(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
2016 年 10 月 20 日 (20.10.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/165165 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2015/078021

(22) 国际申请日: 2015 年 4 月 30 日 (30.04.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510184781.9 2015 年 4 月 17 日 (17.04.2015) CN

(71) 申请人: **宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.)** [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(72) 发明人: **钟焰涛 (ZHONG, Yantao)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 **傅文治 (FU, Wenzhi)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 **蒋罗 (JIANG, Luo)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(74) 代理人: **广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO.. LTD)**; 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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。

[见续页]

(54) Title: DEVICE ACCESS PROCESSING METHOD, DEVICE ACCESS PROCESSING APPARATUS AND TERMINAL

(54) 发明名称 : 设备接入的处理方法、设备接入的处理装置和终端

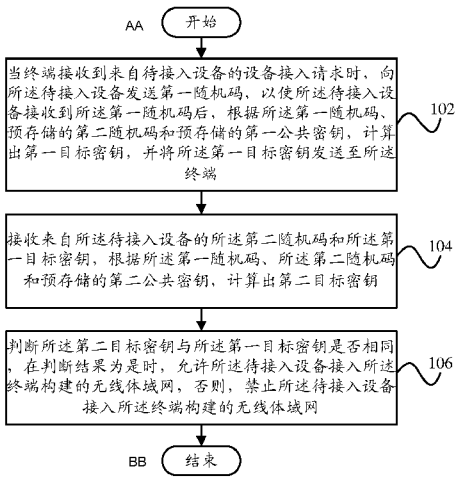

图 1

102 Send, when a terminal receives a device access request from a device to be accessed, a first random code to the device to be accessed, such that the device to be accessed calculates, after receiving the first random code, a first target key according to the first random code, a pre-stored second random code and a pre-stored first public key, and sends the first target key to the terminal

104 Receive the second random code and the first target key from the device to be accessed, and calculate, according to the first random code, the second random code and a pre-stored second public key, a second target key

106 Judge whether the second target key is the same as the first target key, allow, when a judgment result is yes, the device to be accessed to access a wireless body area network constructed by the terminal, and inhibit, otherwise, from accessing the device, to be accessed, to the wireless body area network constructed by the terminal

AA Start

BB End

(57) **Abstract**: The present invention provides a device access processing method, a processing apparatus and a terminal. The processing method comprises: a terminal sends, when receiving a device access request from a device to be accessed, a first random code to the device to be accessed, and the device to be accessed calculates, after receiving the first random code, a first target key according to the first random code, a pre-stored second random code and a pre-stored first public key, and sends the first target key to the terminal; receive the second random code and the first target key from the device to be accessed, and calculate, according to the first random code, the second random code and a pre-stored second public key, a second target key; and judge whether the second target key is the same as the first target key, allow, if so, the device to be accessed to access a wireless body area network, and inhibit, otherwise, from accessing to the wireless body area network. The technical solution of the present invention is general, low in calculation quantity and capable of efficiently performing security certification on an access device in a wireless body area network.

(57) **摘要**: 本发明提出了一种设备接入的处理方法、一种处理装置和一种终端，其中，处理方法包括：终端接收到来自待接入设备的设备接入请求时，向待接入设备发送第一随机码，待接入设备接收到第一随机码后，根据第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将第一目标密钥发送至终端；接收来自待接入设备的第二随机码和第一目标密钥，根据第一随机码、第二随机码和预存储的第二公共密钥，计算出第二目标密钥；判断第二目标密钥与第一目标密钥是否相同，若是，允许待接入设备接入无线体域网，否则，禁止接入无线体域网。本发明的技术方案通用、计算量低、且能高效地对无线体域网中的接入设备进行安全认证。

WO 2016/165165 A1

(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))。

设备接入的处理方法、设备接入的处理装置和终端

本申请要求于2015年04月17日提交中国专利局，申请号为CN 201510184781.9、发明名称为“设备接入的处理方法、设备接入的处理装置和终端”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

本发明涉及终端接入认证技术领域，具体而言，涉及一种设备接入的处理方法，一种设备接入的处理装置和一种终端。

背景技术

WBAN（Wireless Body Area Network，无线体域网）是以人体为中心的短距离无线网络，具体地说，它是附着在人体上的一种网络，由一套小巧可移动、具有通信功能的传感器和一个身体主站组成。作为一种新兴的技术，无线体域网在医疗、保健、消费类电子等领域有着非常广阔的应用前景。为了防止恶意结点接入WBAN进而对WBAN进行攻击破坏，必须对接入WBAN的设备进行认证。目前，现有技术方案中，主要有三种认证方法：

1）一种认证方法是：WBAN身体主体（如终端）与外部接入设备（如传感器）进行双向身份认证，但该双向身份认证过程中涉及到加解密操作，且加解密操作所需的计算量非常大，在计算能力有限的移动设备和可穿戴设备上实现会造成较大的延迟。

2）另一种认证方法是：通过传感器采集一定时长的心电信号后，通过检测信号特征点，截取一段包含完整生理信号周期信息的稳定波形，生成模板T，模板 T 在设备与身体主站（移动终端）之间安全共享，传感器可以通过安全的超短距离传输技术将模板 T 安全传送给移动终端，移动终端存储模板 T，并注册用户以进行身份识别。该方法依赖于采集心电信号的传感器，适用于医疗设备组网，普通用户（非医疗WBAN用户）无法使用。

3）最后一种认证方法是：将体域网看成一个整体，每个传感器节点和控

制单元都视作一个天线，从而利用不同天线的接收信号强度差异探测待认证节点的距离是否足够近，基于近距离可信原则对待认证节点进行认证。但是，该方法是通过信号强度确定待接入节点足够靠近 WBAN，从而对其认证，没有考虑攻击者可能在WBAN用户身边（如，座位前后）放置恶意攻击节点。

上述三种认证方法在一定条件下实现了 WBAN 与接入设备间的认证，但各有自己的缺陷：或认证操作比较繁琐，或局限性的，或安全性不够。

因此，如何提高无线体域网的接入认证方法的通用性，且在降低接入认证计算量的同时，对无线体域网中接入设备进行高效、安全的认证，成为亟待解决的问题。

发明内容

本发明正是基于上述问题，提出了一种新的设备接入的处理方案，该方案通用、计算量低、且能高效地对无线体域网中的接入设备进行安全认证。

有鉴于此，本发明的一方面提出了一种设备接入的处理方法，包括：当终端接收到来自待接入设备的设备接入请求时，向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端；接收来自所述待接入设备的所述第二随机码和所述第一目标密钥，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥；判断所述第二目标密钥与所述第一目标密钥是否相同，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

