(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
2019 年 1 月 17 日 (17.01.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/010669 A1

(51) 国际专利分类号:
G07C 9/00 (2006.01) *G08C 17/02* (2006.01)
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2017/092797

(22) 国际申请日: 2017 年 7 月 13 日 (13.07.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 深 圳 市 汇 顶 科 技 股 份 有 限 公 司 (SHENZHEN GOODIX TECHNOLOGY CO., LTD.) [CN/CN]; 中 国 广 东 省 深 圳 市 福 田 区 保 税 区 腾 飞 工 业 大 厦 B 座 13 层, Guangdong 518045 (CN)。

(72) 发明人: 唐 杰 (TANG, Jie); 中 国 广 东 省 深 圳 市 福 田 区 保 税 区 腾 飞 工 业 大 厦 B 座 13 层, Guangdong 518045 (CN)。

(74) 代理人: 北 京 合 智 同 创 知 识 产 权 代 理 有 限 公 司 (BEIJING HEADSTAY INTELLECTUAL PROPERTY AGENCY); 中 国 北 京 市 海 淀 区 大 钟 寺 13 号 院 1 号 楼 华 杰 大 厦 5A1-2, Beijing 100098 (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, 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,

WO 2019/010669 A1

(54) **Title:** METHOD, APPARATUS AND SYSTEM FOR IDENTITY VALIDITY VERIFICATION

(54) **发明名称:** 一种身份合法性验证的方法、装置及系统

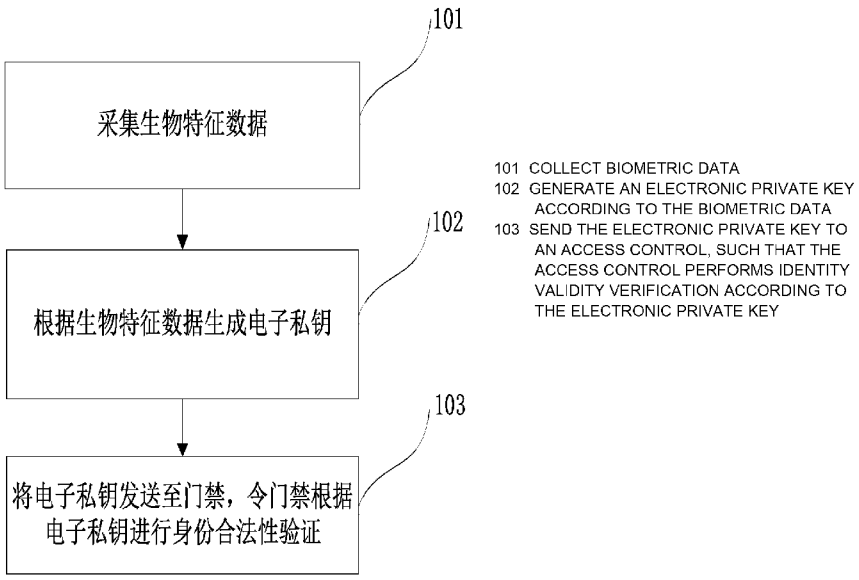


图 1

(57) **Abstract:** Provided is a method for identity validity verification, wherein same belongs to the technical field of information security. The method for identity validity verification applied to an electronic terminal comprises: collecting biometric data; generating an electronic private key according to the biometric data; and sending the electronic private key to an access control, such that the access control performs identity validity verification according to the electronic private key. The present application avoids arranging a dedicated fingerprint identification device at a specific location, thereby preventing fingerprint data of a user from being left on the fingerprint identification device, and thus enhancing the security while being convenient for the user.

[见续页]

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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))。

(57) 摘要：本申请实施例提供一种身份合法性验证的方法，属于信息安全技术领域。其中应用于电子终端的身份合法性验证的方法包括：采集生物特征数据；根据所述生物特征数据生成电子私钥；将所述电子私钥发送至所述门禁，令所述门禁根据所述电子私钥进行身份合法性验证。本申请避免了将专用的指纹识别设备设置在特定位置，进而避免了指纹识别设备上留有用户的指纹数据，在给用户带来方便的同时增强了安全性。

一种身份合法性验证的方法、装置及系统

技术领域

本申请实施例涉及信息安全技术领域，尤其涉及一种身份合法性验证的方法、装置及系统。

背景技术

传统的门禁通常需要通过刷 IC 卡、输入密码、呼叫等方式来开门，这些方式无一例外需要零距离操作。对于使用 IC 卡的方式，经常出现遗失补办、易被复制等麻烦，这不仅增加了管理难度，增加了成本，安全性也备受考验。同样的，对于输入密码的方式，由于密码容易泄露，门禁的安全性难以保证。基于传统门禁的种种缺陷，带有指纹识别技术的门禁系统应用而生。

