送至上述物联网设备，以基于上述第一挑战值和上述目标数字证书的内容确定上述控制设备上的目标应用程序对上述物联网设备的控制权限。

[0013] 一种权限确定方法，应用于物联网设备，包括：

[0014] 接收控制设备发送的目标数字证书，上述目标数字证书为认证机构采用认证私钥对目标服务器认证后得到的证书；

[0015] 采用内置的认证公钥对上述目标数字证书进行校验；

[0016] 当校验通过时，取得上述目标数字证书的内容，并返回第一挑战信息至上述控制设备，以使上述控制设备将第一挑战信息发送至上述目标服务器，上述第一挑战信息用于指示上述目标服务器生成第一挑战值，并将上述第一挑战值返回至上述控制设备；

[0017] 接收上述控制设备发送的上述第一挑战值；

[0018] 基于上述第一挑战值和上述目标数字证书的内容确定上述控制设备上的目标应用程序对上述物联网设备的控制权限。

[0019] 一种权限确定方法，应用于目标服务器，包括：

[0020] 将目标数字证书发送至控制设备，以使得上述控制设备将上述目标数字证书发送至物联网设备，上述目标数字证书用于指示上述物联网设备进行校验，并在校验通过时，取得上述目标数字证书的内容，并返回第一挑战信息至上述控制设备，上述目标数字证书包括认证机构采用认证私钥对上述目标服务器认证后得到的证书；

[0021] 接收上述控制设备发送的上述第一挑战信息；

[0022] 基于上述第一挑战信息生成第一挑战值；

- [0023] 将上述第一挑战值发送至上述控制设备，以使得上述控制设备将上述第一挑战值发送至上述物联网设备，上述第一挑战值和上述目标数字证书的内容用于上述物联网设备确定上述控制设备上的目标应用程序对上述物联网设备的控制权限。
- [0024] 相应地，本申请实施例提供一种权限确定装置，应用于控制设备，包括：
- [0025] 第一接收模块，用于接收目标服务器发送的目标数字证书，上述目标数字证书包括认证机构采用认证私钥对上述目标服务器认证后得到的证书；
- [0026] 第一发送模块，用于将上述目标数字证书发送至物联网设备，以使上述物联网设备采用内置的认证公钥对上述目标数字证书进行校验，并在校验通过时，取得上述目标数字证书的内容；
- [0027] 第二接收模块，用于接收上述物联网设备基于对上述目标数字证书校验通过后返回的第一挑战信息；
- [0028] 第二发送模块，用于将上述第一挑战信息发送至上述目标服务器，以使上述目标服务器基于上述第一挑战信息生成第一挑战值；
- [0029] 第三接收模块，用于接收上述目标服务器发送的上述第一挑战值，并将上述第一挑战值发送至上述物联网设备，以基于上述第一挑战值和上述目标数字证书的内容确定上述控制设备上的目标应用程序对上述物联网设备的控制权限。
- [0030] 相应地，本申请实施例提供一种权限确定装置，应用于物联网设备，包括：
- [0031] 第四接收模块，用于接收控制设备发送的目标数字证书，上述目标数字证书为认证机构采用认证私钥对目标服务器认证后得到的证书；
- [0032] 第一校验模块，用于采用内置的认证公钥对上述目标数字证书进行校验；
- [0033] 第三发送模块，用于当校验通过时，取得上述目标数字证书的内容，并发送第一挑战信息至上述控制设备，以使上述控制设备将第一挑战信息发送至上述目标服务器，上述第一挑战信息用于指示上述目标服务器生成第一挑战值，并将上述第一挑战值返回至上述控制设备；
- [0034] 第五接收模块，用于接收上述控制设备发送的第一挑战值；
- [0035] 确定模块，用于基于上述第一挑战值和上述目标数字证书的内容确定上述控制设备上的目标应用程序对上述物联网设备的控制权限。

[0036] 相应地，本申请实施例提供一种权限确定装置，应用于目标服务器，包括：

[0037] 第四发送模块，用于将目标数字证书发送至控制设备，以使得上述控制设备将上述目标数字证书发送至物联网设备，上述目标数字证书用于指示上述物联网设备进行校验，并在校验通过时，取得上述目标数字证书的内容，并返回第一挑战信息至上述控制设备，上述目标数字证书包括认证机构采用认证私钥对上述目标服务器认证后得到的证书；

[0038] 第六接收模块，用于接收上述控制设备发送的上述第一挑战信息；

[0039] 生成模块，用于基于上述第一挑战信息生成第一挑战值；

[0040] 第五发送模块，用于将上述第一挑战值发送至上述控制设备，以使得上述控制设备将上述第一挑战值发送至上述物联网设备，上述第一挑战值和上述目标数字证书的内容用于上述物联网设备确定上述控制设备上的目标应用程序对上述物联网设备的控制权限。

[0041] 此外，本申请实施例还提供一种计算机设备，包括处理器和存储器，上述存储器存储有计算机程序，上述处理器用于运行上述存储器内的计算机程序实现本申请实施例提供的权限确定方法。

[0042] 此外，本申请实施例还提供一种计算机可读存储介质，上述计算机可读存储介质存储有计算机程序，上述计算机程序适于处理器进行加载，以执行本申请实施例所提供的任一种权限确定方法中的步骤。

发明的有益效果

有益效果

[0043] 在本申请的实施例中，先接收目标服务器发送的目标数字证书，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书。然后将目标数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对目标数字证书进行校验，并在校验通过时，取得目标数字证书的内容。接着，接收物联网设备基于对目标数字证书校验通过后返回的第一挑战信息。再将第一挑战信息发送至目标服务器，以使目标服务器基于第一挑战信息生成第一挑战值。最后接收目标服务器发送的上述第一挑战值，并将第一挑战值发送至物联网设备，以基于第一挑战值和目标数字证书的内容确定控制设备的目标应用程序对物联网

设备的控制权限。

[0044] 即在本申请实施例中，由于目标服务器和目标应用程序是属于同一个商家的，因此，目标服务器信任目标应用程序。当物联网设备采用认证公钥对目标数字证书的校验通过时，说明该目标数字证书为认证机构认证过的证书。因为认证机构是物联网设备信任的机构，所以物联网设备可以信任目标数字证书的内容，以便可以根据目标数字证书的内容和目标服务器发送的第一挑战值确定是否可以信任目标服务器，从而确定是否可以信任目标应用程序，进而使得即使控制设备上的目标应用程序不是物联网设备对应的应用程序，通过控制设备上的目标应用程序控制物联网设备时也可以保证安全性。

对附图的简要说明

附图说明

[0045] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0046] 图1是本申请实施例提供的权限确定方法的流程示意图；

[0047] 图2是本申请实施例提供的另一种权限确定方法的流程示意图；

[0048] 图3是本申请实施例提供的另一种权限确定方法的流程示意图；

[0049] 图4是本申请实施例提供的另一种权限确定方法的交互示意图；

[0050] 图5是本申请实施例提供的权限确定装置的结构示意图；

[0051] 图6是本申请实施例提供的另一种权限确定装置的结构示意图；

[0052] 图7是本申请实施例提供的另一种权限确定装置的结构示意图；

[0053] 图8是本申请实施例提供的计算机设备的结构示意图。

发明实施例

本发明的实施方式

[0054] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域技术人员在没有作出创造性劳动前

提下所获得的所有其他实施例，都属于本申请保护的范围。

[0055] 本申请实施例提供一种权限确定方法、装置、计算机设备和计算机可读存储介质。其中，该权限确定装置可以集成在计算机设备中，该计算机设备可以是服务器，也可以是控制设备，也可以是物联网设备。

[0056] 其中，服务器可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、网络加速服务（Content Delivery Network，CDN）、以及大数据和人工智能平台等基础云计算服务的云服务器。

[0057] 控制设备可以是智能手机、平板电脑、笔记本电脑以及台式计算机等，但并不局限于此。

[0058] 物联网设备指可以与其他设备进行网络通信的设备，比如，可以是智能空调、智能音箱等设备。

[0059] 服务器、控制设备以及物联网设备可以通过有线或无线通信方式进行直接或间接地连接，本申请在此不做限制。

[0060] 以下分别进行详细说明。需要说明的是，以下实施例的描述顺序不作为对实施例优选顺序的限定。

[0061] 相关技术中，对物联网设备进行控制的过程可以为：通过控制设备上的物联网设备对应的应用程序发送控制指令至物联网设备，物联网设备再执行控制指令对应的操作。

[0062] 为了保证安全性，在通过控制设备上的物联网设备对应的应用程序控制物联网设备之前，会对物联网设备对应的应用程序的权限进行校验。校验的过程可以为：在控制设备上下载物联网设备对应的应用程序，将应用程序携带的私钥进行存储，在物联网设备上设置私钥对应的公钥，通过公钥确定控制设备的安全性。

[0063] 然而，在控制设备上的存储的私钥容易被破解，当被破解时，没有权限的控制设备也可根据破解得到的私钥对物联网设备进行控制，从而导致不安全。

[0064] 此外，如果用户想通过控制设备上的其他应用程序控制物联网设备，由于其他

应用程序没有携带私钥（其他应用程序与物联网设备不属于同一个商家，所以物联网设备的商家不能将私钥设置在其他应用程序上），使得不能对控制设备上的其他应用程序的权限进行校验，从而使得存在安全性的问题。因此，相关技术中，还不能通过其他应用程序控制物联网设备。

[0065] 为了解决上述的安全性的问题，本申请实施例提供了一种权限确定方法，在该方法中，先接收目标服务器发送的目标数字证书，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书。然后将目标数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对目标数字证书进行校验，并在校验通过时，取得目标数字证书的内容。接着，接收物联网设备基于对目标数字证书校验通过后返回的第一挑战信息。再将第一挑战信息发送至目标服务器，以使目标服务器基于第一挑战信息生成第一挑战值。最后接收目标服务器发送的第一挑战值，并将第一挑战值发送至物联网设备，以基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。

[0066] 即在本申请实施例中，由于目标服务器和目标应用程序是属于同一个商家的，因此，目标服务器信任目标应用程序。当物联网设备采用认证公钥对目标数字证书的校验通过时，说明该目标数字证书为认证机构认证过的证书。因为认证机构是物联网设备信任的机构，所以物联网设备可以信任目标数字证书的内容，以便可以根据目标数字证书的内容和目标服务器发送的第一挑战值确定是否可以信任目标服务器，从而确定是否可以信任目标应用程序，进而使得即使控制设备上的目标应用程序不是物联网设备对应的应用程序，通过控制设备上的目标应用程序控制物联网设备时也可以保证安全性。

[0067] 下面对本申请实施例提供的权限确定方法进行详细的描述。如图1所示，该权限确定方法的具体流程如下：

[0068] S101、接收目标服务器发送的目标数字证书，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书。

[0069] 其中，认证机构指电子商务认证中心（Certificate Authority, CA）。由于认证结构是受信任的第三方，因此，当认证结构对目标服务器进行认证后，说