在该技术方案中，通过向待接入设备发送一个第一随机码，可以使待接入设备根据第一随机码、预存储的第二随机码和第一公开密钥，按照自身的加密算法计算出一个第一目标密钥，并将第一目标密钥发送至终端，这样，终端就可以根据第一随机码、预存储的第二随机码和第二公开密钥，按照自身的算法计算出一个第二目标密码，并与所接收到的第一目标密钥进行比对，以根据判断结果判断该待接入设备是否为终端允许接入的合法

设备，若是，则允许该待接入设备接入终端构建的无线体域网，否则，说明该待接入设备是非法设备，会对无线体域网的安全性带来威胁，则禁止该待接入设备接入终端构建的无线体域网，从而实现通过简单的、计算量较低的加密算法就可以高效地完成对待接入设备进入无线体域网的安全认证，可以有效地避免非法待接入设备接入终端构建的无线体域网而对该无线体域网造成破坏。

在上述技术方案中，优选地，在允许所述待接入设备接入所述终端构建的无线体域网之后，根据所述第二随机码和所述第二公共密钥，计算出第三目标密钥；将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送接入所述无线体域网的确认信息，否则，不发送接入所述无线体域网的确认信息。

在该技术方案中，在终端根据第二随机码和第二公共密钥，计算出第三目标密钥后，可以将第三目标密钥传送至待接入设备，以使待接入设备根据第二随机码和第一公开密钥，计算出第四目标密钥后，将第四目标密钥与接收到的第三目标密钥进行比对，若比较结果为第三目标密钥与第四目标密钥相同，则待接入设备就会再次确认接入了正确的无线体域网，就会向终端发送确认信息，以完成接入，当然，当判断结果为第三目标密钥与第四目标密钥不相同时，说明待接入设备有可能误接入了错误的无线体域网，也即目前终端所构建的无线体域网并不是待接入设备真正需要接入的无线体域网，则该待接入设备就不会向终端发送确认信息，也不会接入该无线体域网，通过上述过程，可以实现待接入设备的接入认证过程的双向认证，提高待接入设备接入过程的准确性，这样不仅可以防止非法待接入设备接入当前终端构建的无线体域网，提高无线体域网接入安全性，又可以防止待接入设备误接入错误的无线体域网，从而提高待接入设备接入过程的准确性，当然，由于该双向认证过程不需要对待接入设备的类型进行限定，因此，该双向认证方法具有很高的通用性，适用于对各种类型的待接入设备进行安全认证。

在上述技术方案中，优选地，还包括：当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

在该技术方案中，通过向终端和终端允许接入的合法待接入设备预置相同的第一公共密钥和所述第二公共密钥，以及控制他们使用相同的加密算法，可以确保在待接入设备接入终端构建的无线体域网的过程中，唯有合法的待接入设备才能计算出与终端相同的目标密钥，进而顺利地通过无线体域网的接入安全认证，而非法待接入设备由于并不具备与终端相同的加密计算中不可以缺少的公共密钥，更不具备与终端相同的加密算法，因此，不可能计算出与终端相同的目标密钥，从而无法顺利地通过无线体域网的接入安全认证，无法接入终端构建的无线体域网，这样就可以实现最大程度地确保待接入设备接入无线体域网的安全性。其中，第一公开密钥和第二公开密钥包括但不限于：用户设定的口令、密码等。用以获得目标密钥的计算方法优选地采用密码学哈希函数。

在上述技术方案中，优选地，还包括：当所述终端允许或禁止所述待接入设备接入所述无线体域网时，发出提示信号；以及当所述待接入设备接入所述无线体域网后，所述终端与所述待接入设备通过 WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式通信。

在该技术方案中，通过向用户发送提示信息，使得用户了解当前待接入设备的接入状态，以对待接入设备的接入状态进行有效的监控。当然，还可以根据接入设备和终端当前所处的环境，为终端和接入设备选择更为便捷的通信方式，如 WIFI、蓝牙、红外、NFC、有线网络、无线网络等。

在上述技术中，优选地，上述任一项技术方案中的设备接入的处理方法，所述待接入设备包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

在该技术方案中，待接入设备包括但不限于普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备，所有可以通过无线体域网与终端进行通

信，以提高用户便利性的设备均可。

本发明的另一方面提出了一种设备接入的处理装置，包括：发送单元，当终端接收到来自待接入设备的设备接入请求时，向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端；接收单元，接收来自所述待接入设备的所述第二随机码和所述第一目标密钥；计算单元，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥；判断单元，判断所述第二目标密钥与所述第一目标密钥是否相同；处理单元，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

在该技术方案中，通过向待接入设备发送一个第一随机码，可以使待接入设备根据第一随机码、预存储的第二随机码和第一公开密钥，按照自身的加密算法计算出一个第一目标密钥，并将第一目标密钥发送至终端，这样，终端就可以根据第一随机码、预存储的第二随机码和第二公开密钥，按照自身的算法计算出一个第二目标密码，并与所接收到的第一目标密钥进行比对，以根据判断结果判断该待接入设备是否为终端允许接入的合法设备，若是，则允许该待接入设备接入终端构建的无线体域网，否则，说明该待接入设备是非法设备，会对无线体域网的安全性带来威胁，则禁止该待接入设备接入终端构建的无线体域网，从而实现通过简单的、计算量较低的加密算法就可以高效地完成对待接入设备进入无线体域网的安全认证，可以有效地避免非法待接入设备接入终端构建的无线体域网而对该无线体域网造成破坏。

在上述技术方案中，优选地，所述计算单元还用于：在允许所述待接入设备接入所述终端构建的无线体域网之后，根据所述第二随机码和所述第二公共密钥，计算出第三目标密钥；所述发送单元还用于：将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送

接入所述无线体域网的确认信息，否则，不发送接入所述无线体域网的确认信息。

在该技术方案中，在终端根据第二随机码和第二公共密钥，计算出第三目标密钥后，可以将第三目标密钥传送至待接入设备，以使待接入设备根据第二随机码和第一公开密钥，计算出第四目标密钥后，将第四目标密钥与接收到的第三目标密钥进行比对，若比较结果为第三目标密钥与第四目标密钥相同，则待接入设备就会再次确认接入了正确的无线体域网，就会向终端发送确认信息，以完成接入，当然，当判断结果为第三目标密钥与第四目标密钥不相同时，说明待接入设备有可能误接入了错误的无线体域网，也即目前终端所构建的无线体域网并不是待接入设备真正需要接入的无线体域网，则该待接入设备就不会向终端发送确认信息，也不会接入该无线体域网，通过上述过程，可以实现待接入设备的接入认证过程的双向认证，提高待接入设备接入过程的准确性，这样不仅可以防止非法待接入设备接入当前终端构建的无线体域网，提高无线体域网接入安全性，又可以防止待接入设备误接入错误的无线体域网，从而提高待接入设备接入过程的准确性，当然，由于该双向认证过程不需要对待接入设备的类型进行限定，因此，该双向认证方法具有很高的通用性，适用于对各种类型的待接入设备进行安全认证。

