(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
2015 年 5 月 7 日 (07.05.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/061992 A1

(51) 国际专利分类号:
H04L 9/14 (2006.01)

(21) 国际申请号: PCT/CN2013/086247

(22) 国际申请日: 2013 年 10 月 30 日 (30.10.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **华为终端有限公司 (HUAWEI DEVICE CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地 B 区 2 号楼, Guangdong 518129 (CN)。

(72) 发明人: **庞高昆 (PANG, Gaokun)**; 中国广东省深圳市龙岗区坂田华为基地 B 区 2 号楼, Guangdong 518129 (CN)。 **丁志明 (DING, Zhiming)**; 中国广东省深圳市龙岗区坂田华为基地 B 区 2 号楼, Guangdong 518129 (CN)。

(74) 代理人: **深圳市威世博知识产权代理事务所（普通合伙） (CHINA WISPRO INTELLECTUAL PROPERTY LLP.)**; 中国广东省深圳市南山区高新区粤兴三道 8 号中国地质大学产学研基地中地大楼 A806, Guangdong 518057 (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, LT, 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, NA, RW, SD, SL, 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))。

(54) **Title**: KEY CONFIGURATION METHOD, SYSTEM AND APPARATUS

(54) **发明名称** : 一种密钥配置方法、系统和装置

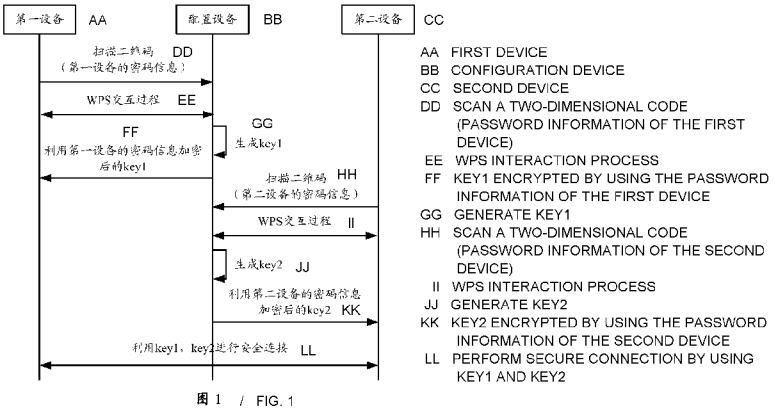

图 1 / FIG. 1

(57) **Abstract**: The present invention provides a key configuration method, system and apparatus. The method comprises: a configuration device obtaining a public key of a second device and sending the public key of the second device to a first device; the first device generating a first shared key, and sending, by means of the public key of the second device, information for obtaining the first shared key to the second device; or the first device generating the first shared key by means of the public key of the second device, and sending the information for obtaining the first shared key to the second device; and the second device generating the first shared key by means of a private key of the second device and the information for obtaining the first shared key, the first shared key being used for a secure connection between the first device and the second device. By means of the present invention, the security of the interaction between the first device and the second device can be improved.

(57) **摘要**:

[见续页]

WO 2015/061992 A1

本发明提供了一种密钥配置方法、系统和装置，其中方法包括：所述配置设备获取第二设备的公钥，将所述第二设备的公钥发送给第一设备；所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备；或者所述第一设备利用第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给第二设备；所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。通过本发明能够提高第一设备和第二设备之间交互的安全性。

一种密钥配置方法、系统和装置

[1] 【技术领域】

[2] 本发明涉及网络通信技术领域，特别涉及一种密钥配置方法、系统和装置。

[3] 【背景技术】

[4] WiFi（Wireless Fidelity，无线保真）技术从1997年无线局域网标准IEEE802.11发布以来，在拥有众多在业界领先的公司组成的WiFi联盟的大力推动下，同时以其具有的部署快速、使用便利和传输速率高等优势，发展迅猛。WiFi技术现在已经被广泛应用于各个行业，现在的笔记本电脑、PDA（Personal Digital Assistant，掌上电脑）和手机等都支持WiFi技术，WiFi网络的接入点遍布于酒店、咖啡厅、学校和医院等场所，可以说WiFi技术在生活中无所不在。

[5] 随着WiFi技术的发展和广泛应用，与之相关的安全技术需求也随之产生，WPA（Wi-Fi Protected Access，WiFi安全接入）是WiFi中使用的安全技术，它需要用户设置Credential（信任状, 包括帐号名、密码）以及WPA相关的其它参数，例如加密算法等等，但当用户不理解这些参数的含义时，因此就不懂如何设置这些参数，从而阻碍了WPA安全技术的应用，这就会导致用户因为不懂如何设置WPA参数而选择在没有安全机制保护的情况下使用网络。WPS（WiFi Protected Setup， Wifi安全建立）就是为了帮助用户设置信任状的技术。WPS主要强调两点：安全和简单，即配置过程要简单，配置后的网络要安全。现有的WPS主要基于密钥交换算法防止偷听、字典攻击等某些攻击行为。

[6] 目前WPS应用的场景，主要包括以下两种：第一种是作为enrollee（被注册方）的终端与作为registrar（注册器）的WiFi网络的AP（Access Point，接入点）之间进行信任状的配置，以便后续终端与AP之间能够基于信任状进行认证以建立安全的连接。第二种是P2P（Peer to Peer，点到点）场景中的认证配置过程，WiFi技术中P2P的研究是为了在没有诸如蜂窝网或热点等基础设施的情况下，终端设备之间也能够通过WiFi功能实现端到端的直接发现，在该场景下，一个终端作为client（客户端），另一个终端

作为GO（Group Owner，组长设备），在client和GO之间进行密钥的配置，以便后续client和GO之间能够基于配置的密钥进行数据交互。

[7] WiFi技术逐步应用于诸如智能电网、传感器网络、医疗网络等新领域，大量WiFi设备属于无头设备（Headless Devices），所谓无头设备就是没有显示屏幕、没有键盘、没有近场通信等人机接口的设备，对于这些无头设备之间的连接就需要一个第三方的配置设备来实现，例如通过配置设备将AP和机顶盒连接起来，或者通过配置设备将传感器和传感器连接起来等等。对于这种基于第三方的配置设备的帮助在两个设备之间进行的密钥配置现有技术中采用如下方式：

[8] 如图1中所示，配置设备扫描第一设备上的二维码，获取二维码中包含的第一设备的密码信息，并且扫描第二设备上的二维码，获取二维码中包含的第二设备的密码信息；配置设备基于第一设备的密码信息与第一设备执行WPS交互过程，并生成密钥key1，利用第一设备的密码信息对key1进行加密后发送给第一设备；以及配置设备基于第二设备的密码信息与第二设备执行WPS交互过程，并生成密钥key2，利用第二设备的密码信息对key2进行加密后发送给第二设备。之后，第一设备和第二设备就基于key1和key2进行安全连接，即基于key1和key2进行交互。

[9] 然而，上述方式中由于第一设备和第二设备的密码信息处于公开状态，易于被非法获取，即任何第三方的设备都能够获取到并生成密钥后发送给第一设备和第二设备，这样就很容易对第一设备和第二设备之间的交互进行偷听，安全性较差。

[10] 【发明内容】

[11] 有鉴于此，本发明实施例提供了一种基于第三方配置设备的密钥配置方法、系统和装置，以便于提高第一设备和第二设备之间交互的安全性。

[12] 第一方面，本发明实施例提供了一种密钥配置方法，所述密钥配置方法包括：

[13] 第一设备接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥；利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备，或者所述第一设备利用所述第二设备的公钥生成第一共享密钥，将用于得到所述第一共享密钥的信息发送给所述第二设备；

[14] 以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[15] 结合第一方面，在第一种可能的实现方式中，所述第一设备利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：所述第一设备生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备；

[16] 以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

[17] 所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：所述第一设备生成密码，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备，利用密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为第一共享密钥；

[18] 以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[19] 结合第一方面，在第二种可能的实现方式中，所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：所述第一设备生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该随机值进行加密后，将加密结果发送给第二设备；

[20] 以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[21] 结合第一方面，在第三种可能的实现方式中，利用所述第二设备的公钥将用于得到所述第一共享密钥的信息发送给所述第二设备包括：所述第一设备利用第二设备的公钥将第一设备的公钥进行加密后，将加密结果发送给第二设备；

[22] 以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密后，得到所述第一设备的公钥，并且生成密码，将该密码作为所述第一共享密钥；

[23] 该方法还包括：第一设备接收所述第二设备利用所述第一设备的公钥将该密码进行加密后的加密结果，利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为所述第一共享密钥。

[24] 结合第一方面，在第四种可能的实现方式中，该方法还包括：所述第一设备和所述第二设备预定密钥交换算法；

[25] 所述第一设备利用第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给第二设备包括：所述第一设备利用第二设备的公钥和自身的私钥按照所述密钥交换算法生成第一共享密钥，并将第一设备的公钥发送给所述第二设备；

[26] 以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[27] 结合第一方面的第四种可能的实现方式，在第五种可能的实现方式中，所述第一设备和所述第二设备预定密钥交换算法包括：

[28] 所述第一设备和所述第二设备上预先配置有所述密钥交换算法所使用的参数；或者，

[29] 通过所述配置设备将所述密钥交换算法所使用的参数发送给所述第一设备和所述第二设备。

[30] 结合第一方面、第一方面的第一种可能的实现方式、第一方面的第二种可能的实现方式、第一方面的第三种可能的实现方式、第一方面的第四种可能的实现方式或者第一方面的第五种可能的实现方式，在第六种可能的实现方式中，所

述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接包括：

[31] 所述第一设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给所述第二设备；以便所述第二设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接；或者，

[32] 所述第一设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对所述第二设备发送的信任状的加密结果进行解密得到所述信任状，所述信任状的加密结果为所述第二设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对所述信任状进行加密后得到，所述信任状用于所述第一设备和所述第二设备之间的安全连接。

[33] 结合第一方面的第六种可能的实现方式，在第七种可能的实现方式中，若所述第一设备是注册器Registrar、中心节点或者组长设备GO，则由所述第一设备生成所述信任状并将所述信任状的加密结果发送给所述第二设备；

[34] 若所述第二设备是Registrar、中心节点或GO，则由所述第二设备生成所述信任状并将所述信任状的加密结果发送给所述第一设备。

[35] 结合第一方面、第一方面的第一种可能的实现方式、第一方面的第二种可能的实现方式、第一方面的第三种可能的实现方式、第一方面的第四种可能的实现方式、第一方面的第五种可能的实现方式、第一方面的第六种可能的实现方式或者第一方面的第七种可能的实现方式，在第八种可能的实现方式中，所述第一设备接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥具体为：

[36] 所述第一设备接收配置设备在获取到所述第二设备的公钥和所述第一设备的公钥后发送的加密结果，所述加密结果为所述配置设备利用所述第一设备的公钥加密的所述第二设备的公钥；

[37] 该方法还包括：所述第一设备对所述加密结果进行解密，得到所述第二设备的公钥。

[38] 结合第一方面、第一方面的第一种可能的实现方式、第一方面的第二种可能的

实现方式、第一方面的第三种可能的实现方式、第一方面的第四种可能的实现方式、第一方面的第五种可能的实现方式、第一方面的第六种可能的实现方式或者第一方面的第七种可能的实现方式，在第九种可能的实现方式中，所述第一设备接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥具体为：

[39] 所述第一设备与所述配置设备建立安全连接以生成第二共享密钥；

[40] 所述第一设备接收所述配置设备在获取到第二设备的公钥后发送的加密结果，所述加密结果为所述配置设备利用所述第二共享密钥加密的所述第二设备的公钥；

[41] 该方法还包括：

[42] 所述第一设备利用所述第二共享密钥对接收到的所述加密结果进行解密后，得到所述第二设备的公钥。

[43] 结合第一方面的第九种可能的实现方式，在第十种可能的实现方式中，所述第一设备与所述配置设备建立安全连接以生成第二共享密钥包括：

[44] 所述第一设备与所述配置设备通过无线保真安全建立WPS交互方式共享信任状，将所述信任状作为所述第二共享密钥；或者，

[45] 所述第一设备接收所述配置设备发送的所述配置设备的公钥，所述第一设备利用所述配置设备的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥，以便所述配置设备获取到所述第一设备的公钥后，利用所述第一设备的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥。

[46] 结合第一方面的第四种可能的实现方式，在第十一种可能的实现方式中，在所述第一设备得到所述第二设备的公钥之后，所述方法还包括：所述第一设备生成新的公钥和新的私钥；

[47] 所述第一设备发送给所述第二设备的第一设备的公钥为所述新的公钥；所述第二设备在生成所述第一共享密钥时利用的第一设备的公钥为所述新的公钥；所述第一设备在生成所述第一共享密钥时利用的自身的私钥为所述新的私钥。

[48] 结合第一方面、第一方面的第一种至第十一种可能的实现方式中的任一种，在

第十二种可能的实现方式中，所述第一设备是被注册方enrollee，所述第二设备是registrar，或者所述第一设备是客户端client，所述第二设备是GO，或者所述第一设备是无线终端，所述第二设备是接入点，或者所述第一设备是中心节点，所述第二设备是传感器节点。

[49] 结合第一方面、第一方面的第一种至第十二种可能的实现方式中的任一种，在第十三种可能的实现方式中，该方法还包括：所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的步骤，所述第二设备的信道信息为所述配置设备从所述第二设备获取后发送给所述第一设备的。

[50] 结合第一方面、第一方面的第一种至第十三种可能的实现方式中的任一种，在第十四种可能的实现方式中，所述配置设备通过扫描二维码、通用串行总线USB或者近场通信的方式从所述第一设备或者第二设备获取信息。

[51] 结合第一方面、第一方面的第一种至第十四种可能的实现方式中的任一种，在第十五种可能的实现方式中，该方法还包括：所述第一设备利用所述第二设备的公钥生成验证值，将所述验证值发送给所述第二设备；

[52] 以便所述第二设备在生成所述第一共享密钥之前，利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成所述第一共享密钥的步骤。

[53] 第二方面，本发明实施例提供了一种密钥配置方法，所述密钥配置方法包括：

[54] 所述配置设备获取第二设备的公钥，将所述第二设备的公钥发送给第一设备；

[55] 以便所述第一设备利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备；或者以便所述第一设备利用所述第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给所述第二设备；

[56] 以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[57] 结合第二方面，在第一种可能的实现方式中，以便所述第一设备利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：以便所述第一设备生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述

密码进行加密得到加密结果，将所述加密结果发送给所述第二设备；

[58] 以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

[59] 以便所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：以便所述第一设备生成密码，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备，利用密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为第一共享密钥；

[60] 以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[61] 结合第二方面，在第二种可能的实现方式中，以便所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：以便所述第一设备生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该随机值进行加密后，将加密结果发送给第二设备；

[62] 以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[63] 结合第二方面，在第三种可能的实现方式中，以便所述第一设备利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备包括：以便所述第一设备利用第二设备的公钥将第一设备的公钥进行加密后，将加密结果发送给第二设备；

[64] 以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进

行解密后，得到所述第一设备的公钥，并且生成密码，将该密码进行加密后，将加密结果发送给所述第一设备；

[65] 以便所述第一设备利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为第一共享密钥。

[66] 结合第二方面，在第四种可能的实现方式中，所述方法还包括：所述第一设备和所述第二设备预定密钥交换算法；

[67] 以便所述第一设备利用第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给第二设备包括：以便所述第一设备利用第二设备的公钥和自身的私钥按照所述密钥交换算法生成第一共享密钥，并将第一设备的公钥发送给所述第二设备；

[68] 以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[69] 结合第二方面的第四种可能的实现方式，在第五种可能的实现方式中，所述第一设备和所述第二设备预定共享密钥交换算法包括：

[70] 所述第一设备和所述第二设备上预先配置有所述密钥交换算法所使用的参数；或者，

[71] 所述配置设备将所述密钥交换算法所使用的参数发送给所述第一设备和所述第二设备。

[72] 结合第二方面、第二方面的第一种至第五种可能的实现方式中的任一种，在第六种可能的实现方式中，所述配置设备获取第一设备的公钥；

[73] 所述配置设备将所述第二设备的公钥发送给第一设备包括：所述配置设备利用所述第一设备的公钥加密所述第二设备的公钥，将加密结果发送给所述第一设备；以便所述第一设备对所述加密结果进行解密，得到所述第二设备的公钥。

[74] 结合第二方面、第二方面的第一种至第五种可能的实现方式中的任一种，在第七种可能的实现方式中，该方法还包括：所述配置设备与所述第一设备建立安全连接以生成第二共享密钥；

[75] 将所述第二设备的公钥发送给第一设备包括：所述配置设备利用所述第二共享

密钥将所述第二设备的公钥进行加密后，将加密结果发送给所述第一设备；以便所述第一设备利用所述第二共享密钥对接收到的加密结果进行解密后，得到所述第二设备的公钥。

[76] 结合第二方面的第七种可能的实现方式，在第八种可能的实现方式中，所述配置设备与所述第一设备建立安全连接以生成第二共享密钥包括：

[77] 所述配置设备与所述第一设备通过WPS交互方式共享信任状，将所述信任状作为所述第二共享密钥；或者，

[78] 所述配置设备将自身的公钥发送给所述第一设备，所述配置设备和所述第一设备分别利用对方的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥。

[79] 结合第二方面、第二方面的第一种至第八种可能的实现方式中的任一种，在第九种可能的实现方式中，所述第一设备是被注册方enrollee，所述第二设备是registrar，或者所述第一设备是客户端client，所述第二设备是GO，或者所述第一设备是无线终端，所述第二设备是接入点，或者所述第一设备是中心节点，所述第二设备是传感器节点。

[80] 结合第二方面、第二方面的第一种至第九种可能的实现方式中的任一种，在第十种可能的实现方式中，该方法还包括：所述配置设备获取第二设备的信道信息并发送给所述第一设备；以便所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的步骤。

