

(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
2018 年 12 月 20 日 (20.12.2018)



(10) 国际公布号
WO 2018/227685 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2017/093224

(22) 国际申请日: 2017 年 7 月 17 日 (17.07.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710462756.1 2017年6月16日 (16.06.2017) CN

(71) 申请人: 深圳市盛路物联通讯技术有限公司(SHENZHEN SHENGLU IOT COMMUNICATION TECHNOLOGY CO.,LTD.) [CN/CN]; 中国广东省深圳市南山区南山街道科技园科技中三路5号国人通信大厦B栋328室, Guangdong 518057 (CN)。

(74) 代理人: 深圳中一联合知识产权代理有限公司 (SHENZHEN ZHONGYI UNION INTELLECTUAL PROPERTY AGENCY CO.,LTD.); 中国广东省深圳市福田区园岭街道深南中路1014号报春大厦9楼(5号信箱), Guangdong 518028 (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, 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,

(54) Title: METHOD AND SYSTEM FOR SECURE ACCESS OF TERMINAL DEVICE TO INTERNET OF THINGS

(54) 发明名称: 一种终端设备安全接入物联网的方法及系统

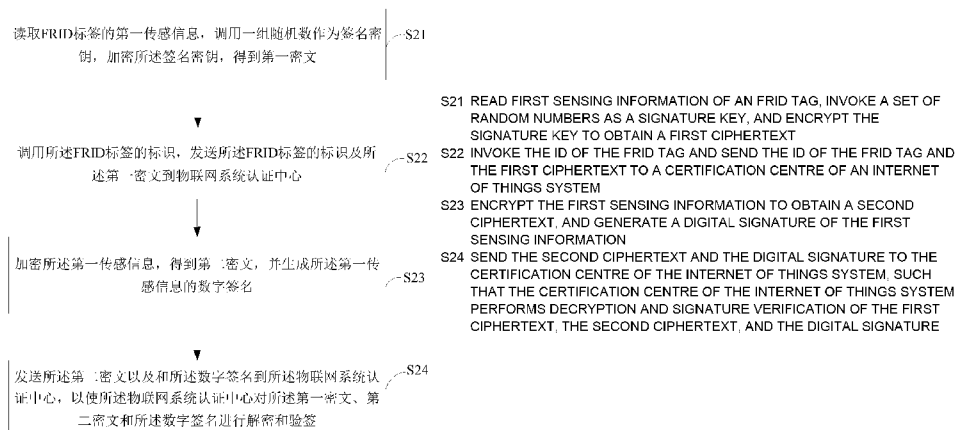


图 2

(57) Abstract: Provided in the present embodiment are a method and a system for secure access of a terminal device to the Internet of Things. The method comprises: reading first sensing information of an FRID tag, invoking a set of random numbers as a signature key, and encrypting the signature key to obtain a first ciphertext; invoking the ID of the FRID tag and sending the ID of the FRID tag and the first ciphertext to a certification centre of an Internet of Things system; encrypting the first sensing information to obtain a second ciphertext, and generating a digital signature of the first sensing information; sending the second ciphertext and the digital signature to the certification centre of the Internet of Things system. In the present embodiment, an FRID card reader twice performs encryption of information to be sent, ensuring secure transmission of the information; generating a digital signature of the first sensing information facilitates subsequent signature verification of same, further ensuring the security of the information received by the certification centre of the Internet of Things system.

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：本实施例提供了一种终端设备安全接入物联网的方法及系统。所述方法包括：读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，并加密所述签名密钥，得到第一密文；调用所述FRID标签的标识，发送所述FRID标签的标识及所述第一密文到物联网系统认证中心；加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名；发送所述第二密文以及和所述数字签名到所述物联网系统认证中心。本实施例中FRID读卡器对待发送的信息进行了两次加密，保证了信息的安全发送；生成第一传感信息的数字签名，方便后续对其进行验签，进一步保证了物联网系统认证中心所接收到的信息的安全性。

说明书

发明名称：一种终端设备安全接入物联网的方法及系统

技术领域

[0001] 本发明实施例属于物联网系统信息安全领域，尤其涉及一种终端设备安全接入物联网的方法及系统。

背景技术

[0002] 物联网ITO (Internet of Things)是把所有物品通过射频识别技术(Radio Frequency Identification, RFID)、红外感应器、全球定位系统、激光扫描器等传感设备，按照约定的协议，与互联网连接起来，进行信息交换和通讯，实现智能化识别、定位、跟踪、监控和管理。物联网应用可以分为传感网络，传输网络，应用网络三层，系统应用流程可以分为：首先对设备或物体进行标识，再实现对所述的设备或物体进行智能化识别，智能化识别方法的任务和目的就是提供关于各种物品、设备甚至可以移动的生物的信息；为了实现这一目的，可在各种设备或物体上附着RFID标签，RFID标签中存储着规范而具有互用性的信息，在需要将这些的设备或物体接入物联网系统时，通过RFID读卡器扫描附着于设备或物体上的RFID标签，从所述RFID标签中读取必要的信息以将其接入物联网系统中。但使用RFID读卡器获取RFID标签中传感信息以将其接入物联网系统时，直接将读取到的传感信息发送到物联网系统进行验证，这一过程中不存在对传感信息的保护，因此，存在传感信息外漏或被篡改的危险。

技术问题

[0003] 鉴于现有技术中存在的不足，本发明实施例提供了一种终端设备安全接入物联网的方法及系统，旨在解决现有的终端设备接入物联网系统的方法中，FRID标签的传感信息容易被泄漏或篡改，从而不能保证传感信息安全的问题。

问题的解决方案

技术解决方案

[0004] 本发明实施例第一方面，提供了一种终端设备安全接入物联网的方法，所述终端设备安全接入物联网的方法包括：

- [0005] 读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，加密所述签名密钥，得到第一密文；
- [0006] 调用所述FRID标签的标识，发送所述FRID标签的标识及所述第一密文到物联网系统认证中心；
- [0007] 加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名；
- [0008] 发送所述第二密文以及所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第一密文、第二密文和所述数字签名进行解密和验签。
- [0009] 优选地，所述读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，加密所述签名密钥，得到第一密文，具体包括：
- [0010] 读取FRID标签的第一传感信息，调用随机数发生器生产一组随机数，将所述随机数作为签名密钥；
- [0011] 调用预先存储的密钥加密所述签名密钥，生成第一密文。
- [0012] 优选地，所述加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名，具体包括：
- [0013] 调用轻量级密码算法，加密所述第一传感信息成第二密文；
- [0014] 调用摘要算法，通过所述摘要算法以及所述签名密钥生成所述第一传感信息的数字签名。
- [0015] 优选地，在所述发送所述第二密文以及所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第一密文、第二密文和所述数字签名进行解密和验签之后，还包括：
- [0016] 接收物联网系统认证中心发送的授权接入信息，根据所述授权接入信息连接FRID标签所属的终端设备到物联网。
- [0017] 优选地，所述终端设备安全接入物联网系统的方法还包括：
- [0018] 物联网系统认证中心接收并存储所述FRID读卡器发送的FRID标签的标识和第一密文；并接收所述FRID读卡器发送的第二密文及数字签名；
- [0019] 物联网系统认证中心解密所述第一密文得到签名密钥，并解密所述第二密文得

