(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
2020 年 9 月 24 日 (24.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/186902 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2020/070659

(22) 国际申请日: 2020 年 1 月 7 日 (07.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910210669.6 2019年3月19日 (19.03.2019) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: **黄琪 (HUANG, Qi)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **廖晖 (LIAO, Hui)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: **北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION)**; 中国北京市海淀区上地三街9号嘉华大厦B座409, Beijing 100085 (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,

WO 2020/186902 A1

(54) **Title:** METHOD AND SYSTEM FOR OPERATING INTERNET OF THINGS DEVICE

(54) 发明名称: 用于操作物联网设备的方法和系统

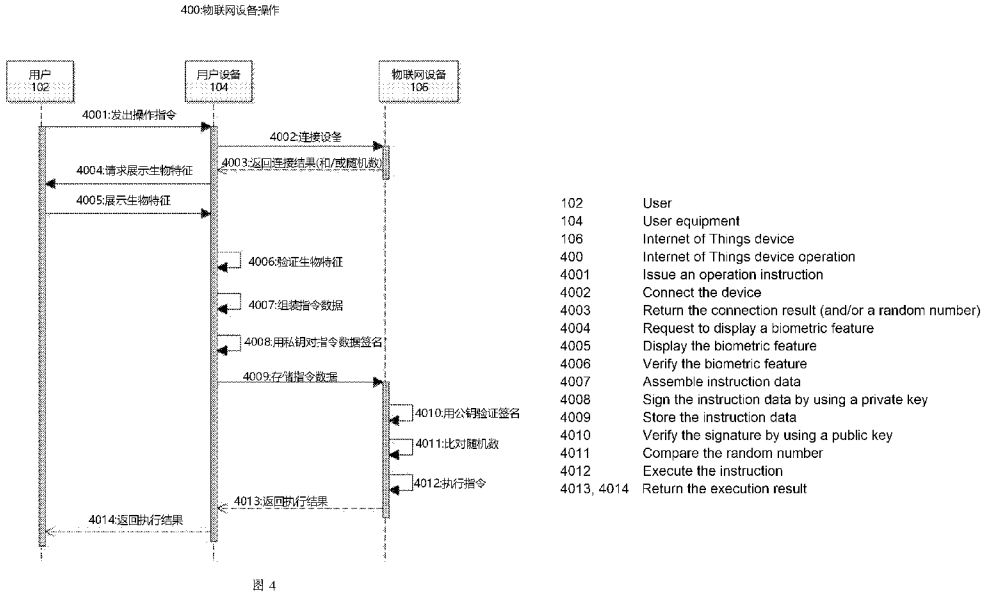

图 4

(57) **Abstract:** Disclosed is a method for operating an Internet of Things device, comprising: a user equipment receives an operation instruction for an Internet of Things device from a user; the user equipment identifies a biometric feature of the user; the user equipment verifies the identity of the user on the basis of the biometric feature; if the identity of the user is successfully verified, the user equipment signs the operation instruction by using a first user key of the user; the user equipment transmits the signed operation instruction to the Internet of Things device; the Internet of Things device verifies the signature of the signed operation instruction by using a second user

[见续页]

JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, 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, 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))。

key of the user, wherein the second user key and the first user key constitute a key pair; and if the signature is successfully verified, the Internet of Things device executes the operation instruction. Also disclosed are a method executed by the user equipment, a method executed by the Internet of Things device, and a corresponding system.

(57) 摘要：公开了一种用于操作物联网设备的方法，包括：由用户设备从用户接收对物联网设备的操作指令；由所述用户设备识别所述用户的生物特征；基于所述生物特征，由所述用户设备验证所述用户的身份；如果所述用户的身份被成功验证，则由所述用户设备使用所述用户的第一用户密钥来对所述操作指令进行签名；由所述用户设备将经签名的操作指令传送至所述物联网设备；由所述物联网设备使用所述用户的第二用户密钥来验证所述经签名的操作指令的签名，所述第二用户密钥与所述第一用户密钥构成密钥对；以及如果所述签名被成功验证，则由所述物联网设备执行所述操作指令。还公开了由用户设备执行的方法、由物联网设备执行的方法和相应的系统。

用于操作物联网设备的方法和系统

技术领域

[01]本说明书的一个或多个实施例涉及物联网设备，尤其涉及用于操作物联网设备的方法和系统。

背景技术

[02]当今，物联网（IoT）设备得到了越来越多的应用。用户可直接操作物联网设备，或者可通过其它设备（例如智能电话等用户设备）来间接操作物联网设备。在远程操作物联网设备的情况下，用户通常首先将用户设备与物联网设备绑定，随后通过用户设备来向物联网设备发出指令。然而，使用用户设备操作物联网设备的方法可能存在安全隐患。

[03]因此，需要能够增强操作物联网设备时的安全性的方法和系统。

发明内容

[04]为了克服现有技术的缺陷，本说明书的一个或多个实施例提供了能够增强操作物联网设备时的安全性的技术方案。

[05]本说明书的一个或多个实施例通过以下技术方案来实现其上述目的。

[06]在一个方面中，公开了一种用于操作物联网设备的方法，包括：由用户设备从用户接收对物联网设备的操作指令；由所述用户设备识别所述用户的生物特征；基于所述生物特征，由所述用户设备验证所述用户的身份；如果所述用户的身份被成功验证，则由所述用户设备使用所述用户的第一用户密钥来对所述操作指令进行签名；由所述用户设备将经签名的操作指令传送至所述物联网设备；由所述物联网设备使用所述用户的第二用户密钥来验证所述经签名的操作指令的签名，所述第二用户密钥与所述第一用户密钥构成密钥对；以及如果所述签名被成功验证，则由所述物联网设备执行所述操作指令。

[07]优选地，所述方法进一步包括：由所述用户设备从所述物联网设备接收随机数，所述随机数由所述物联网设备生成并存储；由所述用户设备将所述随机数与所述经签名的操作指令一起传送至所述物联网设备；在所述签名被成功验证后，由所述物联网设备将从所述用户设备接收的随机数与由所述物联网设备生成的随机数进行比对；以及仅当由所述物联网设备将从所述用户设备接收的随机数与由所述物联网设备生成的随机数一

致时，才由所述物联网设备执行所述操作指令。

[08]优选地，所述方法进一步包括：在执行所述操作指令后，由所述物联网设备使所述随机数失效。

[09]优选地，所述第一用户密钥为所述用户的用户私钥，且所述第二用户密钥为所述用户的用户公钥。

[10]优选地，所述第一用户密钥和所述第二用户密钥为所述用户的同一用户密钥。

[11]优选地，所述方法进一步包括：在操作所述物联网设备之前，经由所述用户设备绑定所述物联网设备。

[12]优选地，经由所述用户设备绑定所述物联网设备进一步包括：由所述用户设备识别所述用户的生物特征；基于所述生物特征，由所述用户设备验证所述用户的身份；以及如果所述用户的身份被成功验证，则由所述用户设备将所述第二用户密钥传送至所述物联网设备。

[13]优选地，所述方法进一步包括由所述用户设备生成所述第一用户密钥和所述第二用户密钥。

[14]优选地，由所述用户设备生成所述第一用户密钥和所述第二用户密钥进一步包括：由所述用户设备录入所述用户的所述生物特征；以及在录入所述生物特征之后，由所述用户设备为所述用户生成所述第一用户密钥和所述第二用户密钥。

[15]优选地，所述第一用户密钥和所述第二用户密钥被存储在所述用户设备的安全环境中，所述安全环境为可信执行环境或硬件安全元件。

[16]在另一方面中，公开了一种由用户设备执行的方法，包括：从用户接收对物联网设备的操作指令；识别所述用户的生物特征；基于所述生物特征，验证所述用户的身份；如果所述用户的身份被成功验证，则使用所述用户的第一用户密钥来对所述操作指令进行签名；将经签名的操作指令传送至所述物联网设备，其中所述签名能被所述物联网设备用来使用第二用户密钥认证所述用户的所述身份，所述第二用户密钥与所述第一用户密钥构成密钥对。

[17]在又一方面中，公开了一种由物联网设备执行的方法，包括：从用户设备接收由第一用户密钥和第二用户密钥构成的密钥对中的第二用户密钥；从所述用户设备接收操作指令，所述操作指令是用所述第一用户密钥签名的；使用所述第二用户密钥来验证所述

操作指令的签名；以及如果所述签名被成功验证，则由所述物联网设备执行所述操作指令。

[18]优选地，所述方法进一步包括：生成第一随机数；以及将所述第一随机数传送至所述用户设备。

[19]优选地，所述方法进一步包括：在从所述用户设备接收操作指令时还接收第二随机数；将所述第二随机数与所述第一随机数进行比对；以及仅当所述第二随机数与所述第一随机数相一致时才执行所述操作指令。