[81] 结合第二方面、第二方面的第一种至第十种可能的实现方式中的任一种，在第十一种可能的实现方式中，所述配置设备通过扫描二维码、通用串行总线USB或者近场通信的方式从所述第一设备或者第二设备获取信息。

[82] 第三方面，本发明实施例提供了一种密钥配置方法，该方法包括：

[83] 第二设备向配置设备提供第二设备的公钥，以便所述配置设备将所述第二设备的公钥发送给第一设备；

[84] 所述第二设备接收所述第一设备利用所述第二设备的公钥发送来的用于得到第一共享密钥的信息；或者接收所述第一设备利用所述第二设备的公钥生成第一

共享密钥后，发送来的用于得到第一共享密钥的信息；

[85] 所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[86] 结合第三方面，在第一种可能的实现方式中，所述第二设备接收所述第一设备利用第二设备的公钥发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到的；

[87] 所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

[88] 所述第二设备接收所述第一设备利用第二设备的公钥发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成密码后，利用所述第二设备的公钥将所述密码进行加密得到的；

[89] 所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[90] 结合第三方面，在第二种可能的实现方式中，所述第二设备接收所述第一设备利用第二设备的公钥发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成随机值，利用第二设备的公钥对该随机值进行加密后得到的，所述第一设备利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥；

[91] 所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第

一共享密钥。

[92] 结合第三方面，在第三种可能的实现方式中，所述第二设备接收所述第一设备利用所述第二设备的公钥发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备利用第二设备的公钥将第一设备的公钥进行加密后得到的加密结果；

[93] 所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥对所述加密结果进行解密后，得到所述第一设备的公钥，并生成密码，将该密码作为所述第一共享密钥，利用所述第一设备的公钥将该密码进行加密后，将加密结果发送给第一设备；

[94] 以便所述第一设备利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为所述第一共享密钥。

[95] 结合第三方面，在第四种可能的实现方式中，所述方法还包括：所述第二设备和所述第一设备预定密钥交换算法；

[96] 接收所述第一设备利用所述第二设备的公钥生成第一共享密钥后，发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备利用第二设备的公钥和自身的私钥按照所述密钥交换算法生成第一共享密钥后，发送来的第一设备的公钥；

[97] 所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[98] 结合第三方面的第四种可能的实现方式，在第五种可能的实现方式中，所述第二设备和所述第一设备预定密钥交换算法包括：

[99] 所述第二设备和所述第一设备上预先配置有所述密钥交换算法所使用的参数；或者，

[100] 所述第二设备和所述第一设备接收所述配置设备发送的所述密钥交换算法所使用的参数。

[101] 结合第三方面，第三方面的第一种至第五种可能的实现方式中的任一种，在第六种可能的实现方式中，所述第一共享密钥用于所述第一设备和所述第二设备

之间的安全连接包括：

[102] 所述第二设备接收第一设备发送的加密结果，该加密结果是所述第一设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后得到的；所述第二设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接；或者，

[103] 所述第二设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给所述第一设备；以便所述第一设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接。

[104] 结合第三方面的第六种可能的实现方式，在第七种可能的实现方式中，若所述第一设备是注册器Registrar、中心节点或者组长设备GO，则由所述第一设备生成所述信任状并将所述信任状的加密结果发送给所述第二设备；

[105] 若所述第二设备是Registrar、中心节点或GO，则由所述第二设备生成所述信任状并将所述信任状的加密结果发送给所述第一设备。

[106] 结合第三方面，第三方面的第一种至第七种可能的实现方式中的任一种，在第八种可能的实现方式中，该方法还包括：

[107] 所述第二设备将自身的信道信息提供给所述配置设备，以便所述配置设备将第二设备的信道信息发送给所述第一设备；以便所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的步骤。

[108] 结合第三方面，第三方面的第一种至第八种可能的实现方式中的任一种，在第九种可能的实现方式中，所述第二设备或者所述第一设备通过二维码、USB或近场通信的方式供所述配置设备获取信息。

[109] 结合第三方面，第三方面的第一种至第九种可能的实现方式中的任一种，在第十种可能的实现方式中，该方法还包括：

[110] 所述第二设备接收所述第一设备利用第二设备的公钥生成的验证值，所述第二

设备利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成所述第一共享密钥的步骤。

[111] 第四方面，该密钥配置装置包括：

[112] 配置接收单元，用于接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥；

[113] 密钥处理单元，用于利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备；或者利用所述第二设备的公钥生成第一共享密钥，将用于得到所述第一共享密钥的信息发送给所述第二设备；以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[114] 结合第四方面，在第一种可能的实现方式中，所述密钥处理单元，具体用于生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备，以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

[115] 所述密钥处理单元，具体用于生成密码，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备，利用密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为第一共享密钥，以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[116] 结合第四方面，在第二种可能的实现方式中，所述密钥处理单元，具体用于生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该随机值进行加密后，将加密结果发送给第二设备，以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[117] 结合第四方面，在第三种可能的实现方式中，所述密钥处理单元，具体用于利用第二设备的公钥将第一设备的公钥进行加密后，将加密结果发送给第二设备

；接收所述第二设备发送的加密结果，该加密结果是所述第二设备利用自身的私钥对接收到的加密结果进行解密后，得到所述第一设备的公钥，并且生成密码，将该密码作为所述第一共享密钥，利用所述第一设备的公钥将该密码进行加密后得到的；利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为所述第一共享密钥。

[118] 结合第四方面，在第四种可能的实现方式中，所述密钥处理单元，具体用于利用第二设备的公钥和自身的私钥按照所述第一设备和所述第二设备预定的密钥交换算法生成第一共享密钥，并将第一设备的公钥发送给所述第二设备，以便所述第二设备利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[119] 结合第四方面的第四种可能的实现方式，在第五种可能的实现方式中，所述密钥处理单元预先配置有所述密钥交换算法所使用的参数；

[120] 或者，所述配置接收单元，还用于接收所述配置设备发送的所述密钥交换算法所使用的参数，并提供给所述密钥处理单元。

[121] 结合第四方面、第四方面的第一种至第五种可能的实现方式中的任一种，在第六种可能的实现方式中，该密钥配置装置还包括：

[122] 安全连接单元，用于在所述密钥处理单元得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给所述第二设备；以便所述第二设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接；或者，用于利用得到的第一共享密钥或者第一共享密钥的衍生密钥对所述第二设备发送的信任状的加密结果进行解密得到所述信任状，所述信任状的加密结果为所述第二设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对所述信任状进行加密后得到，所述信任状用于所述第一设备和所述第二设备之间的安全连接。

[123] 结合第四方面、第四方面的第一种至第六种可能的实现方式中的任一种，在第七种可能的实现方式中，所述配置接收单元，具体用于接收配置设备在获取到

所述第二设备的公钥和所述第一设备的公钥后发送的加密结果，所述加密结果为所述配置设备利用所述第一设备的公钥加密的所述第二设备的公钥；

[124] 所述密钥处理单元，还用于对所述加密结果进行解密，得到所述第二设备的公钥。

[125] 结合第四方面、第四方面的第一种至第六种可能的实现方式中的任一种，在第八种可能的实现方式中，所述配置接收单元，具体用于与所述配置设备建立安全连接以生成第二共享密钥；接收所述配置设备在获取到第二设备的公钥后发送的加密结果，所述加密结果为所述配置设备利用所述第二共享密钥加密的所述第二设备的公钥；

[126] 所述密钥处理单元，还用于利用所述第二共享密钥对接收到的所述加密结果进行解密后，得到所述第二设备的公钥。

[127] 结合第四方面的第八种可能的实现方式，在第九种可能的实现方式中，所述配置接收单元在与所述配置设备建立安全连接以生成第二共享密钥时，具体与所述配置设备通过无线保真安全建立WPS交互方式共享信任状，将所述信任状作为所述第二共享密钥；或者，具体接收所述配置设备发送的所述配置设备的公钥，所述第一设备利用所述配置设备的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥。

[128] 结合第四方面的第四种可能的实现方式，在第十种可能的实现方式中，所述密钥处理单元在得到所述第二设备的公钥之后，还用于生成新的公钥和新的私钥；

[129] 所述第一设备发送给所述第二设备的第一设备的公钥为所述新的公钥；所述第二设备在生成所述第一共享密钥时利用的第一设备的公钥为所述新的公钥；所述第一设备在生成所述第一共享密钥时利用的自身的私钥为所述新的私钥。

[130] 结合第四方面、第四方面的第一种至第十种可能的实现方式中的任一种，在第十一种可能的实现方式中，所述第一设备是被注册方enrollee，所述第二设备是registrar，或者所述第一设备是客户端client，所述第二设备是GO，或者所述第一设备是无线终端，所述第二设备是接入点，或者所述第一设备是中心节点，所述第二设备是传感器节点。

[131] 结合第四方面、第四方面的第一种至第十一种可能的实现方式中的任一种，在第十二种可能的实现方式中，所述配置接收单元，还用于接收所述配置设备从所述第二设备获取后发送来的第二设备的信道信息；

[132] 所述密钥处理单元根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的操作。

[133] 结合第四方面、第四方面的第一种至第十二种可能的实现方式中的任一种，在第十三种可能的实现方式中，所述密钥处理单元，还用于利用所述第二设备的公钥生成验证值，将所述验证值发送给所述第二设备；以便所述第二设备在生成所述第一共享密钥之前，利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成所述第一共享密钥的操作。

[134] 第五方面，该密钥配置装置包括：

[135] 信息获取单元，用于获取第二设备的公钥；

[136] 信息发送单元，用于将所述第二设备的公钥发送给第一设备；

[137] 以便所述第一设备利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备；或者以便所述第一设备利用所述第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给所述第二设备；

[138] 以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[139] 结合第五方面，在第一种可能的实现方式中，所述信息发送单元，还用于将密钥交换算法所使用的参数发送给所述第一设备和所述第二设备,所述密钥交换算法用于所述第一设备和所述第二设备利用自身的私钥和对方的公钥按照所述密钥交换算法生成第一共享密钥。

[140] 结合第五方面或者第五方面的第一种可能的实现方式，在第二种可能的实现方式中，所述信息获取单元，还用于获取第一设备的公钥；

[141] 所述信息发送单元，具体用于利用所述第一设备的公钥加密所述第二设备的公钥，将加密结果发送给所述第一设备，以便所述第一设备对所述加密结果进行解密，得到所述第二设备的公钥。

[142] 结合第五方面或者第五方面的第一种可能的实现方式，在第三种可能的实现方式中，所述信息发送单元，还用于与所述第一设备建立安全连接以生成第二共享密钥；在将所述第二设备的公钥发送给第一设备时，具体利用所述第二共享密钥将所述第二设备的公钥进行加密后，将加密结果发送给所述第一设备，以便所述第一设备利用所述第二共享密钥对接收到的加密结果进行解密后，得到所述第二设备的公钥。

[143] 结合第五方面的第三种可能的实现方式，在第四种可能的实现方式中，所述信息发送单元在与所述第一设备建立安全连接以生成第二共享密钥时，具体用于与所述第一设备通过WPS交互方式共享信任状，将所述信任状作为所述第二共享密钥；或者，将自身的公钥发送给所述第一设备，利用第一设备的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥。

[144] 结合第五方面、第五方面的第一种至第四种可能的实现方式中的任一种，在第五种可能的实现方式中，所述信息获取单元，还用于获取第二设备的信道信息；

[145] 所述信息发送单元，还用于将所述第二设备的信道信息发送给所述第一设备，以便所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的操作。

[146] 结合第五方面、第五方面的第一种至第五种可能的实现方式中的任一种，在第六种可能的实现方式中，所述信息获取单元，具体用于通过扫描二维码、通用串行总线USB或者近场通信的方式从所述第一设备或者第二设备获取信息。

[147] 第六方面，该密钥配置装置包括：

[148] 信息提供单元，用于向配置设备提供第二设备的公钥，以便所述配置设备将所述第二设备的公钥发送给第一设备；

[149] 信息接收单元，用于接收所述第一设备利用所述第二设备的公钥发送来的用于得到第一共享密钥的信息；或者接收所述第一设备利用所述第二设备的公钥生成第一共享密钥后，发送来的用于得到第一共享密钥的信息；

[150] 密钥处理单元，用于利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之

间的安全连接。

[151] 结合第六方面，在第一种可能的实现方式中，所述信息接收单元，具体用于接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到的；

[152] 所述密钥处理单元，具体用于利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

[153] 所述信息接收单元，具体用于接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成密码后，利用所述第二设备的公钥将所述密码进行加密得到的；

[154] 所述密钥处理单元，具体用于利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[155] 结合第六方面，在第二种可能的实现方式中，所述信息接收单元，具体用于接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成随机值，利用第二设备的公钥对该随机值进行加密后得到的，所述第一设备利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥；

[156] 所述密钥处理单元，具体用于利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[157] 结合第六方面，在第三种可能的实现方式中，所述信息接收单元，具体用于接收所述第一设备利用第二设备的公钥将第一设备的公钥进行加密后得到的加密结果；

[158] 所述密钥处理单元，具体用于利用自身的私钥对所述加密结果进行解密后，得到所述第一设备的公钥，并生成密码，将该密码作为所述第一共享密钥，利用所述第一设备的公钥将该密码进行加密后，将加密结果发送给第一设备，以便所述第一设备利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为所述第一共享密钥。

[159] 结合第六方面，在第四种可能的实现方式中，所述信息接收单元，具体用于接收所述第一设备利用第二设备的公钥和自身的私钥按照密钥交换算法生成第一共享密钥后，发送来的第一设备的公钥；所述密钥交换算法是所述第一设备和所述第二设备预定的；

[160] 所述密钥处理单元，具体用于利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[161] 结合第六方面的第四种可能的实现方式，在第五种可能的实现方式中，所述密钥处理单元预先配置有所述密钥交换算法所使用的参数；或者，

[162] 所述信息接收单元，还用于接收所述配置设备发送的所述密钥交换算法所使用的参数，并提供给所述密钥处理单元。

[163] 结合第六方面、第六方面的第一种至第五种可能的实现方式中的任一种，在第六种可能的实现方式中，该密钥配置装置还包括：

[164] 安全连接单元，用于接收第一设备发送的加密结果，该加密结果是所述第一设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后得到的；利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接；或者，

[165] 用于在所述密钥处理单元得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给所述第一设备；以便所述第一设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接。

[166] 结合第六方面、第六方面的第一种至第六种可能的实现方式中的任一种，在第七种可能的实现方式中，所述信息提供单元，还用于将第二设备的信道信息提供给所述配置设备，以便所述配置设备将第二设备的信道信息发送给所述第一设备；以便所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的操作。

[167] 结合第六方面、第六方面的第一种至第七种可能的实现方式中的任一种，在第

八种可能的实现方式中，所述信息提供单元，具体用于通过二维码、USB或近场通信的方式向所述配置设备提供信息。

[168] 结合第六方面、第六方面的第一种至第七种可能的实现方式中的任一种，在第九种可能的实现方式中，所述信息接收单元，还用于接收所述第一设备利用第二设备的公钥生成的验证值；

[169] 所述密钥处理单元，还用于利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成所述第一共享密钥的操作。

[170] 第七方面，该密钥配置系统包括：如第四方面所述的密钥配置装置、如第五方面所述的密钥配置装置以及如第六方面所述的密钥配置装置；或者，

[171] 如第四方面的第一种可能的实现方式所述的密钥配置装置、如第五方面所述的密钥配置装置以及如第六方面的第一种可能的实现方式所述的密钥配置装置；或者，

[172] 如第四方面的第二种可能的实现方式所述的密钥配置装置、如第五方面所述的密钥配置装置以及第六方面的第二种可能的实现方式所述的密钥配置装置；或者，

[173] 如第四方面的第三种可能的实现方式所述的密钥配置装置、如第五方面所述的密钥配置装置以及如第六方面的第三种可能的实现方式所述的密钥配置装置；或者，

[174] 如第四方面的第四种可能的实现方式所述的密钥配置装置、如第五方面所述的密钥配置装置以及如第六方面的第四种可能的实现方式所述的密钥配置装置；或者，

[175] 如第四方面的第五种可能的实现方式所述的密钥配置装置、如第五方面的第一种可能的实现方式所述的密钥配置装置以及如第六方面的第五种可能的实现方式所述的密钥配置装置；或者，

[176] 如第四方面的第六种可能的实现方式所述的密钥配置装置、如第五方面所述的密钥配置装置以及如第六方面的第六种可能的实现方式所述的密钥配置装置；或者，

[177] 如第四方面的第七种可能的实现方式所述的密钥配置装置、如第五方面的第二

种可能的实现方式所述的密钥配置装置以及如第六方面、第六方面的第一种至第六种可能的实现方式中的任一种所述的密钥配置装置；或者，

[178] 如第四方面的第八种可能的实现方式所述的密钥配置装置、如第五方面的第三种可能的实现方式所述的密钥配置装置以及如第六方面、第六方面的第一种至第六种可能的实现方式中的任一种所述的密钥配置装置；或者，

[179] 如第四方面的第九种可能的实现方式所述的密钥配置装置、如第五方面的第四种可能的实现方式所述的密钥配置装置以及如第六方面、第六方面的第一种至第六种可能的实现方式中的任一种所述的密钥配置装置；或者，

[180] 如第四方面的第十种可能的实现方式所述的密钥配置装置、如第五方面所述的密钥配置装置以及如第六方面的第四种可能的实现方式所述的密钥配置装置；或者，

[181] 如第四方面的第十一种可能的实现方式所述的密钥配置装置、如第五方面、第五方面的第一种至第四种可能的实现方式中的任一种所述的密钥配置装置以及如第六方面、第六方面的第一种至第六种可能的实现方式中的任一种所述的密钥配置装置；或者，

[182] 如第四方面的第十二种可能的实现方式所述的密钥配置装置、如第五方面的第五种可能的实现方式所述的密钥配置装置以及如第六方面的第七种可能的实现方式所述的密钥配置装置；或者，