在上述技术方案中，优选地，还包括：当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

在该技术方案中，通过向终端和终端允许接入的合法待接入设备预置相同的第一公共密钥和所述第二公共密钥，以及控制他们使用相同的加密算法，可以确保在待接入设备接入终端构建的无线体域网的过程中，唯有合法的待接入设备才能计算出与终端相同的目标密钥，进而顺利地通过无线体域网的接入安全认证，而非法待接入设备由于并不具备与终端相同的加密计算中不可以缺少的公共密钥，更不具备与终端相同的加密算法，因

此，不可能计算出与终端相同的目标密钥，从而无法顺利地通过无线体域网的接入安全认证，无法接入终端构建的无线体域网，这样就可以实现最大程度地确保待接入设备接入无线体域网的安全性。其中，第一公开密钥和第二公开密钥包括但不限于：用户设定的口令、密码等。用以获得目标密钥的计算方法优选地采用密码学哈希函数。

在上述技术方案中，优选地，还包括：提示单元，当所述终端允许或禁止所述待接入设备接入所述无线体域网时，发出提示信号；以及控制单元，当所述待接入设备接入所述无线体域网后，控制所述终端与所述待接入设备通过WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式通信。

在该技术方案中，通过向用户发送提示信息，使得用户了解当前待接入设备的接入状态，以对待接入设备的接入状态进行有效的监控。当然，还可以根据接入设备和终端当前所处的环境，为终端和接入设备选择更为便捷的通信方式，如WIFI、蓝牙、红外、NFC、有线网络、无线网络等。

在上述技术方案中，优选地，上述任一项所述的设备接入的处理装置，所述待接入设备包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

在该技术方案中，待接入设备包括但不限于普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备，所有可以通过无线体域网与终端进行通信，以提高用户便利性的设备均可。

本发明的第三方面提出了一种终端，包括通信总线、输入装置、输出装置、存储器以及处理器，其中：

所述通信总线，用于实现所述输入装置、输出装置、存储器以及处理器之间的连接通信；

所述输入装置，用于接收设备接入请求、第二随机码和第一目标密钥；

所述输出装置，用于发送第一随机码、预存储的第二随机码和预存储的第一公共密钥；

所述存储器中存储一组程序代码，且处理器调用存储器中存储的程序代

码，用于执行以下操作：

当通过所述输入装置接收到来自待接入设备的设备接入请求时，通过所述输出装置向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端；

通过所述输入装置接收来自所述待接入设备的所述第二随机码和所述第一目标密钥，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥；

判断所述第二目标密钥与所述第一目标密钥是否相同，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

在上述技术方案中，优选地，所述处理器在允许所述待接入设备接入所述终端构建的无线体域网之后，还用于执行以下操作：

根据所述第二随机码和所述第二公共密钥，计算出第三目标密钥；

通过所述输出装置将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送接入所述无线体域网的确认信息，否则，不发送接入所述无线体域网的确认信息。

在上述技术方案中，优选地，当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

在上述技术方案中，优选地，所述处理器还用于执行以下操作：

当所述终端允许或禁止所述待接入设备接入所述无线体域网时，通过所述输出装置发出提示信号；以及

当所述待接入设备接入所述无线体域网后，所述终端与所述待接入设

备通过WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式通信。

在上述技术方案中，优选地，所述待接入设备包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

通过本发明的技术方案，能够提高无线体域网的接入认证方法的通用性，且在降低接入认证计算量的同时，对无线体域网中接入设备进行高效、安全的认证。

附图说明

图 1 示出了根据本发明的一个实施例的设备接入的处理方法的流程示意图；

图 2 示出了根据本发明的一个实施例的设备接入的处理装置的示意框图；

图 3 示出了根据本发明的一个实施例的终端的结构示意图；

图 4 示出了根据本发明的一个实施例的 WBAN 的结构示意图；

图 5 示出了根据本发明的另一个实施例的设备接入的处理方法的流程示意图；

图 6 示出了根据本发明的一个实施例的主站配置的流程示意图；

图 7 示出了根据本发明的一个实施例的待接入设备配置的流程示意图；

图 8 示出了根据本发明的一个实施例的主站与待接入设备之间双向认证过程的流程示意图；

图 9 示出了根据本发明的另一个实施例的终端的结构示意图。

具体实施方式

为了可以更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的一个实施例的设备接入的处理方法的流程示意图。

如图 1 所示，根据本发明的一个实施例的设备接入的处理方法，包括：步骤 102，当终端接收到来自待接入设备的设备接入请求时，向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端；步骤 104，接收来自所述待接入设备的所述第二随机码和所述第一目标密钥，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥；步骤 106，判断所述第二目标密钥与所述第一目标密钥是否相同，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

在该技术方案中，通过向待接入设备发送一个第一随机码，可以使待接入设备根据第一随机码、预存储的第二随机码和第一公开密钥，按照自身的加密算法计算出一个第一目标密钥，并将第一目标密钥发送至终端，这样，终端就可以根据第一随机码、预存储的第二随机码和第二公开密钥，按照自身的算法计算出一个第二目标密码，并与所接收到的第一目标密钥进行比对，以根据判断结果判断该待接入设备是否为终端允许接入的合法设备，若是（即第二目标密钥与第一目标密钥相同），则允许该待接入设备接入终端构建的无线体域网，否则，说明该待接入设备是非法设备，会对无线体域网的安全性带来威胁，则禁止该待接入设备接入终端构建的无线体域网，从而实现通过简单的、计算量较低的加密算法就可以高效地完成对待接入设备进入无线体域网的安全认证，可以有效地避免非法待接入设备接入终端构建的无线体域网而对该无线体域网造成破坏。

在上述技术方案中，优选地，在允许所述待接入设备接入所述终端构建的无线体域网之后，根据所述第二随机码和所述第二公共密钥，计算出

第三目标密钥；将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送接入所述无线体域网的确认信息，否则，不发送接入所述无线体域网的确认信息。

在该技术方案中，在终端根据第二随机码和第二公共密钥，计算出第三目标密钥后，可以将第三目标密钥传送至待接入设备，以使待接入设备根据第二随机码和第一公开密钥，计算出第四目标密钥后，将第四目标密钥与接收到的第三目标密钥进行比对，若比较结果为第三目标密钥与第四目标密钥相同，则待接入设备就会再次确认接入了正确的无线体域网，就会向终端发送确认信息，以完成接入，当然，当判断结果为第三目标密钥与第四目标密钥不相同时，说明待接入设备有可能误接入了错误的无线体域网，也即目前终端所构建的无线体域网并不是待接入设备真正需要接入的无线体域网，则该待接入设备就不会向终端发送确认信息，也不会接入该无线体域网，通过上述过程，可以实现待接入设备的接入认证过程的双向认证，提高待接入设备接入过程的准确性，这样不仅可以防止非法待接入设备接入当前终端构建的无线体域网，提高无线体域网接入安全性，又可以防止待接入设备误接入错误的无线体域网，从而提高待接入设备接入过程的准确性，当然，由于该双向认证过程不需要对待接入设备的类型进行限定，因此，该双向认证方法具有很高的通用性，适用于对各种类型的待接入设备进行安全认证。