[20]优选地，所述方法进一步包括：在执行所述操作指令后，使所述第一随机数失效。

[21]在又一方面中，公开了一种系统，所述系统包括：用户设备和物联网设备，所述用户设备具有生物特征识别能力，所述用户设备用于：从用户接收对物联网设备的操作指令；识别所述用户的生物特征；基于所述生物特征，验证所述用户的身份；以及如果所述用户的身份被成功验证，则使用所述用户的第一用户密钥来对所述操作指令进行签名；所述物联网设备用于：从所述用户设备接收所述经签名的操作指令；使用所述用户的第二用户密钥来验证所述经签名的操作指令的签名，所述第二用户密钥与所述第一用户密钥构成密钥对；以及如果所述签名被成功验证，则执行所述操作指令。

[22]优选地，所述系统还包括路由器，所述用户设备经由所述路由器与所述物联网通信。

[23]在又一方面中，公开了一种存储指令的计算机可读存储介质，所述指令当被计算机执行时，使所述计算机执行上述方法。

[24]与现有技术相比，本说明书的一个或多个实施例能够增强操作物联网设备时的安全性。

附图说明

[25]以上发明内容以及下面的具体实施方式在结合附图阅读时会得到更好的理解。需要说明的是，附图仅作为所请求保护的发明的示例。在附图中，相同的附图标记代表相同或类似的元素。

[26]图 1 示出根据本说明书实施例的系统的示意图。

[27]图 2 示出根据本说明书的实施例的用于录入生物特征的过程的示意图。

[28]图 3 示出根据本说明的实施例的用于绑定物联网设备的过程的示意图。

[29]图 4 示出根据本说明的实施例的用于操作物联网设备的过程的示意图。

[30]图 5 示出根据本说明的实施例的用于操作物联网设备的一种方法的示意图。

[31]图 6 示出根据本说明的实施例的用于操作物联网设备的另一种方法的示意图。

[32]图 7 示出根据本说明的实施例的用于操作物联网设备的另一种方法的示意图。

具体实施方式

[33]以下具体实施方式的内容足以使任何本领域技术人员了解本说明书的一个或多个实施例的技术内容并据以实施，且根据本说明书所揭露的说明书、权利要求及附图，本领域技术人员可轻易地理解本说明书的一个或多个实施例相关的目的及优点。

[34]生物特征识别技术是一种利用人体生物特征进行身份认证的技术。相比传统的身份认证方法，包括身份标识物品（诸如钥匙、证件、ATM 卡等）和身份标识知识（诸如用户名和密码），生物特征识别技术更具安全、保密和方便性。生物特征识别技术具有不易遗忘、防伪防盗性能好、随身“携带”和随时随地可用等优点。

[35]当今已经出现了许多种类的生物特征识别技术，如指纹识别、掌纹（手掌几何学）识别、虹膜识别、人脸识别、声音识别、签名识别、基因识别等。在后文中，通常用指纹作为示例，但应当领会，可采用除指纹外的其它生物特征。

[36]系统概述

[37]参见图 1，其示出了根据本说明书一实施例的系统 100 的示意图。如图所示，系统 100 可包括用户设备 104 和物联网设备 106。其中，用户设备 104 由用户 102 使用。

[38]用户设备 104 优选地是移动设备，例如移动通信设备（例如智能电话等）、平板计算机、笔记本计算机、个人数字助理等等。然而，用户设备 104 也可以是其它设备，例如台式计算机、机顶盒等等。

[39]通常，用户设备 104 可包括生物特征识别能力，例如用户设备 104 可包括指纹扫描仪，该指纹扫描仪可扫描用户 102 的指纹，并将所扫描的数据进行处理，以对用户 102 的指纹进行识别从而认证用户。

[40]物联网设备 106 通常是由物联网连接的物品，其通常具备网络连接能力以便通过物联网与其它设备进行交互。在许多实施例中，可将物联网设备 106 与如上所述的用户设备 104 进行绑定，以便通过该用户设备 104 来控制物联网设备 106 或与物联网设备 106

进行其它交互。

[41]物联网设备 106 的示例包括但不限于工业机器人、智能医疗设备、汽车、门锁、电饭煲、冰箱等工业设备和家用设备。在下面的示例中以智能电饭煲为例进行说明，但应领会，本说明书实施例不限于特定的物联网设备。

[42]在一些示例中，可在用户设备 104 上安装用于与物联网设备 106 交互的应用。该应用可以是针对一个或多个物联网设备的应用。例如，该应用可以是专用于智能电饭煲的智能电饭煲应用。或者，该应用可以是某品牌的物联网设备的通用应用。或者，该应用可以是系统级物联网设备应用。在下面的示例中以智能电饭煲应用为例进行说明，但应领会，本说明书实施例不限于智能电饭煲应用。

[43]如图 1 所示，在一些示例中，系统 100 还可包括路由器 108，用户设备 104 和物联网设备 106 可通过路由器 108 建立网络连接，从而允许通过用户设备 104 经由网络与物联网设备 106 通信。优选地，该网络为无线网络。

[44]替代地，系统 100 可不包括路由器 108，且用户设备 104 和物联网设备 106 可通过其它方式连接，例如经由红外、蓝牙、Zigbee 等方式连接。

[45]生物特征录入

[46]如图 2 所示，其示出了根据本说明书的实施例的用于录入生物特征的过程 200 的示意图，其中涉及用户 102 和用户设备 104。

[47]为了在稍后使用生物特征进行身份认证，通常需要首先将用户 102 的生物特征录入，以便将生物特征与用户 102 相关联。

[48]如图 2 的操作 2001 所示，用户 102 可向用户设备 104 请求开通生物特征识别。例如，用户 102 可点击用户设备 104 中的智能电饭煲应用上的控件，以便请求开通生物特征识别。例如，用户 102 可点击用户设备 104 上的“使用指纹识别”按钮来向用户设备 104 发出开通生物特征识别的请求。用户设备也可在用户打开或使用智能电饭煲应用时提示用户开通生物特征识别。

[49]在一些实施例中，用户 102 可能尚未在用户设备 104 上录入生物特征。在此情况下，可继续执行如下所述的生物特征录入过程。

[50]如图 2 的操作 2002 所示，可经由用户设备 104 提示用户展示生物特征。例如，可提示用户 102 将其手指放到指纹扫描仪上。在一些情况下，此操作可被省略。例如，当用

户特征是虹膜时，可无需提示用户而直接扫描用户的虹膜。

[51]随后，如图 2 的操作 2003 所示，用户 102 可根据提示展示生物特征。例如，用户 102 可将手指放到用户设备 104 的指纹扫描仪上。

[52]随后，如图 2 的操作 2004 所示，用户 102 的生物特征可被传入用户设备 104。例如，用户设备 104 的指纹扫描仪可读取用户 102 的生物特征。

[53]随后，如图 2 的操作 2005 所示，用户设备 104 可存储用户 102 的生物特征。

[54]在扫描过程中还可能需要提示用户 102 移动手指，以便获得完整的指纹数据。

[55]在稍后的身份认证过程中，可扫描待进行身份认证的用户的指纹，提取指纹特征与所存储的用户指纹特征进行比较，以确定两者是否匹配，从而认证该用户的身份。

[56]在另一些实施例中，用户 102 可能已经在用户设备 104 上录入了生物特征。例如，用户 102 可能先前已经在用户设备 104 上录入了指纹等，此时可无需重新录入生物特征，而是使用已经录入的生物特征。

[57]在另一些示例中，不管用户设备 104 上是否已经存在已录入的生物特征，可针对特定物联网设备录入专用生物特征。例如，可使用该智能电饭煲应用来录入专用于智能电饭煲的生物特征。使用专用于特定物联网设备的生物特征可进一步增加安全性。

[58]不同于现有技术，在本说明书的实施例中，如图 2 的操作 2006 所示，用户设备 104 还可为用户 102 生成公钥/私钥对。优选地，如下面详细描述的，用户公钥稍后可被存储到物联网设备 106 中，而用户私钥可被存储在用户设备 104 上，从而使得可以用物联网设备 106 上的用户私钥来对用户设备 104 上的公钥进行验证。

[59]替代地，还可采用对称加密方案。例如，用户设备 104 可生成单个用户密钥，且该单个用户密钥可被存储在用户设备 104 上，且该单个用户密钥稍后可被存储到物联网设备 106 上，从而使得可以用物联网设备 106 上的用户密钥来对用户设备 104 上的用户密钥进行验证。