[183] 如第四方面的第十三种可能的实现方式所述的密钥配置装置、如第五方面、第五方面的第一种至第五种可能的实现方式中的任一种所述的密钥配置装置以及如第六方面的第九种可能的实现方式所述的密钥配置装置；或者，

[184] 如第四方面、第四方面的第一种至第十三种可能的实现方式中的任一种所述的密钥配置装置、如第五方面的第六种可能的实现方式所述的密钥配置装置以及如第六方面的第八种可能的实现方式所述的密钥配置装置。

[185] 由以上技术方案可以看出，第三方的配置设备在本发明仅用于进行第一设备和第二设备之间公钥和设备信息的传递，而用于第一设备和第二设备之间安全连接的第一共享密钥是在第一设备和第二设备分别生成的，并且第一设备和第二设备之间也不直接进行第一共享密钥的传递，而是将用于得到第一共享密钥的

信息传递给第二设备，必须由第二设备的私钥才能生成第一共享密钥。因此，即便攻击者窃听到配置设备、第一设备和第二设备之间传递的公钥也无法得到第一共享密钥，从而提高了第一设备和第二设备之间交互的安全性。

[186] 【附图说明】

[187] 图1为现有技术中基于第三方的配置设备的密钥配置方法流程示意图；

[188] 图2为本发明实施例一提供的密钥配置方法的流程示意图；

[189] 图3为本发明实施例二提供的密钥配置方法的流程示意图；

[190] 图4为本发明实施例三提供的密钥配置方法的流程示意图；

[191] 图5为本发明实施例四提供的密钥配置方法的流程示意图；

[192] 图6为本发明实施例五提供的密钥配置方法的流程示意图；

[193] 图7为本发明实施例六提供的密钥配置方法的流程示意图；

[194] 图8为本发明实施例提供的系统组成示意图；

[195] 图9为本发明实施例提供的设置于第一设备中的密钥配置装置的结构示意图；

[196] 图10为本发明实施例提供的设置于配置设备中的密钥配置装置的结构示意图；

[197] 图11为本发明实施例提供的设置于第二设备中的密钥配置装置的结构示意图；

[198] 图12为本发明实施例提供的配置设备的硬件结构示意图；

[199] 图13为本发明实施例提供的第一设备的硬件结构示意图；

[200] 图14为本发明实施例提供的第二设备的硬件结构示意图。

[201] 【具体实施方式】

[202] 为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

[203] 本发明的核心思想在于：第三方的配置设备获取第二设备的公钥；将第二设备的公钥发送给第一设备；第一设备生成共享密钥，并利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备，或者第一设备利用第二设备的公钥生成第一共享密钥，并将用于得到第一共享密钥的信息发送给第二设备；按照第二设备的设备信息将第一设备的公钥发送给第二设备；第二设备利用自身的私钥和用于得到第一共享密钥的信息生成共享密钥，该共享密钥用于第一设备和第二设备之间的安全连接。

[204] 在上述核心思想之下，本发明可以采用密钥交换的方式进行共享密钥的配置，也可以不采用密钥交换的方式进行共享密钥的配置。下面分别通过几个具体的实施例对本发明提供的方法进行详细描述。

[205] 实施例一、

[206] 在本实施例中，采用的是密钥交换的方式进行共享密钥的配置，第一设备和第二设备预定密钥交换算法，密钥交换算法是后续第一设备和第二设备在生成共享密钥时所采用的算法，可以采用但不限于：D-H算法、RSA算法或ElGamal算法等，根据不同的密钥交换算法，预先共享的参数有所不同。密钥交换算法的核心在于：设备公开自身的公钥，保留自己的私钥，利用对方的公钥和自己的私钥生成共享密钥，利用该共享密钥确保穿越不安全网络的消息的安全性。

[207] 共享密钥交换算法所使用的参数的方式可以包括但不限于以下两种：第一种方式：预先在第一设备和第二设备上配置密钥交换算法所使用的参数；第二种方式：通过第三方的配置设备将密钥交换算法所使用的参数发送给第一设备和第二设备。

[208] 在本发明的各实施例中均以D-H算法为例，第一设备和第二设备预先共享参数g和P，预先在第一设备和第二设备上共享参数g和P，其中P是素数，g是P的原根。另外，在第一设备和第二设备都具有各自的公钥和私钥，第一设备上的公钥和私钥分别为PkeyA和keyA，第二设备上的公钥和私钥分别为PkeyB和keyB。本发明后续实施例二和三中均存在上述配置，不再一一赘述。

[209] 图2为本发明实施例一提供的密钥配置方法的流程示意图，如图2所示，该流程可以包括以下步骤：

[210] 步骤201：配置设备获取第一设备的公钥PkeyA和设备信息

[211] 所述设备信息：至少包括第一设备的地址信息。

[212] 本步骤是本实施例中的可选步骤。

[213] 步骤202：配置设备获取第二设备的公钥PkeyB和设备信息。

[214] 所述设备信息：至少包括第二设备的地址信息。

[215] 本发明并不对上述两个步骤的先后顺序进行限制，可以以任意的顺序先后执行，也可以同时执行。

[216] 上述设备信息主要是地址信息，还可以包括但不限于以下设备信息：UUID（Universally Unique Identifier，通用唯一识别码）、制造商、序列号、设备能力等。设备能力指的是该设备支持的算法、认证方法、设备角色信息、设备类型信息等，其中设备角色信息是指该设备在注册时充当的角色，可以是enrollee、registrar、client或GO等。设备类型信息可以是WiFi无线终端（诸如手机、电脑、传感器等）、接入点（在wifi网络中是AP）、传感器节点、中心节点等。在本实施例中配置设备获取的设备信息主要是地址信息。

[217] 第一设备的公钥PkeyA、第一设备的设备信息以及第二设备的公钥PkeyB、第二设备的设备信息可以通过多种方式获取，例如通过NFC、USB等安全媒介获取，特别地，对于无头设备而言优选通过扫描识别码的方式，即将第一设备的公钥PkeyA和第一设备的设备信息编码到第一设备的扫描识别码，配置设备通过扫描该扫描识别码就能够获取到第一设备的公钥PkeyA和第一设备的设备信息，对于第二设备同样如此。其中扫描识别码可以是诸如二维码、条形码等。

[218] 步骤203：配置设备根据第一设备的设备信息将第二设备的公钥PkeyB和设备信息发送给第一设备。

[219] 在本步骤中，为了进一步提高安全性和可靠性，配置设备可以利用第一设备的公钥PkeyA加密第二设备的公钥PkeyB和设备信息，然后将加密结果发送给第一设备。

[220] 在此对利用公钥加密的方式进行说明，主要分为两种加密方式：

[221] 第一种加密方式：如果公钥是用于非对称加密的公钥，可以直接用于加密，需要使用对应的私钥进行解密。

[222] 第二种加密方式：如果公钥是用于密钥交换的公钥，则采用公钥的部分信息进行加密，或者基于公钥衍生的信息进行加密，解密时需要采用对称密钥来解密，而不是利用对应的私钥解密。

[223] 后续的加密、解密过程可以根据具体情况采用上述加密方式中的其中一种。

[224] 此处的加密采用的是第二种加密方式。

[225] 步骤204：第一设备利用第二设备的公钥PkeyB生成验证值，将生成的验证值发送给第二设备。

[226] 如果配置设备发送来的是加密结果，则第一设备首先对加密结果进行解密后得到第二设备的公钥PkeyB和设备信息。

[227] 本步骤中利用第二设备的公钥PkeyB生成的验证值可以是但不限于是PkeyB的hash（哈希）值，也可以是利用其它预设算法生成的验证值。

[228] 步骤205：第一设备利用第二设备的设备信息向第二设备发送第一设备的公钥PkeyA。

[229] 第一设备获取到第二设备的地址信息后，将上述验证值和PkeyA发送给第二设备。由于本实施例采用的是密钥交换的方式进行共享密钥的配置，因此本实施例中第一设备发送给第二设备的用于得到共享密钥的信息为第一设备的公钥PkeyA。

[230] 另外，需要说明的是，上述步骤204和步骤205同样没有先后顺序的限制，可以以任意的顺序先后执行，也可以同时执行。

[231] 步骤206：第二设备利用自身的公钥PkeyB对接收到的验证值进行验证，如果验证通过，则记录第一设备的公钥PkeyA。

[232] 需要说明的是，步骤204以及本步骤中第二设备对验证值进行的验证是为了进一步提高安全性和可靠性所执行的操作，并不是本发明所必须的步骤。如果没有步骤204，则第二设备直接记录接收到的PkeyA。

[233] 第二设备在进行验证时，可以利用自身的公钥PkeyB采用与第一设备相同的生成验证值的方法生成验证值，将生成的验证值与接收到的验证值进行对比，如果一致，则验证通过，否则验证失败。如果验证失败，则可以丢弃接收到的第一设备的公钥PkeyA，不再执行后续流程，并且可以进一步提示用户配置失败，例如采用指示灯的方式，或者在屏幕上显示的方式，或者语音的方式等等。

[234] 步骤207：第一设备和第二设备分别利用对方的公钥和自身的私钥产生共享密钥。

[235] 需要说明的是，第一设备可以在步骤203之后任意时刻产生共享密钥，即在获取到第二设备的公钥后就可以产生共享密钥，并不一定在此步骤中。

[236] 第一设备和第二设备采用预先共享的密钥交换算法来产生共享密钥，以D-H算法为例，第一设备的公钥PkeyA=(g^keyA)mod(P)，其中keyA为第一设备的私钥

，为随机数，第二设备中的PkeyB=(g^keyB)mod(P)，keyB为第二设备的私钥，也是随机数。上述公式中，^为次幂的运算符，X^Y表示X的Y次幂，mod为取模的运算符，XmodY表示X对Y取模。第一设备利用PkeyB和keyA产生共享密钥DHkeyA，即：

[237] DHkeyA=((PkeyB)^keyA)mod(P)

[238] 第二设备利用PkeyA和keyB产生共享密钥DHkeyB，即：

[239] DHkeyB=((PkeyA)^keyB)mod(P)

[240] 由D-H算法可知，DHkeyA= DHkeyB。

[241] 步骤208：第一设备和第二设备基于共享密钥进行安全连接。

[242] 即第一设备和第二设备可以基于共享密钥进行后续的交互，后续的交互可以包括但不限于：认证过程、关联过程、数据交互过程等。至于如何利用共享密钥进行安全连接可以采用现有技术，在此不再赘述。

[243] 更进一步地，除了直接基于共享密钥进行安全连接之外，第一设备和第二设备可以基于共享的密钥衍生算法对共享密钥生成衍生密钥，利用衍生密钥进行后续的安全连接。本发明对于密钥衍生算法不加以限制，只要第一设备和第二设备预先约定了一致的密钥衍生算法即可。

[244] 或者进一步利用共享密钥传递信任状：第一设备在生成共享密钥后，生成信任状，并利用共享密钥或者共享密钥的衍生密钥对信任状进行加密后，将加密结果传递给第二设备；第二设备利用生成的共享密钥或者共享密钥的衍生密钥对加密结果进行解密得到信任状。或者，第二设备在生成共享密钥后生成信任状，并利用共享密钥或者共享密钥的衍生密钥对信任状进行加密后，将加密结果传递给第一设备；第一设备利用生成的共享密钥或者共享密钥的衍生密钥对加密结果进行解密得到信任状。

[245] 这里具体是第一设备向第二设备发送信任状还是第二设备向第一设备发送信任状，可以根据设备类型决定，如果第一设备是registrar、中心节点或者GO，则可以由第一设备生成信任状并发送给第二设备。

[246] 实施例二、

[247] 本实施例采用的也是密钥交换的方式进行共享密钥的配置，图3为本发明实施

例二提供的密钥配置方法的流程示意图，在本实施例中对与实施例一相同的步骤不再赘述，参见实施例一中的描述。如图3所示，该流程包括以下步骤：

[248] 步骤301同步骤201。

[249] 步骤302同步骤302。

[250] 步骤303：配置设备与第一设备建立安全连接以生成共享密钥DHkeyC'和DHkeyA'。

[251] 本步骤的实现方式可以采用但不限于以下两种：

[252] 第一种方式：配置设备与第一设备之间通过现有的WPS交互方式共享信任状（即背景技术中关于图1的描述中生成的key1），以该信任状作为共享密钥DHkey'。

[253] 第二种方式：配置设备将自身的公钥PkeyC发送给第一设备，配置设备利用第一设备的公钥PkeyA和配置设备的私钥keyC执行密钥交换算法，生成共享密钥DHkeyC'，第一设备利用配置设备的公钥PkeyC和第一设备的私钥keyA执行密钥交换算法，生成共享密钥DHkeyA'。

[254] 这种方式下，需要预先在配置设备与第一设备预先共享密钥交换算法所使用的参数。以D-H算法为例的话，配置设备也预先获取到共享参数g和P。配置设备中的PkeyC=(g^keyC)mod(P)，配置设备生成的共享密钥DHkeyC'=((PkeyA)^keyC)mod(P)，第一设备生成的共享密钥DHkeyA'=((PkeyC)^keyA)mod(P)。由D-H算法可知，DHkeyC'= DHkeyA'。

[255] 步骤304：配置设备利用共享密钥DHkeyC'将第二设备的公钥PkeyB和设备信息进行加密后，将加密结果发送给第一设备。

[256] 步骤305：第一设备利用共享密钥DHkeyA'对接收到的加密结果进行解密后，获取第二设备的公钥PkeyB和设备信息。

[257] 或者，在步骤304中配置设备也可以利用共享密钥DHkeyC'先生成衍生密钥，再利用衍生密钥将第二设备的公钥PkeyB和设备信息进行加密后发送给第一设备，具体衍生密钥的生成方式在此不加以显示，只要配置设备和第一设备预先约定即可。相应地，在步骤305中，第一设备利用共享密钥DHkeyA'先生成衍生密钥，再利用衍生密钥对接收到的加密结果进行解密。

[258] 步骤306：第一设备生成新的私钥keyA’和新的公钥PkeyA’。

[259] 本步骤是为了进一步增强交互的安全性所执行的步骤，第一设备产生新的随机数作为私钥keyA’，然后利用该新的私钥生成新的公钥PkeyA’，以D-H算法为例，PkeyA’ =(g^keyA’)mod(P)。

[260] 后续步骤307至步骤311分别同实施例一中的步骤204至步骤208，只是其中涉及到的第一设备的公钥和私钥分别替换为步骤306中新的公钥PkeyA’和keyA’。

[261] 实施例三、

[262] 本实施例采用的也是密钥交换的方式进行共享密钥的配置，图4为本发明实施例三提供的密钥配置方法的流程示意图，同样，在本实施例中对与实施例一相同的步骤不再赘述，参见实施例一中的描述。如图4中所示，该流程包括以下步骤：

[263] 步骤401同步骤201，需要说明的是，在本步骤中配置设备获取到的第一设备的设备信息中至少包括第一设备的地址信息和第一设备的设备角色信息或设备类型信息，其中设备角色信息是指该设备在注册时充当的角色，例如可以是enrollee、registrar、client或GO等。设备类型信息可以是无线终端、接入点、传感器节点、中心节点等。

[264] 步骤402同步骤202，同样，配置设备获取到的第二设备的设备信息中至少包括第二设备的地址信息和第二设备的设备角色信息或设备类型信息。

[265] 与实施例一中的描述相同的，第一设备的公钥PkeyA、设备信息以及第二设备的公钥PkeyB、设备信息可以通过多种方式获取，例如通过NFC、USB等安全媒介获取，特别地，对于无头设备而言优选通过扫描识别码的方式，即将第一设备的公钥PkeyA和设备信息写入第一设备上的扫描识别码，配置设备通过扫描该扫描识别码就能够获取到第一设备的公钥PkeyA和设备信息，对于第二设备同样如此。其中扫描识别码可以是诸如二维码、条形码等。

[266] 步骤403：配置设备根据第一设备和第二设备的设备角色信息或设备类型信息，确定是将第一设备的公钥和设备信息发送给第二设备，或者将第二设备的公钥和设备信息发送给第一设备。

[267] 在本步骤中，如果第一设备是enrollee，第二设备是registrar，或者第一设备是c

lient，第二设备是GO，或者第一设备是无线终端，第二设备是接入点，则确定将第二设备的公钥和设备信息发送给第一设备，目的是第一设备能够快速扫描发现第二设备，提高效率。如果第一设备是中心节点，第二设备是传感器节点，则确定将第二设备的公钥和设备信息发送给第一设备，目的是中心节点能够快速发现传感器节点。如果第一设备和第二设备的角色或类型对等，例如都是传感器节点，或者都是client等，那么无论确定将第二设备的公钥和设备信息发送给第一设备，还是将第一设备的公钥和设备信息发送给第二设备均可。本步骤为可选的。

[268] 假设步骤403确定将第二设备的公钥和设备信息发送给第一设备，步骤404同步骤203。

[269] 步骤405至步骤409同步骤204至步骤208。

[270] 但在本实施例中，执行步骤405之前，第一设备可以首先根据自己以及第二设备的设备角色信息或设备类型信息确定第一设备与第二设备建立连接的方式，从而决定在步骤405中采用什么消息类型发送验证值和第一设备的公钥PkeyA。例如，若第一设备为enrollee，第二设备是registrar，或者第一设备为无线终端，第二设备为接入点，则第一设备可以通过探测消息将验证值和第一设备的公钥PkeyA发送给第二设备。若第一设备为registrar，第二设备是enrollee，或者第一设备是接入点，第二设备是无线终端，则第一设备可以通过广播消息将验证值和第一设备的公钥PkeyA发送给第二设备。若第一设备是GO，第二设备是client，则第一设备可以通过邀请消息将验证值和第一设备的公钥PkeyA发送给第二设备。若第一设备是client，第二设备是GO，则第一设备可以通过探测消息将验证值和第一设备的公钥PkeyA发送给第二设备。若第一设备是传感器节点，第二设备是中心节点，则第一设备可以通过请求消息将验证值和第一设备的公钥PkeyA发送给第二设备。若第一设备是中心节点，第二设备是传感器节点，则第一设备可以通过邀请消息或广播消息将验证值和第一设备的公钥PkeyA发送给第二设备。