到第一传感信息；

[0020] 物联网系统认证中心通过所述第一传感信息和所述签名密钥对所述数字签名进行验签，得到验签结果，并根据所述验签结果判断是否发送授权接入信息到所述FRID读卡器。

[0021] 本发明实施例的第二方面，提供一种终端设备安全接入物联网的系统，所述终端设备安全接入物联网的系统包括：FRID读卡器、物联网系统认证中心，其中，所述FRID读卡器包括：

[0022] 第一加密单元，用于读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，加密所述签名密钥，得到第一密文；

[0023] 第一发送单元，用于调用所述FRID标签的标识，发送所述FRID标签的标识及所述第一密文到物联网系统认证中心；

[0024] 第二加密单元，用于加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名；

[0025] 第二发送单元，用于发送所述第二密文以及所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第一密文、第二密文和所述数字签名进行解密和验签。

[0026] 优选地，所述第一加密单元，具体包括：

[0027] 签名密钥生成模块，用于读取FRID标签的第一传感信息，调用随机数发生器生产一组随机数，将所述随机数作为签名密钥；

[0028] 签名密钥加密模块，用于调用预先存储的密钥加密所述签名密钥，生成第一密文。

[0029] 优选地，所述第二加密单元，具体包括：

[0030] 第二密文生成模块，用于调用轻量级密码算法，加密所述第一传感信息成第二密文；

[0031] 数字签名生成模块，用于调用摘要算法，通过所述摘要算法以及所述签名密钥生成所述第一传感信息的数字签名。

[0032] 优选地，所述FRID读卡器还包括：

[0033] 终端设备接入单元，用于接收物联网系统认证中心发送的授权接入信息，根据

所述授权接入信息连接FRID标签所属的终端设备到物联网。

[0034] 本发明实施例的第三方面，提供一种物联网系统认证中心所述物联网系统认证中心包括：

[0035] 接收单元，用于接收并存储所述FRID读卡器发送的FRID标签的标识和第一密文；并接收所述FRID读卡器发送的第二密文及数字签名；

[0036] 解密单元，用于解密所述第一密文得到签名密钥，解密所述第二密文得到第一传感信息；

[0037] 授权接入信息生成单元，用于通过所述第一传感信息和所述签名密钥对所述数字签名进行验签，得到验签结果；根据所述验签结果判断是否发送授权接入信息到所述FRID读卡器。

发明的有益效果

有益效果

[0038] 在本发明实施例中，FRID读卡器接收到FRID标签的第一传感信息后，调用一组随机数作为与FRID标签的第一传感信息相对应的签名密钥，将所述签名密钥加密后生成第一密文和所述FRID标签的标识一起发送到物联网认证中心，由于在发送前对其进行了加密保证了所述签名密钥在发送过程中不被修改，并且和所述FRID标签一一对应；FRID读卡器对获取的第一传感信息加密生成第二密文，并生成与所述第一传感信息对应的数字签名，以便后续物联网系统认证中心根据所述FRID标签的标识选择对应的签名密钥对所接收到的信息进行验签。此过程中在FRID读卡器一端形成加密系统，在发送第一传感信息前对第一传感信息和签名密钥分别进行加密，两次加密保证了信息的安全发送；生成第一传感信息的数字签名，方便后续对其进行验签，进一步保证了物联网系统认证中心所接收到的信息的安全性。

对附图的简要说明

附图说明

[0039] 图1是现有技术中FRID标签和FRID读卡器工作原理示意图；

[0040] 图2是本发明第一实施例提供的一种终端设备安全接入物联网的方法的流程图

；

[0041] 图3是本发明第二实施例提供的一种终端设备安全接入物联网的方法的流程图；

[0042] 图4是本发明第三实施例提供的一种终端设备安全接入物联网的方法的流程图；

[0043] 图5是本发明第四实施例提供的一种终端设备安全接入物联网的信息交互示意图；

[0044] 图6是本发明第四实施例提供的一种终端设备安全接入物联网的系统的结构框图；

发明实施例

本发明的实施方式

[0045] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0046] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0047] 实施例1

[0048] 物联网即通过射频识别(RFID)、红外感应器、全球定位系统、激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络概念。其中无线射频识别技术基本原理是利用射频信号和空间耦合（电感或电磁耦合）传输特性,实现对被识别物体的自动识别。无线射频识别系统由电子标签和读写器（读卡器）两个部份组成如图1所示，在其实际应用中，电子标签附在被识别物体的表面或者内部，当该物体带着标签经过读写器作用范围时，读写器可以用非接触方式读取电子标签里面存放的信息或将预定数据写入电子标签实现了对带标签物体自动识别和自动收集数据的功能。读写器将收集到的信息发送到数据管理系统（物联网系统）即可实现将各种物体通过网络连接起来。但在读写器将收集到的信息发送至物联网系统的过程中存在数据泄漏或数据被篡改的可能，因此，在本发明第一实施例中提供了一种终端设备安全接入物联网的方法，如图2所示，其中：

[0049] 步骤S21, 读取FRID标签的第一传感信息, 调用一组随机数作为签名密钥, 加密所述签名密钥, 得到第一密文;

[0050] 该步骤中, FRID读卡器扫描要接入物联网的终端设备上附着的RFID标签, 读取RFID标签中包含的传感信息, 即第一传感信息, 所述第一传感信息包括终端设备的名称、型号、终端设备的为唯一标识码、对外开放权限等信息。根据所述第一传感信息, 调用RFID读卡器中的随机数发生器中的一组随机数, 设置所述随机数为与所述第一传感信息相对应的签名密钥。由于随机数具有随机性, 每次产生的随机数都存在一定的差异, 因此, 在RFID读卡器读取到一组第一传感信息时, 将一个随机数作为该组第一传感信息的签名密钥, 可以使第一传感信息与签名密钥一一对应。所述签名密钥被发送至物联网系统的认证中心, 用于后续对第一传感信息真实唯一性的验证。