明认证机构信任目标服务器，则物联网设备可以信任目标服务器。

[0070] 目标数字证书指一串能够表明目标服务器身份信息的数字。目标服务器先在认证机构上进行认证后，可以得到目标数字证书。

[0071] 控制设备可以通过控制设备上的目标应用程序接收目标数字证书。目标应用程序指实际控制物联网设备的应用程序，目标应用程序可以为物联网设备的商家研发的应用程序，即物联网设备对应的应用程序，也可以其他商家研发的应用程序（由于当目标应用程序为物联网设备对应的应用程序时，应用本申请实施例提供的权限确定方法也可以提供控制物联网设备的安全性。因此，目标应用程序也可以为物联网设备对应的应用程序）。

[0072] 应理解，在本申请的方法实施例中，控制设备可以通过目标应用程序实现与目标服务器和物联网设备之间的信息交互。比如，可以通过目标应用程序将目标数字证书发送至物联网设备，又比如，可以通过目标应用程序接收第一挑战信息并通过目标应用程序将第一挑战信息发送至目标服务器。

[0073] 目标服务器可以为物联网设备的商家生产的初始服务器，则此时目标应用程序为物联网设备对应的应用程序。

[0074] 或者，目标服务器也可以为其他商家（除了生产该物联网设备的商家之外的商家）的服务器，此时，目标应用程序为控制设备上的其他应用程序（其他应用程序指控制设备上已安装的除了物联网设备对应的应用程序之外的应用程序）。

[0075] 比如，物联网设备为A商家生产的设备，物联网设备对应的应用程序为A应用程序。B商家研发了B应用程序，则目标服务器可以为B商家的服务器，目标应用程序可以为B应用程序。

[0076] 当控制设备的用户想通过控制设备上的目标应用程序控制物联网设备时，用户可以对控制设备上的目标应用程序进行操作，使得控制设备的目标应用程序生成权限验证请求，并将该权限验证请求发送至目标服务器，目标服务器再基于该权限验证请求将目标数字证书发送至控制设备，控制设备从而接收到目标数字证书。

[0077] 或者，也可以在用户安装完成目标应用程序时自动生成权限验证请求，并将该

权限验证请求发送至目标服务器，目标服务器再基于该权限验证请求将目标数字证书发送至控制设备，控制设备从而接收到目标数字证书。

[0078] 对于控制设备接收目标数字证书的时间，用户可以根据实际情况进行设置，本申请在此不做限定。

[0079] S102、将目标数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对目标数字证书进行校验，并在校验通过时，取得目标数字证书的内容。

[0080] 当目标应用程序为控制设备上的其他应用程序时，由于其他应用程序对应的目标服务器为其他商家的服务器，因此，生产物联网设备的商家无法将物联网设备的私钥存储在目标服务器上。所以，可以先让物联网设备信任的认证机构采用认证私钥对目标服务器进行认证，然后在物联网设备上设置认证机构的认证公钥。

[0081] 接着，控制设备在获取到目标数字证书后，再将目标数字证书发送至物联网设备，使得物联网设备采用内置的认证公钥对目标数字证书进行校验。如果校验通过，说明该目标数字证书是认证机构认证过的证书，即说明物联网设备可以信任该目标数字证书的内容。

[0082] 目标数字证书的内容可以包括但不限于目标服务器的身份信息、认证机构的信息以及目标服务器的第一公钥等信息。

[0083] S103、接收物联网设备基于对目标数字证书校验通过后返回的第一挑战信息。

[0084] 物联网设备在对目标数字证书校验通过后，将第一挑战信息返回至控制设备，控制设备从而接收到第一挑战信息。其中，第一挑战信息可以为一串随机字符串。

[0085] 应理解，物联网设备在对目标数字证书校验通过后，也可以不将第一挑战信息返回至控制设备，当接收到控制设备发送的挑战信息获取请求时，如果对目标数字证书校验通过，再将第一挑战信息返回至控制设备。控制设备可以将挑战信息获取请求和目标数字证书一起发送至物联网设备。或者，控制设备也可以先将目标数字证书发送至物联网设备，然后再将挑战信息获取请求发送至物联网设备。

[0086] 物联网设备可以在对目标数字证书校验通过时生成该第一挑战信息并返回该第

一挑战信息。或在，物联网设备也可以先生成第一挑战信息，然后在目标数字证书校验通过时返回该第一挑战信息。对于物联网设备生成第一挑战信息的时间，用户可以根据实际情况进行选择，本申请在此不做限定。

[0087] S104、将第一挑战信息发送至目标服务器，以使目标服务器基于第一挑战信息生成第一挑战值。

[0088] 控制设备接收到第一挑战信息后，将第一挑战信息发送至目标服务器，使得目标服务器基于第一挑战信息生成第一挑战值。

[0089] 可选地，目标服务器可以是采用目标服务器的第一私钥对第一挑战信息进行签名，从而得到第一挑战值。

[0090] 或者，目标服务器可以采用预设的加密算法对第一挑战信息进行加密，从而得到第一挑战值。此时，目标数字证书的内容包括预设的加密算法对应的解密算法。

[0091] 需要说明的是，由于目标应用程序与目标服务器是属于同一商家的，因此，目标服务器可以信任该目标应用程序。因此，当目标服务器接收到第一挑战信息之后，可以不对目标应用程序进行校验。

[0092] 或者，为了进一步保证安全，目标服务器也可以校验控制设备的权限，即校验控制设备的目标应用程序的权限。当校验通过后，目标服务器再基于第一挑战信息生成第一挑战值。

[0093] 对于目标服务器校验目标应用程序的权限的方法，用户可以根据实际情况进行选择。比如，可以通过目标应用程序将令牌和第一挑战信息一起发送至目标服务器，目标服务器接收到后，将令牌与本身存储的令牌进行比对，如果该令牌与本身存储的令牌相同，则对目标应用程序的校验通过。

[0094] 又比如，控制设备和目标服务器均可以根据预设规则生成随机数，然后控制设备采用存储的公钥对随机数进行加密，并通过目标应用程序将加密后的随机数和第一挑战信息一起发送至目标服务器。目标服务器接收到后，采用存储的私钥对随机数进行解密，并将解密后的随机数与根据预设规则生成的随机数进行比对，如果解密后的随机数与根据预设规则生成的随机数相同，则对目标应用程序的校验通过。本申请在此不做具体限定。

- [0095] S105、接收目标服务器发送的第一挑战值，并将第一挑战值发送至物联网设备，以基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。
- [0096] 控制设备接收到目标服务器发送的第一挑战值之后，将第一挑战值发送至物联网设备，使得物联网设备基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。
- [0097] 其中，基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限的过程可以为：
- [0098] 因为物联网设备信任目标数字证书的内容，所以当物联网设备采用目标数字证书的内容对第一挑战值的校验通过时且校验通过时得到的第一挑战信息与物联网设备发送的第一挑战信息相同时，说明物联网设备可以信任目标服务器，而目标服务器信任目标应用程序，所以，此时物联网设备可以将该目标应用程序标记为具备对物联网设备的控制权限的应用程序。
- [0099] 当采用目标数字证书的内容对第一挑战值的校验不通过时，说明物联网设备不可以信任目标服务器，则将该目标应用程序标记为不具备对物联网设备的控制权限的应用程序。
- [0100] 可选地，当目标服务器采用目标服务器的第一私钥对第一挑战信息进行签名，得到第一挑战值且目标数字证书的内容包括目标服务器的第一公钥时，采用目标数字证书的内容对第一挑战值进行校验的过程可以为：采用第一公钥对第一挑战值进行校验。
- [0101] 又或者，当目标服务器采用预设的加密算法对第一挑战信息进行加密，得到第一挑战值且目标数字证书的内容包括预设的加密算法对应的解密算法时，采用目标数字证书的内容对第一挑战值进行校验的过程可以为：采用解密算法对第一挑战值进行解密。
- [0102] 由以上可知，本申请实施例提供了一种权限确定方法，在该方法中，先接收目标服务器发送的目标数字证书，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书。然后将目标数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对目标数字证书进行校验，并在校验通过时，取

得目标数字证书的内容。接着，接收物联网设备基于对目标数字证书校验通过后返回的第一挑战信息。再将第一挑战信息发送至目标服务器，以使目标服务器基于第一挑战信息生成第一挑战值。最后接收目标服务器发送的第一挑战值，并将第一挑战值发送至物联网设备，以基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。

[0103] 即在本申请实施例中，由于目标服务器和目标应用程序是属于同一个商家的，因此，目标服务器信任目标应用程序。当物联网设备采用认证公钥对目标数字证书的校验通过时，说明该目标数字证书为认证机构认证过的证书。因为认证机构是物联网设备信任的机构，所以物联网设备可以信任目标数字证书的内容，以便可以根据目标数字证书的内容和目标服务器发送的第一挑战值确定是否可以信任目标服务器，从而确定是否可以信任目标应用程序，进而使得即使控制设备上的目标应用程序不是物联网设备对应的应用程序，通过控制设备上的目标应用程序控制物联网设备时也可以保证安全性。

[0104] 在一些实施例中，目标数字证书包括第一数字证书，第一数字证书可以为认证机构采用认证私钥对目标服务器的第一公钥认证后得到的证书。

[0105] 相应地，将目标数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对目标数字证书进行校验，并在校验通过时，取得目标数字证书的内容，包括：

[0106] 将第一数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对第一数字证书进行校验，并在校验通过时，取得目标服务器的第一公钥。

[0107] 接收物联网设备基于对目标数字证书校验通过后返回的第一挑战信息，包括：

[0108] 接收物联网设备基于对第一数字证书校验通过后返回的第一挑战信息。

[0109] 将第一挑战信息发送至所述目标服务器，以使目标服务器基于第一挑战信息生成第一挑战值，包括：

[0110] 将第一挑战信息发送至目标服务器，以使目标服务器采用目标服务器的第一私钥对第一挑战信息进行签名，得到第一挑战值。

[0111] 接收目标服务器发送的第一挑战值，并将第一挑战值发送至物联网设备，以基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网

设备的控制权限，包括：

- [0112] 接收目标服务器发送的第一挑战值，并将第一挑战值发送至物联网设备，以使物联网设备采用第一公钥对第一挑战值进行校验，并在校验通过时，将控制设备上的目标应用程序标记为具备对物联网设备的控制权限的应用程序。
- [0113] 在本实施例中，认证机构采用认证私钥对目标服务器的第一公钥进行签名，得到第一数字证书。物联网设备采用认证公钥对第一数字证书进行校验后，如果校验通过，则可以得到第一公钥，并且说明物联网设备可以信任第一公钥。然后物联网设备再采用第一公钥对采用第一私钥签名后得到的第一挑战值进行校验，如果校验通过，说明物联网设备可以信任目标服务器，而目标服务器信任目标应用程序，所以物联网设备可以信任目标应用程序，即将目标应用程序标记为具备对物联网设备的控制权限的应用程序。
- [0114] 需要说明的是，当物联网设备采用第一公钥对第一挑战值校验通过时，也可以将第一数字证书标为具备权限的证书。
- [0115] 虽然物联网设备校验了控制设备的目标应用程序的权限，但是，目标应用程序还没校验物联网设备的权限。因此，在另一些实施例中，将目标数字证书发送至物联网设备，包括：
- [0116] 控制设备先向物联网设备发送证书获取请求。物联网设备收到证书获取请求后，基于证书获取请求返回的第二数字证书。然后控制设备接收第二数字证书，第二数字证书为认证机构采用认证私钥对物联网设备的第二公钥进行签名后得到的证书。
- [0117] 接着，控制设备采用内置的认证公钥对第二数字证书进行校验，在校验通过时，取得物联网设备的第二公钥。
- [0118] 控制设备再生成第二挑战信息，并将第二挑战信息发送至物联网设备，以使物联网设备基于第二挑战信息生成第二挑战值。
- [0119] 最后，控制设备接收第二挑战值，并根据第二公钥对第二挑战值进行校验。当校验通过时，说明该物联网设备是可以信任的，则将目标数字证书发送至物联网设备。
- [0120] 应理解，在目标应用程对物联网设备的权限的校验过程中，控制设备也可以通