[271] 可选地，配置设备获取的第一设备和第二设备的设备信息中还可以包括信道信息，这种情况下，第一设备可以根据第二设备的信道信息快速发现第二设备，

并执行步骤405和步骤406，即将验证值和第一设备的公钥PkeyA发送给第二设备。

[272] 除此之外，该实施例从步骤405开始也可以按照实施例二中从步骤306开始执行直至第一设备和第二设备基于共享密钥进行安全连接。

[273] 实施例四、

[274] 本实施例采用的并不是密钥交换的方式进行的共享密钥配置，图5为本发明实施例四提供的密钥配置方法的流程示意图，在本实施例中重点突出与实施例一不同的步骤，与实施例一中相同的步骤不再赘述。如图5中所示，该流程包括以下步骤：

[275] 步骤501同步骤201。

[276] 步骤502同步骤202。

[277] 步骤503同步骤203。

[278] 步骤504同步骤204。

[279] 步骤505：第一设备生成一个password（密码），利用第二设备的公钥PkeyB将该password进行加密后，将加密结果发送给第二设备。

[280] 此处的加密采用的是实施例一中所述的第一种加密方法。

[281] 也就是说，第一设备获取到第二设备的地址信息后，将验证值和password进行加密后的加密结果发送给第二设备。也就是说，本实施例中第一设备发送给第二设备的用于得到共享密钥的信息为第一设备生成的上述password。

[282] 第一设备生成password的方式可以是任意的，比如采用产生随机数作为password的方式，或者采用预设算法生成password的方式等等。

[283] 步骤506：第二设备利用自身的公钥PkeyB对接收到的验证值进行验证，如果验证通过，则采用自身的私钥keyB对接收到的加密结果进行解密，得到password。

[284] 在本实施例中，第二设备的公私钥对（PkeyB，keyB），通过一定的加解密算法，使得利用PkeyB进行加密的加密结果能够通过keyB进行解密，这种加解密算法可以采用现有的各种方式，在此不再一一赘述。

[285] 步骤507：第一设备和第二设备利用上述password生成共享密钥。

[286] 在本步骤中，第一设备和第二设备可以直接将password作为共享密钥，也可以

利用预先约定的密钥衍生算法对所述password生成衍生密钥后，将该衍生密钥作为共享密钥。

[287] 同样第一设备生成共享密钥的操作可以在生成password之后的任意时刻执行，并不限于在本步骤中执行。

[288] 步骤508同步骤208。

[289] 需要说明的是，实施例二中步骤303至步骤306所描述的技术内容以及实施例三中步骤403所描述的技术内容对于实施例四同样适用，在此不再赘述。

[290] 实施例五、

[291] 除了实施例一中所述的生成共享密钥的方式之外，还存在另一种生成共享密钥的方式，参见图6，本实施例所示的流程包括以下步骤：

[292] 步骤601同步骤201。

[293] 步骤602同步骤202。

[294] 步骤603同步骤203。

[295] 步骤604同步骤204。

[296] 步骤605：第一设备生成随机值Nonce，利用第二设备的公钥PkeyB和该随机值Nonce生成共享密钥DHkey。

[297] 在此，除了利用第二设备的公钥PkeyB和随机值Nonce生成共享密钥DHkey之外，还可以采用其他第一设备和第二设备约定的信息和随机值生成共享密钥DHkey，例如可以采用第二设备的MAC（Media Access Control，媒体访问控制）值、第二设备的公钥Pkey的hash值等等。

[298] 步骤606：第一设备利用第二设备的公钥PkeyB对该随机值Nonce进行加密后，将加密结果发送给第二设备。

[299] 本实施例中用于得到共享密钥的信息为该随机值Nonce。这里的加密方式可以为实施例一中所述的第一种加密方法。

[300] 第二设备接收到该加密结果后，对加密结果进行解密，得到该随机值Nonce。

[301] 步骤607同步骤206，只是验证通过后，记录的是随机值Nonce。

[302] 步骤608：第二设备利用自身的公钥PkeyB和随机值Nonce生成共享密钥DHkey。

[303] 在此只要第一设备和第二设备预先约定生成共享密钥的算法即可，在此不具体限制生成共享密钥的算法。

[304] 步骤609同步骤208。

[305] 实施例六、

[306] 图7为本发明实施例六提供的密钥配置方法的流程示意图，如图7所示，该方法包括：

[307] 步骤701同步骤201。

[308] 步骤702同步骤202。

[309] 步骤703同步骤203。

[310] 步骤704：第一设备向第二设备发送自身的公钥PkeyA。

[311] 在此，为了提高安全性，第一设备可以利用第二设备的公钥PkeyB加密PkeyA后发送给第二设备，第二设备利用自身的私钥keyB进行解密后得到PkeyA。

[312] 此处的加密采用的是实施例一中所述的第一种加密方式。

[313] 步骤705：第二设备利用第一设备的公钥PkeyA加密一个密码，将加密结果发送给第一设备。其中该密码可以是信任状或者会话密钥等，可以是随机生成的，也可以是按照某个算法生成的，在此不加以限制。

[314] 在此第二设备可以利用第一设备的公钥PkeyA生成一个验证值，例如生成PkeyA的hash值发送给第一设备，第一设备接收到验证值后首先利用自身的公钥PkeyA生成验证值，将生成的验证值与接收到的验证值进行比对，如果一致，则确定验证通过，继续执行步骤706。

[315] 步骤706：第一设备利用自己的私钥keyA对加密结果进行解密，得到密码。

[316] 步骤707：第一设备和第二设备利用上述的密码或者密码的衍生密钥进行后续的安全连接。

[317] 实施例七中用于得到共享密钥的信息就是第一设备的公钥。

[318] 以上是对本发明所提供的方法进行的描述，下面对对应的系统进行详细描述。图8为本发明实施例提供的系统组成示意图，如图8所示，该系统包括第一设备、第二设备和第三方的配置设备。

[319] 其中配置设备，用于获取第二设备的公钥，将第二设备的公钥发送给第一设备

。

[320] 第一设备主要负责生成第一共享密钥并将用于得到第一共享密钥的信息提供给第二设备，供第二设备生成第一共享密钥。具体地，第一设备可以采用以下两种方式实现该功能：

[321] 第一种方式：第一设备生成第一共享密钥，根据第二设备的设备信息，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备。这种方式对应于上述实施例四中所描述的方式

[322] 第二种方式：利用第二设备的公钥生成第一共享密钥，并根据第二设备的设备信息，将用于得到第一共享密钥的信息发送给第二设备。这种方式对应于上述实施例一至三中所描述的方式。

[323] 第二设备，用于利用自身的私钥以及用于得到第一共享密钥的信息生成第一共享密钥，上述的第一共享密钥用于第一设备和第二设备之间的安全连接。

[324] 需要说明的是，在此第一共享密钥的名称是为了与后续优选实施方式中配置设备和第一设备之间共享的第二共享密钥相区别。

[325] 下面对第一设备的两种实现方式分别进行详细描述。对于第一种方式而言，第一设备生成password，将该password作为第一共享密钥，或者利用密钥衍生算法对该password生成衍生密钥，将该衍生密钥作为第一共享密钥；然后利用第二设备的公钥将密码进行加密后，将加密结果发送给第二设备。这种方式下，用于得到第一共享密钥的信息为password。其中第一设备生成password的方式可以是任意的，比如采用产生随机数作为password的方式，或者采用预设算法生成password的方式等等。

[326] 第二设备利用自身的私钥对加密结果进行解密得到密码，将密码作为第一共享密钥，或者利用密钥衍生算法对密码生成衍生密钥，将该衍生密钥作为第一共享密钥。在这种方式下，第二设备的公私钥对（PkeyB，keyB），通过一定的加解密算法，使得利用公钥PkeyB进行加密的加密结果能够通过私钥keyB进行解密，这种加解密算法已经是现有十分成熟的方式，在此不再一一赘述。

[327] 在第一种方式中，还存在一种实现，即第一设备生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该

随机值进行加密后，将加密结果发送给第二设备。第二设备利用自身的私钥对该加密结果进行加密得到该随机值，然后利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥。在这种实现中，所述第一设备和第二设备约定的信息可以是第二设备的公钥、第二设备公钥的hash值、第二设备的MAC地址等信息，这些信息可以由第三方的配置设备从第二设备获取后发送给第一设备，甚至还可以是第一设备和第二设备预先配置好的一些特定值。

[328] 对于第二种方式而言，第一设备和第二设备需要预定密钥交换算法，这里可以采用的密钥交换算法可以是但不限于是D-H算法、RSA算法或EIGamal算法等，根据不同的密钥交换算法，预先共享的参数有所不同。以D-H算法为例，第一设备和第二设备预先共享参数g和P，预先在第一设备和第二设备上共享参数g和P，其中P是素数，g是P的原根。

[329] 第一设备和第二设备共享密钥交换算法所使用的参数的方式可以包括但不限于以下两种：其一、预先在第一设备和第二设备上配置密钥交换算法所使用的参数；其二、通过第三方的配置设备将密钥交换算法所使用的参数发送给第一设备和第二设备。

[330] 在第二种方式下，第一设备具体用于利用第二设备的公钥和自身的私钥按照密钥交换算法生成第一共享密钥，并将第一设备的公钥发送给第二设备。这种方式下，用于得到第一共享密钥的信息为第一设备的公钥。

[331] 以D-H算法为例，第一设备的公钥PkeyA为：PkeyA=(g^keyA)mod(P)，其中keyA为第一设备的私钥，为随机数，生成的第一共享密钥DHkeyA为：DHkeyA=((PkeyB)^keyA)mod(P)。

[332] 第二设备具体用于利用第一设备的公钥以及自身的私钥按照密钥交换算法生成第一共享密钥。第二设备的公钥PkeyB为：PkeyB=(g^keyB)mod(P)，keyB为第二设备的私钥，也是随机数。生成的第一共享密钥DHkeyB为：DHkeyB=((PkeyA)^keyB)mod(P)。由D-H算法可知，DHkeyA= DHkeyB。

[333] 在上述第二种方式下，第一设备和第二设备可以采用以下两种方式共享密钥交换算法所使用的参数：

[334] 1）第一设备和第二设备上预先配置有密钥交换算法所使用的参数，即采用静

态配置的方式。

[335] 2）配置设备将密钥交换算法所使用的参数发送给第一设备和第二设备，即由第三方的配置设备完成第一设备和第二设备上密钥交换算法所使用的参数配置。

[336] 在以上第一种方式或第二种方式的基础上，配置设备还用于获取第二设备和第一设备的设备信息。本发明实施例中涉及的设备信息可以包括但不限于：地址信息、设备能力、制造商、序列号、UUID等，其中设备能力指的是该设备支持的算法、认证方法、设备角色信息、设备类型信息等，其中设备角色信息是指该设备在注册时充当的角色，可以是enrollee、registrar、client或GO等。设备类型信息可以是无线终端、接入点、传感器节点、中心节点等。

[337] 在此涉及到的设备信息至少包含地址信息；这样配置设备能够根据第一设备的地址信息，执行将第二设备的公钥和设备信息发送给第一设备的操作；以及获取第二设备的地址信息，并将第二设备的地址信息发送给第一设备；使第一设备能够依据第二设备的地址信息发送用于得到第一共享密钥的信息。

[338] 更进一步地，在上述第一种方式或第二种方式的基础上，配置设备还用于获取第一设备的公钥；在将第二设备的公钥和设备信息发送给第一设备时，具体利用第一设备的公钥加密第二设备的公钥和设备信息，这里的加密可以采用实施例一中所述的第二种加密方式，将加密结果发送给第一设备。

[339] 此时的第一设备对加密结果进行解密，得到第二设备的公钥和设备信息。该种优选实施方式对应实施例一中所描述内容。

[340] 具体地，在上述第一种方式或第二种方式的基础上，配置设备从第一设备或第二设备获取信息时，包括公钥和设备信息，具体通过扫描二维码、USB或者近场通信的方式从第一设备或者第二设备获取信息。

[341] 可选的，第一设备还可以利用第二设备的公钥生成验证值，该验证值可以是但不限于是第二设备的公钥的hash值，或者是利用其它预设算法生成的验证值，然后根据第二设备的设备信息将该验证值发送给第二设备。

[342] 第二设备在生成第一共享密钥之前，利用自身的公钥对接收到的验证值进行验证，如果验证通过，则继续执行生成第一共享密钥的操作；否则，丢弃第一设

备的公钥，不再执行后续操作，并且可以进一步提示用户配置失败，例如采用指示灯的方式，或者在屏幕上显示的方式，或者语音的方式等等。该优选的实施方式对应于实施例一中所描述内容。

[343] 可选的，配置设备与第一设备，还可以用于建立安全连接以生成第二共享密钥。在此具体可以采用以下两种：其一、配置设备与第一设备之间通过现有的WPS交互方式共享信任状，以该信任状作为第二共享密钥；其二、配置设备将自身的公钥发送给第一设备，配置设备利用第一设备的公钥和配置设备的私钥执行密钥交换算法，生成第二共享密钥，第一设备利用配置设备的公钥和第一设备的私钥执行密钥交换算法，生成第二共享密钥。

[344] 配置设备在将第二设备的公钥和设备信息发送给第一设备时，具体利用第二共享密钥将第二设备的公钥和设备信息进行加密后，将加密结果发送给第一设备。第一设备利用第二共享密钥对接收到的加密结果进行解密后，得到第二设备的公钥和设备信息。这种优选的实施方式对应于实施例二所描述的内容。

[345] 可选的，在上述第一种方式或第二种方式的基础上，第一设备在得到第二设备的公钥和设备信息之后，还可以生成新的公钥和新的私钥。此时，上述第一设备发送给第二设备的第一设备的公钥为新的公钥；第二设备在生成第一共享密钥时利用的第一设备的公钥为新的公钥；第一设备在生成第一共享密钥时利用的自身的私钥为新的私钥。这种实施方式能够进一步增强交互的安全性，对应于实施例二中所描述的内容。

[346] 可选的，在上述第一种方式或第二种方式的基础上，可以进一步利用设备信息中包含的设备角色信息或设备类型信息，即配置设备还可以用于根据第一设备和第二设备的设备角色信息或设备类型信息，确定是将第二设备的公钥和设备信息发送给第一设备，还是将第一设备的公钥和设备信息发送给第二设备。

[347] 如果第一设备是被注册方enrollee，第二设备是注册器registrar，或者第一设备是客户端client，第二设备是组长设备GO，或者第一设备是无线终端，第二设备是接入点，则配置设备确定将第二设备的公钥和设备信息发送给第一设备，这样能够便于第一设备快速扫描发现第二设备，提高效率。或者如果第一设备是中心节点，第二设备是传感器节点，则配置设备确定将第二设备的公钥和设备

信息发送给第一设备，目的是中心节点能够快速发现传感器节点。这种优选的实施方式对应于实施例三中所描述的内容。

[348] 如果第一设备和第二设备的角色或类型对等，例如都是传感器节点，或者都是client等，那么无论确定将第二设备的公钥和设备信息发送给第一设备，还是将第一设备的公钥和设备信息发送给第二设备均可。

[349] 优选地，在上述第一种方式或第二种方式的基础上，还可以利用设备信息中包括信道信息的，即第一设备还用于根据第二设备的信道信息快速发现第二设备，以执行将用于得到第一共享密钥的信息发送给第二设备。

[350] 另外，第一设备和第二设备除了直接利用第一共享密钥进行安全连接之外，还可以基于共享的密钥衍生算法对第一共享密钥生成衍生密钥，利用衍生密钥进行安全连接。后续的安全连接可以包括但不限于：认证过程、关联过程、数据交互过程等。至于如何利用共享密钥进行安全连接可以采用现有技术，在此不再赘述。

[351] 上述的配置设备可以包括一台或多台服务器，或者包括一台或多台计算机，上述的第一设备和第二设备可以是诸如个人计算机、笔记本电脑、无线电话、个人数字助理（PDA）、传感器节点、AP等。需要说明的是，本发明所提供的方式和系统并不限于WiFi网络，可以用于任意的诸如蓝牙、Zigbee等无线网络，甚至可以应用于有线网络中的密钥配置。

[352] 图9为本发明实施例提供的设置于第一设备中的密钥配置装置的结构示意图，如图9中所示，该密钥配置装置包括：配置接收单元90和密钥处理单元91。

[353] 配置接收单元90负责接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥。

[354] 密钥处理单元91负责利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备；或者第一设备利用第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给第二设备；以便第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成第一共享密钥，第一共享密钥用于第一设备和第二设备之间的安全连接。

[355] 得到第一共享密钥的方式可以采用以下几种：

[356] 第一种方式：密钥处理单元91生成密码，将密码作为第一共享密钥，利用第二设备的公钥将密码进行加密得到加密结果，将加密结果发送给第二设备，以便第二设备利用自身的私钥对加密结果进行解密得到密码，将密码作为第一共享密钥。

[357] 第二种方式：密钥处理单元91生成密码，利用第二设备的公钥将密码进行加密得到加密结果，将加密结果发送给第二设备，利用密钥衍生算法对密码生成衍生密钥，将该衍生密钥作为第一共享密钥，以便第二设备利用自身的私钥对加密结果进行解密得到密码，利用密钥衍生算法对密码生成衍生密钥，将该衍生密钥作为第一共享密钥。

