(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 7 月 9 日 (09.07.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/100675 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2013/091236

(22) 国际申请日: 2013 年 12 月 31 日 (31.12.2013)

(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总部办公楼, Guangdong 518129 (CN)。 **丁志明 (DING, Zhiming)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **李小仙 (LI, Xiaoxian)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **陆苏 (LU, Su)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, 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)。

(54) **Title**: NETWORK CONFIGURATION METHOD, AND RELATED DEVICE AND SYSTEM

(54) **发明名称** : 一种网络配置方法、相关装置及系统

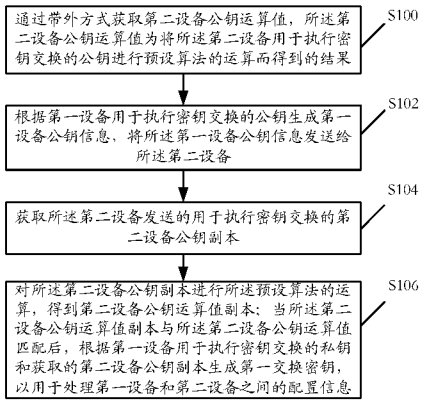

图 1 / **Fig. 1**

S100 OBTAIN A PUBLIC KEY CALCULATION VALUE OF A SECOND DEVICE BY MEANS OF AN OUT-OF-BAND MANNER, THE PUBLIC KEY CALCULATION VALUE OF THE SECOND DEVICE BEING A RESULT OBTAINED BY PERFORMING PRESET-ALGORITHM CALCULATION ON A KEY EXCHANGE PUBLIC KEY OF THE SECOND DEVICE

S102 GENERATE PUBLIC KEY INFORMATION OF A FIRST DEVICE ACCORDING TO A KEY EXCHANGE PUBLIC KEY OF THE FIRST DEVICE, AND SEND THE PUBLIC KEY INFORMATION OF THE FIRST DEVICE TO THE SECOND DEVICE

S104 OBTAIN A KEY EXCHANGE PUBLIC KEY COPY SENT BY THE SECOND DEVICE, OF THE SECOND DEVICE

S106 PERFORM PRESET-ALGORITHM CALCULATION ON THE PUBLIC KEY COPY OF THE SECOND DEVICE, SO AS TO OBTAIN A PUBLIC KEY CALCULATION VALUE COPY OF THE SECOND DEVICE; AND AFTER THE PUBLIC KEY CALCULATION VALUE COPY OF THE SECOND DEVICE MATCHES THE PUBLIC KEY CALCULATION VALUE OF THE SECOND DEVICE, GENERATE A FIRST EXCHANGE KEY ACCORDING TO A KEY EXCHANGE PRIVATE KEY OF THE FIRST DEVICE AND THE OBTAINED PUBLIC KEY COPY OF THE SECOND DEVICE, SO AS TO PROCESS CONFIGURATION INFORMATION BETWEEN THE FIRST DEVICE AND THE SECOND DEVICE

(57) **Abstract**: Disclosed is a network configuration method. The method comprises: obtaining a public key calculation value of a second device by means of an out-of-band manner, the public key calculation value of the second device being a result obtained by performing preset-algorithm calculation on a key exchange public key of the second device; generating public key information of a first device according to a key exchange public key of the first device, and sending the public key information of the first device to the second device, so that the second device obtains a public key of the first device according to the public key information of the first device; obtaining a key exchange public key copy sent by the second device, of the second device; performing preset-algorithm calculation on the public key copy of the second device, so as to obtain a public key calculation value copy of the second device; and after the public key calculation value copy of the second device matches the public key calculation value of the second device, generating a first exchange key according to a key exchange private key of the first device and the obtained public key copy of the second device, so as to process configuration information between the first device and the second device. By using the present invention, procedures for network configuration are simplified.