过目标应用程序实现与物联网设备的信息交互。控制设备在对第二挑战值校验的同时，还可以校验物联网设备的设备信息。设备信息包括但不限于物联网设备的商家标识、物联网设备的设备标识以及物联网设备的序列号等。

[0121] 物联网设备基于第二挑战信息生成第二挑战值的过程可以为：物联网设备采用第二私钥对第二挑战信息进行签名，得到第二挑战值。

[0122] 在本实施例中，控制设备信任认证机构。在物联网设备中内置认证公钥，并采用认证公钥对采用认证私钥签名后的第二数字证书进行校验，如果校验通过，则可以得到第二公钥，并说明第二数字证书为认证机构认证过的证书，即说明控制设备可以信任第二公钥。当控制设备采用第二公钥对第二挑战值的校验通过时，说明控制设备可以信任物联网设备，即说明控制设备上的目标应用程序可以信任物联网设备。

[0123] 控制设备在与物联网设备进行信息交互之前，控制设备需先与物联网设备建立连接。控制设备与物联网设备建立连接的过程可以为：接收物联网设备广播的待配网信息。根据待配网信息与物联网设备建立连接。基于连接将目标数字证书发送至物联网设备。

[0124] 物联网设备可以通过蓝牙广播待配网信息，或者，物联网设备也通过软无线接入点（SoftAP）广播待配网信息。

[0125] 待配网信息包括但不限于物联网设备的商家标识、物联网设备的设备标识，物联网设备的序列号以及媒体存取控制位址（Media Access Control Address, MAC）等。

[0126] 控制设备接收到待配网信息之后，将待配网信息进行显示，以便用户可以了解到该待配网信息。用户对显示的待配网信息进行选择，控制设备响应于用户的选择操作，与待配网信息对应的物联网设备建立连接。后续控制设备与物联网设备之间的信息交互，可以通过该连接进行。比如，通过该连接将目标数字证书发送至物联网设备，又比如，通过该连接接收物联网设备发送的第一挑战信息。

[0127] 需要说明的是，在控制设备与物联网设备建立连接的过程中，为了保证安全性，还可以提示用户输入物联网设备的识别码（Personal Identification

Number, PIN)

[0128] 当控制设备通过SoftAP与物联网设备建立连接后，控制设备无法使用网络，即此时控制设备属于离线状态，即控制设备无法将第一挑战信息发送至目标服务器。因此，当控制设备可以在接收到第一挑战信息后，或者在对第二挑战值的校验通过后，控制设备可以连接至路由器，并将路由器的服务集标识（Service Set Identifier, SSID）和密码发送至物联网设备，物联网设备基于该服务集标识和密码连接至路由器。然后控制设备再通过路由器将第一挑战信息发送至目标服务器，通过路由器接收目标服务器发送的第一挑战值，以及通过路由器将第一挑战值发送至物联网设备。

[0129] 此外，在将目标应用程序标记为具备对物联网设备的控制权限的应用程序之后，控制设备可以基于该路由器，通过目标应用程序发送控制指令至物联网设备，以使物联网设备执行与控制指令对应的操作。

[0130] 或者，如果控制设备与物联网设备建立的是蓝牙连接，则控制设备基于蓝牙连接，通过目标应用程序发送控制指令至物联网设备，以使物联网设备执行与控制指令对应的操作。

[0131] 其中，物联网设备执行与控制指令对应的操作的过程可以为：物联网设备先查看控制指令中携带的目标应用程序的标记，如果该目标应用程序已经被标记为具备控制权限的应用程序，则物联网设备可以执行与控制指令对应的操作。

[0132] 或者，控制设备可以基于该路由器或蓝牙连接，将第一数字证书和控制指令一起发送至物联网设备，物联网设备接收到之后，由于之前已经对第一数字证书进行校验，因此，当接收到第一数字证书时可以执行控制指令对应的操作。

[0133] 在另一些实施例，在将控制设备上的目标应用程序标记为具备对物联网设备的控制权限的应用程序之后，控制设备可以连接到路由器，并将路由器的服务集标识（Service Set Identifier, SSID）和密码发送至物联网设备，物联网设备基于该服务集标识和密码连接至路由器。或者，控制设备和物联网设备可以建立蓝牙连接。最后控制设备基于路由器或蓝牙连接控制物联网设备。

[0134] 其中，控制设备控制物联网设备的过程可以为：通过目标应用程序将控制指令发送至物联网设备。物联网设备接收后，查看目标应用程序的标记。如果目标

应用程序的标记为具备控制权限的应用程序，物联网设备则执行控制指令对应的操作。

[0135] 或者，控制设备控制物联网设备的过程也可以为：当控制设备对物联网设备的权限的校验通过时，控制设备可以通过目标应用程序将控制权限信息（Access Control List, ACL）发送至物联网设备中，物联网设备如果还没校验控制设备上的目标应用程序，则将该控制权限信息标记为不信任，如果物联网设备对目标应用程序的校验通过时，则将控制权限信息标记为信任并进行存储。

[0136] 然后控制设备可以将控制指令和控制权限信息一起发送至物联网设备。物联网设备在接收到控制指令和控制权限信息后，将接收的控制权限信息与存储的控制权限信息比对，如果接收的控制权限信息与存储的控制权限信息相同，则执行控制指令对应的操作。

[0137] 下面对本申请实施例提供的另一种权限确定方法进行详细的描述。如图2所示，该权限确定方法的具体流程如下：

[0138] S201、接收控制设备发送的目标数字证书，目标数字证书为认证机构采用认证私钥对目标服务器认证后得到的证书。

[0139] 其中，认证机构指电子商务认证中心（Certificate Authority, CA）。由于认证结构是受信任的第三方，因此，当认证结构对目标服务器进行认证后，说明认证机构信任目标服务器，则物联网设备可以信任目标服务器。

[0140] 目标数字证书指一串能够表明目标服务器身份信息的数字。目标服务器先在认证机构上进行认证后，可以得到目标数字证书。然后目标服务器再将目标数字证书发送给控制设备。

[0141] 控制设备可以通过控制设备上的目标应用程序接收目标数字证书。目标应用程序指实际控制物联网设备的应用程序，目标应用程序可以为物联网设备的商家研发的应用程序，即物联网设备对应的应用程序，也可以其他商家研发的应用程序（由于当目标应用程序为物联网设备对应的应用程序时，应用本申请实施例提供的权限确定方法也可以提供控制物联网设备的安全性。因此，目标应用程序也可以为物联网设备对应的应用程序）。

[0142] 目标服务器可以为物联网设备的商家生产的初始服务器，则此时目标应用程序

为物联网设备对应的应用程序。

[0143] 或者，目标服务器也可以为其他商家（除了生产该物联网设备的商家之外的商家）的服务器，此时，目标应用程序为控制设备上的其他应用程序（其他应用程序指控制设备上已安装的除了物联网设备对应的应用程序之外的应用程序）。

[0144] 比如，物联网设备为A商家生产的设备，物联网设备对应的应用程序为A应用程序。B商家研发了B应用程序，则目标服务器可以为B商家的服务器，目标应用程序可以为B应用程序。

[0145] 当控制设备的用户想通过控制设备上的目标应用程序控制物联网设备时，用户可以对控制设备上的目标应用程序进行操作，使得控制设备将目标数字证书发送至物联网设备，物联网设备从而接收到目标数字证书。

[0146] S202、采用内置的认证公钥对目标数字证书进行校验。

[0147] 物联网设备在接收到目标数字证书之后，采用内置的认证公钥对目标数字证书进行校验。

[0148] S203、当校验通过时，取得目标数字证书的内容，并返回第一挑战信息至控制设备，以使控制设备将第一挑战信息发送至目标服务器，第一挑战信息用于指示目标服务器生成第一挑战值，并将第一挑战值返回至控制设备。

[0149] 如果校验通过，说明该目标数字证书是认证机构认证过的证书，即说明物联网设备可以信任该目标数字证书的内容。则将第一挑战信息发送至控制设备，控制设备再将第一挑战信息发送至目标服务器。

[0150] 目标服务器接收到第一挑战信息后，可以采用目标服务器的第一私钥对第一挑战信息进行签名，从而得到第一挑战值。

[0151] 或者，目标服务器可以采用预设的加密算法对第一挑战信息进行加密，从而得到第一挑战值。此时，目标数字证书的内容包括预设的加密算法对应的解密算法。

[0152] 目标数字证书的内容可以包括但不限于目标服务器的身份信息、认证机构的信息以及目标服务器的第一公钥等信息。第一挑战信息可以为一串随机字符串。

[0153] 物联网设备可以在对目标数字证书校验通过时生成该第一挑战信息并返回该第

一挑战信息。或在，物联网设备也可以先生成第一挑战信息，然后在目标数字证书校验通过时返回该第一挑战信息。对于物联网设备生成第一挑战信息的时间，用户可以根据实际情况进行选择，本申请在此不做限定。

[0154] S204、接收控制设备发送的第一挑战值。

[0155] 目标服务器将第一挑战值发送至控制设备之后，控制设备再将第一条挑战值发送给物联网设备，物联网设备从而接收到第一挑战值。

[0156] S205、基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。

[0157] 因为物联网设备信任目标数字证书的内容，所以当采用目标数字证书的内容对第一挑战值的校验通过且校验通过时得到的第一挑战信息与物联网设备发送的第一挑战信息相同时，说明物联网设备可以信任目标服务器，而目标服务器信任目标应用程序，所以，此时物联网设备可以将该目标应用程序标记为具备对物联网设备的控制权限的应用程序。

[0158] 需要说明的是，当校验通过时，也可以将目标数字证书标为具备权限的证书。

[0159] 当采用目标数字证书的内容对第一挑战值的校验不通过时，说明物联网设备不可以信任目标服务器，则将该目标应用程序标记为不具备对物联网设备的控制权限的应用程序。

[0160] 可选地，当目标服务器采用目标服务器的第一私钥对第一挑战信息进行签名，得到第一挑战值且目标数字证书的内容包括目标服务器的第一公钥时，采用目标数字证书的内容对第一挑战值进行校验的过程可以为：采用第一公钥对第一挑战值进行校验。

[0161] 又或者，当目标服务器采用预设的加密算法对第一挑战信息进行加密，得到第一挑战值且目标数字证书的内容包括预设的加密算法对应的解密算法时，采用目标数字证书的内容对第一挑战值进行校验的过程可以为：采用解密算法对第一挑战值进行解密。

[0162] 在本实施例中，物联网设备先接收控制设备发送的目标数字证书，目标数字证书为认证机构采用认证私钥对目标服务器认证后得到的证书。然后，物联网设

备采用内置的认证公钥对目标数字证书进行校验。当校验通过时，物联网设备取得目标数字证书的内容，并返回第一挑战信息至控制设备，以使控制设备将第一挑战信息发送至目标服务器，第一挑战信息用于指示目标服务器生成第一挑战值，并将第一挑战值返回至控制设备。物联网设备接收控制设备发送的第一挑战值，最后基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。