指纹识别是指利用生物识别技术，对目标的指纹特征进行识别分析处理后进行判断的一种技术。由于指纹具有唯一性，对指纹特征的识别可以被用来确定个人信息，其在安全性、管理性等相关领域发展迅速。为了实现指纹识别，需要配置专用的指纹识别设备，并设置在固定的位置，由此造成用户的指纹信息容易留在专用的指纹识别设备上，存在安全隐患。

发明内容

有鉴于此，本申请实施例所解决的技术问题之一在于提供一种身份合法性验证的方法，用以克服现有技术中的上述技术问题。

基于上述目的，本申请的第一方面，提供一种身份合法性验证的方法，应用于与门禁进行通讯的电子终端，包括：

采集生物特征数据；

根据所述生物特征数据生成电子私钥；

将所述电子私钥发送至所述门禁，令所述门禁根据所述电子私钥进行身份合法性验证。

基于上述目的，本申请的第二方面，提供一种身份合法性验证的方法，应用于与电子终端进行通讯的门禁，包括：

接收电子终端发送的电子私钥；

将所述电子私钥与预先存储的电子公钥进行配对，以进行身份合法性验证。

基于上述目的，本申请的第三方面，提供一种身份合法性验证的装置，应用于与门禁进行通讯的电子终端，包括：

生物特征采集模组，用于采集生物特征数据；

第一处理模块，用于根据所述生物特征数据生成电子私钥；

第一通讯模块，用于将所述电子私钥发送至所述门禁，令所述门禁根据所述电子私钥进行身份合法性验证。

基于上述目的，本申请的第四方面，提供一种身份合法性验证的装置，包括：

第二通讯模块，用于接收电子终端发送的电子私钥；

第二处理模块，用于将所述电子私钥与预先存储的电子公钥进行配对，以进行身份合法性验证。

基于上述目的，在本申请的第五方面，还提供一种身份合法性验证系统，包括上述第三方面的装置和第四方面的装置。

由以上技术方案可见，本申请实施例的身份合法性验证的方法、装置及系统，通过在电子终端上采集用户指纹数据，并与门禁进行数据交互，完成用户的身份认证，避免了将专用的指纹识别设备设置在特定位置，同时指纹识别设备上不再留有用户的指纹信息，给用户带来方便的同时增强了安全性。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术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实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

图 1 为本申请实施例一的身份合法性验证的方法的流程图；

图 2 为本申请实施例二的身份合法性验证的方法的流程图；

图 3 为本申请实施例三的身份合法性验证的方法的流程图；

图 4 为本申请实施例四的身份合法性验证的装置的结构图；

图 5 为本申请实施例五的身份合法性验证的装置的结构图；

图 6 为本申请实施例六的身份合法性验证的系统的结构图。

具体实施方式

当然，实施本申请实施例的任一技术方案必不一定需要同时达到以上的所有优点。

为了使本领域的人员更好地理解本申请实施例中的技术方案，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，所描述的实施例仅是本申请实施例一部分实施例，而不是全部的实施例。基于本申请实施例中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于本申请实施例保护的范围。

下面结合本申请实施例附图进一步说明本申请实施例具体实现。

如图 1 所示，为本申请实施例一的身份合法性验证方法的流程图。本实施例应用于与门禁进行通讯的电子终端，包括以下步骤：

S101：采集生物特征数据。

在本实施例中，通过设置在电子终端比如智能手机上的生物特征采集模

组，比如指纹采集模组，采集生物特征数据如用户的指纹数据，这里的电子终端包括但不限于智能手机和平板电脑，本实施例及以下实施例以智能手机为例对本申请的方案进行说明，需要指出的是，这里的说明仅仅起到示例性的作用，而不应当被理解为对本申请方案的限定。

随着科技的发展，指纹芯片的价格越来越低，智能手机搭载指纹芯片的期望也越来越高,通过指纹采集模组采集用户的指纹数据也越来越容易实现，在本实施例及以下实施例中，指纹采集模组可以是基于电场感应的生物特征采集模组，对应地，生物特征数据为生物特征电场数据；同时，指纹采集模组也可以是基于光学感应的生物特征采集模组，对应地，生物特征数据为生物特征图像数据。这里的生物特征数据主要为指纹纹路的图案，但并不排除只从在该指纹纹路的图案中获取用户包括指纹纹路的细节特征点，比如谷脊特征点等。

S102：根据生物特征数据生成电子私钥。

建立生物特征数据与第一数组之间的函数映射关系，其中，第一数组为包含多个字符串的集合，将多个字符串排序后通过时间指针读出，即第一数组中的数据即字符串与时间段一一对应，也即任一时间段唯一对应一个字符串。时间段的时间间隔可以根据具体需要设置，比如，设置为 60 秒，即在 60 秒内生成的一个字符串，在下一个 60 秒为另一个字符串。不同的时间段对应的字符串不同。这里第一数组与生物特征数据具有唯一对应关系，不同用户对应的第一数组不同，且对于不同用户，生物特征数据与第一数组之间的映射函数也不同，这样，使得生成的电子私钥具有唯一性，只对应一个用户。显而易见的，将第一数组中的字符串作为电子私钥，其并不包含生物特征数据，即使第一数组中的字符串被他人获取，也不能根据被获取的字符串得到用户的私人信息，比如指纹纹路的图案。