(57) **摘要**:

[见续页]

WO 2015/100675 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明实施例公开一种网络配置方法，包括：通过带外方式获取第二设备公钥运算值，第二设备公钥运算值为将第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息，将第一设备公钥信息发送给第二设备，以使第二设备根据第一设备公钥信息获取第一设备的公钥；获取第二设备发送的用于执行密钥交换的第二设备公钥副本；对第二设备公钥副本进行预设算法的运算，得到第二设备公钥运算值副本；当第二设备公钥运算值副本与第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。采用本发明，简化网络配置流程。

一种网络配置方法、相关装置及系统

技术领域

本发明涉及通信领域，尤其涉及一种网络配置方法、相关装置及系统。

背景技术

无线保真（Wireless Fidelity，Wi-Fi）是一种广泛应用的无线通信技术，具有部署快速、使用便利和传输速率高等优势，被广泛应用于各个行业，Wi-Fi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Wi-Fi在生活中无所不在。

尽管Wi-Fi网络越来越流行，但是由于Wi-Fi网络设置复杂，设备商依然要投入大量的支持成本来帮助用户建立 Wi-Fi 网络以及解决使用过程中的问题。在那些成功设置了无线网络的用户中，依然有 60%-70%的用户没有配置任何的安全参数，网络很受容易遭到攻击。为了解决用户在使用无线网络时的困惑，Wi-Fi联盟推出了Wi-Fi安全设置（Wi-Fi Protected Setup，WPS）规范，又称Wi-Fi简单配置（Wi-Fi Simple Configuration，WSC），旨在简化用户在设置WLAN（Wireless Local Area Network，无线局域网）时的操作，让那些对无线设置和安全没有太多了解的用户也可以简单方便地设置安全的 WLAN，可以方便地向网络中添加设备。

WPS的主要应用场景为：1. 初始WLAN设置，指用一配置设备为一个新的AP建立WLAN；2. WLAN建立后，向该WLAN增添新的设备。

WPS标准提出了三种配置方式，即个人身份识别码（Personal Identification Number，PIN）方式、按钮控制（Push Button Control，PBC）方式、近距离通信（Near Field Communication，NFC）方式。PIN方式即用户在注册器上输入待配置设备的PIN码；PBC方式即用户在注册器和待配置设备上几乎同时按下按钮；NFC方式则有三种方式：1，通过NFC直接传配置信息；2，通过NFC向配置设备传输待配置设备的密码；3，通过NFC进行connection handover，双方交换Diffie-Hellman（DH）公钥的hash值。

然而，PIN 方式需要人为输入 PIN 码，比较繁琐且安全性不高，PBC 方式虽然操作简单但无法抵抗主动攻击，NFC 方式要求设备必须都具有 NFC 接口，普适性较低。此外，WPS 采用 M1-M8 8 条消息来进行验证，消息繁多复杂，对终端的处理能力要求也较高，配置效率低下；而且需要配置的双方设备的带外信道（即除 Wi-Fi 信道以外的其它信道）宽带有限，在配置过程中交互消息繁多复杂，或者交互消息内容过大，同样也将导致配置效率低下。

发明内容

本发明实施例所要解决的技术问题在于，提供一种网络配置方法、相关装置及系统，简化了网络配置流程，并提高了配置的安全性，大大提高了用户的配置体验。

第一方面，本发明实施例提供了一种网络配置方法，包括：

通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；

根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息，将所述第一设备公钥信息发送给所述第二设备，以使所述第二设备根据所述第一设备公钥信息获取第一设备的公钥；

获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本；

对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

结合第一方面，在第一种可能的实现方式中，所述根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息之前还包括：

通过带外方式获取第二设备密钥信息。

结合第一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，所述根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括：

利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

结合第一方面，或者第一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，所述根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括:

利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

结合第一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，所述获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本包括:

接收所述第二设备发送的第二设备公钥信息，所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本；所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；所述第一设备公钥运算值副本为将自身的公钥进行预设算法的运算而得到的结果；或者

接收所述第二设备发送的第二设备公钥信息；当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；利用第一设备获取的第二设备密钥信息解密所述第二设备公钥信息，得到第二设备公钥副本。

结合第一方面，或者第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，或者第一方面的第三种可能的实现方式，或者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，所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；

以所述第一交换密钥为加密密钥，加密配置信息后发送给所述第二设备。

结合第一方面，或者第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，或者第一方面的第三种可能的实现方式，或者第一方

面的第四种可能的实现方式，在第六种可能的实现方式中，所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

接收所述第二设备发送的配置信息; 所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息; 所述第二交换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果;