[358] 第三种方式：密钥处理单元91生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该随机值进行加密后，将加密结果发送给第二设备，以便第二设备利用自身的私钥对加密结果进行解密得到随机值，利用第一设备与第二设备约定的信息和随机值生成第一共享密钥。

[359] 第四种方式：密钥处理单元91利用第二设备的公钥将第一设备的公钥进行加密后，将加密结果发送给第二设备；接收第二设备发送的加密结果，该加密结果是第二设备利用自身的私钥对接收到的加密结果进行解密后，得到第一设备的公钥，并且生成密码，将该密码作为共享密钥，利用第一设备的公钥将该密码进行加密后得到的；利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为第一共享密钥。

[360] 第五种方式：密钥处理单元91利用第二设备的公钥和自身的私钥按照第一设备和第二设备预定的密钥交换算法生成第一共享密钥，并将第一设备的公钥发送给第二设备，以便第二设备利用自身的私钥以及第一设备的公钥按照密钥交换算法生成第一共享密钥。

[361] 其中，密钥处理单元91可以预先配置有密钥交换算法所使用的参数；或者，配置接收单元91接收配置设备发送的密钥交换算法所使用的参数，并提供给密钥处理单元91。

[362] 更进一步地，该密钥配置装置还可以包括：安全连接单元92。

[363] 安全连接单元92在密钥处理单元91得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给第二设备；以便第二设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到信任状，信任状用于第一设备和第二设备之间的安全连接（图中所示为该种实现）。或者，用于利用得到的第一共享密钥或者第一共享密钥的衍生密钥对第二设备发送的信任状的加密结果进行解密得到信任状，信任状的加密结果为第二设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后得到，信任状用于第一设备和第二设备之间的安全连接。

[364] 为了增强安全性，配置接收单元90可以接收配置设备在获取到第二设备的公钥和第一设备的公钥后发送的加密结果，加密结果为配置设备利用第一设备的公钥加密的第二设备的公钥。此时，密钥处理单元91，还可以用于对加密结果进行解密，得到第二设备的公钥。

[365] 还有一种实现：配置接收单元90与配置设备建立安全连接以生成第二共享密钥；接收配置设备在获取到第二设备的公钥后发送的加密结果，加密结果为配置设备利用第二共享密钥加密的第二设备的公钥。此时，密钥处理单元91利用第二共享密钥对接收到的加密结果进行解密后，得到第二设备的公钥。

[366] 其中，配置接收单元90在与配置设备建立安全连接以生成第二共享密钥时，具体与配置设备通过WPS交互方式共享信任状，将信任状作为第二共享密钥；或者，具体接收配置设备发送的配置设备的公钥，第一设备利用配置设备的公钥和自身的私钥按照预先约定的密钥交换算法生成第二共享密钥。

[367] 为了更进一步地提高安全性，密钥处理单元91在得到第二设备的公钥之后，还可以生成新的公钥和新的私钥；这样，第一设备发送给第二设备的第一设备的公钥就为该新的公钥；第二设备在生成第一共享密钥时利用的第一设备的公钥为新的公钥；第一设备在生成第一共享密钥时利用的自身的私钥为新的私钥。

[368] 优选地，配置接收单元90还可以接收配置设备从第二设备获取后发送来的第二设备的信道信息。这样，密钥处理单元91根据第二设备的信道信息就能够快速发现第二设备，以执行将用于得到第一共享密钥的信息发送给第二设备的操作

。

[369] 除此之外，密钥处理单元91还可以利用第二设备的公钥生成验证值，将验证值发送给第二设备；以便第二设备在生成第一共享密钥之前，利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成第一共享密钥的操作。

[370] 图10为本发明实施例提供的设置于配置设备中的密钥配置装置的结构示意图，如图10所示，该密钥配置装置包括：信息获取单元11和信息发送单元12。

[371] 其中，信息获取单元11负责获取第二设备的公钥。

[372] 信息发送单元12负责将第二设备的公钥发送给第一设备。

[373] 这样第一设备就能够利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备；或者第一设备就能够利用第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给第二设备。

[374] 然后第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成第一共享密钥，第一共享密钥用于第一设备和第二设备之间的安全连接。

[375] 如果第一设备和第二设备基于预定的密钥交换算法实现第一共享密钥的生成，则信息发送单元12，还可以将密钥交换算法所使用的参数发送给第一设备和第二设备，该密钥交换算法用于第一设备和第二设备利用自身的私钥和对方的公钥按照密钥交换算法生成第一共享密钥。

[376] 为了提高信息传递的安全性，信息获取单元11可以获取第一设备的公钥。由信息发送单元12利用第一设备的公钥加密第二设备的公钥，将加密结果发送给第一设备，以便第一设备对加密结果进行解密，得到第二设备的公钥。

[377] 还存在另外一种方式：信息发送单元12与第一设备建立安全连接以生成第二共享密钥；在将第二设备的公钥发送给第一设备时，具体利用第二共享密钥将第二设备的公钥进行加密后，将加密结果发送给第一设备，以便第一设备利用第二共享密钥对接收到的加密结果进行解密后，得到第二设备的公钥。

[378] 具体地，信息发送单元12在与第一设备建立安全连接以生成第二共享密钥时，与第一设备通过WPS交互方式共享信任状，将信任状作为第二共享密钥；或者，将自身的公钥发送给第一设备，利用第一设备的公钥和自身的私钥按照预先

约定的密钥交换算法生成第二共享密钥。

[379] 为了提高第一设备发现第二设备的效率，信息获取单元11还可以获取第二设备的信道信息。此时，信息发送单元12将第二设备的信道信息发送给第一设备，以便第一设备根据第二设备的信道信息快速发现第二设备，以执行将用于得到第一共享密钥的信息发送给第二设备的操作。

[380] 具体地，信息获取单元11通过扫描二维码、通用串行总线USB或者近场通信的方式从第一设备或者第二设备获取信息。

[381] 图11为本发明实施例提供的设置于第二设备中的密钥配置装置的结构示意图，如图11所示，该密钥配置装置可以包括：信息提供单元21、信息接收单元22和密钥处理单元23。

[382] 信息提供单元21负责向配置设备提供第二设备的公钥，以便配置设备将第二设备的公钥发送给第一设备。

[383] 信息接收单元22负责接收第一设备利用第二设备的公钥发送来的用于得到第一共享密钥的信息；或者接收第一设备利用第二设备的公钥生成第一共享密钥后，发送来的用于得到第一共享密钥的信息。

[384] 密钥处理单元23负责利用自身的私钥以及用于得到第一共享密钥的信息生成第一共享密钥，第一共享密钥用于第一设备和第二设备之间的安全连接。

[385] 得到第一共享密钥的方式可以采用以下几种：

[386] 第一种方式：信息接收单元22接收第一设备发送的加密结果，加密结果是第一设备生成密码，将密码作为第一共享密钥，利用第二设备的公钥将密码进行加密得到的。

[387] 此时，密钥处理单元23利用自身的私钥对加密结果进行解密得到密码，将密码作为第一共享密钥。

[388] 第二种方式：信息接收单元22接收第一设备发送的加密结果，加密结果是第一设备生成密码后，利用第二设备的公钥将密码进行加密得到的。

[389] 此时的密钥处理单元23利用自身的私钥对加密结果进行解密得到密码，利用密钥衍生算法对密码生成衍生密钥，将该衍生密钥作为第一共享密钥。

[390] 第三种方式：信息接收单元22接收第一设备发送的加密结果，加密结果是第一

设备生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该随机值进行加密后得到的。

[391] 此时的密钥处理单元23利用自身的私钥对加密结果进行解密得到随机值，利用第一设备与第二设备约定的信息和随机值生成第一共享密钥。

[392] 第四种方式：信息接收单元22接收第一设备利用第二设备的公钥将第一设备的公钥进行加密后得到的加密结果。

[393] 此时密钥处理单元23利用自身的私钥对加密结果进行解密后，得到第一设备的公钥，并生成密码，将该密码作为第一共享密钥，利用第一设备的公钥将该密码进行加密后，将加密结果发送给第一设备，以便第一设备利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为第一共享密钥。

[394] 第五种方式：信息接收单元22接收第一设备利用第二设备的公钥和自身的私钥按照密钥交换算法生成第一共享密钥后，发送来的第一设备的公钥；密钥交换算法是第一设备和第二设备预定的。

[395] 此时，密钥处理单元23利用自身的私钥以及第一设备的公钥按照密钥交换算法生成第一共享密钥。

[396] 这种方式下，密钥处理单元23可以预先配置有密钥交换算法所使用的参数。或者，信息接收单元22接收配置设备发送的密钥交换算法所使用的参数，并提供给密钥处理单元23。

[397] 更进一步地，该密钥配置装置还可以包括：安全连接单元24。

[398] 安全连接单元24接收第一设备发送的加密结果，该加密结果是第一设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后得到的；利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到信任状，信任状用于第一设备和第二设备之间的安全连接（图中示出的为该种实现）。或者，用于在密钥处理单元23得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给第一设备；以便第一设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到信任状，信任状用于第一设备和第二设备之间的安全连接。

[399] 为了提高第一设备发现第二设备的效率，上述的信息提供单元21还可以将第二设备的信道信息提供给配置设备，以便配置设备将第二设备的信道信息发送给第一设备；以便第一设备根据第二设备的信道信息快速发现第二设备，以执行将用于得到第一共享密钥的信息发送给第二设备的操作。

[400] 具体地，信息提供单元21可以通过二维码、USB或近场通信的方式向配置设备提供信息。

[401] 另外，为了进一步提高安全性，信息接收单元22还可以接收第一设备利用第二设备的公钥生成的验证值。

[402] 此时密钥处理单元23利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成第一共享密钥的操作。

[403] 从硬件结构上考虑，上述的配置设备如图12所示，包括处理器、存储器和通信总线，所述处理器通过通信总线与存储器连接，所述存储器中保存有实现密钥配置方法的指令，进一步地，所述配置设备还包括通信接口，通过通信接口与其他设备通信连接。

[404] 当处理器调取存储器中实现密钥配置方法的指令时，可以执行如下步骤：

[405] 获取第二设备的公钥，将所述第二设备的公钥发送给第一设备；

[406] 以便所述第一设备利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备；或者以便所述第一设备利用所述第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给所述第二设备；

[407] 以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[408] 当处理器调取存储器中实现密钥配置方法的指令时，可以执行前述方法实施例中配置设备所执行的步骤，具体可参考前述方法实施例，在此不再赘述。

[409] 上述的第一设备如图13所示，包括处理器、存储器和通信总线，所述处理器通过通信总线与存储器连接，所述存储器中保存有实现密钥配置方法的指令，进一步地，所述第一设备还包括通信接口，通过通信接口与其他设备通信连接。

[410] 当处理器调取存储器中实现密钥配置方法的指令时，可以执行如下步骤：

[411] 接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥，利用所述第二设备的公钥将用于得到所述第一共享密钥的信息发送给所述第二设备；或者所述第一设备利用所述第二设备的公钥生成第一共享密钥，将用于得到所述第一共享密钥的信息发送给所述第二设备；

[412] 以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[413] 当处理器调取存储器中实现密钥配置方法的指令时，可以执行前述方法实施例中第一设备所执行的步骤，具体可参考前述方法实施例，在此不再赘述。

[414] 上述的第二设备如图14所示，包括处理器、存储器和通信总线，所述处理器通过通信总线与存储器连接，所述存储器中保存有实现密钥配置方法的指令，进一步地，所述第二设备还包括通信接口，通过通信接口与其他设备通信连接。

[415] 当处理器调取存储器中实现密钥配置方法的指令时，可以执行如下步骤：

[416] 向配置设备提供第二设备的公钥，以便所述配置设备将所述第二设备的公钥发送给第一设备；

[417] 接收所述第一设备利用所述第二设备的公钥发送来的用于得到第一共享密钥的信息；或者接收所述第一设备利用所述第二设备的公钥生成第一共享密钥后，发送来的用于得到第一共享密钥的信息；

[418] 利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[419] 当处理器调取存储器中实现密钥配置方法的指令时，可以执行前述方法实施例中第二设备所执行的步骤，具体可参考前述方法实施例，在此不再赘述。

[420] 本发明所描述的设备在架构上都包含一些基本组件，如总线、处理系统、存储系统、一个或多个输入/输出系统、和通信接口等。总线可以包括一个或多个导线，用来实现设备中各组件之间的通信。处理系统包括各类型的用来执行指令、处理进程或线程的处理器或微处理器。存储系统可以包括存储动态信息的随机访问存储器（RAM）等动态存储器，和存储静态信息的只读存储器（ROM）等静态存储器，以及包括磁或光学记录介质与相应驱动的大容量存储器。输入

系统供用户输入信息到服务器或终端设备，如键盘、鼠标、手写笔、声音识别系统、或生物测定系统等，如果是无头设备，则可以不包含人机交互功能的输入系统。输出系统包括用来输出信息的显示器、打印机、扬声器、指示灯等。通信接口用来使服务器或终端设备与其它系统或系统进行通信。通信接口之间可通过有线连接、无线连接、或光连接连接到网络中。

[421] 各设备上均包含有用来管理系统资源、控制其它程序运行的操作系统软件，以及用来实现特定功能的应用软件。

[422] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

权利要求书

[权利要求 1] 一种密钥配置方法，其特征在于，所述密钥配置方法包括：

第一设备接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥；利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备，或者，所述第一设备利用所述第二设备的公钥生成第一共享密钥，将用于得到所述第一共享密钥的信息发送给所述第二设备；

以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 2] 根据权利要求1所述的方法，其特征在于，所述第一设备利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：所述第一设备生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备；

以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：所述第一设备生成密码，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备，利用密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为第一共享密钥；

以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享

密钥。

[权利要求 3] 根据权利要求1所述的方法，其特征在于，所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：所述第一设备生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该随机值进行加密后，将加密结果发送给第二设备；

以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[权利要求 4] 根据权利要求1所述的方法，其特征在于，所述利用所述第二设备的公钥将用于得到所述第一共享密钥的信息发送给所述第二设备包括：所述第一设备利用第二设备的公钥将第一设备的公钥进行加密后，将加密结果发送给第二设备；

以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密后，得到所述第一设备的公钥，并且生成密码，将该密码作为所述第一共享密钥；

该方法还包括：第一设备接收所述第二设备利用所述第一设备的公钥将该密码进行加密后的加密结果，利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为所述第一共享密钥。

[权利要求 5] 根据权利要求1所述的方法，其特征在于，所述方法还包括：所述第一设备和所述第二设备预定密钥交换算法；

所述第一设备利用第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给第二设备包括：所述第一设备利用第二设备的公钥和自身的私钥按照所述密钥交换算法生成第一共享密钥，并将第一设备的公钥发送给所述第二设备；

以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[权利要求 6] 根据权利要求5所述的方法，其特征在于，所述第一设备和所述第二设备预定密钥交换算法包括：

所述第一设备和所述第二设备上预先配置有所述密钥交换算法所使用的参数；或者，

通过所述配置设备将所述密钥交换算法所使用的参数发送给所述第一设备和所述第二设备。

[权利要求 7] 根据权利要求1-6任一所述的方法，其特征在于，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接包括：

所述第一设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给所述第二设备；以便所述第二设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接；或者，

所述第一设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对所述第二设备发送的信任状的加密结果进行解密得到所述信任状，所述信任状的加密结果为所述第二设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对所述信任状进行加密后得到，所述信任状用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 8] 根据权利要求7所述的方法，其特征在于，若所述第一设备是注册器Registrar、中心节点或者组长设备GO，则由所述第一设备生成所述信任状并将所述信任状的加密结果发送给所述第二设备；

若所述第二设备是Registrar、中心节点或GO，则由所述第二设备

生成所述信任状并将所述信任状的加密结果发送给所述第一设备。

[权利要求 9] 根据权利要求1至8任一权项所述的方法，其特征在于，

所述第一设备接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥具体为：

所述第一设备接收配置设备在获取到所述第二设备的公钥和所述第一设备的公钥后发送的加密结果，所述加密结果为所述配置设备利用所述第一设备的公钥加密的所述第二设备的公钥；

该方法还包括：所述第一设备对所述加密结果进行解密，得到所述第二设备的公钥。

[权利要求 10] 根据权利要求1至8任一权项所述的方法，其特征在于，

所述第一设备接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥具体为：

所述第一设备与所述配置设备建立安全连接以生成第二共享密钥；

所述第一设备接收所述配置设备在获取到第二设备的公钥后发送的加密结果，所述加密结果为所述配置设备利用所述第二共享密钥加密的所述第二设备的公钥；

该方法还包括：

所述第一设备利用所述第二共享密钥对接收到的所述加密结果进行解密后，得到所述第二设备的公钥。

[权利要求 11] 根据权利要求10所述的方法，其特征在于，所述第一设备与所述配置设备建立安全连接以生成第二共享密钥包括：

所述第一设备与所述配置设备通过无线保真安全建立WPS交互方式共享信任状，将所述信任状作为所述第二共享密钥；或者，

所述第一设备接收所述配置设备发送的所述配置设备的公钥，所述第一设备利用所述配置设备的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥，以便所述配置设备获取

到所述第一设备的公钥后，利用所述第一设备的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥。

[权利要求 12] 根据权利要求5所述的方法，其特征在于，在所述第一设备得到所述第二设备的公钥之后，所述方法还包括：所述第一设备生成新的公钥和新的私钥；

所述第一设备发送给所述第二设备的第一设备的公钥为所述新的公钥；所述第二设备在生成所述第一共享密钥时利用的第一设备的公钥为所述新的公钥；所述第一设备在生成所述第一共享密钥时利用的自身的私钥为所述新的私钥。

[权利要求 13] 根据权利要求1至12任一权项所述的方法，其特征在于，

所述第一设备是被注册方enrollee，所述第二设备是registrar，或者所述第一设备是客户端client，所述第二设备是GO，或者所述第一设备是无线终端，所述第二设备是接入点，或者所述第一设备是中心节点，所述第二设备是传感器节点。