在上述技术方案中，优选地，还包括：当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

在该技术方案中，通过向终端和终端允许接入的合法待接入设备预置相同的第一公共密钥和所述第二公共密钥，以及控制他们使用相同的加密算法，可以确保在待接入设备接入终端构建的无线体域网的过程中，唯有

合法的待接入设备才能计算出与终端相同的目标密钥，进而顺利地通过无线体域网的接入安全认证，而非法待接入设备由于并不具备与终端相同的加密计算中不可以缺少的公共密钥，更不具备与终端相同的加密算法，因此，不可能计算出与终端相同的目标密钥，从而无法顺利地通过无线体域网的接入安全认证，无法接入终端构建的无线体域网，这样就可以实现最大程度地确保待接入设备接入无线体域网的安全性。其中，第一公开密钥和第二公开密钥包括但不限于：用户设定的口令、密码等。用以获得目标密钥的计算方法优选地采用密码学哈希函数。

在上述技术方案中，优选地，还包括：当所述终端允许或禁止所述待接入设备接入所述无线体域网时，发出提示信号；以及当所述待接入设备接入所述无线体域网后，所述终端与所述待接入设备通过 WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式通信。

在该技术方案中，通过向用户发送提示信息，使得用户了解当前待接入设备的接入状态，以对待接入设备的接入状态进行有效的监控。当然，还可以根据接入设备和终端当前所处的环境，为终端和接入设备选择更为便捷的通信方式，如 WIFI、蓝牙、红外、NFC、有线网络、无线网络等。

在上述技术中，优选地，上述任一项技术方案中的设备接入的处理方法，所述待接入设备包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

在该技术方案中，待接入设备包括但不限于普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备，所有可以通过无线体域网与终端进行通信，以提高用户便利性的设备均可。

图 2 示出了根据本发明的一个实施例的设备接入的处理装置的示意框图。

如图 2 所示，根据本发明的一个实施例的设备接入的处理装置 200，包括：发送单元 202，当终端接收到来自待接入设备的设备接入请求时，向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端；

接收单元 204，接收来自所述待接入设备的所述第二随机码和所述第一目标密钥；计算单元 206，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥；判断单元，判断所述第二目标密钥与所述第一目标密钥是否相同；处理单元 208，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

在该技术方案中，通过向待接入设备发送一个第一随机码，可以使待接入设备根据第一随机码、预存储的第二随机码和第一公开密钥，按照自身的加密算法计算出一个第一目标密钥，并将第一目标密钥发送至终端，这样，终端就可以根据第一随机码、预存储的第二随机码和第二公开密钥，按照自身的算法计算出一个第二目标密码，并与所接收到的第一目标密钥进行比对，以根据判断结果判断该待接入设备是否为终端允许接入的合法设备，若是，则允许该待接入设备接入终端构建的无线体域网，否则，说明该待接入设备是非法设备，会对无线体域网的安全性带来威胁，则禁止该待接入设备接入终端构建的无线体域网，从而实现通过简单的、计算量较低的加密算法就可以高效地完成对待接入设备进入无线体域网的安全认证，可以有效地避免非法待接入设备接入终端构建的无线体域网而对该无线体域网造成破坏。

在上述技术方案中，优选地，所述计算单元 206 还用于：在允许所述待接入设备接入所述终端构建的无线体域网之后，根据所述第二随机码和所述第二公共密钥，计算出第三目标密钥；所述发送单元还用于：将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送接入所述无线体域网的确认信息，否则，不发送接入所述无线体域网的确认信息。

在该技术方案中，在终端根据第二随机码和第二公共密钥，计算出第三目标密钥后，可以将第三目标密钥传送至待接入设备，以使待接入设备根据第二随机码和第一公开密钥，计算出第四目标密钥后，将第四目标密

钥与接收到的第三目标密钥进行比对，若比较结果为第三目标密钥与第四目标密钥相同，则待接入设备就会再次确认接入了正确的无线体域网，就会向终端发送确认信息，以完成接入，当然，当判断结果为第三目标密钥与第四目标密钥不相同时，说明待接入设备有可能误接入了错误的无线体域网，也即目前终端所构建的无线体域网并不是待接入设备真正需要接入的无线体域网，则该待接入设备就不会向终端发送确认信息，也不会接入该无线体域网，通过上述过程，可以实现待接入设备的接入认证过程的双向认证，提高待接入设备接入过程的准确性，这样不仅可以防止非法待接入设备接入当前终端构建的无线体域网，提高无线体域网接入安全性，又可以防止待接入设备误接入错误的无线体域网，从而提高待接入设备接入过程的准确性，当然，由于该双向认证过程不需要对待接入设备的类型进行限定，因此，该双向认证方法具有很高的通用性，适用于对各种类型的待接入设备进行安全认证。

在上述技术方案中，优选地，还包括：当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

在该技术方案中，通过向终端和终端允许接入的合法待接入设备预置相同的第一公共密钥和所述第二公共密钥，以及控制他们使用相同的加密算法，可以确保在待接入设备接入终端构建的无线体域网的过程中，唯有合法的待接入设备才能计算出与终端相同的目标密钥，进而顺利地通过无线体域网的接入安全认证，而非法待接入设备由于并不具备与终端相同的加密计算中不可以缺少的公共密钥，更不具备与终端相同的加密算法，因此，不可能计算出与终端相同的目标密钥，从而无法顺利地通过无线体域网的接入安全认证，无法接入终端构建的无线体域网，这样就可以实现最大程度地确保待接入设备接入无线体域网的安全性。其中，第一公开密钥和第二公开密钥包括但不限于：用户设定的口令、密码等。用以获得目标密钥的计算方法优选地采用密码学哈希函数。

在上述技术方案中，优选地，还包括：提示单元 210，当所述终端允许或禁止所述待接入设备接入所述无线体域网时，发出提示信号；以及控制单元 212，当所述待接入设备接入所述无线体域网后，控制所述终端与所述待接入设备通过 WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式通信。

在该技术方案中，通过向用户发送提示信息，使得用户了解当前待接入设备的接入状态，以对待接入设备的接入状态进行有效的监控。当然，还可以根据接入设备和终端当前所处的环境，为终端和接入设备选择更为便捷的通信方式，如 WIFI、蓝牙、红外、NFC、有线网络、无线网络等。