不同用户的生物特征数据不同，同时，对于不同的用户，其对应的第一数组不同，因此保证了电子私钥的唯一性。

S103：将电子私钥发送至门禁，令门禁根据电子私钥进行身份合法性验证。

在本实施例中，为了防止所述电子私钥在传输过程中被截获，被用于身份验证，主要是被用来解锁门禁以非法进入安全区域，在根据生物特征数据生成电子私钥之后，还包括，在电子终端上对电子私钥进行加密，并将加密后的电子私钥通过电子终端上的通讯模块发送至门禁。这样，避免了用户隐私数据的泄露，增强了安全性。

如图 2 所示，为本申请实施例二的身份合法性验证方法的流程图。本实施例为电子终端与门禁匹配时，电子终端自动启动生物特征采集模组以使用户完成身份验证的方法流程图。本实施例在实施例一的步骤 S101 之前还包括以下步骤：

S201：在有效通讯距离内检测到门禁的无线通讯模块时，与门禁的无线通讯模块进行配对。

在本实施例中，电子终端上完成与门禁之间的通讯的模块为无线通讯模块，包括蓝牙通讯模块或者可见光通讯模块或者红外通讯模块。对应的，门禁的通讯模块为无线通讯模块，包括蓝牙通讯模块或者可见光通讯模块或者红外通讯模块。在本实施中，以蓝牙通讯模块为例对本实施例的方案加以说明。

因蓝牙特有的特点，配对过程只需一次，配对完成后电子终端，比如智能手机会记住与之配对的蓝牙通讯模块，以后就不用再次重新操作配对。同时，目前的智能手机，绝大多数带有蓝牙通讯模块，不用另外购置设备和材料，无需增加成本。当带有蓝牙通讯模块的智能手机靠近门禁一定范围内时，智能手机的蓝牙通讯模块与门禁的蓝牙通讯模块完成匹配，实现了电子终端与门禁的无线连接。比如在所述智能手机的无线通讯模块与门禁的无线通讯模块进入有效通讯距离内时，智能手机自动启动无线通讯模块与门禁的无线通讯模块进行配对。

S202：启动生物特征采集模组。

当电子终端的蓝牙通讯模块检测到门禁的蓝牙通讯模块并与门禁的蓝牙通讯模块连接后，在电子终端上加载生物特征管理页面并加载采集提示项，提示用户输入指纹，并启动生物特征采集模组。用户可以通过将手指按压在生物特征采集模组上供电子终端采集用户的生物特征数据，进而生成对应的电子私钥。

可选的，在本实施例中，生物特征采集模组为基于光学感应的指纹采集模组，对应地，生物特征数据为生物特征图像数据。或者，生物特征采集模组为基于电场感应的指纹采集模组，对应地，生物特征数据为生物特征电场数据。当采集到的生物特征数据为指纹图案时，指纹图案上会有中断点、分叉点和转折点，这些中断点、分叉点和转折点被用作识别指纹图案的特征。因此，要在采集到的指纹图案中提取这些中断点、分叉点和转折点，即根据生物特征数据生成有效生物特征数据，并根据这些有效生物特征数据生成电子私钥。

本申请上述实施例的应用于电子终端的身份合法性验证方法，通过在电子终端上采集用户指纹数据,并与门禁进行数据交互,完成用户的身份认证，避免了将专用的指纹识别设备设置在特定位置，同时指纹识别设备上不再留有用户的指纹信息，给用户带来方便的同时增强了安全性。

如图 3 所示，为本申请实施例三的身份合法性验证方法的流程图。本实施例应用于门禁，包括以下步骤：

S301：接收电子终端发送的电子私钥。

当电子终端与门禁完成匹配后，门禁会接收电子终端发送的电子私钥。电子私钥与用户存在一一对应的关系。

S302：将电子私钥与预先存储的电子公钥进行配对，以进行身份合法性验证。

需要指出的是,用户在能够解锁门禁之前,需要在门禁注册其个人信息。

在本实施例中，将包含生物特征数据的电子公钥预先存储在门禁中，电子公钥由电子终端生成。电子终端在采集用户的生物特征数据后，建立生物特征数据与包含多个字符串的第二数组之间的函数映射关系，将多个字符串排序后通过时间指针读出，将读出的字符串作为电子公钥，或者，对读出的字符串进行变形，将变形后的字符串作为电子公钥。门禁存储电子公钥。以生物特征数据为指纹图案加以说明，即用户需要先通过电子设备比如智能手机采集用户的指纹数据（指纹图案），