[0051] 为了避免签名密钥在发送至物联网系统过程中被篡改, 首先对所述签名密钥进行加密处理以生成第一密文。加密时调用预先存储的物联网系统的公钥对所述签名密钥进行加密; 所述物联网系统的公钥预先存储在所述RFID读卡器中。利用预先存储的物联网系统的公钥对所述签名密钥进行加密生成第一密文, 在发送所述第一密文到物联网系统的过程中即使所述第一密文被无权限终端获取, 由于无权限终端无法获知物联网系统的私钥, 因此, 也无法获取第一密文中的签名密钥的信息, 保证了签名密钥在信息传递过程中的安全、唯一性。

[0052] 优选地, 所述读取FRID标签的第一传感信息, 调用一组随机数作为签名密钥, 加密所述签名密钥, 得到第一密文, 具体包括:

[0053] 读取FRID标签的第一传感信息, 调用随机数发生器生产一组随机数, 将所述随机数作为签名密钥;

[0054] 调用预先存储的密钥加密所述签名密钥, 生成第一密文。

[0055] 具体地, 为了使FRID读卡器与物联网认证中心之间能够安全的进行信息传递, 首先在FRID读卡器一端建立加密系统, 在FRID读卡器读取到传感信息时, 调用加密系统中的随机数发生器产生的一组随机数, 将所述随机数作为与此次读取的第一传感信息相对应的签名密钥, 所述签名密钥用于后续对处理后的第一传感信息的验签。对于产生的签名密钥调用加密系统中预先存储的密钥对其进

行加密，生成第一密文，在后续信息传递的过程中发送所述第一密文，以确保签名密钥在信息传递过程中的安全性。

[0056] 步骤S22，调用所述FRID标签的标识，发送所述FRID标签的标识及所述第一密文到物联网系统认证中心；

[0057] 该步骤中，在对签名密钥加密生成第一密文后，调用所述FRID标签的标识，所述标识用于对所述FRID标签进行唯一标记，并在FRID标签生成时一起生成标识，将所述标识固定在FRID标签中不可改变。在生成FRID标签的标识时可以单纯的利用数字的大小排序生成FRID标签的标识，也可将FRID标签的生成时间及地点相结合生成FRID标签的标识，例如对于不同公司生产的FRID标签可以首先标注公司独有的标识，然后再标注FRID标签的生成时间，对于同一时间生成的标签可以按一定的顺序标注在公司独有的标识后面最终构成FRID标签的标识。在FRID 标签生成时即生成其标识，并将其标识固定在FRID 标签中不可改变，即形成对FRID标签的唯一标记，在将此FRID标签应用到终端设备时并将终端设备连接到物联网系统中后，即可在物联网系统中对所述终端设备进行唯一标识。该步骤中，将FRID标签的标识和第一密文发送中到物联网认证中心，以便后续物联网系统认证中心接收到与所述FRID标签信息时调用与其对应的第一密文对其进行验签。

[0058] 步骤S23，加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名；

[0059] 该步骤中，为了使FRID读卡器得到的第一传感信息能够安全的传送到物联网系统认证中心，首先在FRID读卡器端建立加密系统，对所述第一传感信息进行加密。

[0060] 优选地，所述加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名，具体包括：

[0061] 调用轻量级密码算法，加密所述传感信息成第二密文；

[0062] 调用摘要算法，通过所述摘要算法以及所述签名密钥加密所述第一传感信息以生成所述传感信息的数字签名。

[0063] 具体地，对于FRID读卡器获取的第一传感信息，调用预先存储在FRID读卡器

一端的加密系统中的轻量级密码算法对其进行加密，轻量级密码算法具有执行效率高、计算资源消耗少，适应能力强等特点，所述轻量级密码算法可以为流密码中的RC4算法或分组密码算法中的PRESENT算法等，在此不做限定；在对FRID读卡器获取的第一传感信息进行加密可对所述第一传感信息预先进行判断，若所获取的第一传感信息对于安全性要求不高，或者需要快速对其进行加密，则可以调用FRID读卡器加密系统中预先存储的流密码中的RC4算法对其进行加密，例如FRID读卡器同时获取了对个第一传感信息，需要在短时间内对其进行处理，并且所获得的第一传感信息在进行消息传递时对安全性要求一般，则既可以调用流密码中的RC4算法进行加密。若FRID读卡器获取的第一传感信息在信息传递时要求高的安全性，但对处理时间无特殊要求，则可以调用分组密码算法中的PRESENT算法进行加密运算，以保证其安全性。进一步地，调用FRID读卡器加密系统中的摘要算法从所述第一传感信息生成一个散列值，通过签名密钥对生成的散列值进行加密后生成数字签名。

[0064] 该步骤中，在对第一传感信息进行加密时，通过对获取的第一传感信息进行判断，选择合适的轻量级加密算法，可以在保证第一传感信息安全传递的前提下，提高FRID读卡器对接收到的第一传感信息的处理效率，并且在第一传感信息进行加密的同时，生成第一传感信息的数字签名，以方便后续物联网系统认证中心对接收的加密后的第一传感信息的判断和验签。

[0065] 步骤S24，发送所述FRID标签的标识、所述第二密文以及和所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第二密文和所述数字签名进行解密和验签。

[0066] 该步骤中，FRID读卡器将加密第一传感信息得到的第二密文，数字签名以及与所述第一传感信息对应的FRID标签的标识一起发送至物联网系统认证中心。在发送过程中，若FRID读卡器同时获取了多个FRID标签的第一传感信息并对其进行了处理，则按照预先设定的发送规则对多份处理后的第一传感信息进行发送。可选地，所述预先设定的发送规则可以为按所获取的第一传感信息的信号的强弱来发送处理后的第一传感信息到物联网认证中心；第一传感信息的信号较强时，在一定程度上说明其更容易被接入物联网系统，首先处理容易接入物联

网系统的终端设备，可以节约后续终端设备接入的等待时间，提高接入物联网系统的接入效率。所述预先设定的发送规则还可以为：按照FRID读卡器获取的第一传感信息的时间排序来发送处理后的第一传感信息到物联网认证中心；FRID读卡器对于第一时间获取到的某一终端设备的FRID标签上的第一传感信息，可以在获取后立即对其进行如步骤S21-步骤S23的处理，相对于后获取的终端设备的FRID标签上的第一传感信息，可以较早的发送处理后结果到物联网系统认证中心，从而减少FRID读卡器一端的处理任务积压量。当然也根据情况交替选择上述两种发送规则。具体的选择怎样的发送规则可根据实际情况进行选择，在此不做限定。该步骤中，在发送FRID标签的标识、第二密文以及数字签名到所述物联网系统认证中心时，可以根据实际情况选择发送的规则，既可以满足终端设备快速接入物联网系统的需要也可减少FRID读卡器一端待处理的第一传感信息的任务数量。