[60]优选地，用户设备 104 可包括安全环境，且用户 102 的私钥（和/或生物特征）可被存储在该安全环境中。该安全环境可以是软件层面的安全环境，也可以是硬件层面的安全环境，或两者的结合。

[61]例如，该用户设备 104 可包括可信执行环境 (Trusted Execution Environment, TEE)。可信执行环境是由在用户设备 104 中创建的与用户设备 104 的主操作系统隔离的独立运

行的操作系统实现的安全环境，其可用于保障密钥存储、运算、生物特征识别等操作的安全性。在此情况下，用户 102 的私钥可被存储在该可信执行环境中。

[62]又例如，该用户设备 104 可包括安全元件（Secure Element, SE），该安全元件通常是以芯片形式提供的。为防止外部恶意解析攻击，保护数据安全，在作为安全元件的芯片中通常具有加密/解密逻辑电路。在此情况下，用户 102 的私钥可被存储在该安全元件中。

[63]通过使用安全环境，本说明书实施例可以进一步增强对公钥/私钥对的保护。

[64]随后，如图 2 的操作 2007 所示，可向用户 102 返回生物特征录入结果。例如，可向用户 102 告知用户生物特征录入完成。此外，可选地，也可向用户 102 告知公钥/私钥对生成完成。

[65]物联网设备绑定

[66]在用户 102 可以操作物联网设备 106 之前，通常应当首先将物联网设备 106 与用户 102 进行绑定。图 3 示出了根据本说明的实施例的用于绑定物联网设备的过程 300 的示意图。

[67]在一个实施例中，如图 3 的操作 3001 所示，用户 102 可向用户设备 106 发起绑定请求。例如，用户 102 可以点击用户设备 106 上的智能电饭煲应用中的控件，以选择要绑定的智能电饭煲。例如，该智能电饭煲可以是由用户设备通过搜索局域网内的设备来发现的。

[68]用户设备 104 接收来自用户 102 的绑定请求。如图 3 的操作 3002 所示，基于该绑定请求，用户设备 104 可尝试连接到物联网设备 106。该连接例如可经由如图 1 所示的路由器 108 实现，或经由其它连接方式实现。

[69]可选地，如图 3 的操作 3003 所示，在连接成功后，物联网设备 106 可向用户设备 104 返回连接结果。此外，用户设备也可通知用户连接成功。

[70]在本说明书的实施例中，可在用户设备 104 上执行生物特征认证过程。例如，如图 3 的操作 3004 所示，用户设备 104 可向用户 102 请求展示生物特征。例如，可在用户设备 104 中的智能电饭煲应用中显示：“请扫描指纹！”。

[71]如图 3 的操作 3005 所示，响应于该请求，用户 102 可向用户设备 104 展示其生物特征。例如，用户 102 可将其手指放在用户设备 104 的指纹扫描仪上。

[72]随后，如图 3 的操作 3006 所示，用户设备 104 可接收并验证用户 102 所展示的生物特征。例如，用户设备 104 可通过指纹扫描仪来扫描用户指纹，且用户设备 104 可提取扫描获得的用户指纹的指纹特征并将所提取的指纹特征与所存储的用户指纹特征进行比较，以确定两者是否匹配，从而认证该用户的身份。

[73]在用户提供的指纹特征与所存储的用户指纹特征相匹配的情况下，该用户的身份被成功认证。在用户提供的指纹特征与所存储的用户指纹特征不匹配的情况下，可提示用户指纹不匹配，可重新验证生物特征或者结束绑定过程（例如提示绑定不成功）。

[74]如图 3 的操作 3007 所示，在用户指纹验证成功之后，用户设备 104 可将与经认证的用户 102 相关联的用户公钥传送给物联网设备 106，例如经由在先前的操作 3002 中建立的连接。

[75]在接收到与用户 102 相关联的用户公钥之后，如图 3 的操作 3008 所示，物联网设备 106 可存储该用户公钥，例如存储在该物联网设备 106 的存储器中。类似地，为了进一步增强安全性，物联网设备可将该用户公钥存储在安全环境中，例如可信执行环境或安全元件中。

[76]随后，如图 3 的操作 3010 所示，物联网设备 106 可向用户设备 104 返回结果，例如以确认用户公钥存储成功。

[77]随后，如图 3 的操作 3011 所示，在接收到来自物联网设备 106 的确认之后，用户设备 104 可向用户 102 返回结果，例如经由智能电饭煲应用向用户显示绑定过程完成的提示。

[78]物联网设备操作

[79]参见图 4，其示出了根据本说明的实施例的用于操作物联网设备的过程 400 的示意图。

[80]在一个实施例中，在用户 102 想要操作物联网设备 106 时，如图 4 的操作 4001 所示，用户 102 可经由用户设备 104 发起操作指令。所述操作例如可以是对物联网设备 106 的管理，或者与物联网设备 106 的其它交互。

[81]例如，用户 102 可以点击用户设备中的智能电饭煲应用中的相应控件来操作物联网设备。例如，在智能电饭煲应用中，用户在选择“米种”、“口感”等参数后，可点击智能电饭煲应用上的“开始”按钮，以便向智能电饭煲传送开始煮饭的指令。

[82]用户设备 104 可接收来自用户 102 的操作指令。如图 4 的操作 4002 所示，基于该操作指令，用户设备 104 可尝试连接到物联网设备 106。类似地，该连接例如可经由如图 1 所示的路由器 108 实现，或经由其它连接方式实现。连接也可以是用户打开智能电饭煲应用后自动连接，随后用户可通过应用发出操作指令。

[83]可选地，如图 4 的操作 4003 所示，在连接成功后，物联网设备 106 可向用户设备 104 返回连接结果。

[84]优选地，在连接成功后，如图 4 的操作 4003 所示，物联网设备 106 还向用户设备 104 返回随机数。在打开智能电饭煲应用后自动连接的情况下，在用户发出操作指令后，物联网设备 106 可向用户设备 104 返回随机数。该随机数可由物联网设备 106 生成并存储。随机数可被用来保证操作指令仅被执行一次，从而增加了物联网设备 106 的安全性。可以理解，可使用本领域已知的任何随机数生成方案来生成随机数。

[85]在一些实施例中，物联网设备 106 可不执行生成并存储随机数的步骤。在这样的情况下，单个操作指令可能被多次执行多次。

[86]例如，如图 4 的操作 4004 所示，用户设备 104 可向用户 102 请求展示生物特征。例如，可在用户设备 104 中的智能电饭煲应用中显示：“请扫描指纹！”。

[87]如图 4 的操作 4005 所示，响应于该请求，用户 102 可向用户设备 104 展示其生物特征。例如，用户 102 可将其手指放在用户设备 104 的指纹扫描仪上。

[88]随后，如图 4 的操作 4006 所示，用户设备 104 可接收并验证用户 102 所展示的生物特征。例如，用户设备 104 可通过指纹扫描仪来扫描用户指纹，且用户设备 104 可提取指纹特征并将所提取的指纹特征与所存储的用户指纹特征进行比较，以确定两者是否匹配，从而认证该用户的身份。

[89]在用户提供的指纹特征与所存储的用户指纹特征相匹配的情况下，该用户的身份被成功认证。在用户提供的指纹特征与所存储的用户指纹特征不匹配的情况下，可提示用户指纹不匹配，可重新验证生物特征或者结束操作过程。

[90]在用户指纹验证成功之后，如图 4 的操作 4007 所示，用户设备 104 可组装指令数据。例如，基于由用户 102 经由用户设备 104 发出的指令（例如开始煮饭指令）和在操作 4003 中由物联网设备 106 返回的随机数，用户设备 104 可生成用于物联网设备 106 的指令数据。在不利用随机数（即物联网设备 106 在操作 4003 中不返回随机数）的情况下，用户设备 104 可仅基于由用户 102 发出的指令来组装指令数据。

[91]随后，如图 4 的操作 4008 所示，用户设备 104 可利用其存储的用户私钥对指令数据进行签名。用私钥对数据进行签名的方法对本领域技术人员是公知的，在此不再赘述。同样地，应当领会，在其它实施例中，用户设备 104 可利用其存储的用户公钥/用户密钥来对指令数据进行签名。

[92]随后，如图 4 的操作 4009 所示，用户设备 104 可将经签名的指令数据传送至物联网设备 106，例如经由在操作 4002 中建立的连接。

[93]物联网设备 106 可接收来自用户设备 104 的经签名的指令数据。随后，如图 4 的操作 4010 所示，物联网设备 106 用存储在所述物联网设备 106 中的用户公钥来验证所述用用户私钥签名的指令数据。