生成电子公钥，并将该电子公钥发送至门禁；门禁接收智能手机发送的电子公钥并存储，以用作和上述的电子私钥进行匹配，来对用户的身份进行合法性验证。这样，实现了门禁只存储有对应用户的电子公钥，而没有存储用户的指纹数据，这样进一步的避免了用户的指纹数据泄露，从而增强了安全性。即门禁本地只存储所述电子公钥，而不存储生物特征数据。在本实施例中，门禁还可以提取指纹数据的有效生物特征，即指纹图案的中断点、分叉点和转折点，并根据指纹图案的中断点、分叉点和转折点生成电子公钥。

此外，由于电子终端可以对电子私钥进行加密，因此，当门禁接收到的电子私钥为经过电子终端加密的电子私钥时，门禁对加密后的电子私钥进行解密，并将解密后的电子私钥与门禁存储的电子公钥进行匹配。如果匹配成功，则判定该用户的身份合法，因此该用户的指纹数据可以被用于解锁门禁。如果匹配失败，则判定该用户的身份不合法，该用户的指纹数据不能被用于解锁门禁。

具体的，解密后的电子私钥与所述电子公钥的匹配过程为：先根据解密后的电子私钥和门禁本地存储的电子公钥生成配对凭证，生成配对凭证的算法为预先存储在门禁的生成算法，对应于配对凭证的生成算法，门禁同时预先存储有凭证验证规则，当生成配对凭证后，根据预先设定的凭证验证规则，验证配对凭证，根据验证结果，对用户的身份进行合法性验证。当配对凭证与凭证验证规则匹配时，则判定验证结果成功，则说明用户的身份合法，用户通过电子设备发送的电子私钥能够用于解锁门禁，同时，解锁门禁，允许

用户通行。当验证结果失败时，则说明用户的身份不合法，用户通过电子设备发送的电子私钥不能用于解锁门禁，同时，不解锁门禁，则不允许用户通行。

如图 4 所示，为本申请实施例四的身份合法性验证的装置的结构图。在本实施例中,所述身份合法性验证的装置主要指以智能手机为例的电子终端。本实施例的身份合法性验证装置包括生物特征采集模组 401、第一处理模块 402 和第一通讯模块 403。其中，生物特征采集模组 401 用于采集用户的生物特征数据，第一处理模块 402 用于对采集到的生物特征数据进行识别处理，并生成电子私钥，第一通讯模块 403 用于与门禁的通讯模块连接并进行数据交互，如将电子私钥发送至门禁。第一通讯模块 403 具体可以为无线通讯芯片比如蓝牙芯片。

此外，第一处理模块 402 还具体用于对采集到的生物特征数据进行纹理特征识别，或者，对采集到的生物特征电场数据进行纹理特征识别。

并且，当电子终端的第一通讯模块 403 在有效通讯距离内检测到门禁的通讯模块时,与门禁的通讯模块进行配对,当与门禁的通讯模块成功配对时，在电子终端上加载生物特征管理页面加载采集提示项，启动设置在电子终端上的生物特征采集模组 401 采集生物特征数据。

作为本申请的一个实施例，第一处理模块 402 还包括建立子模块和选择子模块。建立子模块用于建立生物特征数据与包含多个字符串的第一数组之间的函数映射关系，选择子模块用于将上述多个字符串排序后通过时间指针读出，将读出的字符串作为电子私钥，或者，对读出的字符串进行变形，将变形后的字符串作为电子私钥。

如图 5 所示，为本申请实施例五的身份合法性验证的装置的结构图。在本实施例中，身份合法性验证的装置可以是门禁。本实施中的身份合法性验证装置包括第二通讯模块 501 和第二处理模块 502。第二通讯模块 501 对应于实施例四中的第一通讯模块 403，其主要用于与电子终端的通讯芯片匹配

连接，并进行数据交互，第二通讯模块 501 同样可以为蓝牙模块。第二处理模块 502 用于：根据本地存储的电子公钥与电子私钥进行配对，以根据所述生物特征数据对用户的身份进行合法性验证。

此外，电子公钥由电子终端生成。在通过电子终端预先采集所述生物特征数据后，建立生物特征数据与包含多个字符串的第二数组之间的函数映射关系，将多个字符串排序后通过时间指针读出，将读出的字符串作为电子公钥，或者，对读出的字符串进行变形，将变形后的字符串作为电子公钥。

在本申请的一些具体实施例中，第二处理模块 502 包括生成子模块和验证子模块。生成子模块用于根据解密后的电子私钥和门禁本地存储的电子公钥生成配对凭证，验证子模块用于根据预设的凭证验证规则，验证配对凭证，根据验证结果，对用户的身份进行合法性验证。

如图 6 所示，为本申请实施例六的身份合法性验证系统的结构图。本实施的身份合法性验证系统包括上述实施例四以及相关实施例中的电子终端 601 以及实施例五以及相关实施例中的门禁 602。

电子终端 601 通过生物特征采集模组采集生物特征数据，并对采集到的生物特征数据进行识别处理，生成电子私钥并对电子私钥进行加密，门禁 602 中存储的电子公钥与电子私钥进行配对，对生物特征数据对应的用户的身份进行合法性验证，保证了用户的私人数据不被泄露，同时增强了门禁的安全性。