[0067] 本实施例中FRID读卡器一端设置加密系统，接收到FRID标签的第一传感信息后，调用随机数发生器中产生的一组随机数作为与FRID标签的第一传感信息相对应的签名密钥，将所述签名密钥加密后生成第一密文和所述FRID标签的标识一起发送到物联网认证中心，由于在发送前对其进行了加密保证所述签名密钥在发送过程中不被修改，并且和所述FRID标签一一对应；对于接收到的待接入物联网系统的终端设备，将从与所述终端设备对应的FRID标签中获取的第一传感信息加密生成第二密文，并生成与所述第一传感信息对应的数字签名，在发送到物联网系统认证中心进行判断时将所述FRID标签的标识、所述第二密文以及所述数字签名一起发送，以便后续物联网系统认证中心根据所述FRID标签的标识选择对应的签名密钥对所接收到的信息进行验签。此过程中在FRID读卡器一端形成加密系统，在发送第一传感信息前对第一传感信息和签名密钥分别进行加密，两次加密保证了信息的安全发送；生成第一传感信息的数字签名，方便后续对其进行验签，进一步保证了物联网系统认证中心所接收到的信息的安全性。

[0068] 实施例2

[0069] 图3示出了本发明第二实施例提供的一种终端设备安全接入物联网的方法的流

程图，如图3所示的所述方法包括：

- [0070] 步骤S31，读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，加密所述签名密钥，得到第一密文；
- [0071] 步骤S32，调用所述FRID标签的标识，发送所述标识及所述第一密文到物联网系统认证中心；
- [0072] 步骤S33，加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名；
- [0073] 步骤S34，发送所述FRID标签的标识、所述第二密文以及和所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第二密文和所述数字签名进行解密和验签；
- [0074] 其中，步骤31- 34与实施例一中步骤21- 24分别相对应，在此不再赘述。
- [0075] 步骤S35，接收物联网系统认证中心发送的授权接入信息，根据所述授权接入信息连接FRID标签所属的终端设备到物联网系统。
- [0076] 该步骤中，在物联网系统认证中心对所接收到信息认证通过后，即发送授权终端设备接入物联网系统的授权接入信息，FRID读卡器接收到所述授权接入信息后调用与所述授权接入信息对应的FRID标签的标识，通过所述FRID标签的标识选择并确认相应的终端设备的接入。通过FRID标签的标识对待接入物联网系统认证中心的终端设备进行确认，减少了错误接入的概率。
- [0077] 实施例3
- [0078] 图4为实施例三中提供的终端设备安全接入物联网的方法的流程图，其中：
- [0079] 步骤S41，物联网系统认证中心接收并存储所述FRID读卡器发送的FRID标签的标识和第一密文；并接收所述FRID读卡器发送的第二密文及数字签名；
- [0080] 该步骤中，物联网系统认证中心接收所述FRID读卡器发送的FRID标签的标识和第一密文，并将所述FRID标签的标识和第一密文存储在存储器内，在对所述FRID标签的标识和第一密文进行存储时，分析所述FRID标签的标识，按照所述FRID标签的标识的不同类别分类进行存储。例如同一个地区终端设备上所附着的标签根据FRID标签的标识的生产厂家不同将其分类存储，或者按照FRID标签所附着的设备进行分类；具体对物联网系统认证中心接收到的处理后的第一传感信

信息的分类存储方法不做限定。将FRID标签的标识有助于快速的找到要调用的FRID标签的标识，进而快速调用与之对应的签名密钥。

[0081] 步骤S42，物联网系统认证中心解密所述第一密文得到签名密钥，并解密所述第二密文得到第一传感信息；

[0082] 具体地，物联网认证中心解密接收到的第一密文和第二密文，分别得到签名密钥和第一传感信息，在解密前首先调用与第一密文一起存储在物联网系统认证中心的FRID标签的标识和与第二密文一起发送到物联网系统认证中心的FRID标签的标识，对比二者是否一致，在二者一致时，说明要解密的第一密文和第二密文同属于一个FRID标签的信息。然后再对同属于一个FRID标签的第一密文和第二密文进行解密。

[0083] 步骤S43，物联网系统认证中心通过所述第一传感信息和所述签名密钥对所述数字签名进行验签，得到验签结果，并根据所述验签结果判断是否发送授权接入信息到所述FRID读卡器。

[0084] 具体地，解密得到第一传感信息和签名密钥后，调用预先存储在物联网系统认证中心的摘要算法计算出所述第一传感信息的一组散列值，为清楚的描述这里称所述散列值为第一散列值；通过所述签名密钥对所述数字签名进行验签同样得出一组散列值，称其为第二散列值；对比第一散列值与第二散列值是否相同，在二者相同时，说明与第二散列值对应的数字签名是由与第一散列值对应的第一传感信息生成的，并且所述第一传感信息在传递过程中未被篡改，从而完成对所述数字签名的验签。在所述第一传感信息未被篡改时，生成授权与所述第一传感信息对应的FRID标签接入物联网系统的授权接入指令，并发送所述授权接入指令到FRID读卡器，以保证所述FRID标签安全的接入物联网系统。

[0085] 本发明实施例中物联网系统中心对接收到的第一密文、第二密文以及数字签名分别进行解密和验签，解密时首先判断第一密文和第二密文是否同属于一个FRID标签的信息，然后再进行解密，保证了解密后的签名密钥和第一传感信息相对应；由于数字签名代表了文件的特征，文件如果发生改变，数字签名也将发生变化，因此通过对数字签名的验签，既保证了数字签名和第一传感信息来自同一FRID标签，又能确保所述接受的第一传感信息的完整性和原始性。从而再

次确认了第一传感信息传递过程的安全性。

[0086] 实施例4

[0087] 图5示出了上述终端设备安全接入物联网系统的一种信息交互图，详述如下：

[0088] 在步骤S51中，FRID读卡器获取FRID标签中的第一传感信息，并调用一组随机数作为签名密钥；

[0089] 在本发明实施例中FRID读卡器对于要接入物联网系统的终端设备通过扫描或感知FRID标签获取第一传感信息，然后从FRID读卡器中的随机数发生器中获取一组随机数作为与所获取的第一传感信息对应的签名密钥。

[0090] 在步骤S52中，FRID读卡器加密所述签名密钥得到第一密文，并调用FRID标签的标识；

[0091] 本发明实施例中FRID读卡器通过预先存储的密钥对所述签名密钥进行加密得到第一密文，以保证签名密钥在信息传递过程中的安全性；然后调用FRID标签的标识，所述FRID标签的标识用于对FRID标签进行唯一标记。