[0163] 即在本实施例中，由于目标服务器和目标应用程序是属于同一个商家的，因此，目标服务器信任目标应用程序。当物联网设备采用认证公钥对目标数字证书的校验通过时，说明该目标数字证书为认证机构认证过的证书。因为认证机构是物联网设备信任的机构，所以物联网设备可以信任目标数字证书的内容，以便可以根据目标数字证书的内容和目标服务器发送的第一挑战值确定是否可以信任目标服务器，从而确定是否可以信任目标应用程序，进而使得即使控制设备上的目标应用程序不是物联网设备对应的应用程序，通过控制设备上的目标应用程序控制物联网设备时也可以保证安全性。

[0164] 本实施例中的其他实现过程以及对应的有益效果，可以参照上述的方法实施例，本实施在此不再赘述。

[0165] 下面对本申请实施例提供的另一种权限确定方法进行详细的描述。如图3所示，该权限确定方法的具体流程如下：

[0166] S301、将目标数字证书发送至控制设备，以使得控制设备通将目标数字证书发送至物联网设备，目标数字证书用于指示物联网设备进行校验，并在校验通过时，取得目标数字证书的内容，并返回第一挑战信息至控制设备，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书。

[0167] 其中，认证机构指电子商务认证中心（Certificate Authority，CA）。由于认证结构是受信任的第三方，因此，当认证结构对目标服务器进行认证后，说明认证机构信任目标服务器，则物联网设备可以信任目标服务器。

[0168] 目标数字证书指一串能够表明目标服务器身份信息的数字。目标服务器先在认证机构上进行认证后，可以得到目标数字证书。然后目标服务器再将目标数字证书发送至控制设备。

- [0169] 控制设备可以通过控制设备上的目标应用程序接收目标数字证书。目标应用程序指实际控制物联网设备的应用程序，目标应用程序可以为物联网设备的商家研发的应用程序，即物联网设备对应的应用程序，也可以其他商家研发的应用程序（由于当目标应用程序为物联网设备对应的应用程序时，应用本申请实施例提供的权限确定方法也可以提供控制物联网设备的安全性。因此，目标应用程序也可以为物联网设备对应的应用程序）。
- [0170] 目标服务器可以为物联网设备的商家生产的初始服务器，则此时目标应用程序为物联网设备对应的应用程序。
- [0171] 或者，目标服务器也可以为其他商家（除了生产该物联网设备的商家之外的商家）的服务器，此时，目标应用程序为控制设备上的其他应用程序（其他应用程序指控制设备上已安装的除了物联网设备对应的应用程序之外的应用程序）。
- [0172] 比如，物联网设备为A商家生产的设备，物联网设备对应的应用程序为A应用程序。B商家研发了B应用程序，则目标服务器可以为B商家的服务器，目标应用程序可以为B应用程序。
- [0173] 当控制设备的用户想通过控制设备上的目标应用程序控制物联网设备时，用户可以对控制设备上的目标应用程序进行操作，使得控制设备的目标应用程序生成权限验证请求，并将该权限验证请求发送至目标服务器，目标服务器再基于该权限验证请求将目标数字证书发送至控制设备。
- [0174] 或者，也可以在用户安装完成目标应用程序时自动生成权限验证请求，并将该权限验证请求发送至目标服务器，目标服务器再基于该权限验证请求将目标数字证书发送至控制设备。
- [0175] 对于目标服务器发送目标数字证书的时间，用户可以根据实际情况进行设置，本申请在此不做限定。
- [0176] 物联网设备在接收到目标数字证书之后，采用内置的认证公钥对目标数字证书进行校验。如果校验通过，说明该目标数字证书是认证机构认证过的证书，即说明物联网设备可以信任该目标数字证书的内容。则将第一挑战信息返回至控制设备，控制设备从而接收到第一挑战信息。其中，第一挑战信息可以为一串

随机字符串。

[0177] 物联网设备可以在对目标数字证书校验通过时生成该第一挑战信息并返回该第一挑战信息。或在，物联网设备也可以先生成第一挑战信息，然后在对目标数字证书校验通过时返回该第一挑战信息。对于物联网设备生成第一挑战信息的时间，用户可以根据实际情况进行选择，本申请在此不做限定。

[0178] 目标数字证书的内容可以包括但不限于目标服务器的身份信息、认证机构的信息以及目标服务器的第一公钥等信息。

[0179] S302、接收控制设备发送的第一挑战信息。

[0180] 控制设备在接收到第一挑战信息之后，将第一挑战信息发送至目标服务器，目标服务器从而接收到第一挑战信息。

[0181] S303、基于第一挑战信息生成第一挑战值。

[0182] 基于第一挑战信息生成第一挑战值的过程可以为：目标服务器可以是采用目标服务器的第一私钥对第一挑战信息进行签名，从而得到第一挑战值。

[0183] 或者，目标服务器可以采用预设的加密算法对第一挑战信息进行加密，从而得到第一挑战值。此时，目标数字证书的内容包括预设的加密算法对应的解密算法。

[0184] 需要说明的是，由于目标应用程序与目标服务器是属于同一商家的，因此，目标服务器可以信任该目标应用程序。因此，当目标服务器接收到第一挑战信息之后，可以不对目标应用程序进行校验。

[0185] 或者，为了进一步保证安全，目标服务器也可以校验控制设备的权限，即校验控制设备的目标应用程序的权限。当校验通过后，目标服务器再基于第一挑战信息生成第一挑战值。

[0186] 对于目标服务器校验目标应用程序的权限的方法，用户可以根据实际情况进行选择。比如，可以通过目标应用程序将令牌和第一挑战信息一起发送至目标服务器，目标服务器接收到后，将令牌与本身存储的令牌进行比对，如果该令牌与本身存储的令牌相同，则对目标应用程序的校验通过。

[0187] 又比如，控制设备和目标服务器均可以根据预设规则生成随机数，然后控制设备采用存储的公钥对随机数进行加密，并通过目标应用程序将加密后的随机数

和第一挑战信息一起发送至目标服务器。目标服务器接收到后，采用存储的私钥对随机数进行解密，并将解密后的随机数与根据预设规则生成的随机数进行比对，如果解密后的随机数与根据预设规则生成的随机数相同，则对目标应用程序的校验通过。本申请在此不做具体限定。

[0188] S304、将第一挑战值发送至控制设备，以使得控制设备将第一挑战值发送至物联网设备，第一挑战值和目标数字证书的内容用于物联网设备确定控制设备上的目标应用程序对物联网设备的控制权限。

[0189] 物联网设备基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限的过程可以为：

[0190] 因为物联网设备信任目标数字证书的内容，所以当采用目标数字证书的内容对第一挑战值的校验通过且校验通过时得到的第一挑战信息与物联网设备发送的第一挑战信息相同时，说明物联网设备可以信任目标服务器，而目标服务器信任目标应用程序，所以，此时物联网设备可以将该目标应用程序标记为具备对物联网设备的控制权限的应用程序。

[0191] 需要说明的是，当校验通过时，也可以将目标数字证书标为具备权限的证书。

[0192] 当采用目标数字证书的内容对第一挑战值的校验不通过时，说明物联网设备不可以信任目标服务器，则物联网设备将该目标应用程序标记为不具备对物联网设备的控制权限的应用程序。

[0193] 可选地，当目标服务器采用目标服务器的第一私钥对第一挑战信息进行签名，得到第一挑战值且目标数字证书的内容包括目标服务器的第一公钥时，采用目标数字证书的内容对第一挑战值进行校验的过程可以为：采用第一公钥对第一挑战值进行校验。

[0194] 又或者，当目标服务器采用预设的加密算法对第一挑战信息进行加密，得到第一挑战值且目标数字证书的内容包括预设的加密算法对应的解密算法时，采用目标数字证书的内容对第一挑战值进行校验的过程可以为：采用解密算法对第一挑战值进行解密。

[0195] 由以上可知，本申请实施例提供了一种权限确定方法，在该方法中，目标服务

器先将目标数字证书发送至控制设备，以使得控制设备通将目标数字证书发送至物联网设备，目标数字证书用于指示物联网设备进行校验，并在校验通过时，取得目标数字证书的内容，并返回第一挑战信息至控制设备，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书。然后，目标服务器接收控制设备发送的第一挑战信息。接着，目标服务器基于第一挑战信息生成第一挑战值。最后目标服务器将第一挑战值发送至控制设备，以使得控制设备将第一挑战值发送至物联网设备，第一挑战值和目标数字证书的内容用于物联网设备确定控制设备上的目标应用程序对物联网设备的控制权限。

[0196] 即在本申请实施例中，由于目标服务器和目标应用程序是属于同一个商家的，因此，目标服务器信任目标应用程序。当物联网设备采用认证公钥对目标数字证书的校验通过时，说明该目标数字证书为认证机构认证过的证书。因为认证机构是物联网设备信任的机构，所以物联网设备可以信任目标数字证书的内容，以便可以根据目标数字证书的内容和目标服务器发送的第一挑战值确定是否可以信任目标服务器，从而确定是否可以信任目标应用程序，进而使得即使控制设备上的目标应用程序不是物联网设备对应的应用程序，通过控制设备上的目标应用程序控制物联网设备时也可以保证安全性。

[0197] 本实施例中的其他实现过程以及对应的有益效果，可以参照上述的方法实施例，本实施在此不再赘述。

[0198] 下面描述本申请提供的另一种权限的确定方法。参照图4，该权限确定方法包括：

[0199] 目标服务器将第一数字证书发送至控制设备，第一数字证书为认证机构采用认证私钥对目标服务器的第一公钥认证后得到的证书。物联网设备广播待配网信息，控制设备接收到待配网信息之后，根据待配网信息与物联网设备建立连接。

[0200] 控制设备通过目标应用程序向物联网设备发送证书获取请求。物联网设备基于证书获取请求返回第二数字证书至控制设备，第二数字证书为认证机构采用认证私钥对物联网设备的第二公钥进行签名后得到的证书。

[0201] 控制设备采用内置的认证公钥对第二数字证书进行校验，在校验通过时，取得

物联网设备的第二公钥，并生成第二挑战信息，并通过目标应用程序将第二挑战信息发送至物联网设备。

[0202] 物联网设备采用第二私钥对第二挑战信息进行签名，得到第二挑战值，并将第二挑战值发送至控制设备。控制设备根据第二公钥对第二挑战值进行校验。当校验通过时，与路由器建立连接，并将连接的路由器的服务集标识和密码发送至物联网设备。

[0203] 物联网设备连接到该路由器后，控制设备基于该路由器，通过目标应用程序发送控制指令至物联网设备。此时，物联网设备还未校验目标应用程序的权限，因此，响应出现错误并将错误信息发送至控制设备。

[0204] 控制设备接收到错误信息后，通过目标应用程序将第一数字证书和挑战信息获取请求发送至物联网设备。物联网设备采用内置的认证公钥对第一数字证书进行校验，在校验通过时，取得目标服务器的第一公钥，并基于挑战信息获取请求返回第一挑战信息至控制设备。