上述产品可执行本申请实施例所提供的方法，具备执行方法相应的功能模块和有益效果。未在本实施例中详尽描述的技术细节，可参见本申请实施例所提供的方法。

本申请实施例的电子终端以多种形式存在，包括但不限于：

(1)移动通信设备：这类设备的特点是具备移动通信功能，并且以提供话音、数据通信为主要目标。这类终端包括：智能手机(例如 iPhone)、多媒体手机、功能性手机，以及低端手机等。

(2)超移动个人计算机设备:这类设备属于个人计算机的范畴，有计算和处理功能，一般也具备移动上网特性。这类终端包括:PDA、MID 和 UMPC 设备等，例如 iPad。

(3)便携式娱乐设备:这类设备可以显示和播放多媒体内容。该类设备包括:音频、视频播放器(例如 iPod)，掌上游戏机，电子书，以及智能玩具和便携式车载导航设备。

(4)服务器:提供计算服务的设备，服务器的构成包括处理器、硬盘、内存、系统总线等，服务器和通用的计算机架构类似，但是由于需要提供高可靠的服务，因此在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面要求较高。

(5)其他具有数据交互功能的电子装置。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，所述计算机可读记录介质包括用于以计算机（例如计算机）可读的形式存储或传送信息的任何机制。例如，机器可读介质包括只读存储器（ROM）、随机存取存储器（RAM）、磁盘存储介质、光存储介质、闪速存储介质、电、光、声或其他形式的传播信号（例如，载波、红外信号、数字信号等）等，该计算机软件产品包括若干指令用以使得一台计算机设备（可

以是个人计算机，服务器，或者网络设备等）执行各个实施例或者实施例的某些部分所述的方法。

最后应说明的是：以上实施例仅用以说明本申请实施例的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

本领域的技术人员应明白，本申请实施例的实施例可提供为方法、装置(设备)、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

本申请实施例是参照根据本申请实施例的方法、装置(设备)和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，

使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

权利要求书

1、一种身份合法性验证的方法，应用于与门禁进行通讯的电子终端，其特征在于，所述方法包括：

采集生物特征数据；

根据所述生物特征数据生成电子私钥；

将所述电子私钥发送至所述门禁，令所述门禁根据所述电子私钥进行身份合法性验证。

2、根据权利要求 1 所述的方法，其特征在于，所述采集生物特征数据包括:通过设置在电子终端上的生物特征采集模组采集生物特征数据。

3、根据权利要求 2 所述的方法，其特征在于，所述生物特征采集模组为基于光学感应的生物特征采集模组，对应地，所述生物特征数据为生物特征图像数据。

4、根据权利要求 2 所述的方法，其特征在于，所述生物特征采集模组为基于电场感应的生物特征采集模组，对应地，所述生物特征数据为生物特征电场数据。

5、根据权利要求 1-4 任一项所述的方法，其特征在于，在所述采集生物特征数据之前，还包括：

在有效通讯距离内检测到门禁的无线通讯模块时，与所述门禁的无线通讯模块进行配对。

6、根据权利要求 1 所述的方法，其特征在于，所述根据所述生物特征数据生成电子私钥包括：

根据所述生物特征数据生成有效生物特征数据，并根据所述有效生物特征数据生成电子私钥。

7、根据权利要求 1 所述的方法，其特征在于，所述根据所述生物特征数据生成电子私钥包括：

建立所述生物特征数据与包含多个字符串的第一数组之间的函数映射关

系；

将所述多个字符串排序后通过时间指针读出，将读出的字符串作为电子私钥，或者，对读出的字符串进行变形，将变形后的字符串作为电子私钥。

8、根据权利要求 1-7 任一项所述的方法，其特征在于，所述将所述电子私钥发送至所述门禁包括：通过蓝牙将所述电子私钥发送至所述门禁。

9、一种身份合法性验证的方法，应用于与电子终端进行通讯的门禁，其特征在于，包括：

接收电子终端发送的电子私钥；

将所述电子私钥与预先存储的电子公钥进行配对，以进行身份合法性验证。

10、根据权利要求 9 所述的方法，其特征在于，在所述接收电子终端发送的电子私钥之前，还包括：

接收电子终端发送的电子公钥，并存储。

11、根据权利要求 10 所述的方法，其特征在于，所述电子公钥的生成为所述电子终端在采集生物特征数据后，建立所述生物特征数据与包含多个字符串的第二数组的之间的函数映射关系；