[94]如果所述经签名的指令数据无法通过验证，说明该指令数据没有用有效的用户私钥来签名，因此物联网设备 106 将拒绝执行用户指令（例如煮饭指令），并向用户设备 104 返回错误报告。在此情况下，用户设备 104 可向用户 102 显示签名错误的信息。

[95]如果所述经签名的指令数据通过了验证，则说明该指令数据是用有效数据签名的，此时物联网设备 106 继续执行后续步骤。

[96]随后，如果物联网设备 106 先前生成了随机数，则如在图 4 的操作 4011 所示，物联网设备 106 可将该随机数与所存储的先前生成的随机数进行比对。如果指令数据中包括的随机数与所存储的随机数相同，则如在图 4 的操作 4012 中所示，物联网设备 106 可执行指令数据中的指令。例如，物联网设备 106 可提取指令数据中的指令，并执行该指令。

[97]优选地，物联网设备 106 可使所述随机数失效（例如通过删除该随机数）。如果指令数据中包括的随机数与所存储的随机数不同，或者指令数据中不包括随机数，则物联网设备 106 可不执行指令数据中的指令，并向用户设备返回错误报告。

[98]可以领会，比对随机数的步骤也可在密钥验证步骤之前执行。

[99]如果物联网设备 106 先前没有生成随机数，则上述随机数比对操作可以省略。在此情况下，用户设备 104 可多次传送操作指令，且如在图 4 的操作 4012 中所示，物联网设备 106 可多次执行这些操作指令。

[100] 在执行完指令数据中的指令后，如在图 4 的操作 4013 所示，物联网设备 106 可向用户设备返回执行结果。例如，物联网设备 106 可向用户设备 104 返回煮饭指令被成功执行的确认。

[101] 随后，如在图 4 的操作 4014 所示，用户设备 104 可向用户 102 返回该执行结果。例如，用户设备 104 可在智能电饭煲应用中向用户 102 显示“已经开始煮饭！”

[102] 可以看出，在本发明中，通过使用生物特征来验证用户的身份，避免了与用户名/密码被盗等相关的风险，进一步增强了系统的安全性。

[103] 需要领会，本说明书的实施例存在许多变型。

[104] 例如，在一种变型中，不是在用户生物特征录入过程期间生成公钥/私钥对，而是在绑定物联网设备过程期间生成公钥/私钥对。例如，在图 2 中的步骤 2006 可被移动至图 3 中的步骤 3006 之后。

[105] 在再一种变型中，并非所有操作指令均需采用用户生物特征来验证。例如，在一些示例中，用户设备 104 在接收到操作指令后，可首先确定该操作指令的安全等级，且仅将安全等级较高时才请求用户展示生物特征以便验证。

[106] 此外，尽管前文示出的是非对称加密方案（即公钥/私钥对）的示例，但应领会，在其它示例中，也可采用对称加密方案，其中用户公钥和用户私钥均可由相同的用户密钥替换。

[107] 尽管在本文中以物联网设备为例进行说明，但应该理解，所述物联网设备可以用能够经由用户设备来认证的任何设备来替代。

[108] 示例方法

[109] 参见图 5，其示出了根据本说明的实施例的用于操作物联网设备的一种方法 500 的示意图。

[110] 方法 500 可包括：在步骤 502，可由用户设备从用户接收对物联网设备的操作指令。例如，用户可通过点击用户设备上的物联网设备应用界面中的控件来发出该操作指令，比如针对电饭煲的开始煮饭指令。

[111] 方法 500 还可包括：在步骤 504，可由所述用户设备识别所述用户的生物特征。具体而言，如上所述，用户设备可向用户请求展示生物特征，随后接收用户所展示的生物特征。

[112] 方法 500 还可包括：在步骤 506，可基于所述生物特征，由所述用户设备验证所述用户的身份。例如，用户设备可将用户展示的生物特征与先前录入的用户的生物特征进行比较，以验证所述用户是否为与物联网设备相关联的用户。

[113] 方法 500 还可包括：在步骤 508，如果所述用户的身份被成功验证，则可由所述用户设备使用所述用户的第一用户密钥来对所述操作指令进行签名。例如，该第一用户密钥和第二用户密钥可以是由用户设备先前针对已录入生物特征的用户生成的。优选地，所述第一用户密钥为所述用户的用户私钥，且所述第二用户密钥为所述用户的用户公钥。替代地，所述第一用户密钥和所述第二用户密钥为所述用户的同一用户密钥。

[114] 所述第一用户密钥和所述第二用户密钥可以是在生物特征录入或物联网设备绑定过程中由用户设备生成的。由所述用户设备生成所述第一用户密钥和所述第二用户密钥进一步包括：由所述用户设备录入所述用户的所述生物特征；以及在录入所述生物特征之后，由所述用户设备为所述用户生成所述第一用户密钥和所述第二用户密钥。

[115] 优选地，所述第一用户密钥和所述第二用户密钥被存储在所述用户设备的安全环境中，所述安全环境为可信执行环境或硬件安全元件。

[116] 方法 500 还可包括：在步骤 510，可由所述用户设备将经签名的操作指令传送至所述物联网设备。优选地，还由用户设备将先前从物联网设备接收的随机数与所述经签名的操作指令一起传送至物联网设备。

[117] 方法 500 还可包括：在步骤 512，可由所述物联网设备使用所述用户的第二用户密钥来验证所述经签名的操作指令的签名，其中所述第二用户密钥与所述第一用户密钥构成密钥对。

[118] 方法 500 还可包括：在步骤 514，如果所述签名被成功验证，则可由所述物联网设备执行所述操作指令。优选地，所述物联网设备还将从所述用户设备接收的随机数与由所述物联网设备生成的随机数进行比对，并且仅当由所述物联网设备将从所述用户设备接收的随机数与由所述物联网设备生成的随机数一致时，才由所述物联网设备执行所述操作指令。在执行所述操作指令后，可由所述物联网设备使所述随机数失效。

[119] 优选地，在操作所述物联网设备之前，可通过以下操作经由所述用户设备绑定所述物联网设备：由所述用户设备识别所述用户的生物特征；基于所述生物特征，由所述用户设备验证所述用户的身份；以及如果所述用户的身份被成功验证，则由所述用户设备将所述第二用户密钥传送至所述物联网设备。

[120] 参见图 6，其示出了根据本说明的实施例的用于操作物联网设备的另一种方法 600 的示意图。方法 600 可以是由用户设备执行的。

[121] 方法 600 可包括：在步骤 602，可从用户接收对物联网设备的操作指令。

[122] 方法 600 还可包括：在步骤 604，可识别所述用户的生物特征。

[123] 方法 600 还可包括：在步骤 606，可基于所述生物特征，验证所述用户的身份。

[124] 方法 600 还可包括：在步骤 608，如果所述用户的身份被成功验证，则可使用所述用户的第一用户密钥来对所述操作指令进行签名。

[125] 方法 600 还可包括：在步骤 610，可将经签名的操作指令传送至所述物联网设备。其中所述签名能被所述物联网设备用来使用第二用户密钥认证所述用户的所述身份，所述第二用户密钥与所述第一用户密钥构成密钥对。

[126] 相关步骤的具体操作可参考前面针对图 5 的描述。

[127] 参见图 7，其示出了根据本说明的实施例的用于操作物联网设备的另一种方法 700 的示意图。方法 700 可以是由物联网设备执行的。

[128] 方法 700 可包括：在步骤 702，可从用户设备接收由第一用户密钥和第二用户密钥构成的密钥对中的第二用户密钥。

[129] 方法 700 还可包括：在步骤 704，可从所述用户设备接收操作指令，所述操作指令是用所述第一用户密钥签名的。

[130] 方法 700 还可包括：在步骤 706，可使用所述第二用户密钥来验证所述操作指令的签名。

[131] 方法 700 还可包括：在步骤 708，如果所述签名被成功验证，则可由所述物联网设备执行所述操作指令。

[132] 优选地，方法 700 还可包括生成第一随机数并将所述第一随机数传送至所述用户设备。随后，在从所述用户设备接收操作指令，还从所述用户设备接收第二随机数。随后，可将所述第二随机数与所述第一随机数进行比对，并且仅当所述第二随机数与所述第一随机数相一致时才执行所述操作指令。在执行所述操作指令后，使所述第一随机数失效。例如，可删除该第一随机数。

[133] 而且，本申请还公开了一种包括存储于其上的计算机可执行指令的计算机可读存储介质，所述计算机可执行指令在被处理器执行时使得所述处理器执行本文所述的各实施例的方法。