[权利要求 14] 根据权利要求1至13任一权项所述的方法，其特征在于，

该方法还包括：所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的步骤，所述第二设备的信道信息为所述配置设备从所述第二设备获取后发送给所述第一设备的。

[权利要求 15] 根据权利要求1至14任一权项所述的方法，其特征在于，所述配置设备通过扫描二维码、通用串行总线USB或者近场通信的方式从所述第一设备或者第二设备获取信息。

[权利要求 16] 根据权利要求1至15任一权项所述的方法，其特征在于，该方法还包括：所述第一设备利用所述第二设备的公钥生成验证值，将所述验证值发送给所述第二设备；

以便所述第二设备在生成所述第一共享密钥之前，利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成所述第一共享密钥的步骤。

[权利要求 17] 一种密钥配置方法，其特征在于，所述密钥配置方法包括：

所述配置设备获取第二设备的公钥，将所述第二设备的公钥发送给第一设备；

以便所述第一设备利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备；或者以便所述第一设备利用所述第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给所述第二设备；

以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 18] 根据权利要求17所述的方法，其特征在于，以便所述第一设备利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：以便所述第一设备生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备；

以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

以便所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：以便所述第一设备生成密码，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备，利用密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为第一共享密钥；

以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生

算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[权利要求 19] 根据权利要求17所述的方法，其特征在于，以便所述第一设备生成第一共享密钥，利用第二设备的公钥将用于得到第一共享密钥的信息发送给第二设备包括：以便所述第一设备生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该随机值进行加密后，将加密结果发送给第二设备；

以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[权利要求 20] 根据权利要求17所述的方法，其特征在于，以便所述第一设备利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备包括：以便所述第一设备利用第二设备的公钥将第一设备的公钥进行加密后，将加密结果发送给第二设备；

以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥对所述加密结果进行解密后，得到所述第一设备的公钥，并且生成密码，将该密码进行加密后，将加密结果发送给所述第一设备；

以便所述第一设备利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为第一共享密钥。

[权利要求 21] 根据权利要求17所述的方法，其特征在于，所述方法还包括：所述第一设备和所述第二设备预定密钥交换算法；

以便所述第一设备利用第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给第二设备包括：以便所述第一设备利用第二设备的公钥和自身的私钥按照所述密钥交换算法生

成第一共享密钥，并将第一设备的公钥发送给所述第二设备；

以便所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：以便所述第二设备利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[权利要求 22] 根据权利要求21所述的方法，其特征在于，所述第一设备和所述第二设备预定共享密钥交换算法包括：

所述第一设备和所述第二设备上预先配置有所述密钥交换算法所使用的参数；或者，

所述配置设备将所述密钥交换算法所使用的参数发送给所述第一设备和所述第二设备。

[权利要求 23] 根据权利要求17至22任一权项所述的方法，该方法还包括：所述配置设备获取第一设备的公钥；

所述配置设备将所述第二设备的公钥发送给第一设备包括：所述配置设备利用所述第一设备的公钥加密所述第二设备的公钥，将加密结果发送给所述第一设备；以便所述第一设备对所述加密结果进行解密，得到所述第二设备的公钥。

[权利要求 24] 根据权利要求17至22任一权项所述的方法，该方法还包括：所述配置设备与所述第一设备建立安全连接以生成第二共享密钥；

将所述第二设备的公钥发送给第一设备包括：所述配置设备利用所述第二共享密钥将所述第二设备的公钥进行加密后，将加密结果发送给所述第一设备；以便所述第一设备利用所述第二共享密钥对接收到的加密结果进行解密后，得到所述第二设备的公钥。

[权利要求 25] 根据权利要求24所述的方法，其特征在于，所述配置设备与所述第一设备建立安全连接以生成第二共享密钥包括：

所述配置设备与所述第一设备通过WPS交互方式共享信任状，将所述信任状作为所述第二共享密钥；或者，

所述配置设备将自身的公钥发送给所述第一设备，所述配置设备

和所述第一设备分别利用对方的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥。

[权利要求 26] 根据权利要求17至25任一权项所述的方法，其特征在于，

所述第一设备是被注册方enrollee，所述第二设备是registrar，或者所述第一设备是客户端client，所述第二设备是GO，或者所述第一设备是无线终端，所述第二设备是接入点，或者所述第一设备是中心节点，所述第二设备是传感器节点。

[权利要求 27] 根据权利要求17至26任一权项所述的方法，其特征在于，该方法还包括：所述配置设备获取第二设备的信道信息并发送给所述第一设备；以便所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的步骤。

[权利要求 28] 根据权利要求17至27任一权项所述的方法，其特征在于，所述配置设备通过扫描二维码、通用串行总线USB或者近场通信的方式从所述第一设备或者第二设备获取信息。

[权利要求 29] 一种密钥配置方法，其特征在于，该方法包括：

第二设备向配置设备提供第二设备的公钥，以便所述配置设备将所述第二设备的公钥发送给第一设备；

所述第二设备接收所述第一设备利用所述第二设备的公钥发送来的用于得到第一共享密钥的信息；或者接收所述第一设备利用所述第二设备的公钥生成第一共享密钥后，发送来的用于得到第一共享密钥的信息；

所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 30] 根据权利要求29所述的方法，其特征在于，所述第二设备接收所述第一设备利用第二设备的公钥发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备发送的加密结果，

所述加密结果是所述第一设备生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到的；

所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

所述第二设备接收所述第一设备利用第二设备的公钥发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成密码后，利用所述第二设备的公钥将所述密码进行加密得到的；

所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[权利要求 31] 根据权利要求29所述的方法，其特征在于，所述第二设备接收所述第一设备利用第二设备的公钥发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成随机值，利用第二设备的公钥对该随机值进行加密后得到的，所述第一设备利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥；

所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[权利要求 32] 根据权利要求29所述的方法，其特征在于，所述第二设备接收所述第一设备利用所述第二设备的公钥发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备利用第二设备的公钥将第一设备的公钥进行加密后得到的加密结果；

所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥对所述加密结果进行解密后，得到所述第一设备的公钥，并生成密码，将该密码作为所述第一共享密钥，利用所述第一设备的公钥将该密码进行加密后，将加密结果发送给第一设备；

以便所述第一设备利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为所述第一共享密钥。

[权利要求 33] 根据权利要求29所述的方法，其特征在于，所述方法还包括：所述第二设备和所述第一设备预定密钥交换算法；

接收所述第一设备利用所述第二设备的公钥生成第一共享密钥后，发送来的用于得到第一共享密钥的信息包括：所述第二设备接收所述第一设备利用第二设备的公钥和自身的私钥按照所述密钥交换算法生成第一共享密钥后，发送来的第一设备的公钥；

所述第二设备利用自身的私钥以及用于得到第一共享密钥的信息生成所述第一共享密钥包括：所述第二设备利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[权利要求 34] 根据权利要求33所述的方法，其特征在于，所述第二设备和所述第一设备预定密钥交换算法包括：

所述第二设备和所述第一设备上预先配置有所述密钥交换算法所使用的参数；或者，

所述第二设备和所述第一设备接收所述配置设备发送的所述密钥交换算法所使用的参数。

[权利要求 35] 根据权利要求29-34任一所述的方法，其特征在于，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接包括：

所述第二设备接收第一设备发送的加密结果，该加密结果是所述第一设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后得到的；所述第二设备利用得到的第一共享密钥或者第一共享密钥的衍生密

钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接；或者，

所述第二设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给所述第一设备；以便所述第一设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对该加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 36] 根据权利要求35所述的方法，其特征在于，若所述第一设备是注册器Registrar、中心节点或者组长设备GO，则由所述第一设备生成所述信任状并将所述信任状的加密结果发送给所述第二设备；

若所述第二设备是Registrar、中心节点或GO，则由所述第二设备生成所述信任状并将所述信任状的加密结果发送给所述第一设备。

[权利要求 37] 根据权利要求29至36任一权项所述的方法，其特征在于，该方法还包括：

所述第二设备将自身的信道信息提供给所述配置设备，以便所述配置设备将第二设备的信道信息发送给所述第一设备；以便所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的步骤。

[权利要求 38] 根据权利要求29至37任一权项所述的方法，其特征在于，所述第二设备或者所述第一设备通过二维码、USB或近场通信的方式供所述配置设备获取信息。

[权利要求 39] 根据权利要求29至38任一权项所述的方法，其特征在于，该方法还包括：

所述第二设备接收所述第一设备利用第二设备的公钥生成的验证值，所述第二设备利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成所述第一共享密钥的步骤。

[权利要求 40] 一种密钥配置装置，设置于第一设备中，其特征在于，该密钥配置装置包括：

配置接收单元，用于接收配置设备在获取到第二设备的公钥后发送的第二设备的公钥；

密钥处理单元，用于利用所述第二设备的公钥将用于得到第一共享密钥的信息发送给所述第二设备；或者利用所述第二设备的公钥生成第一共享密钥，将用于得到所述第一共享密钥的信息发送给所述第二设备；以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 41] 根据权利要求40所述的密钥配置装置，其特征在于，所述密钥处理单元，具体用于生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备，以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

所述密钥处理单元，具体用于生成密码，利用所述第二设备的公钥将所述密码进行加密得到加密结果，将所述加密结果发送给所述第二设备，利用密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为第一共享密钥，以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[权利要求 42] 根据权利要求40所述的密钥配置装置，其特征在于，所述密钥处理单元，具体用于生成随机值，利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥，利用第二设备的公钥对该随机值进行加密后，将加密结果发送给第二设备，以便所述第二设备利用自身的私钥对所述加密结果进行解密得到所述随机值，利

用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[权利要求 43] 根据权利要求40所述的密钥配置装置，其特征在于，所述密钥处理单元，具体用于利用第二设备的公钥将第一设备的公钥进行加密后，将加密结果发送给第二设备；接收所述第二设备发送的加密结果，该加密结果是所述第二设备利用自身的私钥对接收到的加密结果进行解密后，得到所述第一设备的公钥，并且生成密码，将该密码作为所述第一共享密钥，利用所述第一设备的公钥将该密码进行加密后得到的；利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为所述第一共享密钥。

[权利要求 44] 根据权利要求40所述的密钥配置装置，其特征在于，所述密钥处理单元，具体用于利用第二设备的公钥和自身的私钥按照所述第一设备和所述第二设备预定的密钥交换算法生成第一共享密钥，并将第一设备的公钥发送给所述第二设备，以便所述第二设备利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[权利要求 45] 根据权利要求44所述的密钥配置装置，其特征在于，所述密钥处理单元预先配置有所述密钥交换算法所使用的参数；

或者，所述配置接收单元，还用于接收所述配置设备发送的所述密钥交换算法所使用的参数，并提供给所述密钥处理单元。

[权利要求 46] 根据权利要求40-45任一所述的密钥配置装置，其特征在于，该密钥配置装置还包括：

安全连接单元，用于在所述密钥处理单元得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给所述第二设备；以便所述第二设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接；或者，用于利用得到的第

一共享密钥或者第一共享密钥的衍生密钥对所述第二设备发送的信任状的加密结果进行解密得到所述信任状，所述信任状的加密结果为所述第二设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对所述信任状进行加密后得到，所述信任状用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 47] 根据权利要求40-46任一所述的密钥配置装置，其特征在于，所述配置接收单元，具体用于接收配置设备在获取到所述第二设备的公钥和所述第一设备的公钥后发送的加密结果，所述加密结果为所述配置设备利用所述第一设备的公钥加密的所述第二设备的公钥；

所述密钥处理单元，还用于对所述加密结果进行解密，得到所述第二设备的公钥。

[权利要求 48] 根据权利要求40至46任一权项所述的密钥配置装置，其特征在于，所述配置接收单元，具体用于与所述配置设备建立安全连接以生成第二共享密钥；接收所述配置设备在获取到第二设备的公钥后发送的加密结果，所述加密结果为所述配置设备利用所述第二共享密钥加密的所述第二设备的公钥；

所述密钥处理单元，还用于利用所述第二共享密钥对接收到的所述加密结果进行解密后，得到所述第二设备的公钥。

[权利要求 49] 根据权利要求48所述的密钥配置装置，其特征在于，所述配置接收单元在与所述配置设备建立安全连接以生成第二共享密钥时，具体与所述配置设备通过无线保真安全建立WPS交互方式共享信任状，将所述信任状作为所述第二共享密钥；或者，具体接收所述配置设备发送的所述配置设备的公钥，所述第一设备利用所述配置设备的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥。

[权利要求 50] 根据权利要求44所述的密钥配置装置，其特征在于，所述密钥处

理单元在得到所述第二设备的公钥之后，还用于生成新的公钥和新的私钥；

所述第一设备发送给所述第二设备的第一设备的公钥为所述新的公钥；所述第二设备在生成所述第一共享密钥时利用的第一设备的公钥为所述新的公钥；所述第一设备在生成所述第一共享密钥时利用的自身的私钥为所述新的私钥。

[权利要求 51] 根据权利要求40至50任一权项所述的密钥配置装置，其特征在于，所述第一设备是被注册方enrollee，所述第二设备是registrar，或者所述第一设备是客户端client，所述第二设备是GO，或者所述第一设备是无线终端，所述第二设备是接入点，或者所述第一设备是中心节点，所述第二设备是传感器节点。

[权利要求 52] 根据权利要求40至51任一权项所述的密钥配置装置，其特征在于，所述配置接收单元，还用于接收所述配置设备从所述第二设备获取后发送来的第二设备的信道信息；

所述密钥处理单元根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的操作。

[权利要求 53] 根据权利要求40至52任一权项所述的密钥配置装置，其特征在于，所述密钥处理单元，还用于利用所述第二设备的公钥生成验证值，将所述验证值发送给所述第二设备；以便所述第二设备在生成所述第一共享密钥之前，利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成所述第一共享密钥的操作。

[权利要求 54] 一种密钥配置装置，设置于配置设备中，其特征在于，该密钥配置装置包括：

信息获取单元，用于获取第二设备的公钥；

信息发送单元，用于将所述第二设备的公钥发送给第一设备；

以便所述第一设备利用所述第二设备的公钥将用于得到第一共享

密钥的信息发送给所述第二设备；或者以便所述第一设备利用所述第二设备的公钥生成第一共享密钥，将用于得到第一共享密钥的信息发送给所述第二设备；

以便所述第二设备利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 55] 根据权利要求54所述的密钥配置装置，其特征在于，所述信息发送单元，还用于将密钥交换算法所使用的参数发送给所述第一设备和所述第二设备,所述密钥交换算法用于所述第一设备和所述第二设备利用自身的私钥和对方的公钥按照所述密钥交换算法生成第一共享密钥。

[权利要求 56] 根据权利要求54或55所述的密钥配置装置，其特征在于，所述信息获取单元，还用于获取第一设备的公钥；

所述信息发送单元，具体用于利用所述第一设备的公钥加密所述第二设备的公钥，将加密结果发送给所述第一设备，以便所述第一设备对所述加密结果进行解密，得到所述第二设备的公钥。

[权利要求 57] 根据权利要求54或55所述的密钥配置装置，其特征在于，所述信息发送单元，还用于与所述第一设备建立安全连接以生成第二共享密钥；在将所述第二设备的公钥发送给第一设备时，具体利用所述第二共享密钥将所述第二设备的公钥进行加密后，将加密结果发送给所述第一设备，以便所述第一设备利用所述第二共享密钥对接收到的加密结果进行解密后，得到所述第二设备的公钥。

[权利要求 58] 根据权利要求57所述的密钥配置装置，其特征在于，所述信息发送单元在与所述第一设备建立安全连接以生成第二共享密钥时，具体用于与所述第一设备通过WPS交互方式共享信任状，将所述信任状作为所述第二共享密钥；或者，将自身的公钥发送给所述第一设备，利用第一设备的公钥和自身的私钥按照预先约定的密钥交换算法生成所述第二共享密钥。

[权利要求 59] 根据权利要求54至58任一权项所述的密钥配置装置，其特征在于，所述信息获取单元，还用于获取第二设备的信道信息；

所述信息发送单元，还用于将所述第二设备的信道信息发送给所述第一设备，以便所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的操作。

[权利要求 60] 根据权利要求54至59任一权项所述的密钥配置装置，其特征在于，所述信息获取单元，具体用于通过扫描二维码、通用串行总线USB或者近场通信的方式从所述第一设备或者第二设备获取信息。

[权利要求 61] 一种密钥配置装置，设置于第二设备中，其特征在于，该密钥配置装置包括：

信息提供单元，用于向配置设备提供第二设备的公钥，以便所述配置设备将所述第二设备的公钥发送给第一设备；

信息接收单元，用于接收所述第一设备利用所述第二设备的公钥发送来的用于得到第一共享密钥的信息；或者接收所述第一设备利用所述第二设备的公钥生成第一共享密钥后，发送来的用于得到第一共享密钥的信息；

密钥处理单元，用于利用自身的私钥以及所述用于得到第一共享密钥的信息生成所述第一共享密钥，所述第一共享密钥用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 62] 根据权利要求61所述的密钥配置装置，其特征在于，所述信息接收单元，具体用于接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成密码，将所述密码作为第一共享密钥，利用所述第二设备的公钥将所述密码进行加密得到的；

所述密钥处理单元，具体用于利用自身的私钥对所述加密结果进行解密得到所述密码，将所述密码作为第一共享密钥；或者，

所述信息接收单元，具体用于接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成密码后，利用所述第二设备

的公钥将所述密码进行加密得到的；

所述密钥处理单元，具体用于利用自身的私钥对所述加密结果进行解密得到所述密码，利用所述密钥衍生算法对所述密码生成衍生密钥，将该衍生密钥作为所述第一共享密钥。

[权利要求 63] 根据权利要求61所述的密钥配置装置，其特征在于，所述信息接收单元，具体用于接收所述第一设备发送的加密结果，所述加密结果是所述第一设备生成随机值，利用第二设备的公钥对该随机值进行加密后得到的，所述第一设备利用第一设备与第二设备约定的信息和该随机值生成第一共享密钥；