将所述多个字符串排序后通过时间指针读出，将读出的字符串作为电子公钥，或者，对读出的字符串进行变形，将变形后的字符串作为电子公钥。

12、根据权利要求 9 所述的方法，其特征在于，所述将所述电子私钥与预先存储的电子公钥进行配对包括：

根据所述电子私钥和预先存储的电子公钥生成配对凭证；

根据预设的凭证验证规则，验证所述配对凭证，以进行身份合法性验证。

13、一种身份合法性验证的装置，其特征在于，应用于与门禁进行通讯的电子终端，包括：

生物特征采集模组，用于采集生物特征数据；

第一处理模块，用于根据所述生物特征数据生成电子私钥；

第一通讯模块，用于将所述电子私钥发送至所述门禁，令所述门禁根据

所述电子私钥进行身份合法性验证。

14、根据权利要求 13 所述的装置，其特征在于，所述生物特征采集模组为基于光学感应的生物特征采集模组，对应地，所述生物特征数据为生物特征图像数据。

15、根据权利要求 13 所述的装置，其特征在于，所述生物特征采集模组为基于电场感应的生物特征采集模组，对应地，所述生物特征数据为生物特征电场数据。

16、根据权利要求 13-15 任一项所述的装置，其特征在于，所述第一通讯模块还用于：在有效通讯距离内检测到门禁的无线通讯模块时，与所述门禁的无线通讯模块进行配对。

17、根据权利要求 13 所述的装置，其特征在于，所述第一处理模块还用于：根据所述生物特征数据生成有效生物特征数据，并根据所述有效生物特征数据生成电子私钥。

18、根据权利要求 13 所述的装置，其特征在于，所述第一处理模块包括：

建立子模块，用于建立所述生物特征数据与包含多个字符串的第一数组之间的函数映射关系；

选择子模块，用于将所述多个字符串排序后通过时间指针读出，将读出的字符串作为电子私钥，或者，对读出的字符串进行变形，将变形后的字符串作为电子私钥。

19、根据权利要求 13-18 任一项所述的装置，其特征在于，所述第一通讯模块为蓝牙芯片，所述蓝牙芯片用于将所述电子私钥发送至所述门禁。

20、一种身份合法性验证的装置，其特征在于，应用于与电子终端进行通讯的门禁，包括：

第二通讯模块，用于接收电子终端发送的电子私钥；

第二处理模块，用于将所述电子私钥与预先存储的电子公钥进行配对，以进行身份合法性验证。

21、根据权利要求 20 所述的装置，其特征在于，所述第二通讯模块还用

于接收电子终端发送的电子公钥。

22、根据权利要求 21 所述的装置，其特征在于，所述电子公钥的生成为所述电子终端在采集生物特征数据后，建立所述生物特征数据与包含多个字符串的第二数组的之间的函数映射关系；将所述多个字符串排序后通过时间指针读出，将读出的字符串作为电子公钥，或者，对读出的字符串进行变形，将变形后的字符串作为电子公钥。