在上述技术方案中，优选地，上述任一项所述的设备接入的处理装置，所述待接入设备包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

在该技术方案中，待接入设备包括但不限于普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备，所有可以通过无线体域网与终端进行通信，以提高用户便利性的设备均可。

图 3 示出了根据本发明的一个实施例的终端的结构示意图。

如图 3 所示，根据本发明的一个实施例的终端 300，包括如上述技术方案中任一项所述的设备接入的处理装置 200，因此，该终端具有和上述技术方案中任一项所述的设备接入的处理装置 200 相同的技术效果，在此不再赘述。

图 4 示出了根据本发明的一个实施例的 WBAN 的结构示意图；图 5 示出了根据本发明的另一个实施例的设备接入的处理方法的流程示意图；图 6 示出了根据本发明的一个实施例的主站配置的流程示意图；图 7 示出了根据本发明的一个实施例的待接入设备配置的流程示意图；图 8 示出了根据本发明的一个实施例的主站与待接入设备之间双向认证过程的流程示意图。

下面结合图 4 至图 8，对本发明的技术方案作进一步说明。

如图 4 所示，根据本发明的一个实施例的 WBAN 的结构，WBAN 是附着在人体上的一种网络，由一套小巧可移动、具有通信功能的传感器和一个

身体主站组成。身体主站通常为智能手机、平板电脑等计算、存储能力较强的设备。另外，本实施例的设备接入的处理方案包括三个流程：待接入设备的大体接入流程（如图 5 所示）：主站配置流程（如图 6 所示）、待接入设备配置流程（如图 7 所示）、待接入设备的接入认证流程（如图 8 所示）。该方案使用的参数和符号包括：h：密码学哈希函数； s：秘密值即公开密钥，包含但不限于用户设定的口令、密码之类的值。以下对上述三个流程具体说明：

待接入设备的大体接入流程，包括：

步骤 502，对主站（通常为智能手机、平板电脑等计算、存储能力较强的移动设备）进行配置，即为主站配置必要的认证参数；

步骤 504，对待接入设备进行配置；

步骤 506，对待接入设备进行安全认证。

主站配置流程，具体包含以下步骤：

步骤 602，用户为主站输入秘密值 s。

步骤 604，主站执行其他必要的 WBAN 参数，以完成初始化操作。

待接入设备配置，具体包含以下步骤：

步骤 702，在确定要接入到当前身体主站的 WBAN 时，用户为待接入设备输入与主站配置过程中相同的秘密值 s。

步骤 704，待接入设备执行其他必要的 WBAN 参数，以完成初始化。

接入认证流程如下：

在完成上述的主站配置和待接入设备配置后，开始进行接入认证，接入认证过程共涉及三条消息交互，如图 8 所示：当身体主站接收到待接入设备发送的设备接入请求时，身体主站选取一随机码 a，并发送随机码 a 至待接入设备，待接入设备根据接收到的随机码 a、预存的随机码 b 及秘密值 s，采用密码学哈希函数计算获得目标密钥 c1（c1=h（a，b，s））即第一目标密钥，并将第一目标密钥 c1 及随机码 b 发送至身体主站，同时身体主站根据自身的随机码 a、接收到的随机码 b 及自身的秘密值 s，采用密码学哈希函数计算获得目标密钥 c2（c2=h（a，b，s））即第二目标密钥，身体主站通过判断计算所得的第二目标密钥 c2 与接收到的第一目标密钥 c1 是否

相同，在判断 c1 与 c2 不相同时，禁止待接入设备接入 WBAN；在判断 c1 与 c2 相同时，允许待接入设备接入 WBAN，以完成对待接入设备身份的认证（在本实施例中，由于待接入设备与身体主体具有相同的加密计算中不可以缺少的公共密钥和相同的加密算法，因此，该待接入设备是身体主体允许接入的合法设备，c1 与 c2 相同）。在允许待接入设备接入身体主站构建的无线体域网之后，身体主站根据获得的随机码 b 及自身的秘密值 s，采用密码学哈希函数计算获得目标密钥 d1（d1=h（b，s））即第三目标密钥，并将第三目标密钥 d1 发送至待接入设备，同时待接入设备根据自身随机码 b 及自身秘密值 s，采用密码学哈希函数计算获得目标密钥 d2（d2=h（b，s））即第四目标密钥，待接入设备通过判断计算获得第四目标密钥 d2 与接收到的第三目标密钥 d1 是否相同，在判断 d1 与 d2 相同时，待接入设备就会再次确认接入了正确的无线体域网，就会向终端发送确认信息，以完成接入，当然，在判断 d1 与 d2 不相同时，说明待接入设备有可能误接入了错误的无线体域网，也即目前身体主站所构建的无线体域网并不是待接入设备真正需要接入的无线体域网，则该待接入设备就不会向终端发送确认信息，也不会接入该无线体域网，以完成对身体主站身份的认证，从而实现身体主站和待接入设备之间的双向认证（当然，在本实施例中，由于待接入设备与身体主体具有相同的加密计算中不可以缺少的公共密钥和相同的加密算法，因此，该待接入设备是身体主体允许接入的合法设备，d1 与 d2 相同）。

在上述设备接入的处理方案的具体流程中，通过向身体主站和身体主站允许接入的合法待接入设备预置相同的秘密值 s，以及控制他们使用相同的加密算法密码学哈希函数 h，可以确保在待接入设备接入终端构建的无线体域网的过程中，唯有合法的待接入设备才能计算出与终端相同的目标密钥，进而顺利地通过无线体域网的接入安全认证，而非法待接入设备由于并不具备与终端相同的加密计算中不可以缺少的公共密钥，更不具备与身体主站相同的加密算法，因此，不可能计算出与身体主站相同的目标密钥，从而无法顺利地通过无线体域网的接入安全认证，无法接入身体主站构建的无线体域网，这样就可以实现最大程度地确保待接入设备接入无线体域网的安全性。

本发明实施例还提供了一种终端，图 9 为本发明实施例中另一种终端的结构示意图，如图所示，所述终端可以包括：至少一个输入装置 903，至少一个输出装置 904，至少一个处理器 901，例如 CPU，存储器 905 和至少一个总线 902，处理器 901 可以结合图 2 所示的设备接入的处理装置。

其中，上述总线 902 用于连接上述输入装置 903、输出装置 904、处理器 901 和存储器 905。

其中，上述输入装置 903 具体可为终端的通信接口，例如网络接口，网络接口可以包括标准的有线接口或者无线接口（如 WI-FI 接口），用于接收设备接入请求、第二随机码和第一目标密钥。