[134] 此外，本申请还公开了一种系统，该系统包括用于实现本文所述的各实施例的方法的装置。

[135] 可以理解，根据本说明书的一个或多个实施例的方法可以用软件、固件或其组合来实现。

[136] 应该理解，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同或相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置和系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[137] 应该理解，上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[138] 应该理解，本文用单数形式描述或者在附图中仅显示一个的元件并不代表将该元件的数量限于一个。此外，本文中被描述或示出为分开的模块或元件可被组合为单个模块或元件，且本文中被描述或示出为单个的模块或元件可被拆分为多个模块或元件。

[139] 还应理解，本文采用的术语和表述方式只是用于描述，本说明书的一个或多个实施例并不应局限于这些术语和表述。使用这些术语和表述并不意味着排除任何示意和描述(或其中部分)的等效特征，应认识到可能存在的各种修改也应包含在权利要求范围内。其他修改、变化和替换也可能存在。相应的，权利要求应视为覆盖所有这些等效物。

[140] 同样，需要指出的是，虽然已参照当前的具体实施例来描述，但是本技术领域中的普通技术人员应当认识到，以上的实施例仅是用来说明本说明书的一个或多个实施例，在没有脱离本发明精神的情况下还可做出各种等效的变化或替换，因此，只要在本发明的实质精神范围内对上述实施例的变化、变型都将落在本申请的权利要求书的范围内。

权利要求书

1. 一种用于操作物联网设备的方法，其特征在于，包括:

由用户设备从用户接收对物联网设备的操作指令;

由所述用户设备识别所述用户的生物特征;

基于所述生物特征，由所述用户设备验证所述用户的身份;

如果所述用户的身份被成功验证，则由所述用户设备使用所述用户的第一用户密钥来对所述操作指令进行签名;

由所述用户设备将经签名的操作指令传送至所述物联网设备;

由所述物联网设备使用所述用户的第二用户密钥来验证所述经签名的操作指令的签名，所述第二用户密钥与所述第一用户密钥构成密钥对; 以及

如果所述签名被成功验证，则由所述物联网设备执行所述操作指令。

2. 如权利要求 1 所述的方法，其特征在于，进一步包括:

由所述用户设备从所述物联网设备接收随机数，所述随机数由所述物联网设备生成并存储;

由所述用户设备将所述随机数与所述经签名的操作指令一起传送至所述物联网设备;

在所述签名被成功验证后，由所述物联网设备将从所述用户设备接收的随机数与由所述物联网设备生成的随机数进行比对; 以及

仅当由所述物联网设备将从所述用户设备接收的随机数与由所述物联网设备生成的随机数一致时，才由所述物联网设备执行所述操作指令。

3. 如权利要求 2 所述的方法，其特征在于，进一步包括:

在执行所述操作指令后，由所述物联网设备使所述随机数失效。

4. 如权利要求 1 所述的方法，其特征在于，所述第一用户密钥为所述用户的用户私钥，且所述第二用户密钥为所述用户的用户公钥。

5. 如权利要求 1 所述的方法，其特征在于，所述第一用户密钥和所述第二用户密钥为所述用户的同一用户密钥。

6. 如权利要求 1 所述的方法，其特征在于，进一步包括:

在操作所述物联网设备之前，经由所述用户设备绑定所述物联网设备。

7. 如权利要求 1 所述的方法，其特征在于，经由所述用户设备绑定所述物联网设备进一步包括:

由所述用户设备识别所述用户的生物特征;

基于所述生物特征，由所述用户设备验证所述用户的身份；以及

如果所述用户的身份被成功验证，则由所述用户设备将所述第二用户密钥传送至所述物联网设备。

8. 如权利要求 1 所述的方法，其特征在于，所述方法进一步包括由所述用户设备生成所述第一用户密钥和所述第二用户密钥。

9. 如权利要求 8 所述的方法，其特征在于，由所述用户设备生成所述第一用户密钥和所述第二用户密钥进一步包括:

由所述用户设备录入所述用户的所述生物特征；以及

在录入所述生物特征之后，由所述用户设备为所述用户生成所述第一用户密钥和所述第二用户密钥。

10. 如权利要求 1 所述的方法，其特征在于，所述第一用户密钥和所述第二用户密钥被存储在所述用户设备的安全环境中，所述安全环境为可信执行环境或硬件安全元件。

11. 一种由用户设备执行的方法，其特征在于，包括:

从用户接收对物联网设备的操作指令;

识别所述用户的生物特征;

基于所述生物特征，验证所述用户的身份;

如果所述用户的身份被成功验证，则使用所述用户的第一用户密钥来对所述操作指令进行签名;

将经签名的操作指令传送至所述物联网设备，其中所述签名能被所述物联网设备用来使用第二用户密钥认证所述用户的所述身份，所述第二用户密钥与所述第一用户密钥构成密钥对。

12. 如权利要求 11 所述的方法，其特征在于，进一步包括:

从所述物联网设备接收随机数，所述随机数由所述物联网设备生成并存储;

将所述随机数与所述经签名的操作指令一起传送至所述物联网设备。

13. 如权利要求 11 所述的方法，其特征在于，进一步包括:

在操作所述物联网设备之前，经由所述用户设备绑定所述物联网设备。

14. 如权利要求 13 所述的方法，其特征在于，经由所述用户设备绑定所述物联网设备进一步包括:

识别所述用户的生物特征;

基于所述生物特征，验证所述用户的身份；以及

如果所述用户的身份被成功验证，则将所述第二用户密钥传送至所述物联网设备。

15. 如权利要求 11 所述的方法，其特征在于，进一步包括：

录入所述用户的所述生物特征；以及

在录入所述生物特征之后，为所述用户生成所述第一用户密钥和所述第二用户密钥。

16. 如权利要求 11 所述的方法，其特征在于，所述第一用户密钥和所述第二用户密钥被存储在所述用户设备的安全环境中，所述安全环境为可信执行环境或硬件安全元件。

17. 一种由物联网设备执行的方法，其特征在于，包括：

从用户设备接收由第一用户密钥和第二用户密钥构成的密钥对中的第二用户密钥；

从所述用户设备接收操作指令，所述操作指令是用所述第一用户密钥签名的；

使用所述第二用户密钥来验证所述操作指令的签名；以及

如果所述签名被成功验证，则由所述物联网设备执行所述操作指令。

18. 如权利要求 17 所述的方法，其特征在于，进一步包括：

生成第一随机数；以及

将所述第一随机数传送至所述用户设备。

19. 如权利要求 18 所述的方法，其特征在于，进一步包括：

在从所述用户设备接收操作指令时还接收第二随机数；

将所述第二随机数与所述第一随机数进行比对；以及

仅当所述第二随机数与所述第一随机数相一致时才执行所述操作指令。

20. 如权利要求 19 所述的方法，其特征在于，进一步包括：

在执行所述操作指令后，使所述第一随机数失效。

21. 一种系统，其特征在于，所述系统包括：

用户设备，所述用户设备具有生物特征识别能力，所述用户设备用于：

从用户接收对物联网设备的操作指令；

识别所述用户的生物特征；

基于所述生物特征，验证所述用户的身份；以及

如果所述用户的身份被成功验证，则使用所述用户的第一用户密钥来对所述操作指令进行签名；以及

物联网设备，所述物联网设备用于：

从所述用户设备接收经签名的操作指令；

使用所述用户的第二用户密钥来验证所述经签名的操作指令的签名，所述第二用户密钥与所述第一用户密钥构成密钥对；以及

如果所述签名被成功验证，则执行所述操作指令。

22. 如权利要求 21 所述的系统，其特征在于，

所述用户设备仅一步用于：

从所述物联网设备接收随机数，所述随机数由所述物联网设备生成并存储；以及

将所述随机数与所述经签名的操作指令一起传送至所述物联网设备；

所述物联网设备进一步用于：

在所述签名被成功验证后，将从所述用户设备接收的所述随机数与由所述物联网设备生成的随机数进行比对；以及

仅当由所述物联网设备将从所述用户设备接收的所述随机数与由所述物联网设备生成的随机数一致时，才执行所述操作指令。

23. 如权利要求 22 所述的系统，其特征在于，进一步包括：

在执行所述操作指令后，由所述物联网设备使所述随机数失效。

24. 如权利要求 22 所述的系统，其特征在于，进一步包括：

在操作所述物联网设备之前，所述用户设备被绑定到所述物联网设备。

25. 如权利要求 24 所述的系统，其特征在于，所述绑定包括：

由所述用户设备识别所述用户的生物特征；

基于所述生物特征，由所述用户设备验证所述用户的身份；以及

如果所述用户的身份被成功验证，则由所述用户设备将所述第二用户密钥传送至所述物联网设备。

26. 如权利要求 22 所述的系统，其特征在于，由所述用户设备生成所述第一用户密钥和所述第二用户密钥。

27. 如权利要求 22 所述的系统，其特征在于，由所述用户设备生成所述第一用户密钥和所述第二用户密钥进一步包括：

由所述用户设备录入所述用户的所述生物特征；以及

在录入所述生物特征之后，由所述用户设备为所述用户生成所述第一用户密钥和所述第二用户密钥。

28. 如权利要求 22 所述的系统，其特征在于，所述用户设备包括安全环境，所述第一用户密钥和所述第二用户密钥被存储在所述安全环境中，所述安全环境为可信执行环境或硬件安全元件。