23、根据权利要求 20 所述的装置，其特征在于，所述第二处理模块包括：

生成子模块，用于根据所述电子私钥和预先存储的电子公钥生成配对凭证；

验证子模块，用于根据预设的凭证验证规则，验证所述配对凭证，以进行身份合法性验证。

24、一种身份合法性验证系统，其特征在于，包括如权利要求 13-19 任意一项所述的装置和如利要求 20-23 任意一项所述的装置。

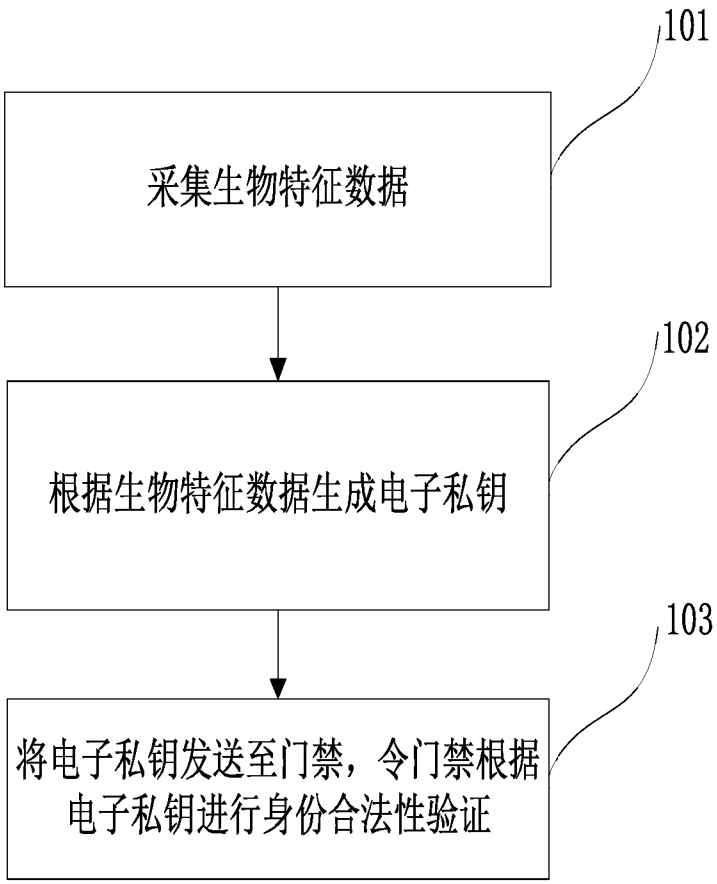

101
采集生物特征数据
102
根据生物特征数据生成电子私钥
103
将电子私钥发送至门禁，令门禁根据电子私钥进行身份合法性验证

图 1

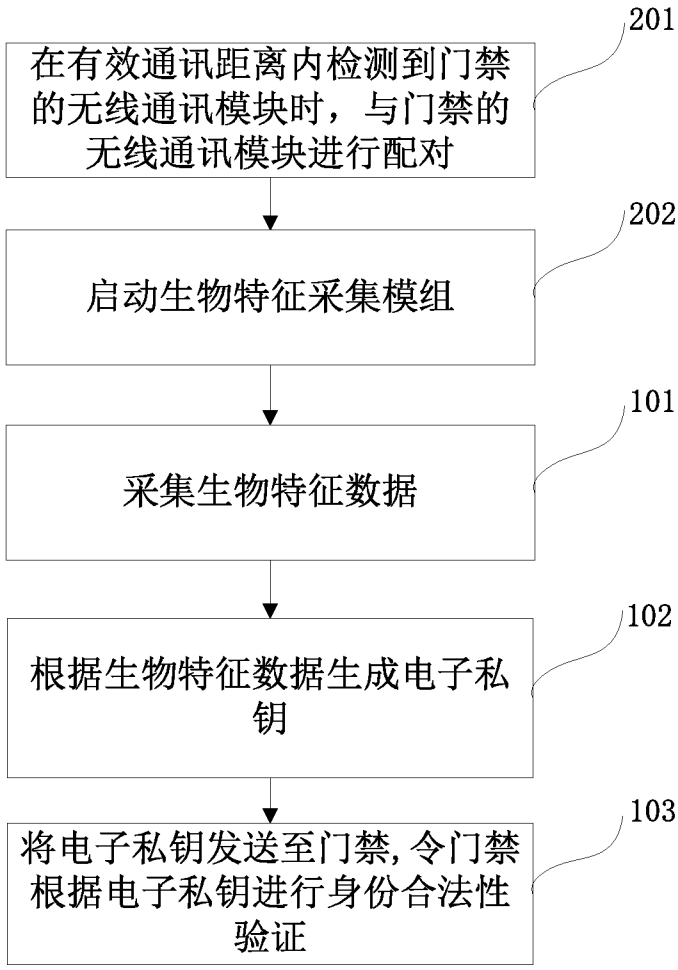

201
在有效通讯距离内检测到门禁的无线通讯模块时，与门禁的无线通讯模块进行配对
202
启动生物特征采集模组
101
采集生物特征数据
102
根据生物特征数据生成电子私钥
103
将电子私钥发送至门禁，令门禁根据电子私钥进行身份合法性验证