所述密钥处理单元，具体用于利用自身的私钥对所述加密结果进行解密得到所述随机值，利用所述第一设备与第二设备约定的信息和所述随机值生成所述第一共享密钥。

[权利要求 64] 根据权利要求61所述的密钥配置装置，其特征在于，所述信息接收单元，具体用于接收所述第一设备利用第二设备的公钥将第一设备的公钥进行加密后得到的加密结果；

所述密钥处理单元，具体用于利用自身的私钥对所述加密结果进行解密后，得到所述第一设备的公钥，并生成密码，将该密码作为所述第一共享密钥，利用所述第一设备的公钥将该密码进行加密后，将加密结果发送给第一设备，以便所述第一设备利用自身的私钥对接收到的加密结果进行解密后，将得到的密码作为所述第一共享密钥。

[权利要求 65] 根据权利要求61所述的密钥配置装置，其特征在于，所述信息接收单元，具体用于接收所述第一设备利用第二设备的公钥和自身的私钥按照密钥交换算法生成第一共享密钥后，发送来的第一设备的公钥；所述密钥交换算法是所述第一设备和所述第二设备预定的；

所述密钥处理单元，具体用于利用自身的私钥以及所述第一设备的公钥按照所述密钥交换算法生成第一共享密钥。

[权利要求 66] 根据权利要求65所述的密钥配置装置，其特征在于，所述密钥处理单元预先配置有所述密钥交换算法所使用的参数；或者，

所述信息接收单元，还用于接收所述配置设备发送的所述密钥交换算法所使用的参数，并提供给所述密钥处理单元。

[权利要求 67] 根据权利要求61-66任一所述的密钥配置装置，其特征在于，该密钥配置装置还包括：

安全连接单元，用于接收第一设备发送的加密结果，该加密结果是所述第一设备在得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后得到的；利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接；或者，

用于在所述密钥处理单元得到第一共享密钥后，生成信任状，并利用第一共享密钥或第一共享密钥的衍生密钥对信任状进行加密后，将加密结果发送给所述第一设备；以便所述第一设备利用得到的第一共享密钥或者第一共享密钥的衍生密钥对加密结果进行解密得到所述信任状，所述信任状用于所述第一设备和所述第二设备之间的安全连接。

[权利要求 68] 根据权利要求61至67任一权项所述的密钥配置装置，其特征在于，所述信息提供单元，还用于将第二设备的信道信息提供给所述配置设备，以便所述配置设备将第二设备的信道信息发送给所述第一设备；以便所述第一设备根据第二设备的信道信息快速发现所述第二设备，以执行所述将用于得到第一共享密钥的信息发送给第二设备的操作。

[权利要求 69] 根据权利要求61至68任一权项所述的密钥配置装置，其特征在于，所述信息提供单元，具体用于通过二维码、USB或近场通信的方式向所述配置设备提供信息。

[权利要求 70] 根据权利要求61至68任一权项所述的密钥配置装置，其特征在于

，所述信息接收单元，还用于接收所述第一设备利用第二设备的公钥生成的验证值；

所述密钥处理单元，还用于利用自身的公钥对接收到的验证值进行验证，在验证通过的情况下，执行生成所述第一共享密钥的操作。

[权利要求 71] 一种密钥配置系统，其特征在于，该密钥配置系统包括：如权利要求40所述的密钥配置装置、如权利要求54所述的密钥配置装置以及如权利要求61所述的密钥配置装置；或者，

如权利要求41所述的密钥配置装置、如权利要求54所述的密钥配置装置以及如权利要求62所述的密钥配置装置；或者，

如权利要求42所述的密钥配置装置、如权利要求54所述的密钥配置装置以及如权利要求63所述的密钥配置装置；或者，

如权利要求43所述的密钥配置装置、如权利要求54所述的密钥配置装置以及如权利要求64所述的密钥配置装置；或者，

如权利要求44所述的密钥配置装置、如权利要求54所述的密钥配置装置以及如权利要求65所述的密钥配置装置；或者，

如权利要求45所述的密钥配置装置、如权利要求55所述的密钥配置装置以及如权利要求66所述的密钥配置装置；或者，

如权利要求46所述的密钥配置装置、如权利要求54所述的密钥配置装置以及如权利要求67所述的密钥配置装置；或者，

如权利要求47所述的密钥配置装置、如权利要求56所述的密钥配置装置以及如权利要求61-67任一所述的密钥配置装置；或者，

如权利要求48所述的密钥配置装置、如权利要求57所述的密钥配置装置以及如权利要求61至67任一权项所述的密钥配置装置；或者，

如权利要求49所述的密钥配置装置、如权利要求58所述的密钥配置装置以及如权利要求61至67任一权项所述的密钥配置装置；或者，

如权利要求50所述的密钥配置装置、如权利要求54所述的密钥配置装置以及如权利要求65所述的密钥配置装置；或者，

如权利要求51所述的密钥配置装置、如权利要求54至58任一权项所述的密钥配置装置以及如权利要求61至67任一权项所述的密钥配置装置；或者，

如权利要求52所述的密钥配置装置、如权利要求59所述的密钥配置装置以及如权利要求68所述的密钥配置装置；或者，

如权利要求53所述的密钥配置装置、如权利要求54至59任一权项所述的密钥配置装置以及如权利要求70所述的密钥配置装置；或者，

如权利要求40至53任一权项所述的密钥配置装置、如权利要求60所述的密钥配置装置以及如权利要求69所述的密钥配置装置。

说明书附图

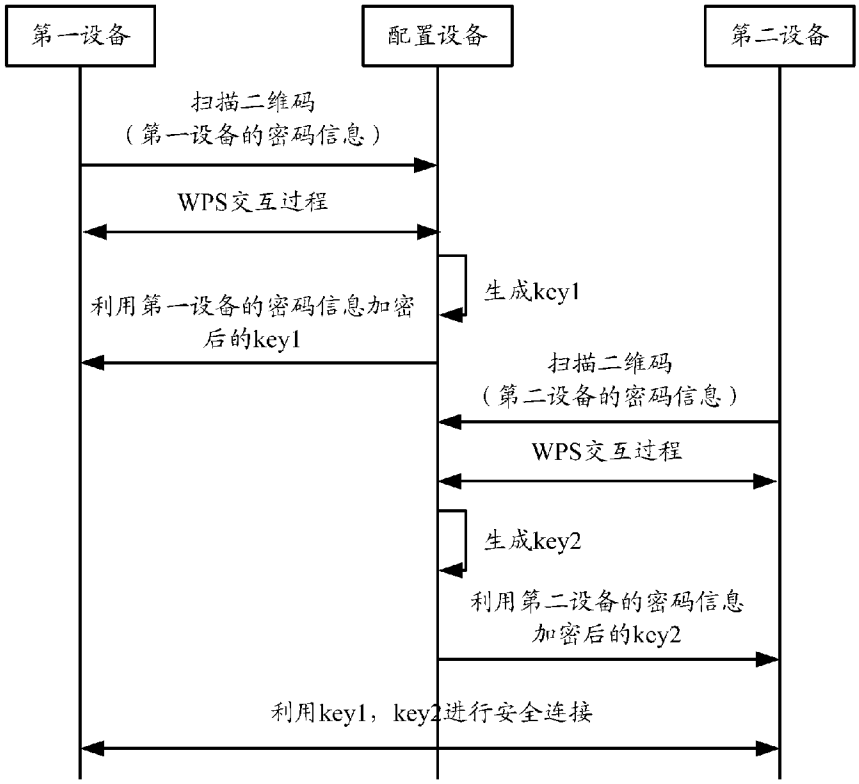
第一设备
配置设备
第二设备
扫描二维码
（第一设备的密码信息）
WPS交互过程
生成key1
利用第一设备的密码信息加密后的key1
扫描二维码
（第二设备的密码信息）
WPS交互过程
生成key2
利用第二设备的密码信息加密后的key2
利用key1，key2进行安全连接

图 1

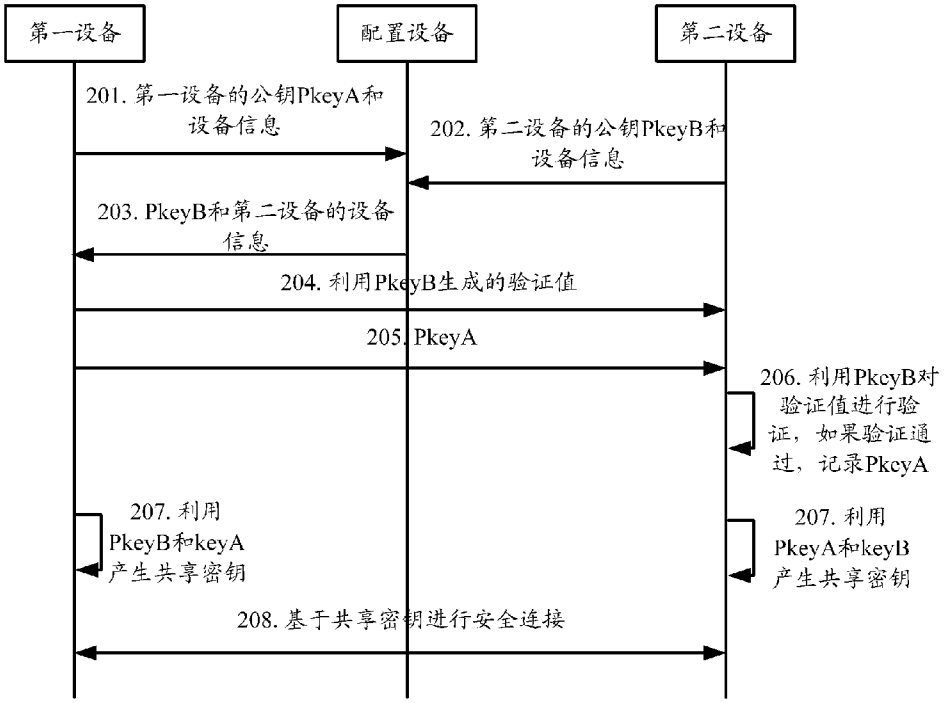
第一设备
配置设备
第二设备
201. 第一设备的公钥PkeyA和设备信息
202. 第二设备的公钥PkeyB和设备信息
203. PkeyB和第二设备的设备信息
204. 利用PkeyB生成的验证值
205. PkeyA
206. 利用PkeyB对验证值进行验证，如果验证通过，记录PkeyA
207. 利用PkeyB和keyA产生共享密钥
207. 利用PkeyA和keyB产生共享密钥
208. 基于共享密钥进行安全连接

图 2

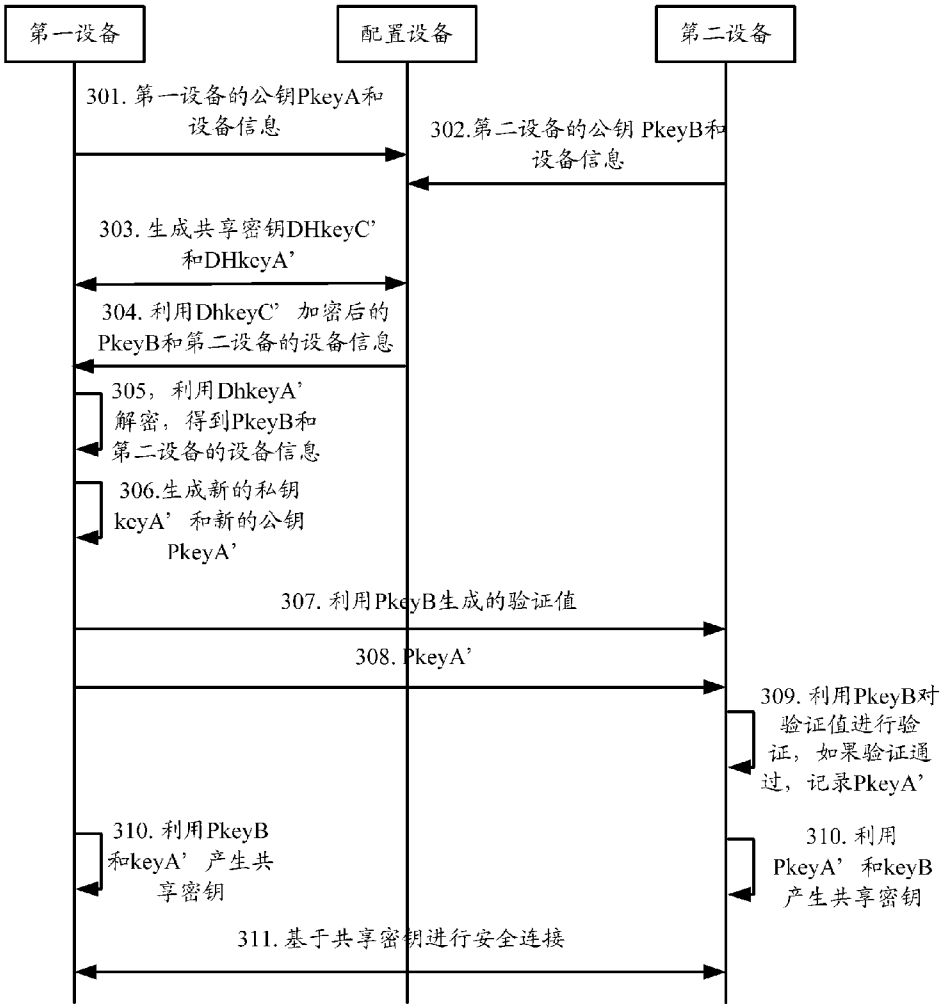
第一设备
配置设备
第二设备
301. 第一设备的公钥PkeyA和设备信息
302.第二设备的公钥 PkeyB和设备信息
303. 生成共享密钥DHkeyC'和DHkeyA'
304. 利用DhkeyC' 加密后的PkeyB和第二设备的设备信息
305，利用DhkeyA'解密，得到PkeyB和第二设备的设备信息
306.生成新的私钥keyA' 和新的公钥PkeyA'
307. 利用PkeyB生成的验证值
308. PkeyA'
309. 利用PkeyB对验证值进行验证，如果验证通过，记录PkeyA'
310. 利用PkeyB和keyA' 产生共享密钥
310. 利用PkeyA' 和keyB产生共享密钥
311. 基于共享密钥进行安全连接

图 3

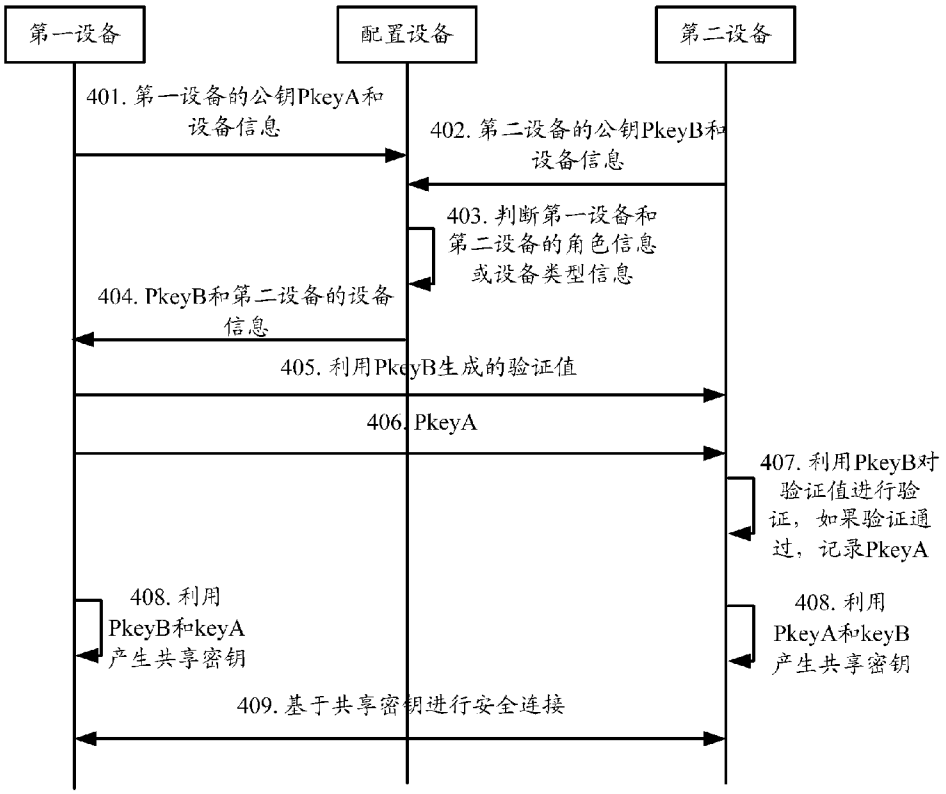
第一设备
配置设备
第二设备
401. 第一设备的公钥PkeyA和设备信息
402. 第二设备的公钥PkeyB和设备信息
403. 判断第一设备和第二设备的角色信息或设备类型信息
404. PkeyB和第二设备的设备信息
405. 利用PkeyB生成的验证值
406. PkeyA
407. 利用PkeyB对验证值进行验证，如果验证通过，记录PkeyA
408. 利用PkeyB和keyA产生共享密钥
408. 利用PkeyA和keyB产生共享密钥
409. 基于共享密钥进行安全连接