[0205] 控制设备将第一挑战信息发送至目标服务器。目标服务器采用第一私钥对第一挑战信息进行签名，得到第一挑战值，并将第一挑战值发送至控制设备。控制设备将第一挑战值发送至物联网设备。

[0206] 物联网设备采用第一公钥对第一挑战值进行校验。校验通过时，取得校验第一挑战信息，如果校验的第一挑战信息与发送的第一挑战信息进行比对，则将第一数字证书标记为具备控制权限的证书。

[0207] 控制设备通过目标应用程序发送控制指令和第一数字证书至物联网设备。由于第一数字证书为具备控制权限的证书，因此，物联网设备执行控制指令对应的操作。

[0208] 本实施例中的名词的含义与上述权限确定方法中相同，具体实现细节可以参考上述方法实施例中的说明。

[0209] 为了更好地实施以上方法，本申请实施例还提供一种权限确定装置，该权限确定装置应用于控制设备中，例如，如图5所示，该权限确定装置可以包括：

[0210] 第一接收模块501，用于接收目标服务器发送的目标数字证书，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书。

- [0211] 第一发送模块502，用于将目标数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对目标数字证书进行校验，并在校验通过时，取得目标数字证书的内容。
- [0212] 第二接收模块503，用于接收物联网设备基于对目标数字证书校验通过后返回的第一挑战信息。
- [0213] 第二发送模块504，用于将第一挑战信息发送至目标服务器，以使目标服务器基于第一挑战信息生成第一挑战值。
- [0214] 第三接收模块505，用于接收目标服务器发送的第一挑战值，并将第一挑战值发送至物联网设备，以基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。
- [0215] 可选地，目标数字证书包括第一数字证书，第一数字证书为认证机构采用认证私钥对目标服务器的第一公钥认证后得到的证书。
- [0216] 相应地，第一发送模块502具体用于执行：
- [0217] 将第一数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对第一数字证书进行校验，并在校验通过时，取得目标服务器的第一公钥。
- [0218] 第二接收模块503具体用于执行：
- [0219] 接收物联网设备基于对第一数字证书校验通过后返回的第一挑战信息。
- [0220] 第二发送模块504具体用于执行：
- [0221] 将第一挑战信息发送至目标服务器，以使目标服务器采用目标服务器的第一私钥对第一挑战信息进行签名，得到第一挑战值。
- [0222] 第三接收模块505具体用于执行：
- [0223] 接收目标服务器发送的第一挑战值，并将第一挑战值发送至物联网设备，以使物联网设备采用第一公钥对第一挑战值进行校验，并在校验通过时，将目标应用程序标记为具备对物联网设备的控制权限的应用程序。
- [0224] 可选地，第一发送模块502具体用于执行：
- [0225] 向物联网设备发送证书获取请求；
- [0226] 接收物联网设备基于证书获取请求返回的第二数字证书，第二数字证书为认证机构采用认证私钥对物联网设备的第二公钥进行签名后得到的证书；

- [0227] 采用内置的认证公钥对第二数字证书进行校验，在校验通过时，取得物联网设备的第二公钥；
- [0228] 生成第二挑战信息，并将第二挑战信息发送至物联网设备，以使物联网设备基于第二挑战信息生成第二挑战值；
- [0229] 接收第二挑战值，并根据第二公钥对第二挑战值进行校验；
- [0230] 当校验通过时，将目标数字证书发送至物联网设备。
- [0231] 可选地，第一发送模块502具体用于执行：
- [0232] 接收物联网设备广播的待配网信息；
- [0233] 根据待配网信息与物联网设备建立连接；
- [0234] 基于连接将目标数字证书发送至物联网设备。
- [0235] 可选地，权限确定装置还包括：
- [0236] 指令发送模块，用于通过目标应用程序发送控制指令至物联网设备，以使物联网设备执行与控制指令对应的操作。
- [0237] 具体实施时，以上各个模块可以作为独立的实体来实现，也可以进行任意组合，作为同一或若干个实体来实现，以上各个模块的具体实施方法以及对应的有益效果可参见前面的方法实施例，在此不再赘述。
- [0238] 为了更好地实施以上方法，本申请实施例还提供一种权限确定装置，该权限确定装置应用于物联网设备中，例如，如图6所示，该权限确定装置可以包括：
- [0239] 第四接收模块601，用于接收控制设备发送的目标数字证书，目标数字证书为认证机构采用认证私钥对目标服务器认证后得到的证书。
- [0240] 第一校验模块602，用于采用内置的认证公钥对目标数字证书进行校验。
- [0241] 第三发送模块603，用于当校验通过时，取得目标数字证书的内容，并发送第一挑战信息至控制设备，以使控制设备将第一挑战信息发送至目标服务器，第一挑战信息用于指示目标服务器生成第一挑战值，并将第一挑战值返回至控制设备。
- [0242] 第五接收模块604，用于接收控制设备发送的第一挑战值。
- [0243] 确定模块605，用于基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。

[0244] 具体实施时，以上各个模块可以作为独立的实体来实现，也可以进行任意组合，作为同一或若干个实体来实现，以上各个模块的具体实施方式以及对应的有益效果可参见前面的方法实施例，在此不再赘述。

[0245] 为了更好地实施以上方法，本申请实施例还提供一种权限确定装置，该权限确定装置应用于目标服务器中，例如，如图7所示，该权限确定装置可以包括：

[0246] 第四发送模块701，用于将目标数字证书发送至控制设备，以使得控制设备将目标数字证书发送至物联网设备，目标数字证书用于指示物联网设备进行校验，并在校验通过时，取得目标数字证书的内容，并返回第一挑战信息至控制设备，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书。

[0247] 第六接收模块702，用于接收控制设备发送的第一挑战信息。

[0248] 生成模块703，用于基于第一挑战信息生成第一挑战值。

[0249] 第五发送模块704，用于将第一挑战值发送至控制设备，以使得控制设备将第一挑战值发送至物联网设备，第一挑战值和目标数字证书的内容用于物联网设备确定控制设备上的目标应用程序对物联网设备的控制权限。

[0250] 具体实施时，以上各个模块可以作为独立的实体来实现，也可以进行任意组合，作为同一或若干个实体来实现，以上各个模块的具体实施方式以及对应的有益效果可参见前面的方法实施例，在此不再赘述。

[0251] 本申请实施例还提供一种计算机设备，如图8所示，其示出了本申请实施例所涉及的计算机设备的结构示意图，具体来讲：

[0252] 该计算机设备可以包括一个或者一个以上处理核心的处理器801、一个或一个以上计算机可读存储介质的存储器802、电源803和输入单元804等部件。本领域技术人员可以理解，图8中示出的计算机设备结构并不构成对计算机设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

[0253] 处理器801是该计算机设备的控制中心，利用各种接口和线路连接整个计算机设备的各个部分，通过运行或执行存储在存储器802内的计算机程序和/或模块，以及调用存储在存储器802内的数据，执行计算机设备的各种功能和处理数据

，从而对计算机设备进行整体监控。可选的，处理器801可包括一个或多个处理核心；优选的，处理器801可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器801中。

[0254] 存储器802可用于存储计算机程序以及模块，处理器801通过运行存储在存储器802的计算机程序以及模块，从而执行各种功能应用以及数据处理。存储器802可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的计算机程序（比如声音播放功能、图像播放功能等）等；存储数据区可存储根据计算机设备的使用所创建的数据等。此外，存储器802可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地，存储器802还可以包括存储器控制器，以提供处理器801对存储器802的访问。

[0255] 计算机设备还包括给各个部件供电的电源803，优选的，电源803可以通过电源管理系统与处理器801逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源803还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0256] 该计算机设备还可包括输入单元804，该输入单元804可用于接收输入的数字或字符信息，以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。

[0257] 尽管未示出，计算机设备还可以包括显示单元等，在此不再赘述。具体在本实施例中，计算机设备中的处理器801会按照如下的指令，将一个或一个以上的计算机程序的进程对应的可执行文件加载到存储器802中，并由处理器801来运行存储在存储器802中的计算机程序，从而实现各种功能，比如：

[0258] 接收目标服务器发送的目标数字证书，目标数字证书包括认证机构采用认证私钥对目标服务器认证后得到的证书；

[0259] 将目标数字证书发送至物联网设备，以使物联网设备采用内置的认证公钥对目标数字证书进行校验，并在校验通过时，取得目标数字证书的内容；

- [0260] 接收物联网设备基于对目标数字证书校验通过后返回的第一挑战信息；
- [0261] 将第一挑战信息发送至目标服务器，以使目标服务器基于第一挑战信息生成第一挑战值；
- [0262] 接收目标服务器发送的第一挑战值，并将第一挑战值发送至物联网设备，以基于第一挑战值和目标数字证书的内容确定控制设备上的目标应用程序对物联网设备的控制权限。
- [0263] 以上各个操作的具体实施以及对应的有益效果可参见前面的实施例，在此不作赘述。
- [0264] 本领域普通技术人员可以理解，上述实施例的各种方法中的全部或部分步骤可以通过计算机程序来完成，或通过计算机程序控制相关的硬件来完成，该计算机程序可以存储于一计算机可读存储介质中，并由处理器进行加载和执行。
- [0265] 为此，本申请实施例提供一种计算机可读存储介质，其中存储有计算机程序，该计算机程序能够被处理器进行加载，以执行本申请实施例所提供的任一种权限确定方法中的步骤。
- [0266] 以上各个操作的具体实施以及对应的有益效果可参见前面的实施例，在此不再赘述。
- [0267] 其中，该计算机可读存储介质可以包括：只读存储器（ROM，Read Only Memory）、随机存取记忆体（RAM，Random Access Memory）、磁盘或光盘等。
- [0268] 由于该计算机可读存储介质中所存储的计算机程序，可以执行本申请实施例所提供的任一种权限确定方法中的步骤，因此，可以实现本申请实施例所提供的任一种权限确定方法所能实现的有益效果，详见前面的实施例，在此不再赘述。
- [0269] 其中，根据本申请的一个方面，提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述权限确定方法。
- [0270] 以上对本申请实施例所提供的一种权限确定方法、装置、计算机设备和计算机可读存储介质进行了详细介绍，本文中应用了具体个例对本申请的原理及实施

方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权利要求书

- [权利要求 1] 一种权限确定方法，其中，应用于控制设备，包括：
- 接收目标服务器发送的目标数字证书，所述目标数字证书包括认证机构采用认证私钥对所述目标服务器认证后得到的证书；
- 将所述目标数字证书发送至物联网设备，以使所述物联网设备采用内置的认证公钥对所述目标数字证书进行校验，并在校验通过时，取得所述目标数字证书的内容；
- 接收所述物联网设备基于对所述目标数字证书校验通过后返回的第一挑战信息；
- 将所述第一挑战信息发送至所述目标服务器，以使所述目标服务器基于所述第一挑战信息生成第一挑战值；
- 接收所述目标服务器发送的所述第一挑战值，并将所述第一挑战值发送至所述物联网设备，以基于所述第一挑战值和所述目标数字证书的内容确定所述控制设备上的目标应用程序对所述物联网设备的控制权限。
- [权利要求 2] 根据权利要求1所述的权限确定方法，其中，所述目标数字证书包括第一数字证书，所述第一数字证书为认证机构采用认证私钥对所述目标服务器的第一公钥认证后得到的证书；
- 相应地，所述将所述目标数字证书发送至物联网设备，以使所述物联网设备采用内置的认证公钥对所述目标数字证书进行校验，并在校验通过时，取得所述目标数字证书的内容，包括：
- 将所述第一数字证书发送至物联网设备，以使所述物联网设备采用内置的认证公钥对所述第一数字证书进行校验，并在校验通过时，取得所述目标服务器的所述第一公钥；
- 所述接收所述物联网设备基于对所述目标数字证书校验通过后返回的第一挑战信息，包括：
- 接收所述物联网设备基于对所述第一数字证书校验通过后返回的第一挑战信息；