[0092] 在步骤S53中，FRID读卡器发送所述FRID标签和所述第一密文到物联网系统认证中心；

[0093] FRID读卡器与物联网系统认证中心通过无线连接，可选地，上述无线连接可以为基于红外、蓝牙、无线保真（Wireless-Fidelity，Wi-Fi）、紫蜂协议（Zigbee）或者啁啾协议的连接，其中，上述啁啾协议是一种轻量级的物联网协议，基于上述啁啾协议传播的数据为啁啾数据，上述啁啾数据仅包含最小的开销负载、传输指向箭头、简单的非唯一性地址以及合适的校验和，是一种轻量级的、传播广泛的数据包。当然，FRID读卡器也可以通过其它方式与物联网系统认证中心连接，此处不作限定。

[0094] 在步骤S54中，物联网系统认证中心接收并存储所述FRID标签的标识和所述第一密文；

[0095] 在步骤S55中，FRID读卡器对所述第一传感信息进行加密得到第二密文，并生成所述第一传感信息的数字签名；

[0096] 本实施例中FRID读卡器对所获取的第一传感信息首先进行加密得到第二密文，并获取所述第一传感信息的数字签名，其中所述第一传感信息由FRID读卡器通

过扫描或感知FRID标签获取。具体加密过程可参照上述步骤S23的实现过程，此处不再赘述。

[0097] 在步骤S56中，FRID读卡器发送所述FRID标签、所述第二密文和所述数字签名到物联网系统认证中心；该步骤中信息传递过程参照上述步骤53的实现过程，不再赘述。

[0098] 在步骤S57中，物联网认证中心解密所存储的第一密文，并对接收到的第二密文和数字签名进行解密和验签；在验签通过时生成授权接入信息；

[0099] 本发明实施例中，物联网系统认证中心首先解密第一密文得到签名密钥，然后解密第二密文得到第一传感信息，通过所得到的第一签名密钥和第一传感信息对数字签名进行验签，以确认第一传感信息的原始性。在对所述数字签名验签通过时，生成授权终端设备接入物联网认证中心的授权接入信息。

[0100] 在步骤S58中，物联网系统认证中心发送授权接入信息到FRID读卡器；

[0101] 在步骤S59中，FRID读卡器根据所接收到的授权接入信息，连接终端设备到物联网系统。

[0102] 由此可见，本发明实施例中，通过在FRID读卡器端对所获取的第一传感和签名密钥分别进行加密，并得到第一传感信息的签名密钥，然后将加密后的信息及数字签名发送到物联网系统认证中心，再由物联网系统认证中心进行两次解密和对数字签名的验签，比包括FRID读卡器对获取的第一传感信息进行信息传递时的安全性，保证终端设备安全接入物联网系统。

[0103] 应理解，在本发明实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0104] 实施例5

[0105] 图6示出了本发明第五实施例提供一种终端设备安全接入物联网的系统的结构框图，为了便于说明，仅示出了与本发明实施例相关的部分。

[0106] 如图6所示，所述一种终端设备安全接入物联网系统的系统包括：FRID读卡器61、物联网系统认证中心62，其中所述FRID读卡器包括：第一加密单元611，第一发送单元612，第二加密单元613，第二发送单元614，其中：

- [0107] 第一加密单元611，用于读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，加密所述签名密钥，得到第一密文；
- [0108] 优选地，所述第一加密单元612，具体包括：
- [0109] 签名密钥生成模块，用于读取FRID标签的第一传感信息，调用随机数发生器生产一组随机数，将所述随机数作为签名密钥；
- [0110] 签名密钥加密模块，用于调用预先存储的密钥加密所述签名密钥，生成第一密文。
- [0111] 第一发送单元612，用于调用所述FRID标签的标识，发送所述FRID标签的标识及所述第一密文到物联网系统认证中心；
- [0112] 第二加密单元613，用于加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名；
- [0113] 优选地，所述第二加密单元613，具体包括：
- [0114] 第二密文生成模块，用于调用轻量级密码算法，加密所述第一传感信息成第二密文；
- [0115] 数字签名生成模块，用于调用摘要算法，通过所述摘要算法以及所述签名密钥生成所述第一传感信息的数字签名。
- [0116] 第二发送单元614，用于发送所述第二密文以及所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第一密文、第二密文和所述数字签名进行解密和验签。
- [0117] 可选的，所述FRID读卡器，还包括：
- [0118] 终端设备接入单元，用于接收物联网系统认证中心发送的授权接入信息，根据所述授权接入信息连接FRID标签所属的终端设备到物联网系统。
- [0119] 所述物联网系统认证中心包括：接收单元621、解密单元622、授权接入信息生成单元623，其中：
- [0120] 接收单元621，用于接收并存储所述FRID读卡器发送的FRID标签的标识和第一密文；并接收所述FRID读卡器发送的第二密文及数字签名；
- [0121] 解密单元622，用于解密所述第一密文得到签名密钥，解密所述第二密文得到第一传感信息；

- [0122] 授权接入信息生成单元623，用于通过所述第一传感信息和所述签名密钥对所述数字签名进行验签，得到验签结果；根据所述验签结果判断是否发送授权接入信息到所述FRID读卡器。
- [0123] 本发明实施例中物联网系统中心对接收到的第一密文、第二密文以及数字签名分别进行解密和验签，解密时首先判断第一密文和第二密文是否同属于一个FRID标签的信息，然后再进行解密，保证了解密后的签名密钥和第一传感信息相对应；由于数字签名代表了文件的特征，文件如果发生改变，数字签名也将发生变化，因此通过对数字签名的验签，既保证了数字签名和第一传感信息来自同一FRID标签，又能确保所述接受的第一传感信息的完整性和原始性。从而再次确认了第一传感信息传递过程的安全性。
- [0124] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。
- [0125] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。
- [0126] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。
- [0127] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。
- [0128] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案

本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

[0129] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

权利要求书

- [权利要求 1] 一种终端设备安全接入物联网的方法，其特征在于，所述终端设备安全接入物联网的方法包括：
- 读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，加密所述签名密钥，得到第一密文；
- 调用所述FRID标签的标识，发送所述FRID标签的标识及所述第一密文到物联网系统认证中心；
- 加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名；
- 发送所述第二密文以及所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第一密文、第二密文和所述数字签名进行解密和验签。
- [权利要求 2] 根据权利要求1所述的终端设备安全接入物联网的方法，其特征在于，所述读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，加密所述签名密钥，得到第一密文，具体包括：
- 读取FRID标签的第一传感信息，调用随机数发生器生产一组随机数，将所述随机数作为签名密钥；
- 调用预先存储的密钥加密所述签名密钥，生成第一密文。
- [权利要求 3] 根据权利要求1所述的终端设备安全接入物联网的方法，其特征在于，所述加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名，具体包括：
- 调用轻量级密码算法，加密所述第一传感信息成第二密文；
- 调用摘要算法，通过所述摘要算法以及所述签名密钥生成所述第一传感信息的数字签名。
- [权利要求 4] 根据权利要求1-3任一项所述的终端设备安全接入物联网的方法，其特征在于，在所述发送所述第二密文以及所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第一密文、第二密文和所述数字签名进行解密和验签之后，还包括：