其中，上述输出装置 904 具体可为终端的通信接口，例如网络接口，网络接口可以包括标准的有线接口或者无线接口（如 WI-FI 接口），用于发送第一随机码、预存储的第二随机码和预存储的第一公共密钥。

上述存储器 905 可以是高速 RAM 存储器，也可为非不稳定的存储器（non-volatile memory），例如磁盘存储器。上述存储器 905 还用于存储一组程序代码，处理器 901 用于调用存储器 905 中存储的程序代码，执行如下操作：

当通过所述输入装置 903 接收到来自待接入设备的设备接入请求时，通过所述输出装置 904 向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端。

通过所述输入装置 903 接收来自所述待接入设备的所述第二随机码和所述第一目标密钥，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥。

判断所述第二目标密钥与所述第一目标密钥是否相同，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

在可选实施例中，所述处理器 901 在允许所述待接入设备接入所述终端构建的无线体域网之后，还可以执行以下操作：

根据所述第二随机码和所述第二公共密钥，计算出第三目标密钥。

通过所述输出装置904将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送接入所述无线体域网的确认信息，否则，不发送接入所述无线体域网的确认信息。

在可选实施例中，当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

在可选实施例中，所述处理器 901 还可以执行以下操作:

当所述终端允许或禁止所述待接入设备接入所述无线体域网时，通过所述输出装置 904 发出提示信号；以及

当所述待接入设备接入所述无线体域网后，所述终端与所述待接入设备通过WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式通信。

在可选实施例中，所述待接入设备可以包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

具体的，本发明实施例中介绍的终端可以用以实施本发明结合图 1、图 5 或图 8 介绍的方法实施例中的部分或全部流程。

以上结合附图详细说明了本发明的技术方案，本发明提出了一种新的设备接入的处理方案，该方案通用、计算量低、且能高效地对无线体域网中的接入设备进行安全认证。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求

1. 一种设备接入的处理方法，其特征在于，包括:

当终端接收到来自待接入设备的设备接入请求时，向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端;

接收来自所述待接入设备的所述第二随机码和所述第一目标密钥，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥;

判断所述第二目标密钥与所述第一目标密钥是否相同，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

2. 根据权利要求 1 所述的设备接入的处理方法，其特征在于，

在允许所述待接入设备接入所述终端构建的无线体域网之后，根据所述第二随机码和所述第二公共密钥，计算出第三目标密钥;

将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送接入所述无线体域网的确认信息，否则，不发送接入所述无线体域网的确认信息。

3. 根据权利要求 1 所述的设备接入的处理方法，其特征在于，还包括:

当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

4. 根据权利要求 1 所述的设备接入的处理方法，其特征在于，还包括:

当所述终端允许或禁止所述待接入设备接入所述无线体域网时，发出提示信号; 以及

当所述待接入设备接入所述无线体域网后，所述终端与所述待接入设备通过 WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式通信。

5. 根据权利要求 1 至 4 中任一项所述的设备接入的处理方法，其特征在于，

所述待接入设备包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

6. 一种设备接入的处理装置，其特征在于，包括：

发送单元，当终端接收到来自待接入设备的设备接入请求时，向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端；

接收单元，接收来自所述待接入设备的所述第二随机码和所述第一目标密钥；

计算单元，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥；

判断单元，判断所述第二目标密钥与所述第一目标密钥是否相同；

处理单元，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

7. 根据权利要求 6 所述的设备接入的处理装置，其特征在于，

所述计算单元还用于：

在允许所述待接入设备接入所述终端构建的无线体域网之后，根据所述第二随机码和所述第二公共密钥，计算出第三目标密钥；

所述发送单元还用于：

将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送接入所述无线体域网的确认信息，否则，不发送接入所述

无线体域网的确认信息。

8. 根据权利要求 6 所述的设备接入的处理装置，其特征在于，还包括：

当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

9. 根据权利要求 6 所述的设备接入的处理装置，其特征在于，还包括：

提示单元，当所述终端允许或禁止所述待接入设备接入所述无线体域网时，发出提示信号；以及

控制单元，当所述待接入设备接入所述无线体域网后，控制所述终端与所述待接入设备通过 WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式通信。

10. 根据权利要求 6 至 9 中任一项所述的设备接入的处理装置，其特征在于，

所述待接入设备包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

11. 一种终端，其特征在于，所述终端包括通信总线、输入装置、输出装置、存储器以及处理器，其中：

所述通信总线，用于实现所述输入装置、输出装置、存储器以及处理器之间的连接通信；

所述输入装置，用于接收设备接入请求、第二随机码和第一目标密钥；

所述输出装置，用于发送第一随机码、预存储的第二随机码和预存储的第一公共密钥；

所述存储器中存储一组程序代码，且处理器调用存储器中存储的程序代码，用于执行以下操作：

当通过所述输入装置接收到来自待接入设备的设备接入请求时，通过所述输出装置向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预

存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端；

通过所述输入装置接收来自所述待接入设备的所述第二随机码和所述第一目标密钥，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥；

判断所述第二目标密钥与所述第一目标密钥是否相同，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网。

12. 根据权利要求 11 所述的终端，其特征在于，所述处理器在允许所述待接入设备接入所述终端构建的无线体域网之后，还用于执行以下操作：

根据所述第二随机码和所述第二公共密钥，计算出第三目标密钥；

通过所述输出装置将所述第三目标密钥发送至所述待接入设备，以使所述待接入设备根据所述第二随机码和所述第一公共密钥，计算出第四目标密钥后，判定所述第三目标密钥与所述第四目标密钥是否相同，并在判定结果为相同时，向所述终端发送接入所述无线体域网的确认信息，否则，不发送接入所述无线体域网的确认信息。

13. 根据权利要求11所述的终端，其特征在于，当所述待接入设备为所述终端允许接入的待接入设备时，所述第一公共密钥和所述第二公共密钥相同，以及所述待接入设备计算所述第一目标密钥和所述第四目标密钥时使用的算法与所述终端计算所述第二目标密钥和所述第三目标密钥时使用的算法相同。