29. 如权利要求 22 所述的系统，其特征在于，还包括路由器，所述用户设备经由所述路由器与所述物联网通信。

30. 一种存储指令的计算机可读存储介质，所述指令当被计算机执行时，使所述计

算机执行如权利要求 1-10 中任一项所述的方法。

31. 一种存储指令的计算机可读存储介质，所述指令当被计算机执行时，使所述计算机执行如权利要求 11-16 中任一项所述的方法。

32. 一种存储指令的计算机可读存储介质，所述指令当被计算机执行时，使所述计算机执行如权利要求 17-20 中任一项所述的方法。

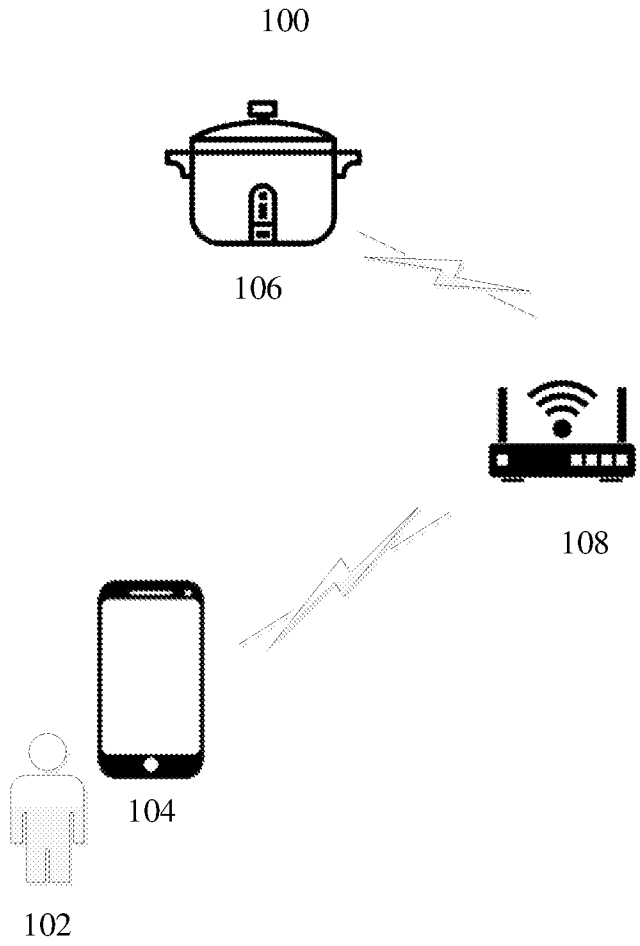

图 1

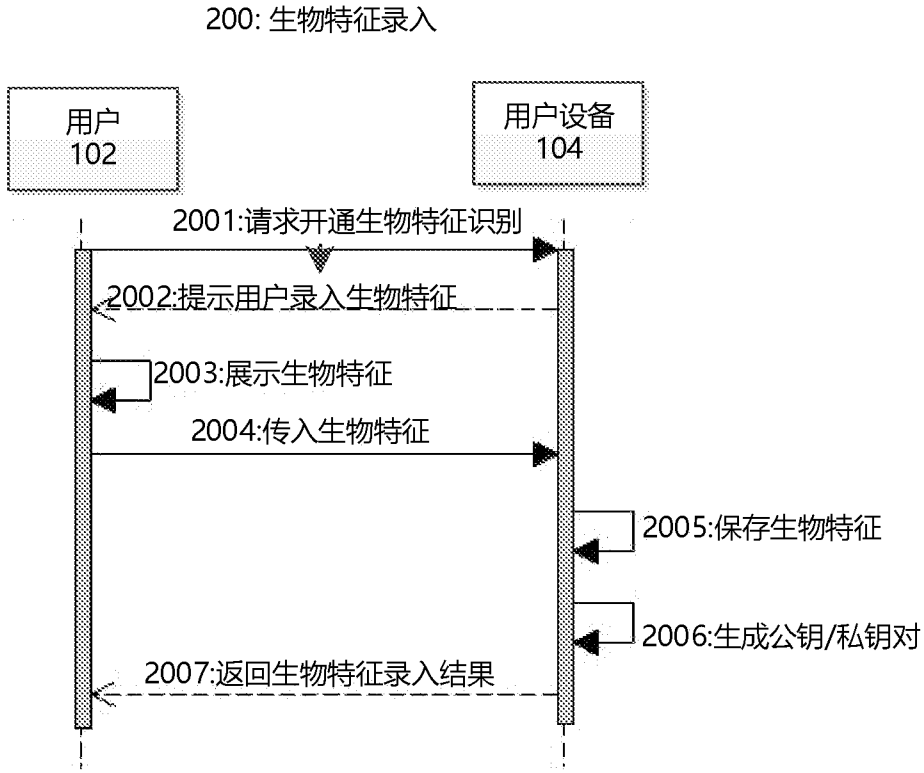
200: 生物特征录入
用户
102
用户设备
104
2001:请求开通生物特征识别
2002:提示用户录入生物特征
2003:展示生物特征
2004:传入生物特征
2005:保存生物特征
2006:生成公钥/私钥对
2007:返回生物特征录入结果

图 2

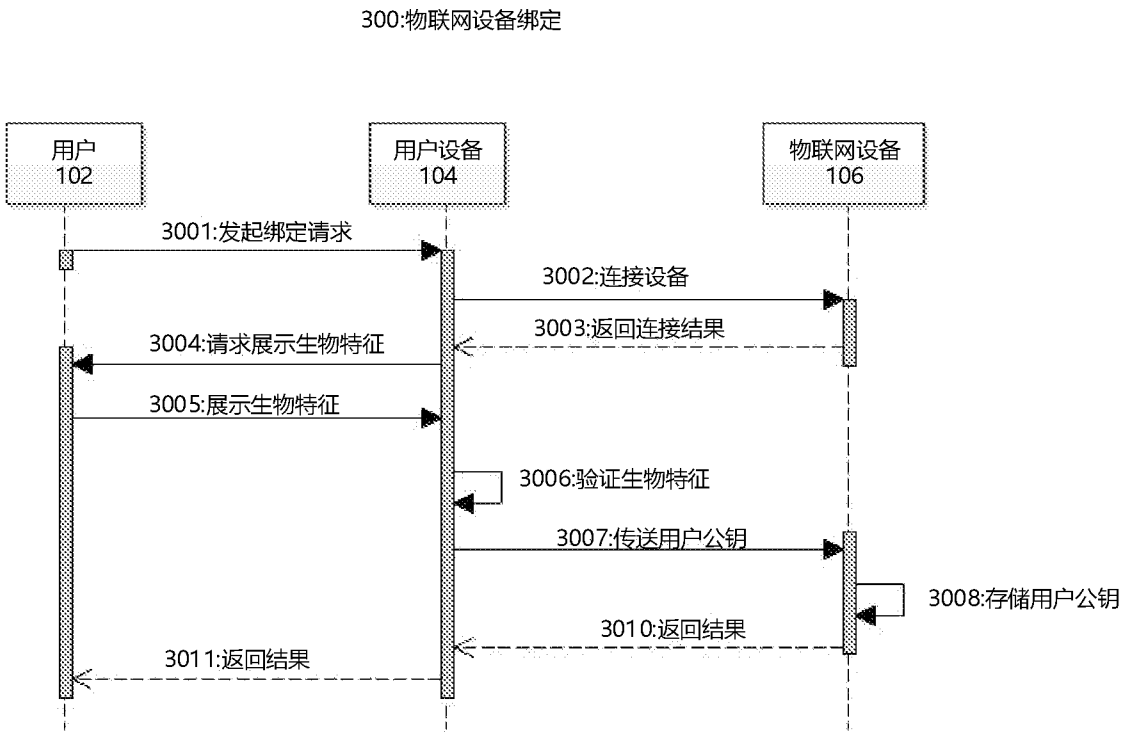
300:物联网设备绑定
用户
102
用户设备
104
物联网设备
106
3001:发起绑定请求
3002:连接设备
3003:返回连接结果
3004:请求展示生物特征
3005:展示生物特征
3006:验证生物特征
3007:传送用户公钥
3008:存储用户公钥
3010:返回结果
3011:返回结果