图 4

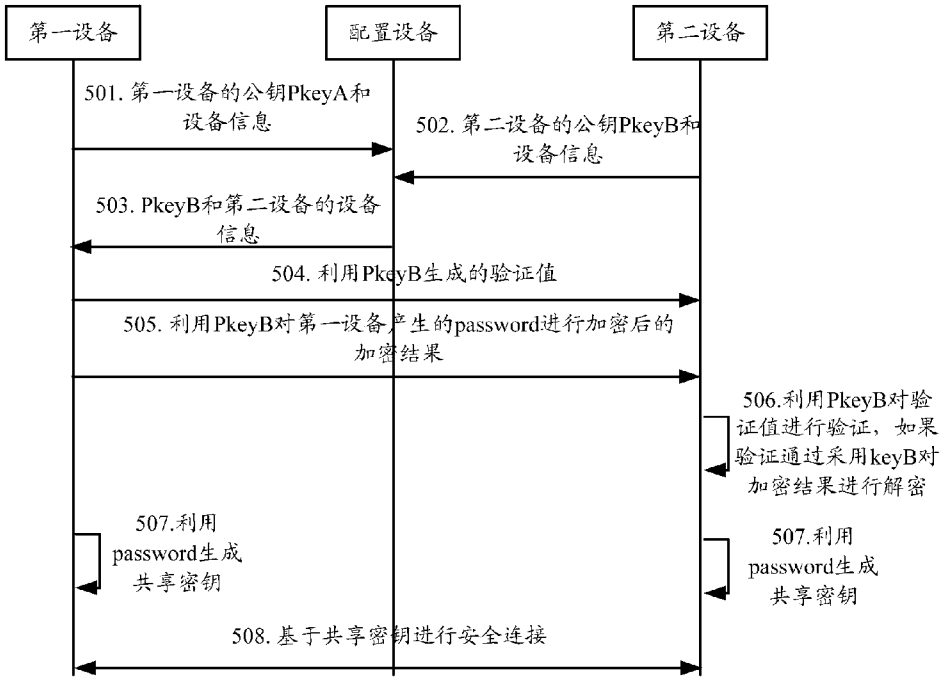
第一设备
配置设备
第二设备
501. 第一设备的公钥PkeyA和设备信息
502. 第二设备的公钥PkeyB和设备信息
503. PkeyB和第二设备的设备信息
504. 利用PkeyB生成的验证值
505. 利用PkeyB对第一设备产生的password进行加密后的加密结果
506.利用PkeyB对验证值进行验证，如果验证通过采用keyB对加密结果进行解密
507.利用password生成共享密钥
507.利用password生成共享密钥
508. 基于共享密钥进行安全连接

图 5

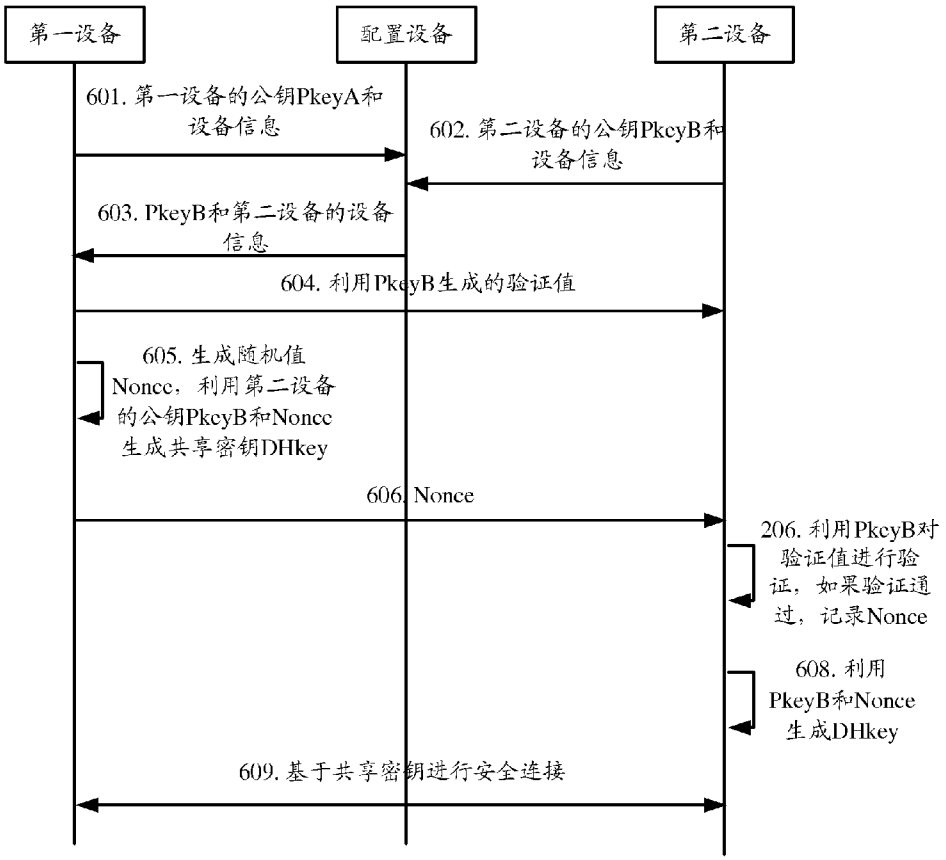
第一设备
配置设备
第二设备
601. 第一设备的公钥PkeyA和设备信息
602. 第二设备的公钥PkeyB和设备信息
603. PkeyB和第二设备的设备信息
604. 利用PkeyB生成的验证值
605. 生成随机值Nonce，利用第二设备的公钥PkeyB和Nonce生成共享密钥DHkey
606. Nonce
206. 利用PkeyB对验证值进行验证，如果验证通过，记录Nonce
608. 利用PkeyB和Nonce生成DHkey
609. 基于共享密钥进行安全连接

图 6

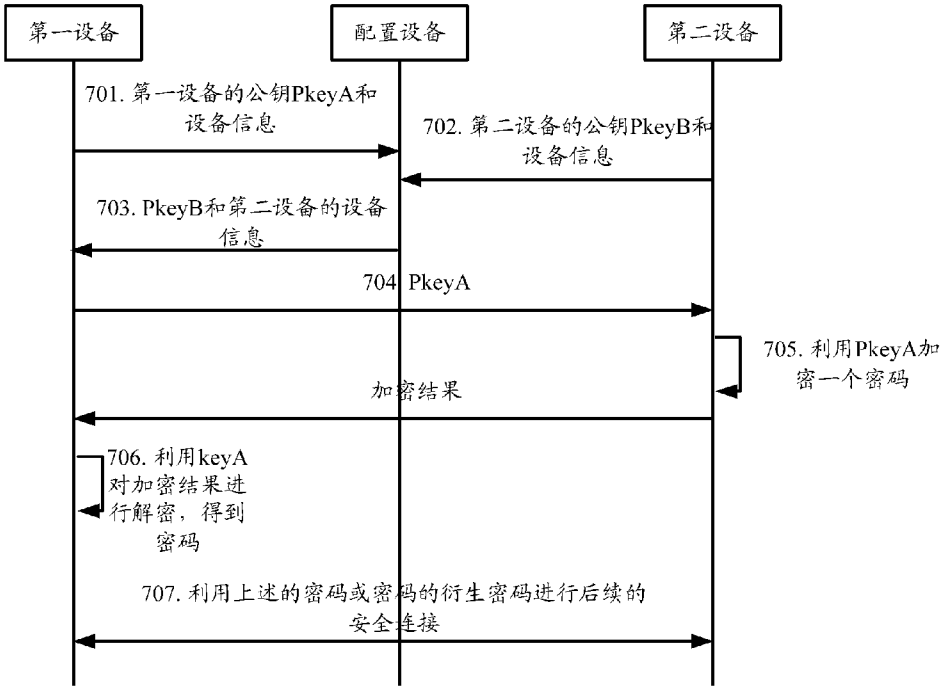
第一设备
配置设备
第二设备
701. 第一设备的公钥PkeyA和设备信息
702. 第二设备的公钥PkeyB和设备信息
703. PkeyB和第二设备的设备信息
704 PkeyA
705. 利用PkeyA加密一个密码
加密结果
706. 利用keyA对加密结果进行解密，得到密码
707. 利用上述的密码或密码的衍生密码进行后续的安全连接

图 7

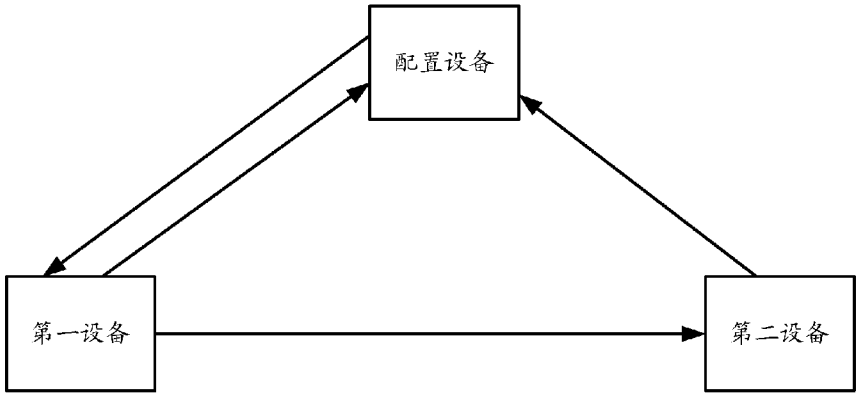

图 8

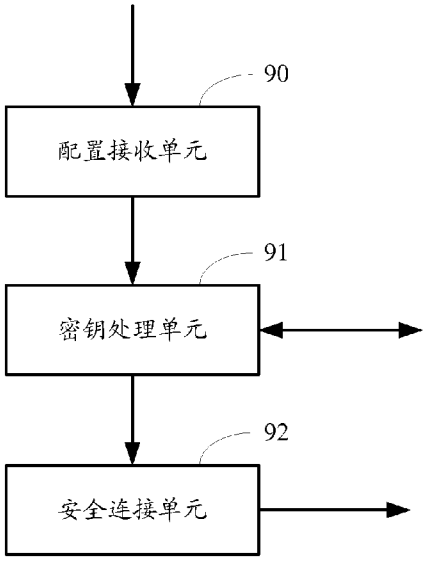

图 9

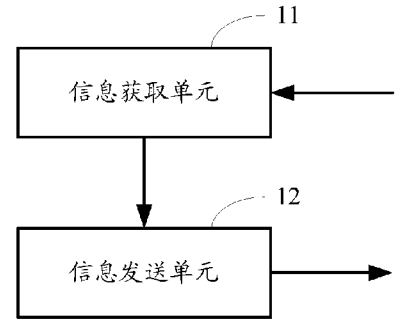

图 10

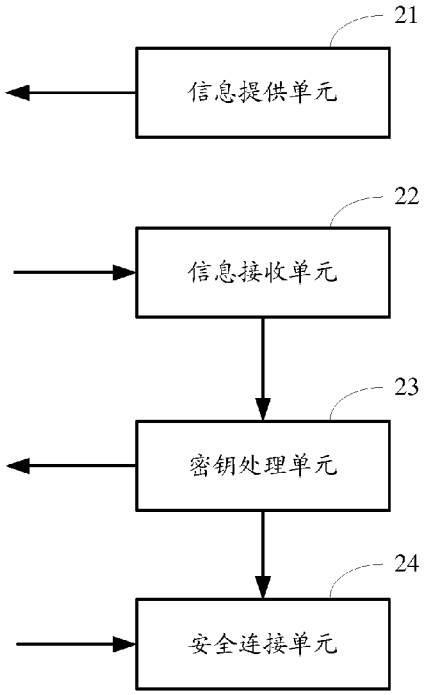

图 11

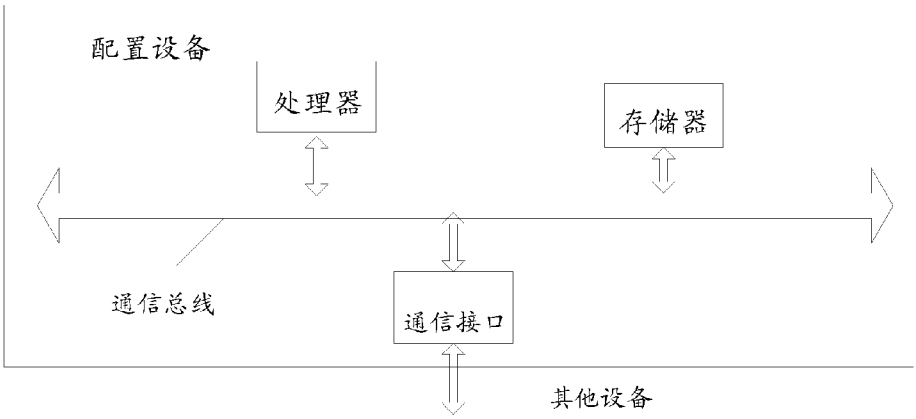

图 12

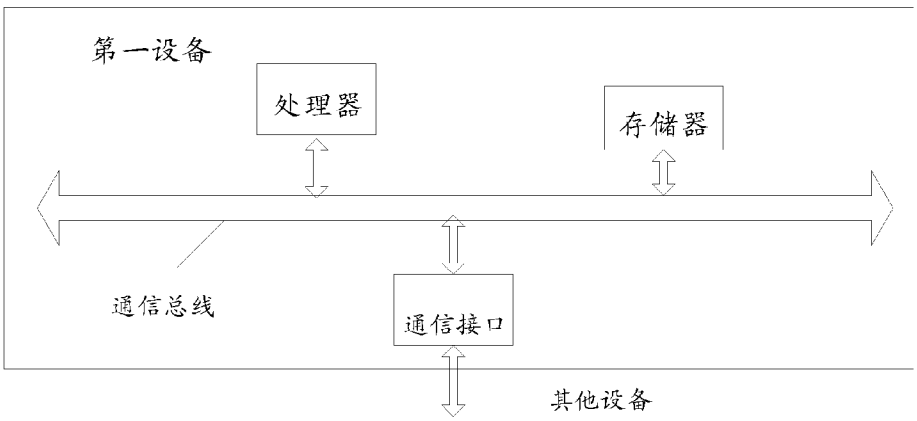

图 13

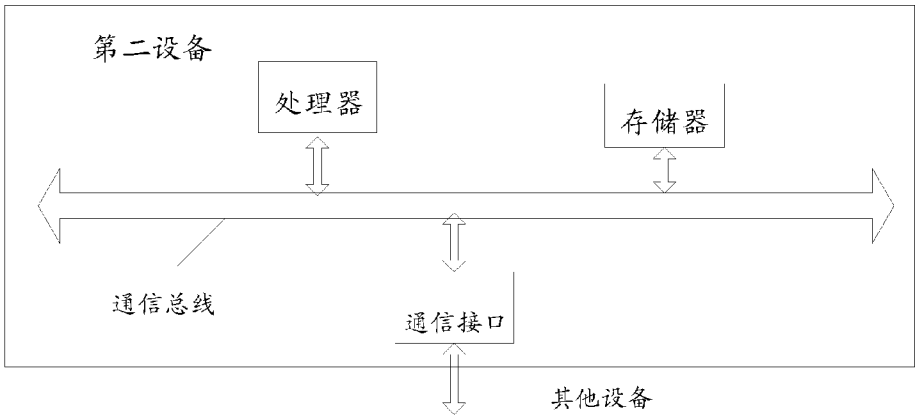

图 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/086247

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14 (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)

IPC: H04L; G06F; H04W; H04Q

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: key public key private key third party configure authentication negotiation headless device sensor wifi credential

VEN: key, public w key, private w key, third w party, configur+, negotiat+, authoriz+, headless, sensor, wifi, credential

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101582906 A (THE PLA INFORMATION ENGINEERING UNIVERSITY), 18 November 2009 (18.11.2009), description, pages 1-2 and 5-8, and figures 1-3	1, 13, 15, 17, 26, 28, 29, 38, 40, 51, 54, 60, 61, 69, 71
A	The same as above	2-12, 14, 16, 18-25, 27, 30-37, 39, 41-50, 52, 53, 55-59, 62-68, 70
A	CN 101267301 A (ALCATEL-LUCENT SHANGHAI BELL CO., LTD.), 17 September 2008 (17.09.2008), the whole document	1-71
A	US 2007118735 A1 (CHERRINGTON, J. et al.), 24 May 2007 (24.05.2007), the whole document	1-71

☐ 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
17 January 2014 (17.01.2014)	**30 January 2014 (30.01.2014)**
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 **LI, Junjie** Telephone No.: (86-10) **62411279**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/086247

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101582906 A	18.11.2009	CN 101582906 B	18.04.2012
CN 101267301 A	17.09.2008	None	
US 2007118735 A1	24.05.2007	WO 2007058907 A2	24.05.2007
		WO 2007058907 A3	22.05.2009

国际检索报告

国际申请号
PCT/CN2013/086247

A. 主题的分类

H04L 9/14 (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)

IPC: H04L; G06F; H04W; H04Q

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：密钥 公钥 私钥 公共密钥 私有密钥 第三方 配置 认证 协商 无头设备 传感器 wifi，信任状；

VEN: key, public w key, private w key, third w party, configur+, negotiat+, authoriz+, headless, sensor, wifi, credential

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 101582906 A (中国人民解放军信息工程大学) 18.11 月 2009 (18.11.2009) 说明书第 1-2，5-8 页，附图 1-3	1,13,15,17,26,28,29,38,40,51,54,60,61,69,71
A	同上	2-12,14,16,18-25,27,30-37,39,41-50,52,53,55-59,62-68,70
A	CN 101267301 A (上海贝尔阿尔卡特股份有限公司) 17.9 月 2008 (17.09.2008) 全文	1-71
A	US 2007118735 A1 (CHERRINGTON J.等) 24.5 月 2007 (24.05.2007) 全文	1-71

☐ 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
17.1 月 2014 (17.01.2014)	**30.1 月 2014 (30.01.2014)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 李俊洁 电话号码：(86-10) **62411279**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/086247

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 101582906 A	18.11.2009	CN 101582906 B	18.04.2012
CN 101267301 A	17.09.2008	无	
US 2007118735 A1	24.05.2007	WO 2007058907 A2	24.05.2007
		WO 2007058907 A3	22.05.2009