接收物联网系统认证中心发送的授权接入信息，根据所述授权接入信息连接FRID标签所属的终端设备到物联网。

[权利要求 5]

根据权利要求4所述的终端设备安全接入物联网的方法，其特征在于，所述终端设备安全接入物联网的方法还包括：

物联网系统认证中心接收并存储所述FRID读卡器发送的FRID标签的标识和第一密文；并接收所述FRID读卡器发送的第二密文及数字签名；

物联网系统认证中心解密所述第一密文得到签名密钥，并解密所述第二密文得到第一传感信息；

物联网系统认证中心通过所述第一传感信息和所述签名密钥对所述数字签名进行验签，得到验签结果，并根据所述验签结果判断是否发送授权接入信息到所述FRID读卡器。

[权利要求 6]

一种终端设备安全接入物联网的系统，其特征在于，所述终端设备安全接入物联网的系统包括：FRID读卡器、物联网系统认证中心，其中所述FRID读卡器包括：

第一加密单元，用于读取FRID标签的第一传感信息，调用一组随机数作为签名密钥，加密所述签名密钥，得到第一密文；

第一发送单元，用于调用所述FRID标签的标识，发送所述FRID标签的标识及所述第一密文到物联网系统认证中心；

第二加密单元，用于加密所述第一传感信息，得到第二密文，并生成所述第一传感信息的数字签名；

第二发送单元，用于发送所述第二密文以及所述数字签名到所述物联网系统认证中心，以使所述物联网系统认证中心对所述第一密文、第二密文和所述数字签名进行解密和验签。

[权利要求 7]

根据权利要求6所述的终端设备安全接入物联网的系统，其特征在于，所述第一加密单元具体包括：

签名密钥生成模块，用于读取FRID标签的第一传感信息，调用随机数发生器生产一组随机数，将所述随机数作为签名密钥；

签名密钥加密模块，用于调用预先存储的密钥加密所述签名密钥，生成第一密文。

[权利要求 8] 根据权利要求6所述的终端设备安全接入物联网的系统，其特征在于，所述第二加密单元具体包括：
第二密文生成模块，用于调用轻量级密码算法，加密所述第一传感信息成第二密文；
数字签名生成模块，用于调用摘要算法，通过所述摘要算法以及所述签名密钥生成所述第一传感信息的数字签名。

[权利要求 9] 根据权利要求6-8任一项所述的终端设备安全接入物联网的系统，其特征在于，所述FRID读卡器还包括：
终端设备接入单元，用于接收物联网系统认证中心发送的授权接入信息，根据所述授权接入信息连接FRID标签所属的终端设备到物联网。

[权利要求 10] 一种物联网系统认证中心，其特征在于，所述物联网系统认证中心包括：
接收单元，用于接收并存储所述FRID读卡器发送的FRID标签的标识和第一密文；并接收所述FRID读卡器发送的第二密文及数字签名；
解密单元，用于解密所述第一密文得到签名密钥，解密所述第二密文得到第一传感信息；
授权接入信息生成单元，用于通过所述第一传感信息和所述签名密钥对所述数字签名进行验签，得到验签结果；根据所述验签结果判断是否发送授权接入信息到所述FRID读卡器。