图 3

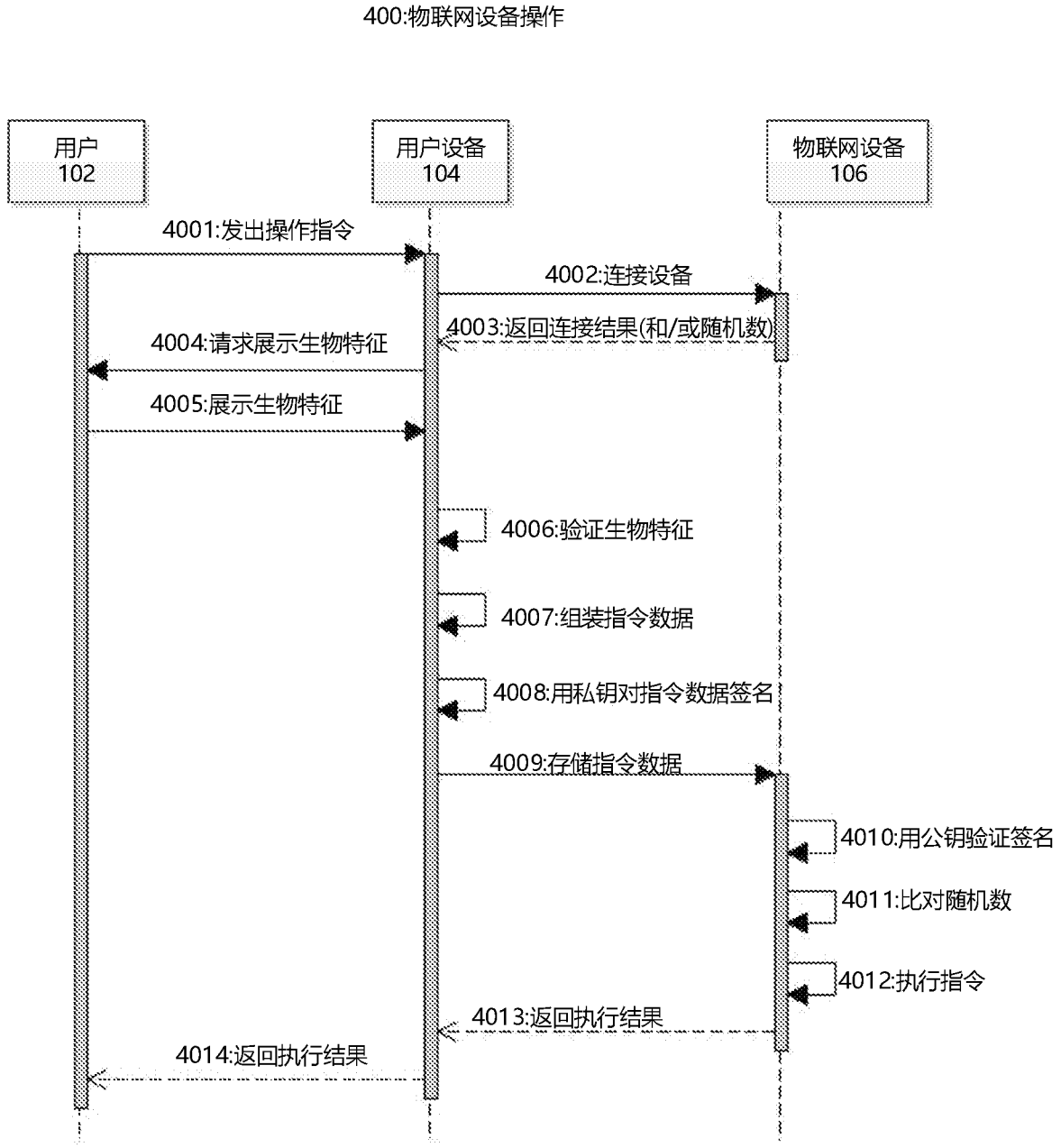
400:物联网设备操作
用户
102
用户设备
104
物联网设备
106
4001:发出操作指令
4002:连接设备
4003:返回连接结果(和/或随机数)
4004:请求展示生物特征
4005:展示生物特征
4006:验证生物特征
4007:组装指令数据
4008:用私钥对指令数据签名
4009:存储指令数据
4010:用公钥验证签名
4011:比对随机数
4012:执行指令
4013:返回执行结果
4014:返回执行结果

图 4

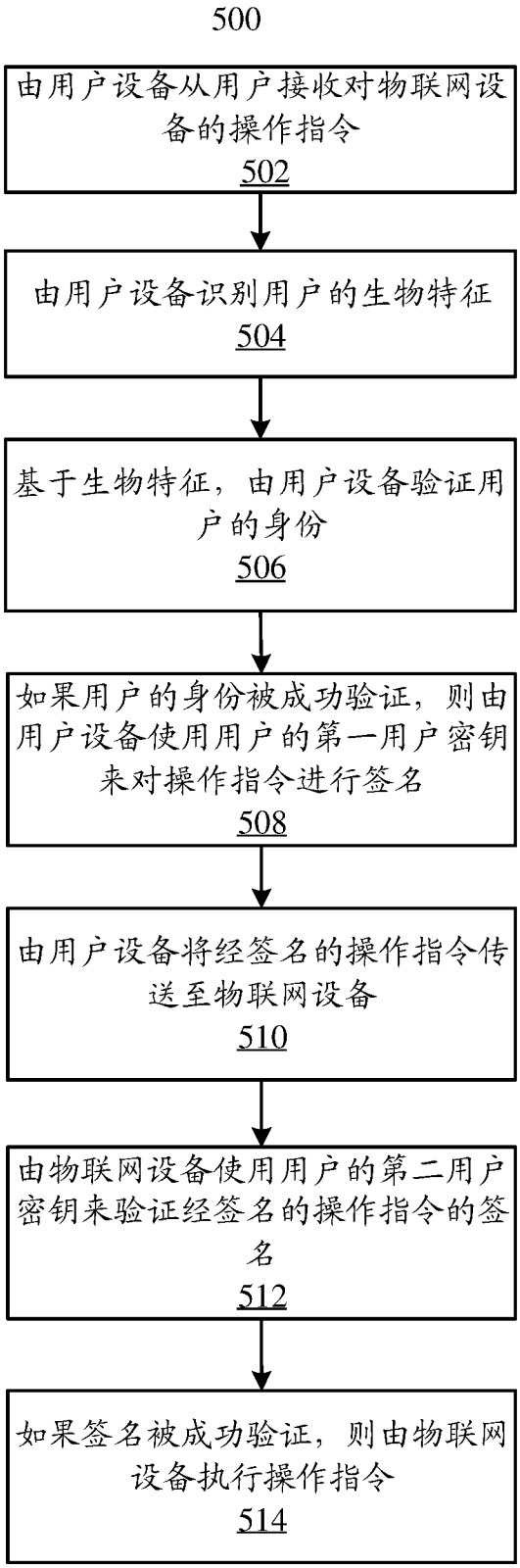
500
由用户设备从用户接收对物联网设备的操作指令
502
由用户设备识别用户的生物特征
504
基于生物特征，由用户设备验证用户的身份
506
如果用户的身份被成功验证，则由用户设备使用用户的第一用户密钥来对操作指令进行签名
508
由用户设备将经签名的操作指令传送至物联网设备
510
由物联网设备使用用户的第二用户密钥来验证经签名的操作指令的签名
512
如果签名被成功验证，则由物联网设备执行操作指令
514