图 2

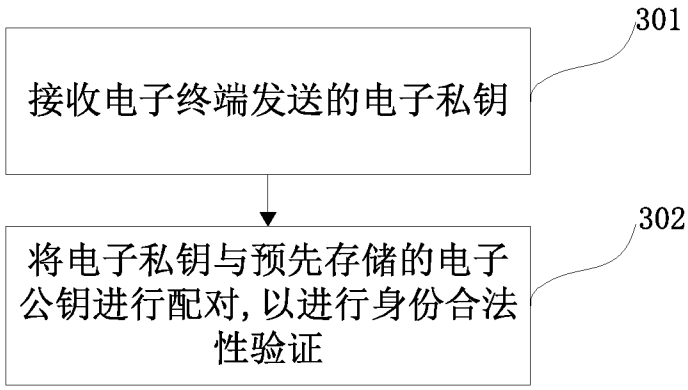

301
接收电子终端发送的电子私钥
302
将电子私钥与预先存储的电子公钥进行配对，以进行身份合法性验证

图 3

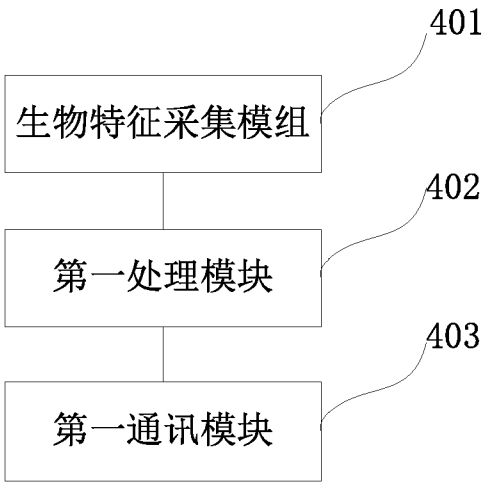

401
生物特征采集模组
402
第一处理模块
403
第一通讯模块

图 4

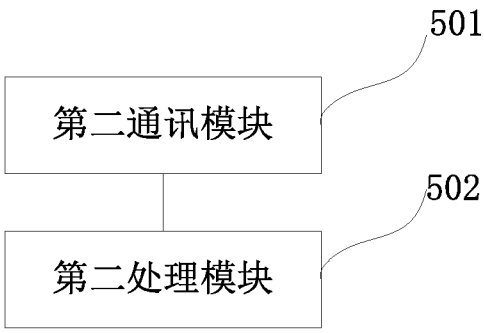

501
第二通讯模块
502
第二处理模块

图 5

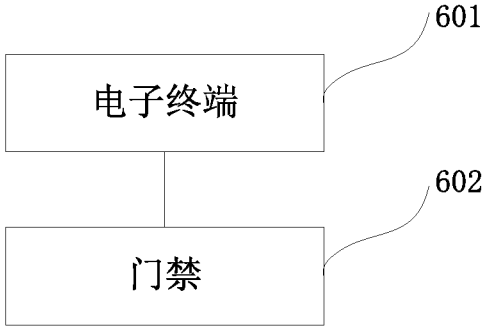

601
电子终端
602
门禁

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/092797

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/00 (2006.01) i; H04L 9/32 (2006.01) i; G08C 17/02 (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)

G07C, H04L, G08C

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)

CPRSABS, CNTXT, CNKI, VEN: 身份, 验证, 认证, 鉴权, 门禁, 采集, 生物特征, 指纹, 虹膜, 加密, 解密, 密钥, 私钥, 公钥, 手机, 移动终端, 移动设备, 便携式终端, 便携式设备, identity, ID, authenticate, verify, entrance guard, access control, collect, gather, biological characteristic, biological feature, fingerprint, iris, encrypt, decrypt, decode, key, private key, public key, cellphone, smart phone, mobile terminal, mobile device, portable terminal, portable device

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 205788363 U (XIANGSHAN SAIBOSI INTELLIGENT TECHNOLOGY CO., LTD.), 07 December 2016 (07.12.2016), description, paragraphs [0015]-[0021], and figure 1	1-24
X	US 2017078260 A1 (SHEN, I-Ting), 16 March 2017 (16.03.2017), description, paragraphs [0078]-[0121], and figures 1-2	1-24
A	CN 203165055 U (SHENZHEN ARATEK BIOMETRICS TECHNOLOGY CO., LTD.), 28 August 2013 (28.08.2013), entire document	1-24
A	CN 101321069 A (LIU, Hongli), 10 December 2008 (10.12.2008), entire document	1-24
A	CN 105991287 A (ALIBABA GROUP HOLDING LIMITED), 05 October 2016 (05.10.2016), entire document	1-24

☐ 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
23 March 2018	17 April 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer CHU, Yanling Telephone No. (86-10) 62089543

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/092797

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 205788363 U	07 December 2016	None	
US 2017078260 A1	16 March 2017	US 9641510 B2	02 May 2017
CN 203165055 U	28 August 2013	None	
CN 101321069 A	10 December 2008	None	
CN 105991287 A	05 October 2016	HK 1229563 A0	17 November 2017

国际检索报告

国际申请号
PCT/CN2017/092797

A. 主题的分类

G07C 9/00(2006.01)i；H04L 9/32(2006.01)i；G08C 17/02(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)

G07C，H04L，G08C

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））

CPRSABS，CNTXT，CNKI，VEN：身份，验证，认证，鉴权，门禁，采集，生物特征，指纹，虹膜，加密，解密，密钥，私钥，公钥，手机，移动终端，移动设备，便携式终端，便携式设备，identity, ID, authenticate, verify, entrance guard, access control, collect, gather, biological characteristic, biological feature, finger-print, iris, encrypt, decrypt, decode, key, private key, public key, cellphone, smart phone, mobile terminal, mobile device, portable terminal, portable device

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
X	CN 205788363 U（象山赛柏斯智能科技有限公司）2016年 12月 7日（2016 - 12 - 07） 说明书第[0015]-[0021]段，附图1	1-24
X	US 2017078260 A1（SHEN I-TING）2017年 3月 16日（2017 - 03 - 16） 说明书第[0078]-[0121]段，附图1-2	1-24
A	CN 203165055 U（深圳市亚略特生物识别科技有限公司）2013年 8月 28日（2013 - 08 - 28） 全文	1-24
A	CN 101321069 A（刘洪利）2008年 12月 10日（2008 - 12 - 10） 全文	1-24
A	CN 105991287 A（阿里巴巴集团控股有限公司）2016年 10月 5日（2016 - 10 - 05） 全文	1-24

☐ 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
2018年 3月 23日	2018年 4月 17日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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 初艳玲 电话号码 (86-10)62089543

表 PCT/ISA/210（第2页）（2009年7月）

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/092797

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	205788363	U	2016年 12月 7日		无		
US	2017078260	A1	2017年 3月 16日	US	9641510	B2	2017年 5月 2日
CN	203165055	U	2013年 8月 28日		无		
CN	101321069	A	2008年 12月 10日		无		
CN	105991287	A	2016年 10月 5日	HK	1229563	A0	2017年 11月 17日