14. 根据权利要求 11 所述的终端，其特征在于，所述处理器还用于执行以下操作：

当所述终端允许或禁止所述待接入设备接入所述无线体域网时，通过所述输出装置发出提示信号；以及

当所述待接入设备接入所述无线体域网后，所述终端与所述待接入设备通过WIFI、蓝牙、红外、NFC、有线网络、无线网络中的至少一种方式

通信。

15. 根据权利要求 11 至 14 中任一项所述的终端，其特征在于，

所述待接入设备包括：普通移动设备、可穿戴设备、可穿戴式传感器和医疗设备中的至少一种设备。

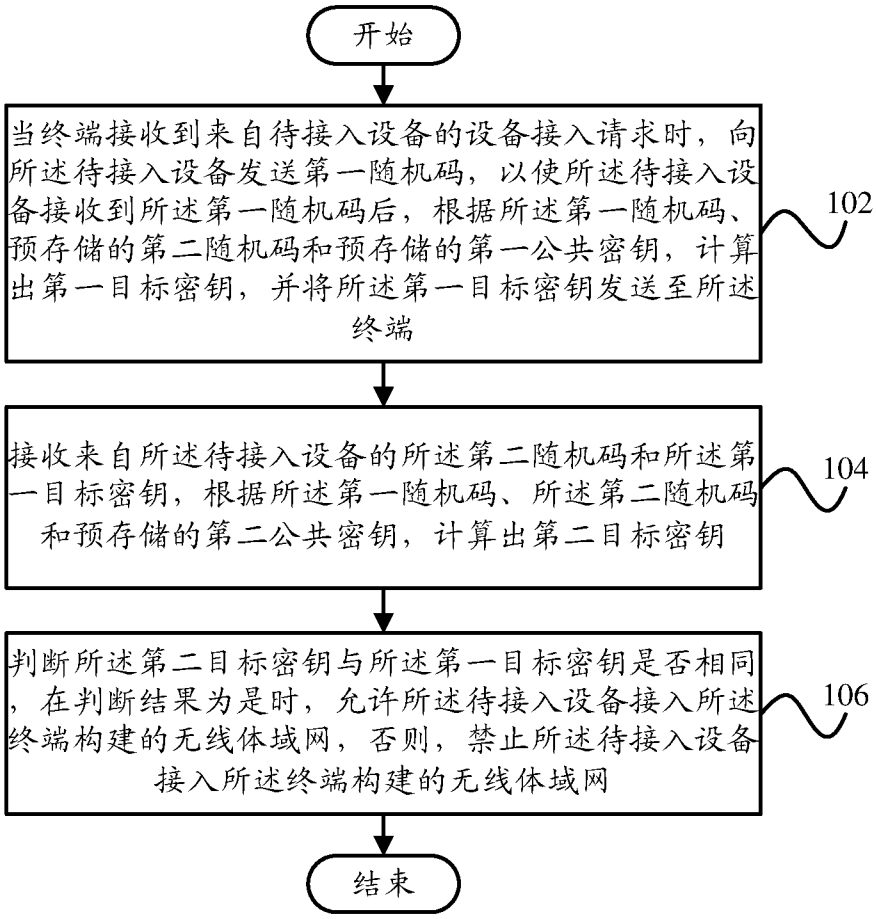
开始
当终端接收到来自待接入设备的设备接入请求时，向所述待接入设备发送第一随机码，以使所述待接入设备接收到所述第一随机码后，根据所述第一随机码、预存储的第二随机码和预存储的第一公共密钥，计算出第一目标密钥，并将所述第一目标密钥发送至所述终端
102
接收来自所述待接入设备的所述第二随机码和所述第一目标密钥，根据所述第一随机码、所述第二随机码和预存储的第二公共密钥，计算出第二目标密钥
104
判断所述第二目标密钥与所述第一目标密钥是否相同，在判断结果为是时，允许所述待接入设备接入所述终端构建的无线体域网，否则，禁止所述待接入设备接入所述终端构建的无线体域网
106
结束