图 5

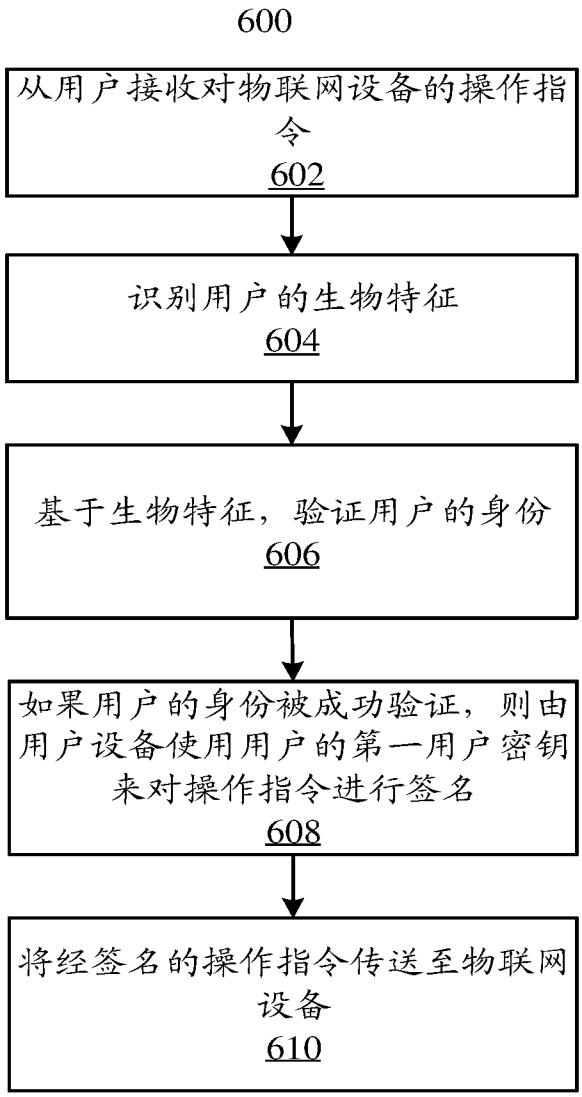
600
从用户接收对物联网设备的操作指令
602
识别用户的生物特征
604
基于生物特征，验证用户的身份
606
如果用户的身份被成功验证，则由用户设备使用用户的第一用户密钥来对操作指令进行签名
608
将经签名的操作指令传送至物联网设备
610

图 6

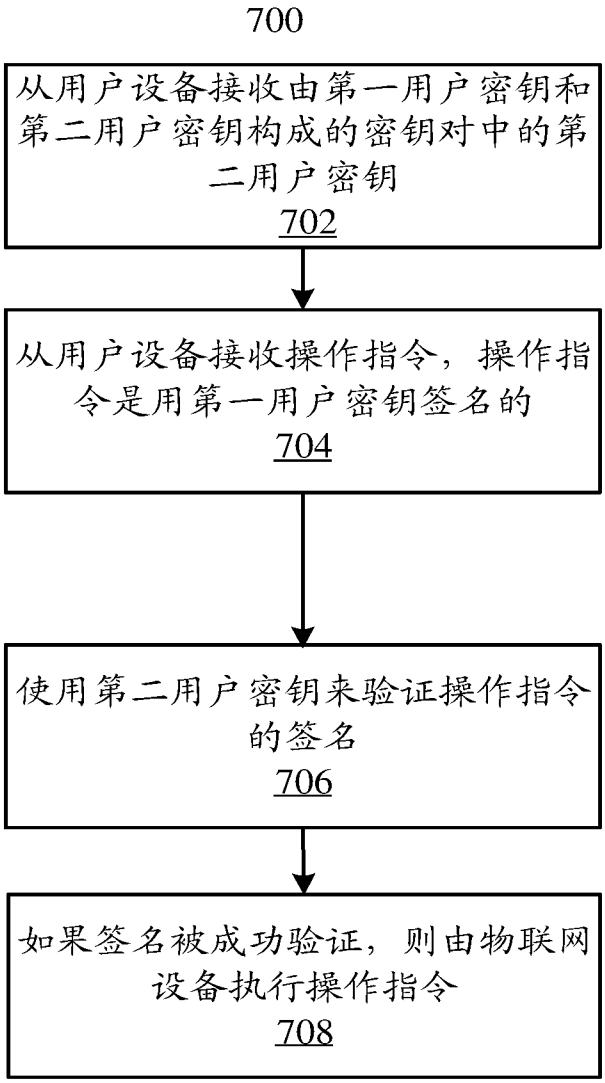
700
从用户设备接收由第一用户密钥和第二用户密钥构成的密钥对中的第二用户密钥
702
从用户设备接收操作指令，操作指令是用第一用户密钥签名的
704
使用第二用户密钥来验证操作指令的签名
706
如果签名被成功验证，则由物联网设备执行操作指令
708

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/070659

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)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)

H04L

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; CNKI; VEN; WOTXT; EPTXT; USTXT: 物联网, 控制信息, 控制指令, 操作信息, 操作指令, 生物, 指纹, 人脸, 面部, 加密, 密钥, 公钥, 私钥, 随机数, internet of things, IoT, controll information, controll instruction, operation information, operation instruction, biometric, fingerprint, face, encrypt, key, public key, private key, random

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110011985 A (ALIBABA GROUP HOLDING LIMITED) 12 July 2019 (2019-07-12) claims 1-32	1-32
X	CN 107919962 A (GUOMIN CERTIFICATION TECHNOLOGY (BEIJING) CO., LTD.) 17 April 2018 (2018-04-17) description, paragraphs [0058]-[0127]	1-32
X	CN 107370597 A (SHENZHEN SNOWBALL TECHNOLOGY CO., LTD.) 21 November 2017 (2017-11-21) description, paragraphs 23-37	1-32
X	US 2017171204 A1 (AFERO, INC.) 15 June 2017 (2017-06-15) description, paragraphs [0132]-[0144] and [0319]	1-32
A	CN 106850664 A (CHONGQING BUHANG TECHNOLOGY CO., LTD.) 13 June 2017 (2017-06-13) entire document	1-32
A	CN 109150508 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 04 January 2019 (2019-01-04) entire document	1-32

☑ 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	Date of mailing of the international search report
07 March 2020	**26 March 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017118181 A1 (DELL SOFTWARE INC.) 27 April 2017 (2017-04-27) entire document	1-32
A	US 2019058586 A1 (SAMSUNG ELECTRONICS CO., LTD.) 21 February 2019 (2019-02-21) entire document	1-32

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/070659

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110011985 A	12 July 2019	None	
CN 107919962 A	17 April 2018	None	
CN 107370597 A	21 November 2017	None	
US 2017171204 A1	15 June 2017	US 10178530 B2	08 January 2019
CN 106850664 A	13 June 2017	None	
CN 109150508 A	04 January 2019	None	
US 2017118181 A1	27 April 2017	US 9825921 B2	21 November 2017
		US 10110571 B2	23 October 2018
		US 2018048627 A1	15 February 2018
		US 9485231 B1	01 November 2016
US 2019058586 A1	21 February 2019	WO 2019035700 A1	21 February 2019
		IN 201741029394 A	22 February 2019

国际检索报告

国际申请号
PCT/CN2020/070659

A. 主题的分类

H04L 29/06(2006.01)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)

H04L

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;CNKI;VEN;WOTXT;EPTXT;USTXT:物联网，控制信息，控制指令，操作信息，操作指令，生物，指纹，人脸，面部，加密，密钥，公钥，私钥，随机数，internet of things，IoT，controll information，controll instruction，operation information，operation instruction，biometric，fingerprint，face，encrypt，key，public key，private key，random

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 110011985 A (阿里巴巴集团控股有限公司) 2019年 7月 12日 (2019-07-12) 权利要求1-32	1-32
X	CN 107919962 A (国民认证科技北京有限公司) 2018年 4月 17日 (2018-04-17) 说明书第[0058]-[0127]段	1-32
X	CN 107370597 A (深圳市雪球科技有限公司) 2017年 11月 21日 (2017-11-21) 说明书第23-37段	1-32
X	US 2017171204 A1 (AFERO INC) 2017年 6月 15日 (2017-06-15) 说明书第[0132]-[0144]段，第[0319]段	1-32
A	CN 106850664 A (重庆步航科技有限公司) 2017年 6月 13日 (2017-06-13) 全文	1-32
A	CN 109150508 A (腾讯科技深圳有限公司) 2019年 1月 4日 (2019-01-04) 全文	1-32
A	US 2017118181 A1 (DELL SOFTWARE INC) 2017年 4月 27日 (2017-04-27) 全文	1-32

☑ 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	国际检索报告邮寄日期
2020年 3月 7日	2020年 3月 26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 谭美玲 电话号码 86-(20)-28950742

国际检索报告

国际申请号
PCT/CN2020/070659

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
A	US 2019058586 A1 (SAMSUNG ELECTRONICS CO LTD) 2019年 2月 21日 (2019-02-21) 全文	1-32

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/070659

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	110011985	A	2019年 7月 12日	无			
CN	107919962	A	2018年 4月 17日	无			
CN	107370597	A	2017年 11月 21日	无			
US	2017171204	A1	2017年 6月 15日	US	10178530	B2	2019年 1月 8日
CN	106850664	A	2017年 6月 13日	无			
CN	109150508	A	2019年 1月 4日	无			
US	2017118181	A1	2017年 4月 27日	US	9825921	B2	2017年 11月 21日
				US	10110571	B2	2018年 10月 23日
				US	2018048627	A1	2018年 2月 15日
				US	9485231	B1	2016年 11月 1日
US	2019058586	A1	2019年 2月 21日	WO	2019035700	A1	2019年 2月 21日
				IN	201741029394	A	2019年 2月 22日