所述将所述第一挑战信息发送至所述目标服务器，以使所述目标服务器基于所述第一挑战信息生成第一挑战值，包括：

将所述第一挑战信息发送至所述目标服务器，以使所述目标服务器采用所述目标服务器的第一私钥对所述第一挑战信息进行签名，得到第一挑战值；

所述接收所述目标服务器发送的所述第一挑战值，并将所述第一挑战值发送至所述物联网设备，以基于所述第一挑战值和所述目标数字证书的内容确定所述控制设备上的目标应用程序对所述物联网设备的控制权限，包括：

接收所述目标服务器发送的所述第一挑战值，并将所述第一挑战值发送至所述物联网设备，以使所述物联网设备采用所述第一公钥对所述第一挑战值进行校验，并在校验通过时，将所述目标应用程序标记为具备对所述物联网设备的控制权限的应用程序。

[权利要求 3]

根据权利要求1所述的权限确定方法，其中，所述将所述目标数字证书发送至物联网设备，包括：

向所述物联网设备发送证书获取请求；

接收所述物联网设备基于所述证书获取请求返回的第二数字证书，所述第二数字证书为所述认证机构采用所述认证私钥对所述物联网设备的第二公钥进行签名后得到的证书；

采用内置的认证公钥对所述第二数字证书进行校验，在校验通过时，取得所述物联网设备的第二公钥；

生成第二挑战信息，并将所述第二挑战信息发送至所述物联网设备，以使所述物联网设备基于第二挑战信息生成第二挑战值；

接收所述第二挑战值，并根据所述第二公钥对所述第二挑战值进行校验；

当校验通过时，将所述目标数字证书发送至所述物联网设备。

[权利要求 4]

根据权利要求1所述的权限确定方法，其中，所述将所述目标数字证书发送至物联网设备，包括：

接收所述物联网设备广播的待配网信息；

根据所述待配网信息与所述物联网设备建立连接；

基于所述连接将所述目标数字证书发送至物联网设备。

[权利要求 5] 根据权利要求2所述的权限确定方法，其中，在所述接收所述目标服务器发送的所述第一挑战值，并将所述第一挑战值发送至所述物联网设备，以使所述物联网设备采用所述第一公钥对所述第一挑战值进行校验，并在校验通过时，将所述目标应用程序标记为具备对所述物联网设备的控制权限的应用程序之后，还包括：

通过所述目标应用程序发送控制指令至所述物联网设备，以使所述物联网设备执行与所述控制指令对应的操作。

[权利要求 6] 根据权利要求1所述的权限确定方法，其中，所述将所述第一挑战信息发送至所述目标服务器，以使所述目标服务器基于所述第一挑战信息生成第一挑战值，包括：

根据预设规则生成随机数，并对所述随机数进行加密，得到加密后的随机数；

将所述加密后的随机数和所述第一挑战信息发送至所述目标服务器，以使所述目标服务器在对所述加密后的随机数的校验通过时，基于所述第一挑战信息生成第一挑战值。

[权利要求 7] 根据权利要求1所述的权限确定方法，其中，所述将所述第一挑战信息发送至所述目标服务器，以使所述目标服务器基于所述第一挑战信息生成第一挑战值，包括：

获取令牌；

将所述令牌和所述第一挑战信息发送至所述目标服务器，以使所述目标服务器将所述令牌与存储的令牌进行比对，若所述令牌与所述存储的令牌相同，则基于所述第一挑战信息生成第一挑战值。

[权利要求 8] 根据权利要求1所述的权限确定方法，其中，在所述接收所述目标服务器发送的所述第一挑战值，并将所述第一挑战值发送至所述物联网设备，以使所述物联网设备采用所述第一公钥对所述第一挑战值进行

校验，并在校验通过时，将所述目标应用程序标记为具备对所述物联网设备的控制权限的应用程序之后，还包括：

发送所述控制设备的控制权限信息至所述物联网设备，以使若所述控制设备上的目标应用程序具备对所述物联网设备的控制权限，所述物联网设备则将所述控制权限信息进行存储；

通过所述目标应用程序发送控制指令和所述控制权限信息至所述物联网设备，以使若所述控制权限信息与存储的控制权限信息相同，所述物联网设备则执行所述控制指令对应的操作。

[权利要求 9]

一种权限确定方法，其中，应用于物联网设备，包括：

接收控制设备发送的目标数字证书，所述目标数字证书为认证机构采用认证私钥对目标服务器认证后得到的证书；

采用内置的认证公钥对所述目标数字证书进行校验；

当校验通过时，取得所述目标数字证书的内容，并返回第一挑战信息至所述控制设备，以使所述控制设备将第一挑战信息发送至所述目标服务器，所述第一挑战信息用于指示所述目标服务器生成第一挑战值，并将所述第一挑战值返回至所述控制设备；

接收所述控制设备发送的所述第一挑战值；

基于所述第一挑战值和所述目标数字证书的内容确定所述控制设备上的目标应用程序对所述物联网设备的控制权限。

[权利要求 10]

根据权利要求9所述的权限确定方法，其中，所述基于所述第一挑战值和所述目标数字证书的内容确定所述控制设备上的目标应用程序对所述物联网设备的控制权限，包括：

采用所述目标数字证书的内容对所述第一挑战值进行校验；

若对所述第一挑战值的校验通过时得到的第一挑战信息与所述物联网设备发送的第一挑战信息相同，则将所述目标应用程序标记为具备对所述物联网设备的控制权限的应用程序。

[权利要求 11]

根据权利要求10所述的权限确定方法，其中，在将所述目标应用程序标记为具备对所述物联网设备的控制权限的应用程序之后，还包括：

获取所述控制设备通过所述目标应用程序发生的控制指令；

若所述目标应用程序为标记的应用程序，则执行所述控制指令对应的操作。

[权利要求 12] 根据权利要求9所述的权限确定方法，其中，在基于所述第一挑战值和所述目标数字证书的内容确定所述控制设备上的目标应用程序对所述物联网设备的控制权限之后，包括：

获取所述控制设备发送的控制权限信息；

若所述控制设备上的目标应用程序具备对所述物联网设备的控制权限，则将所述控制权限信息进行存储；

获取所述控制设备通过所述目标应用程序发送的控制指令和所述控制权限信息；

若所述控制权限信息与存储的控制权限信息相同，则执行所述控制指令对应的操作。

[权利要求 13] 一种权限确定方法，其中，应用于目标服务器，包括：

将目标数字证书发送至控制设备，以使得所述控制设备将所述目标数字证书发送至物联网设备，所述目标数字证书用于指示所述物联网设备进行校验，并在校验通过时，取得所述目标数字证书的内容，并返回第一挑战信息至所述控制设备，所述目标数字证书包括认证机构采用认证私钥对所述目标服务器认证后得到的证书；

接收所述控制设备发送的所述第一挑战信息；

基于所述第一挑战信息生成第一挑战值；

将所述第一挑战值发送至所述控制设备，以使得所述控制设备将所述第一挑战值发送至所述物联网设备，所述第一挑战值和所述目标数字证书的内容用于所述物联网设备确定所述控制设备上的目标应用程序对所述物联网设备的控制权限。

[权利要求 14] 根据权利要求13所述的权限确定方法，其中，所述接收所述控制设备发送的所述第一挑战信息，基于所述第一挑战信息生成第一挑战值，包括：

接收所述控制设备发送的所述第一挑战信息和加密后的随机数；

对所述加密后的随机数进行解密，得到解密后的随机数；

若所述解密后的随机数与根据预设规则生成的随机数相同，则基于所述第一挑战信息生成第一挑战值。

[权利要求 15] 根据权利要求13所述的权限确定方法，其中，所述目标数字证书包括第一数字证书，在将目标数字证书发送至控制设备之前，还包括：将所述目标服务器的第一公钥发送至所述认证机构，以使所述认证机构采用认证私钥对所述第一公钥进行认证，得到第一数字证书；接收所述认证机构返回的第一数字证书。

[权利要求 16] 一种权限确定装置，其中，应用于控制设备，包括：
第一接收模块，用于接收目标服务器发送的目标数字证书，所述目标数字证书包括认证机构采用认证私钥对所述目标服务器认证后得到的证书；
第一发送模块，用于将所述目标数字证书发送至物联网设备，以使所述物联网设备采用内置的认证公钥对所述目标数字证书进行校验，并在校验通过时，取得所述目标数字证书的内容；
第二接收模块，用于接收所述物联网设备基于对所述目标数字证书校验通过后返回的第一挑战信息；
第二发送模块，用于将所述第一挑战信息发送至所述目标服务器，以使所述目标服务器基于所述第一挑战信息生成第一挑战值；
第三接收模块，用于接收所述目标服务器发送的所述第一挑战值，并将所述第一挑战值发送至所述物联网设备，以基于所述第一挑战值和所述目标数字证书的内容确定所述控制设备上的目标应用程序对所述物联网设备的控制权限。

[权利要求 17] 一种权限确定装置，其中，应用于物联网设备，包括：
第四接收模块，用于接收控制设备发送的目标数字证书，所述目标数字证书为认证机构采用认证私钥对目标服务器认证后得到的证书；
第一校验模块，用于采用内置的认证公钥对所述目标数字证书进行校

验；

第三发送模块，用于当校验通过时，取得所述目标数字证书的内容，并发送第一挑战信息至所述控制设备，以使所述控制设备将第一挑战信息发送至所述目标服务器，所述第一挑战信息用于指示所述目标服务器生成第一挑战值，并将所述第一挑战值返回至所述控制设备；

第五接收模块，用于接收所述控制设备发送的第一挑战值；

确定模块，用于基于所述第一挑战值和所述目标数字证书的内容确定所述控制设备上的目标应用程序对所述物联网设备的控制权限。

[权利要求 18] 一种权限确定装置，其中，应用于目标服务器，包括：

第四发送模块，用于将目标数字证书发送至控制设备，以使得所述控制设备将所述目标数字证书发送至物联网设备，所述目标数字证书用于指示所述物联网设备进行校验，并在校验通过时，取得所述目标数字证书的内容，并返回第一挑战信息至所述控制设备，所述目标数字证书包括认证机构采用认证私钥对所述目标服务器认证后得到的证书；

第六接收模块，用于接收所述控制设备发送的所述第一挑战信息；

生成模块，用于基于所述第一挑战信息生成第一挑战值；

第五发送模块，用于将所述第一挑战值发送至所述控制设备，以使得所述控制设备将所述第一挑战值发送至所述物联网设备，所述第一挑战值和所述目标数字证书的内容用于所述物联网设备确定所述控制设备上的目标应用程序对所述物联网设备的控制权限。