图 1


发送单元202
接收单元204
计算单元206
判断单元208
处理单元210
提示单元212
控制单元214
设备接入的处理装置200

图 2

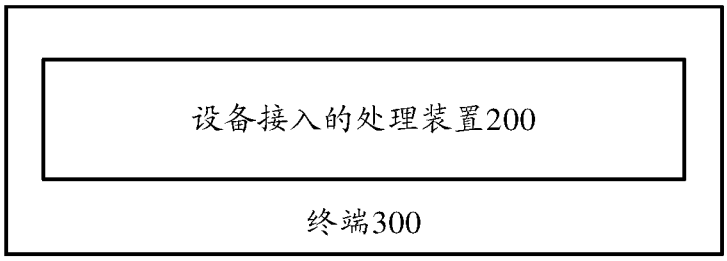

图 3

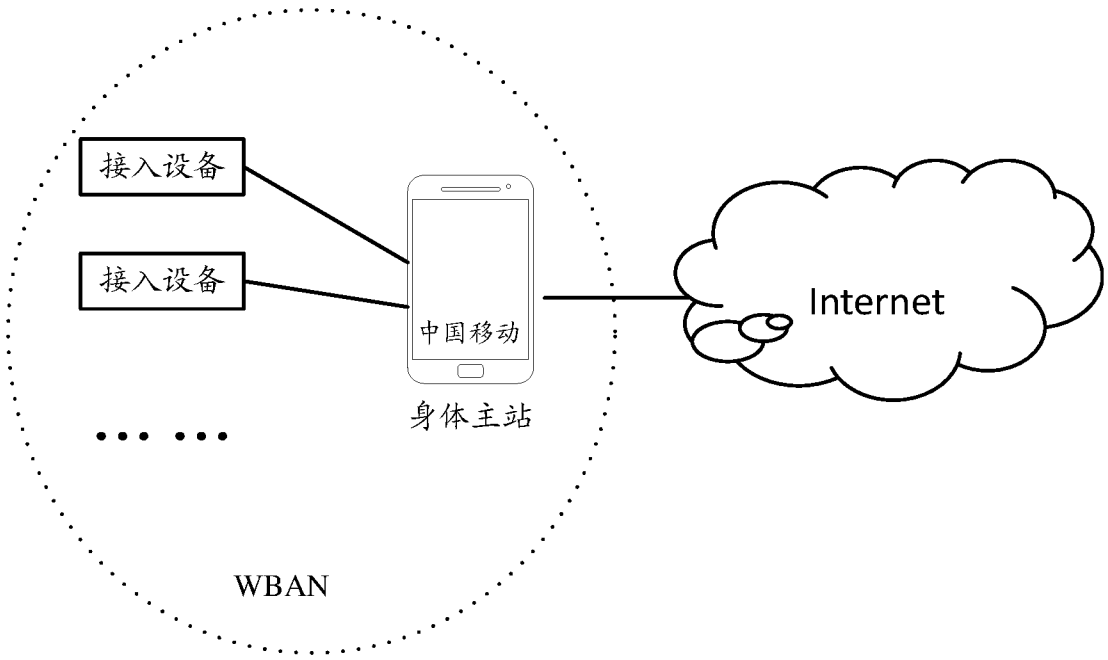

图 4

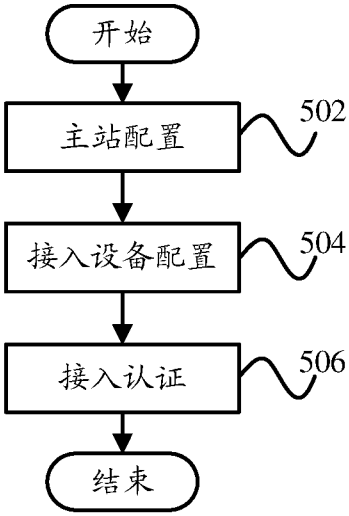
开始
主站配置
502
接入设备配置
504
接入认证
506
结束

图 5

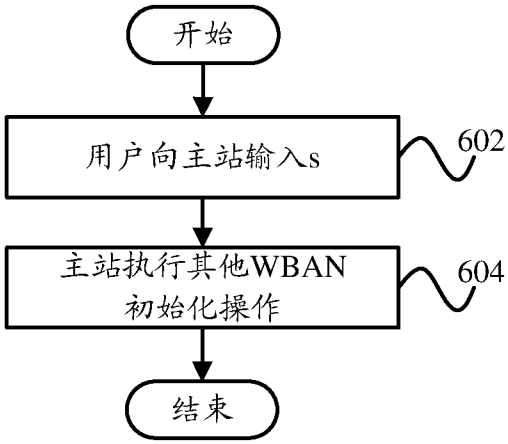
开始
用户向主站输入s
602
主站执行其他WBAN
初始化操作
604
结束

图 6

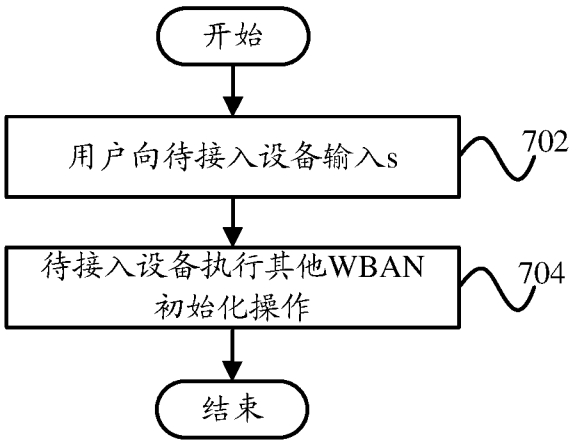
开始
用户向待接入设备输入s
702
待接入设备执行其他WBAN
初始化操作
704
结束

图 7


身体主站
待接入设备
② 发送a
①选取随机值a
③ 选取随机值b,
计算c1=h（a，b，s）
④发送b，c1
⑤验证c2=h（a，b，s），计
算d1=h（b， s）
⑥ 发送d1
⑦ 验证d2=h（b， s）

图 8

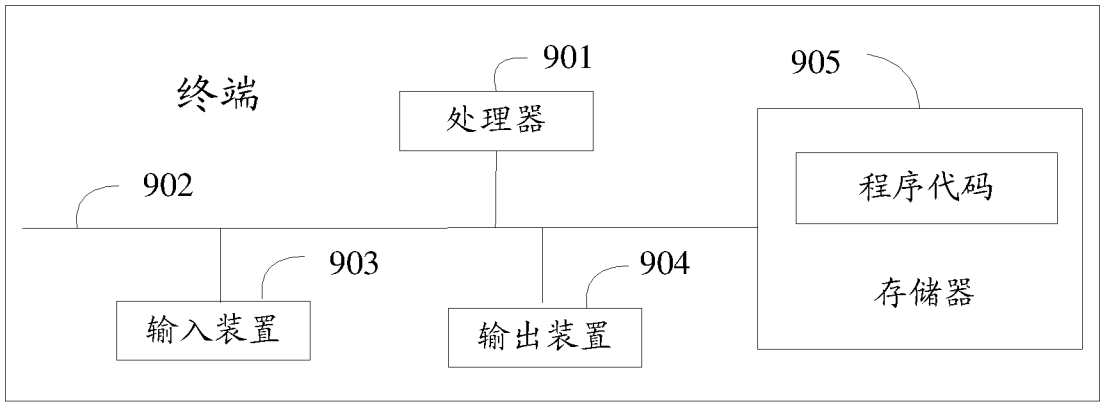
终端
901
处理器
905
程序代码
902
903
904
输入装置
输出装置
存储器

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/078021

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (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)

CNPAT, CNKI, WPI, EPODOC: public key, random number, random value, random code, secret key, public, key, random, wireless body area network, WBAN, generat+, same, identical, compar+, access+, authenticat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101378320 A (UNITEND TECHNOLOGIES INC.), 04 March 2009 (04.03.2009), description, page 3, line 18 to page 9, line 11	1-15
X	CN 1665183 A (XIDIAN UNIVERSITY), 07 September 2005 (07.09.2005), description, page 4, line 2 to page 5, line 21	1-15
A	CN 1708018 A (HUAWEI TECHNOLOGIES CO., LTD.), 14 December 2005 (14.12.2005), the whole document	1-15
A	US 2002073322 A1 (PARK, D.G. et al.), 13 June 2002 (13.06.2002), the whole document	1-15

☐ 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
05 January 2016 (05.01.2016)	**18 January 2016 (18.01.2016)**
Name and mailing address of the ISA/CN: 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 **YAO, Yaqian** Telephone No.: (86-10) **62413297**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/078021

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101378320 A	04 March 2009	None	
CN 1665183 A	07 September 2005	None	
CN 1708018 A	14 December 2005	None	
US 2002073322 A1	13 June 2002	KR 20020045003 A	19 June 2002

国际检索报告

国际申请号 PCT/CN2015/078021

A. 主题的分类

H04L 9/32(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）)

CNPAT,CNKI,WPI,EPODOC:公共密钥，公钥，随机数，随机，随机值，随机码，无线体域网，生成，产生，相同，比较，认证，密钥，接入，public, key, random，wireless body area network, WBAN, generat+, same, identical，compar+, access+, authenticat+

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 101378320 A (北京数字太和科技有限责任公司) 2009年 3月 4日 (2009-03-04) 说明书第3页第18行-第9页第11行	1-15
X	CN 1665183 A (西安电子科技大学) 2005年 9月 7日 (2005-09-07) 说明书第4页第2行-第5页第21行	1-15
A	CN 1708018 A (华为技术有限公司) 2005年 12月 14日 (2005-12-14) 全文	1-15
A	US 2002073322 A1 (PARK, DONG-GOOK 等) 2002年 6月 13日 (2002-06-13) 全文	1-15

☐ 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
2016年 1月 5日	2016年 1月 18日

ISA/CN的名称和邮寄地址	受权官员
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	姚雅倩
传真号 (86-10)62019451	电话号码 (86-10)62413297

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/078021

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 101378320 A	2009年 3月 4日	无	
CN 1665183 A	2005年 9月 7日	无	
CN 1708018 A	2005年 12月 14日	无	
US 2002073322 A1	2002年 6月 13日	KR 20020045003 A	2002年 6月 19日