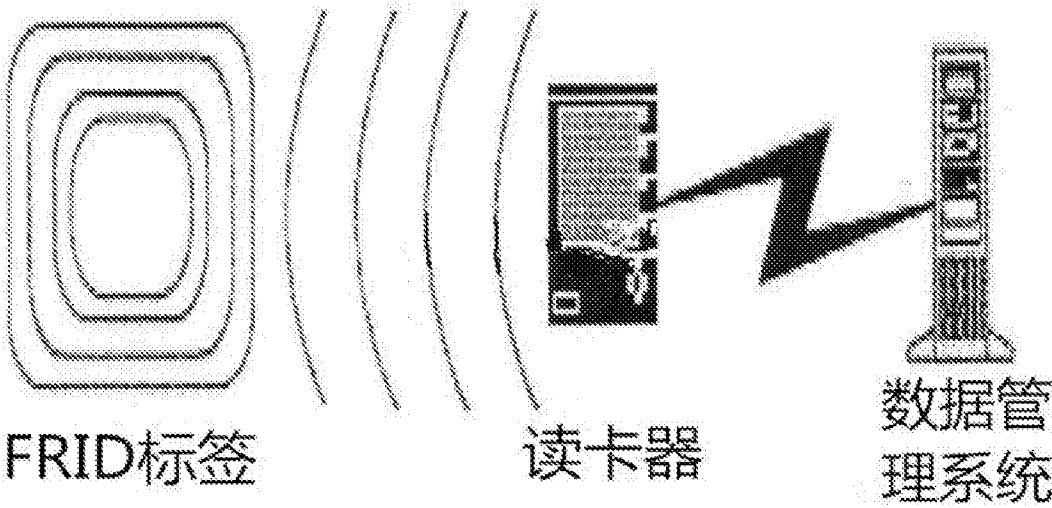


图 1

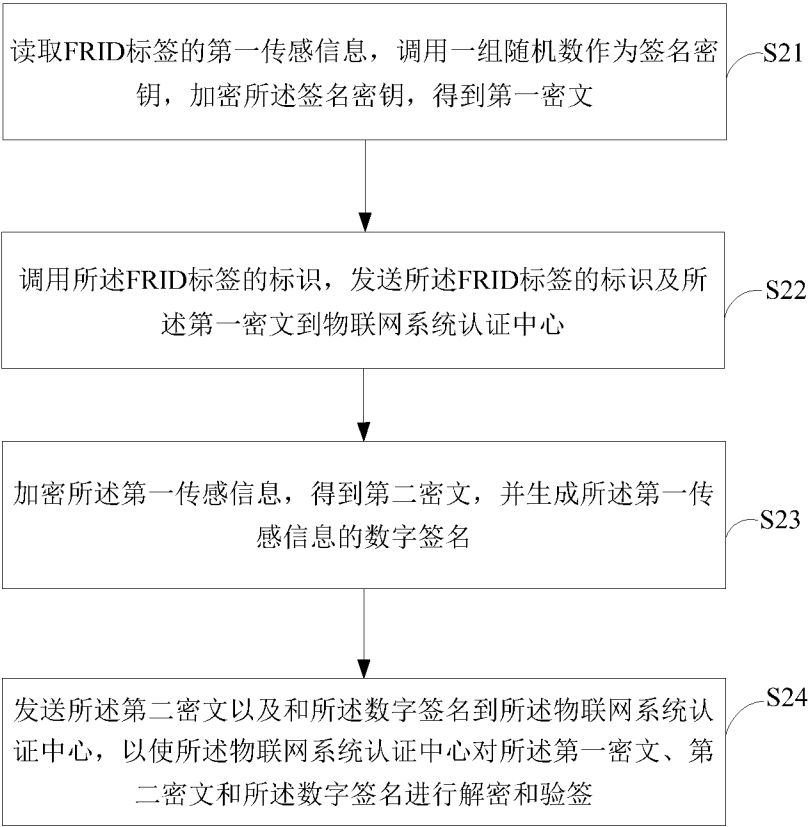


图 2

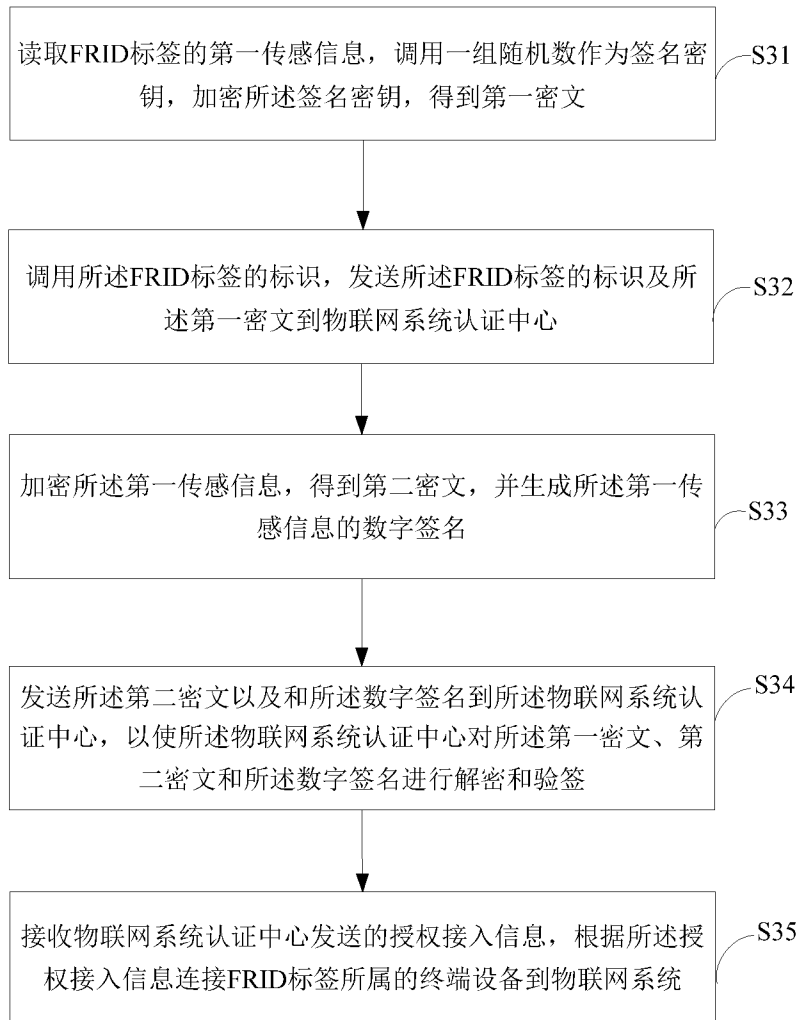


图 3

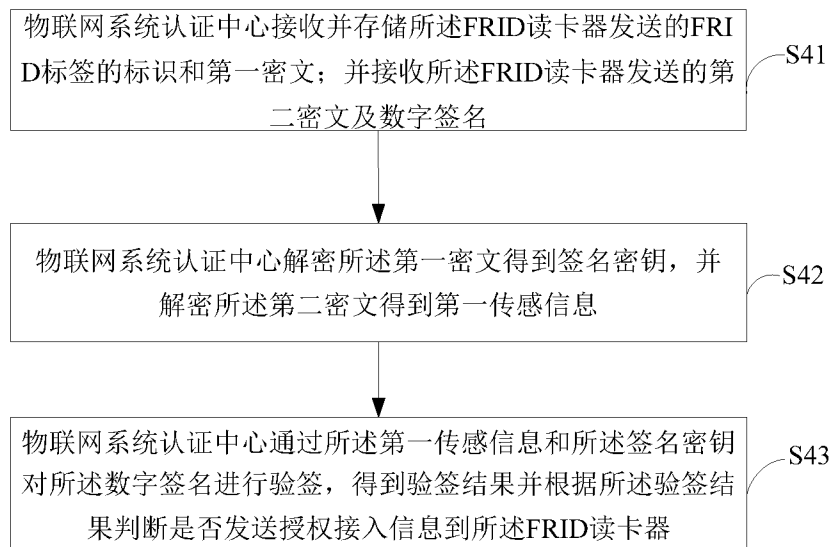


图 4



图 5

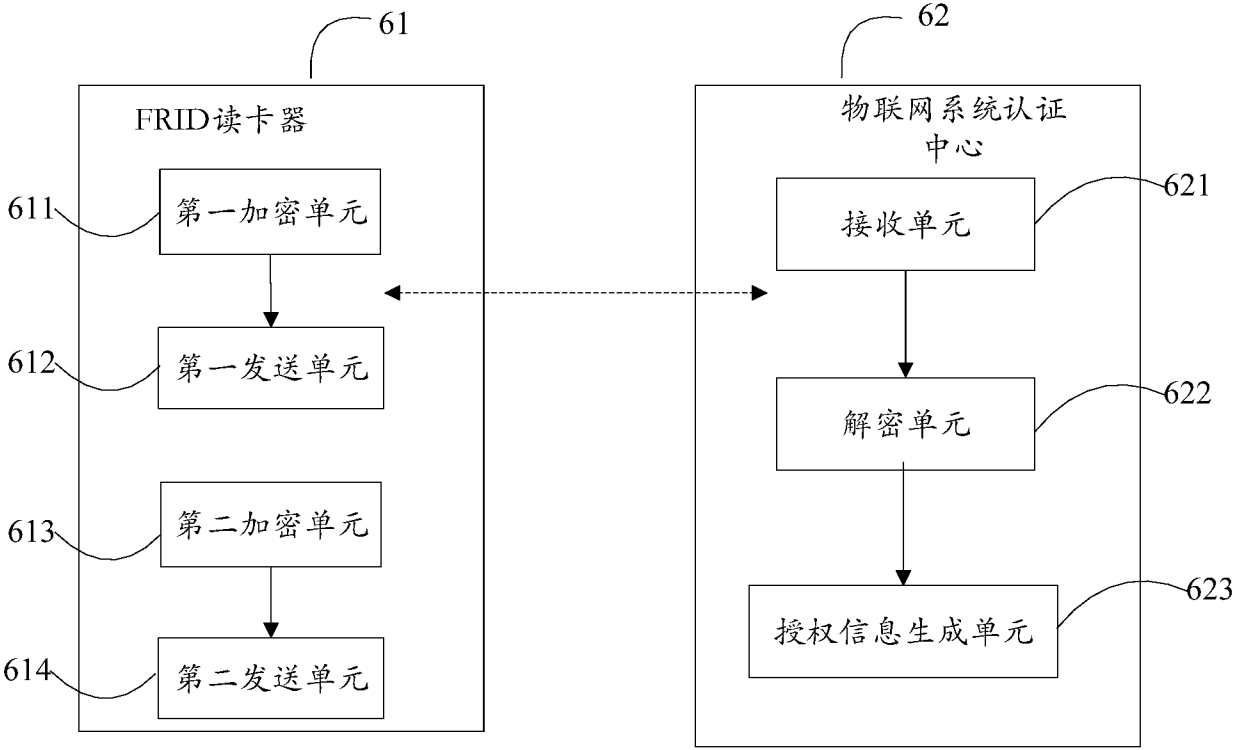


图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/093224

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i; H04L 9/32 (2006.01) i; 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)

WPI; EPODOC; CNPAT; CNKI: 物联网, 密文, 密钥, 加密, 签名, 随机数, 验证, 认证, 安全, 接入授权, 授权接入, 入网, 传感信息, 序列号, ID, 标识, 读卡器, RFID 标签, RFID, 服务器, 中心, access+, internet of things, label, sensor, information, cryptograph+, encrypt+, key, authentication, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	胡祥义等, “基于轻量级加密技术建立物联网感知层信息安全的解决方案”, “网络安全技术与应用”, 31 December 2013 (31.12.2013), number 3, 2.2 Digital Signature Protocol in the Perception Layer, (HU, Xiangyi et al., The Perception Layer Information Security Scheme for Internet of Things Based on Lightweight Cryptography, “Network Security Technology & Application”)	1-10
X	CN 103237302 A (BEIJING INSTITUTE OF SCIENCE AND TECHNOLOGY INFORMATION), 07 August 2013 (07.08.2013), description, paragraphs [0003]-[0009]	1-10
A	CN 102833260 A (HU, Xiangyi), 19 December 2012 (19.12.2012), entire document	
A	CN 102801722 A (WORLD OF THINGS, FUJIAN INFORMATION TECHNOLOGY CO., LTD.), 28 November 2012 (28.11.2012), entire document	1-10
A	US 2016352732 A1 (MASSACHUSETTS INSTITUTE OF TECHNOLOGY), 01 December 2016 (01.12.2016), entire document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 07 February 2018	Date of mailing of the international search report 24 February 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 ZHANG, Huajing Telephone No. (86-10) 62413324

International application No.
PCT/CN2017/093224

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 H04L 9/08(2006.01)i; H04L 9/32(2006.01)i; 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)) WPI;EPDOC;CNPAT;CNKI: 物联网, 密文, 密钥, 加密, 签名, 随机数, 验证, 认证, 安全, 接入授权, 授权接入, 入网, 传感信息, 序列号, ID, 标识, 读卡器, RFID标签, RFID, 服务器, 中心, access+, internet of things, label, sensor, information, cryptograph+, encrypt+, key, authentication, security																