[权利要求 19] 一种计算机设备，其中，包括处理器和存储器，所述存储器存储有计算机程序，所述处理器用于运行所述存储器内的计算机程序，以执行权利要求1至8任一项所述的权限确定方法、权利要求9-12任一项所述的权限确定方法或权利要求13-15任一项所述的权限确定方法。

[权利要求 20] 一种计算机可读存储介质，其中，所述计算机可读存储介质存储有计算机程序，所述计算机程序适于处理器进行加载，以执行权利要求1至8任一项所述的权限确定方法、权利要求9-12任一项所述的权限确

定方法或权利要求13-15任一项所述的权限确定方法。

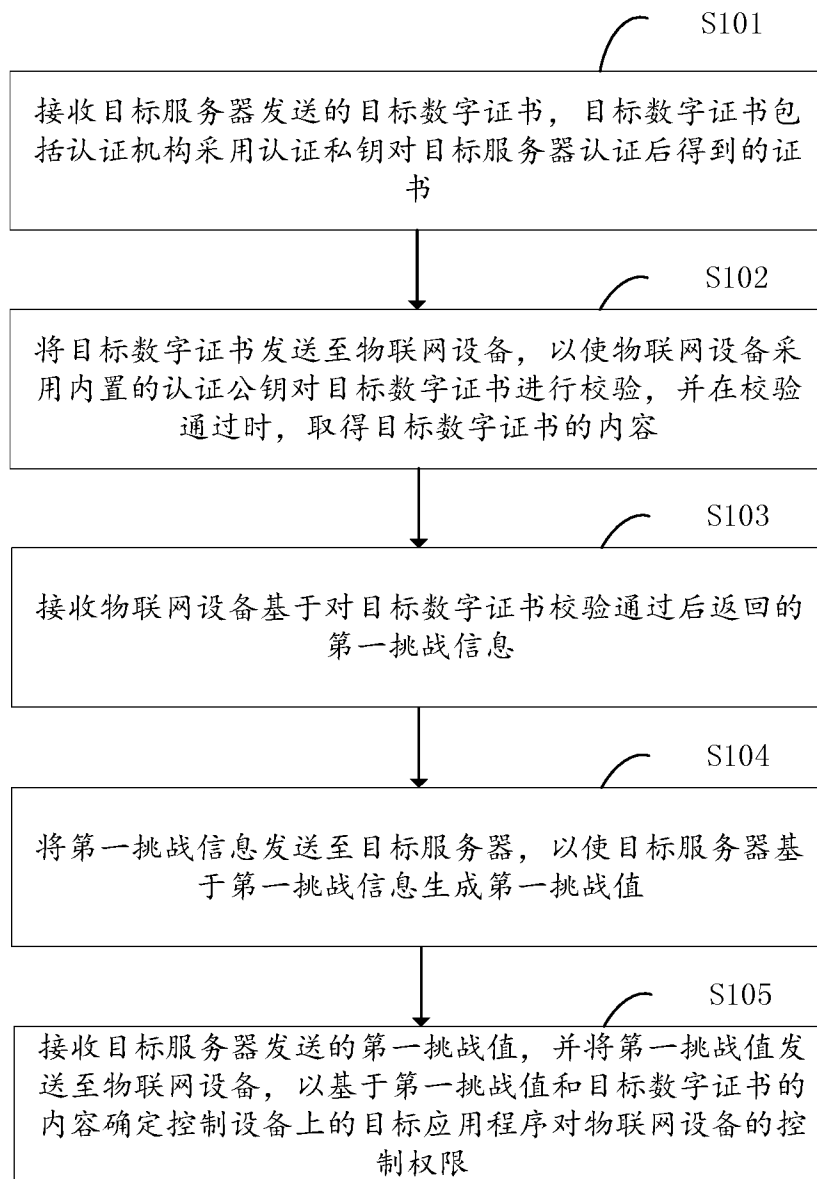


图 1

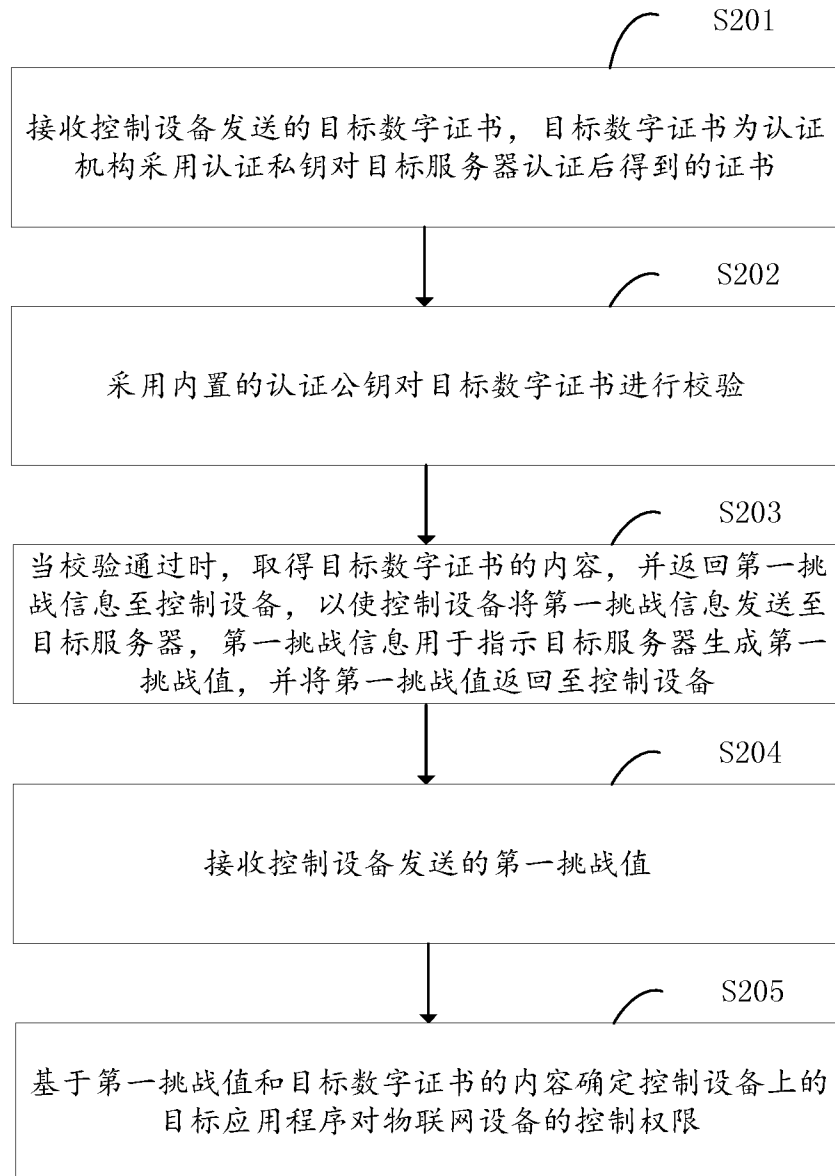


图 2

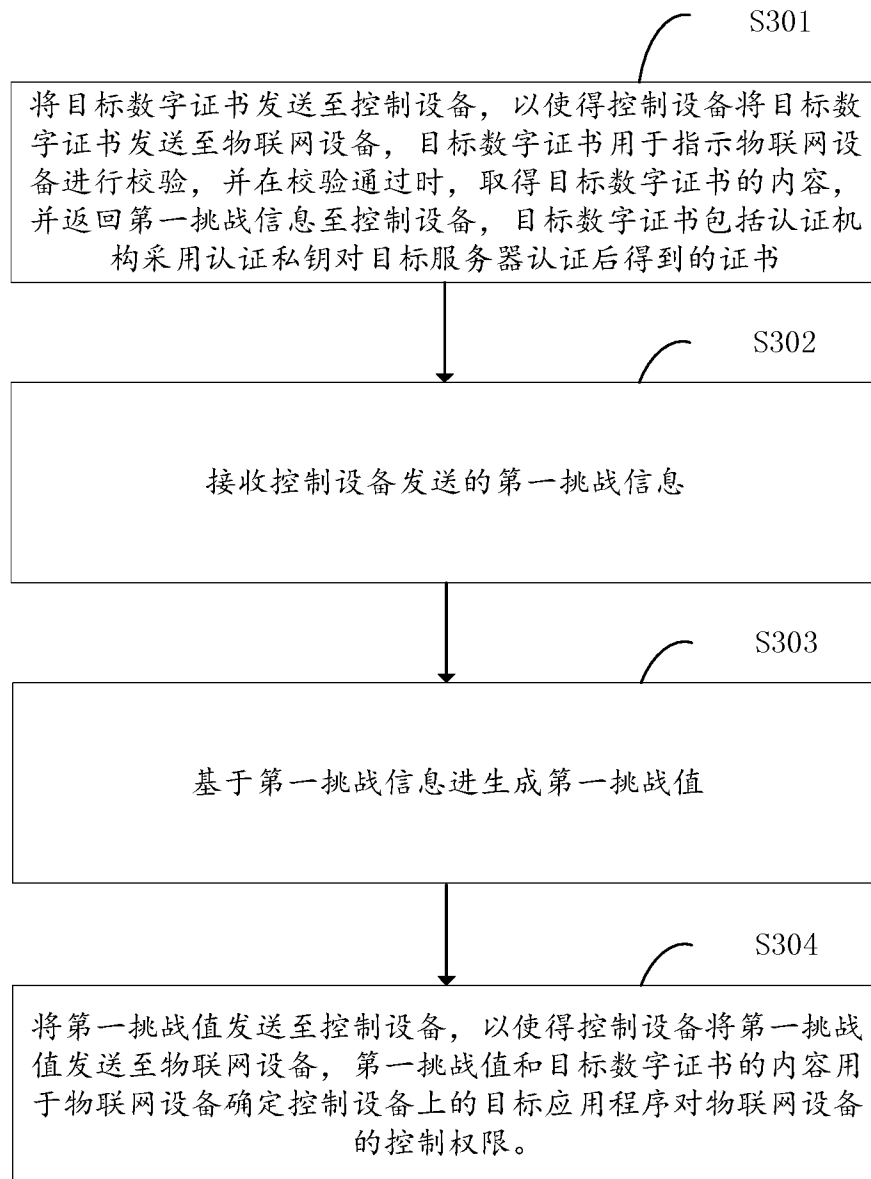


图 3

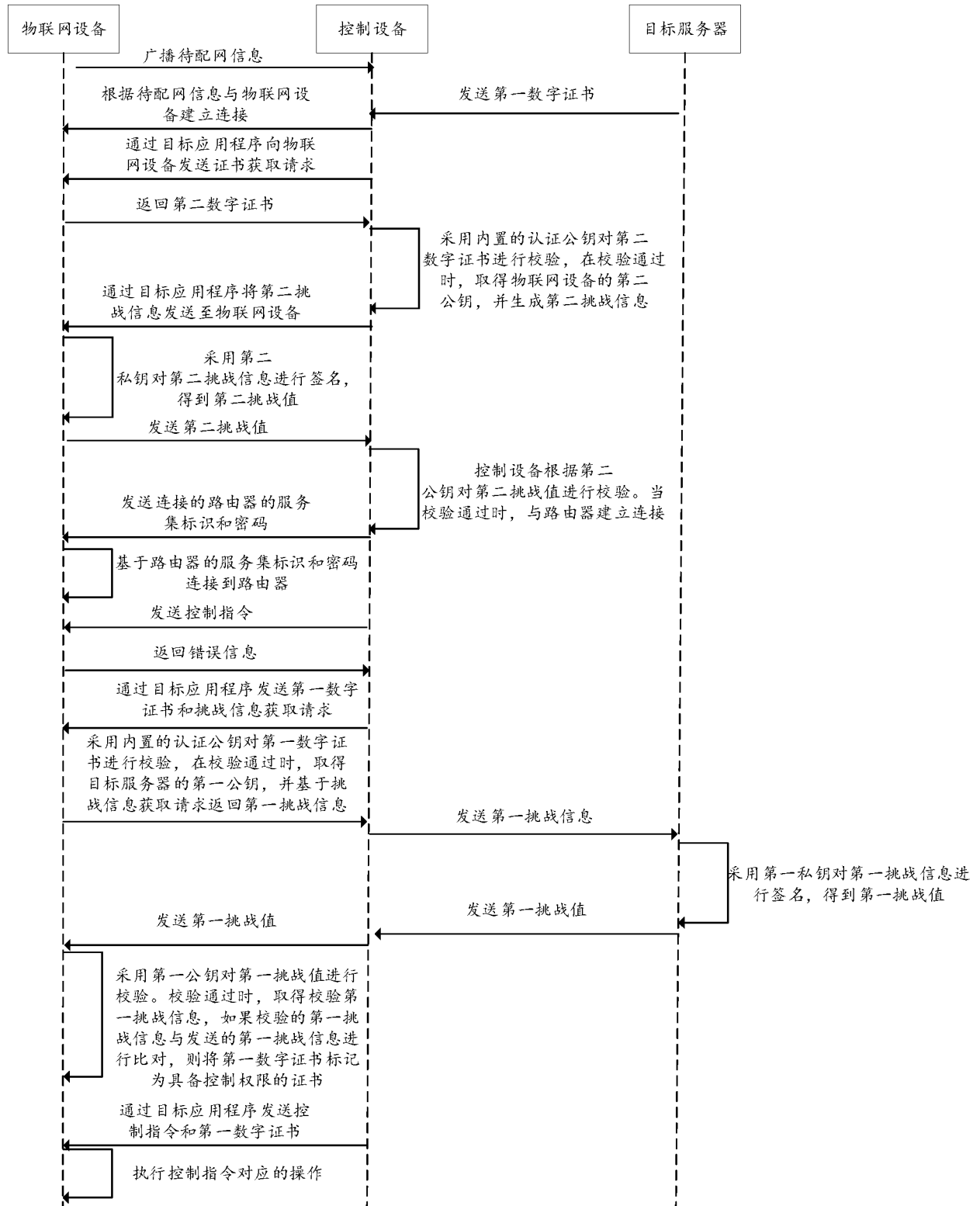


图 4

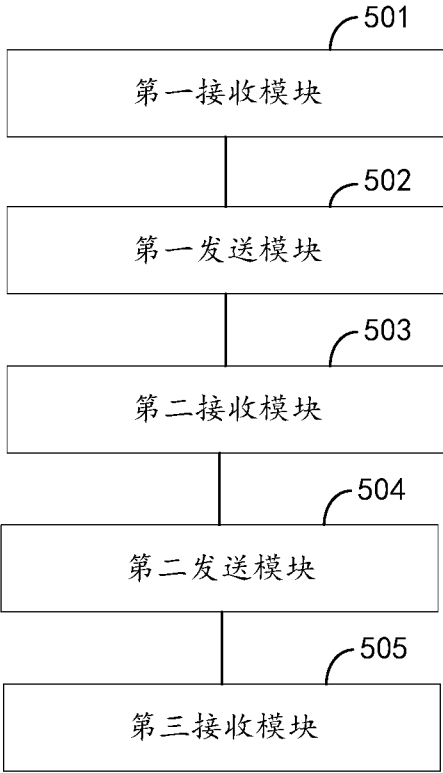


图 5

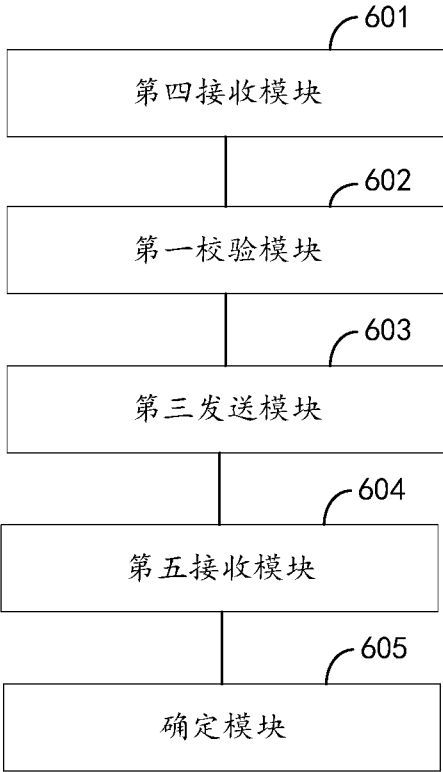


图 6

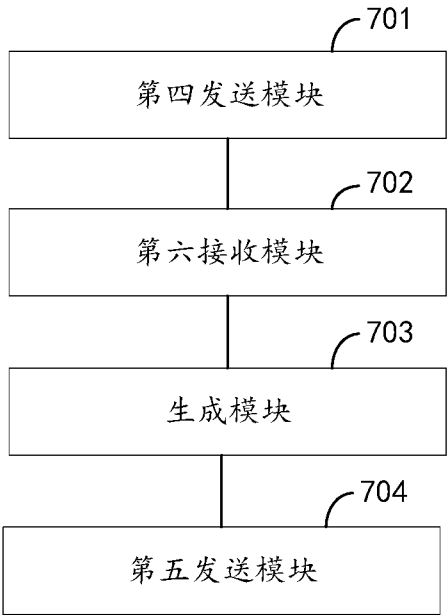


图 7

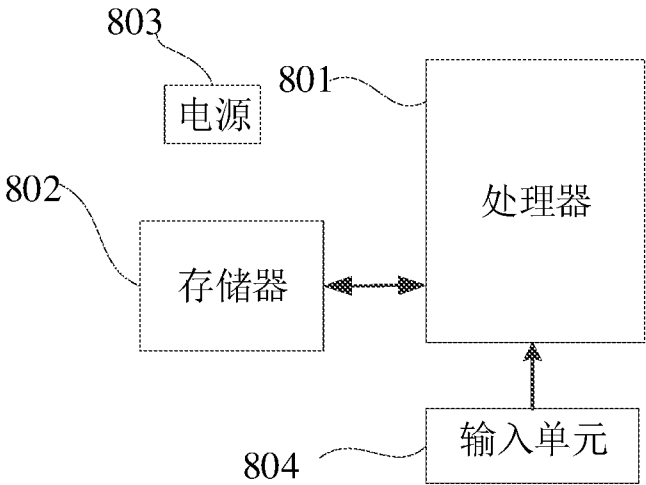


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/130533

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; EPTXT; USTXT; CNKI: 服务器, 证书, 校验, 公钥, 私钥, 物联网, 设备, 智能家居, 应用, 软件, 权限, 挑战, 认证机构, server, certificate, verification, public key, private key, IOT, device, smart home, APP, software, permission, challenge, CA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 114329534 A (SHENZHEN TCL NEW TECHNOLOGY CO., LTD.) 12 April 2022 (2022-04-12) description, paragraphs 53-265	1-20
Y	CN 105245552 A (BEIJING JINGDONG CENTURY TRADING CO., LTD.) 13 January 2016 (2016-01-13) description, paragraphs 21-64, and figure 2	1-20
Y	CN 110690966 A (BEIJING JINMAO GREEN BUILDING TECHNOLOGY CO., LTD.) 14 January 2020 (2020-01-14) description, paragraphs 105-145	1-20
Y	CN 108667780 A (HUAWEI TECHNOLOGIES CO., LTD.) 16 October 2018 (2018-10-16) description, paragraphs 96-205	1-20
A	CN 108366063 A (GUANGDONG MIDEA KITCHEN APPLIANCES MANUFACTURING CO., LTD. et al.) 03 August 2018 (2018-08-03) entire document	1-20
A	JP 2017175226 A (INTEC INC.) 28 September 2017 (2017-09-28) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

14 January 2023

Date of mailing of the international search report

19 January 2023

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/130533

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	114329534	A	12 April 2022	None			
CN	105245552	A	13 January 2016	CN	105245552	B	18 January 2019