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

以所述第一交换密钥解密接收到的所述配置信息。

结合第一方面，或者第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，或者第一方面的第三种可能的实现方式，或者第一方面的第四种可能的实现方式，在第七种可能的实现方式中，所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

以所述第一交换密钥为加密密钥，加密第三设备公钥运算值; 所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果;

将加密后的第三设备公钥运算值发送给所述第二设备; 以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

结合第一方面，或者第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，或者第一方面的第三种可能的实现方式，或者第一方面的第四种可能的实现方式，在第八种可能的实现方式中，所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。

结合第一方面，或者第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，或者第一方面的第三种可能的实现方式，或者第一方面的第四种可能的实现方式，在第九种可能的实现方式中，所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

基于所述第一交换密钥生成进行四步握手过程时的主密钥。

结合第一方面的第五种可能的实现方式，在第十种可能的实现方式中，所述方法还包括:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的配置信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

结合第一方面的第六种可能的实现方式，在第十一种可能的实现方式中，所述以所述第一交换密钥解密接收到的所述配置信息后还包括:

生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对所述配置确认信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

结合第一方面的第七种可能的实现方式，在第十二种可能的实现方式中，所述方法还包括:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的第三设备公钥运算值进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

第二方面，本发明实施例提供了一种网络配置方法，包括:

将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取;

接收所述第一设备发送的第一设备公钥信息，并根据所述第一设备公钥信

息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息；

向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本；

根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

结合第二方面，在第一种可能的实现方式中，所述接收所述第一设备发送的第一设备公钥信息之前还包括：

生成第二设备密钥信息，以供第一设备通过带外方式获取。

结合第二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，接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

所述根据所述第一设备公钥信息获取第一设备的公钥包括：

利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥。

结合第二方面，或者第二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，接收的所述第一设备公钥信息为所述第一设备利用所述第二设备公钥运算值作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

所述根据所述第一设备公钥信息获取第一设备的公钥包括：

利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥。

结合第二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，所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；或者

当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥

信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息。

结合第二方面，或者第二方面的第一种可能的实现方式，或者第二方面的第二种可能的实现方式，或者第二方面的第三种可能的实现方式，或者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，所述根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

接收所述第一设备发送的配置信息; 所述配置信息为第一设备以第一交换密钥为加密密钥进行加密后的配置信息，所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果; 将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密接收到的所述配置信息; 或者

将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥; 以所述第二交换密钥为加密密钥，加密配置信息后发送给所述第一设备。

结合第二方面，或者第二方面的第一种可能的实现方式，或者第二方面的第二种可能的实现方式，或者第二方面的第三种可能的实现方式，或者第二方面的第四种可能的实现方式，在第六种可能的实现方式中，所述根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

接收所述第一设备发送的加密后的第三设备公钥运算值; 将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程;

所述加密后的第三设备公钥运算值为所述第一设备以所述第一交换密钥为加密密钥对第三设备公钥运算值进行加密而得到的结果; 所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果; 所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果。

结合第二方面的第五种可能的实现方式，在第七种可能的实现方式中，所述方法还包括:

接收第一设备发送的经过哈希消息认证运算后的信息，以第二交换密钥或第二交换密钥的衍生密钥作为哈希消息认证码运算的解密密钥，对接收到的所述经过哈希消息认证运算后的信息进行解密验证。

第三方面，本发明实施例提供了一种网络配置装置，包括:

第一获取模块，用于通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果;

第一设备公钥信息生成模块，用于根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息;

第一发送模块，用于将所述第一设备公钥信息发送给所述第二设备，以使所述第二设备根据所述第一设备公钥信息获取第一设备的公钥;

第二设备公钥副本获取模块，用于获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本;

第一配置模块，用于对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本;当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

结合第三方面，在第一种可能的实现方式中，所述装置还包括:

第二获取模块，用于通过带外方式获取第二设备密钥信息。

结合第三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，所述第一设备公钥信息生成模块包括:

第一加密单元，用于利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

结合第三方面，或者第三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，所述第一设备公钥信息生成模块包括:

第二加密单元，用于利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

结合第三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，所述第二设备公钥副本获取模块包括:

第一接收单元和第一解密得到单元，其中，所述第一接收单元用于接收所述第二设备发送的第二设备公钥信息，所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；所述第一解密得到单元用于利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本；所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；所述第一设备公钥运算值副本为将自身的公钥进行预设算法的运算而得到的结果；和/或

第二接收单元和第二解密得到单元，其中，所述第二接收单元用于接收所述第二设备发送的第二设备公钥信息；当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；所述第二解密得到单元用于利用第一设备获取的第二设备密钥信息解密所述第二设备公钥信息，得到第二设备公钥副本。

结合第三方面，或者第三方面的第一种可能的实现方式，或者第三方面的第二种可能的实现方式，或者第三方面的第三种可能的实现方式，或者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，所述第一配置模块包括:

第一运算单元，用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；

配置信息加密单元，用于以所述第一交换密钥为加密密钥，加密配置信息后发送给所述第二设备。

结合第三方面，或者第三方面的第一种可能的实现方式，或者第三方面的第二种可能的实现方式，或者第三方面的第三种可能的实现方式，或者第三方

面的第四种可能的实现方式，在第六种可能的实现方式中，所述第一配置模块包括:

配置信息接收单元，用于接收所述第二设备发送的配置信息；所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息；所述第二交换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果;

第二运算单元，用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

解密单元，用于以所述第一交换密钥解密接收到的所述配置信息。

结合第三方面，或者第三方面的第一种可能的实现方式，或者第三方面的第二种可能的实现方式，或者第三方面的第三种可能的实现方式，或者第三方面的第四种可能的实现方式，在第七种可能的实现方式中，所述第一配置模块包括:

第三运算单元，将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

公钥运算值加密单元，用于以所述第一交换密钥为加密密钥，加密第三设备公钥运算值；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果;

发送单元，用于将加密后的第三设备公钥运算值发送给所述第二设备；以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

结合第三方面，或者第三方面的第一种可能的实现方式，或者第三方面的第二种可能的实现方式，或者第三方面的第三种可能的实现方式，或者第三方面的第四种可能的实现方式，在第八种可能的实现方式中，所述第一配置模块包括:

第四运算单元，用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

会话密钥生成单元，用于基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。

结合第三方面，或者第三方面的第一种可能的实现方式，或者第三方面的第二种可能的实现方式，或者第三方面的第三种可能的实现方式，或者第三方面的第四种可能的实现方式，在第九种可能的实现方式中，所述第一配置模块包括:

第五运算单元，用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

主密钥生成单元，用于基于所述第一交换密钥生成进行四步握手过程时的主密钥。

结合第三方面的第五种可能的实现方式，在第十种可能的实现方式中，所述装置还包括:

第一哈希运算模块，用于以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的配置信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

结合第三方面的第六种可能的实现方式，在第十一种可能的实现方式中，所述装置还包括:

第二哈希运算模块，用于当所述解密单元解密接收到的所述配置信息后，生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对所述配置确认信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

结合第三方面的第七种可能的实现方式，在第十二种可能的实现方式中，所述装置还包括:

第三哈希运算模块，用于以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的第三设备公钥运算值进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

第四方面，本发明实施例提供了一种网络配置装置，包括:

第二设备公钥运算值生成模块，用于将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取;

接收获取模块，用于接收所述第一设备发送的第一设备公钥信息，并根据

所述第一设备公钥信息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息；

第二设备公钥信息发送模块，用于向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本；

第二配置模块，用于根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

结合第四方面，在第一种可能的实现方式中，所述网络配置设备还包括：

随机密钥生成模块，用于生成第二设备密钥信息，以供第一设备通过带外方式获取。

结合第四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，所述接收获取模块接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

所述接收获取模块包括：

第一解密单元，用于利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥。

结合第四方面，或者第四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，所述接收获取模块接收的所述第一设备公钥信息为所述第一设备利用所述第二设备公钥运算值作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

所述接收获取模块包括：

第二解密单元，用于利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥。

结合第四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，所述网络配置设备还包括：

公钥信息第一生成模块，用于利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到第二设备公钥信息；所述第一设备

公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；或者

公钥信息第二生成模块，用于当第一设备通过带外方式获取了第二设备密钥信息时，利用自身的第二设备密钥信息对第二设备的公钥进行对称加密而得到第二设备公钥信息。

结合第四方面，或者第四方面的第一种可能的实现方式，或者第四方面的第二种可能的实现方式，或者第四方面的第三种可能的实现方式，或者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，所述第二配置模块还包括：