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>胡祥义等. “基于轻量级加密技术建立物联网感知层信息安全的解决方案” 《网络安全技术与应用》, 第3期, 2013年 12月 31日 (2013 - 12 - 31), 2.2感知层数字签名协议</td> <td>1-10</td> </tr> <tr> <td>X</td> <td>CN 103237302 A (北京市科学技术情报研究所) 2013年 8月 7日 (2013 - 08 - 07) 说明书第[0003]-[0009]段</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 102833260 A (胡祥义) 2012年 12月 19日 (2012 - 12 - 19) 全文</td> <td></td> </tr> <tr> <td>A</td> <td>CN 102801722 A (福建物联天下信息科技有限公司) 2012年 11月 28日 (2012 - 11 - 28) 全文</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>US 2016352732 A1 (MASSACHUSETTS INSTITUTE OF TECHNOLOGY) 2016年 12月 1日 (2016 - 12 - 01) 全文</td> <td>1-10</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	胡祥义等. “基于轻量级加密技术建立物联网感知层信息安全的解决方案” 《网络安全技术与应用》, 第3期, 2013年 12月 31日 (2013 - 12 - 31), 2.2感知层数字签名协议	1-10	X	CN 103237302 A (北京市科学技术情报研究所) 2013年 8月 7日 (2013 - 08 - 07) 说明书第[0003]-[0009]段	1-10	A	CN 102833260 A (胡祥义) 2012年 12月 19日 (2012 - 12 - 19) 全文		A	CN 102801722 A (福建物联天下信息科技有限公司) 2012年 11月 28日 (2012 - 11 - 28) 全文	1-10	A	US 2016352732 A1 (MASSACHUSETTS INSTITUTE OF TECHNOLOGY) 2016年 12月 1日 (2016 - 12 - 01) 全文	1-10
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
X	胡祥义等. “基于轻量级加密技术建立物联网感知层信息安全的解决方案” 《网络安全技术与应用》, 第3期, 2013年 12月 31日 (2013 - 12 - 31), 2.2感知层数字签名协议	1-10																		
X	CN 103237302 A (北京市科学技术情报研究所) 2013年 8月 7日 (2013 - 08 - 07) 说明书第[0003]-[0009]段	1-10																		
A	CN 102833260 A (胡祥义) 2012年 12月 19日 (2012 - 12 - 19) 全文																			
A	CN 102801722 A (福建物联天下信息科技有限公司) 2012年 11月 28日 (2012 - 11 - 28) 全文	1-10																		
A	US 2016352732 A1 (MASSACHUSETTS INSTITUTE OF TECHNOLOGY) 2016年 12月 1日 (2016 - 12 - 01) 全文	1-10																		
☐ 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 2018年 2月 7日		国际检索报告邮寄日期 2018年 2月 24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 张华晶 电话号码 (86-10)62413324																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/093224

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	103237302	A	2013年 8月 7日	无	
CN	102833260	A	2012年 12月 19日	无	
CN	102801722	A	2012年 11月 28日	无	
US	2016352732	A1	2016年 12月 1日	无	