CN	110690966	A	14 January 2020	CN	110690966	B	09 October 2020
CN	108667780	A	16 October 2018	WO	2018177143	A1	04 October 2018
				US	2020036704	A1	30 January 2020
				EP	3595247	A1	15 January 2020
				IN	201937041064	A	06 December 2019
				CN	108667780	B	14 May 2021
				US	11165767	B2	02 November 2021
				EP	3595247	B1	26 January 2022
				EP	3595247	A4	10 June 2020
CN	108366063	A	03 August 2018	CN	108366063	B	18 June 2021
JP	2017175226	A	28 September 2017	None			

国际检索报告

国际申请号

PCT/CN2022/130533

A. 主题的分类

G06F 21/60 (2013.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNABS; CNTXT; VEN; EPTXT; USTXT; CNKI: 服务器, 证书, 校验, 公钥, 私钥, 物联网, 设备, 智能家居, 应用, 软件, 权限, 挑战, 认证机构, server, certificate, verification, public key, private key, IoT, device, smart home, APP, software, permission, challenge, CA

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 114329534 A (深圳TCL新技术有限公司) 2022年4月12日 (2022 - 04 - 12) 说明书53-265段	1-20
Y	CN 105245552 A (北京京东世纪贸易有限公司) 2016年1月13日 (2016 - 01 - 13) 说明书第21-64段, 图2	1-20
Y	CN 110690966 A (北京金茂绿建科技有限公司) 2020年1月14日 (2020 - 01 - 14) 说明书第105-145段	1-20
Y	CN 108667780 A (华为技术有限公司) 2018年10月16日 (2018 - 10 - 16) 说明书第96-205段	1-20
A	CN 108366063 A (广东美的厨房电器制造有限公司 等) 2018年8月3日 (2018 - 08 - 03) 全文	1-20
A	JP 2017175226 A (INTEC INC) 2017年9月28日 (2017 - 09 - 28) 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2023年1月14日

国际检索报告邮寄日期

2023年1月19日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

王慧敏

电话号码 86-(20)-28958356

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/130533

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	114329534	A	2022年4月12日	无	
CN	105245552	A	2016年1月13日	CN	105245552 B 2019年1月18日
CN	110690966	A	2020年1月14日	CN	110690966 B 2020年10月9日
CN	108667780	A	2018年10月16日	WO	2018177143 A1 2018年10月4日
				US	2020036704 A1 2020年1月30日
				EP	3595247 A1 2020年1月15日
				IN	201937041064 A 2019年12月6日
				CN	108667780 B 2021年5月14日
				US	11165767 B2 2021年11月2日
				EP	3595247 B1 2022年1月26日
				EP	3595247 A4 2020年6月10日
CN	108366063	A	2018年8月3日	CN	108366063 B 2021年6月18日
JP	2017175226	A	2017年9月28日	无	