配置信息接收解密单元，用于接收所述第一设备发送的配置信息；所述配置信息为第一设备以第一交换密钥为加密密钥进行加密后的配置信息，所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密接收到的所述配置信息；和/或

配置信息发送单元，用于将所述第一设备的公钥与第二设备用于执行密钥交换的私钥进行运算得到第二交换密钥；以所述第二交换密钥为加密密钥，加密配置信息后发送给所述第一设备。

结合第四方面，或者第四方面的第一种可能的实现方式，或者第四方面的第二种可能的实现方式，或者第四方面的第三种可能的实现方式，或者第四方面的第四种可能的实现方式，在第六种可能的实现方式中，所述第二配置模块包括：

第三设备公钥运算值接收解密单元，用于接收所述第一设备发送的加密后的第三设备公钥运算值，将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密所述第三设备公钥运算值；所述加密后的第三设备公钥运算值为所述第一设备以所述第一交换密钥为加密密钥对第三设备公钥运算值进行加密而得到的结果；所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的

公钥进行预设算法的运算而得到的结果;

配置子单元,用于利用所述第三设备公钥运算值与所述第三设备进行密钥交换,并完成最终的配置过程。

结合第四方面的第五种可能的实现方式,在第七种可能的实现方式中,所述网络配置设备还包括:

哈希运算验证模块,用于接收第一设备发送的经过哈希消息认证运算后的信息,以第二交换密钥或第二交换密钥的衍生密钥作为哈希消息认证码运算的解密密钥,对接收到的所述经过哈希消息认证运算后的信息进行解密验证。

第五方面,本发明实施例提供了一种网络设备,包括:输入装置、输出装置、存储器和处理器;

其中,所述存储器用于存储程序代码,所述处理器用于调用所述存储器存储的程序代码执行如下步骤:

由所述输入装置通过带外方式获取第二设备公钥运算值,所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果;根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息,通过所述输出装置将所述第一设备公钥信息发送给所述第二设备,以使所述第二设备根据所述第一设备公钥信息获取第一设备的公钥;通过所述输入装置获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本;对所述第二设备公钥副本进行所述预设算法的运算,得到第二设备公钥运算值副本;当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后,根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥,以用于处理第一设备和第二设备之间的配置信息。

结合第五方面,在第一种可能的实现方式中,所述处理器根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息之前还执行:

由所述输入装置通过带外方式获取第二设备密钥信息。

结合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,所述处理器根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括:

利用所述第二设备密钥信息作为对称加密密钥,对所述第一设备用于执行密钥交换的公钥进行对称加密运算,生成第一设备公钥信息。

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，所述处理器根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括:

利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

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，所述处理器通过所述输入装置获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本包括:

通过所述输入装置接收所述第二设备发送的第二设备公钥信息，所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本；所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；所述第一设备公钥运算值副本为将自身的公钥进行预设算法的运算而得到的结果；或者

通过所述输入装置接收所述第二设备发送的第二设备公钥信息；当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；利用第一设备获取的第二设备密钥信息解密所述第二设备公钥信息，得到第二设备公钥副本。

结合第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的第二种可能的实现方式，或者第五方面的第三种可能的实现方式，或者第五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，所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；以所述第一交换密钥为加密密钥，加密配置信息后发送给所述第二设备。

结合第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的

第二种可能的实现方式，或者第五方面的第三种可能的实现方式，或者第五方面的第四种可能的实现方式，在第六种可能的实现方式中，所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

通过所述输入装置接收所述第二设备发送的配置信息；所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息；所述第二交换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果；将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；以所述第一交换密钥解密接收到的所述配置信息。

结合第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的第二种可能的实现方式，或者第五方面的第三种可能的实现方式，或者第五方面的第四种可能的实现方式，在第七种可能的实现方式中，所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；以所述第一交换密钥为加密密钥，加密第三设备公钥运算值；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；将加密后的第三设备公钥运算值发送给所述第二设备；以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

结合第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的第二种可能的实现方式，或者第五方面的第三种可能的实现方式，或者第五方面的第四种可能的实现方式，在第八种可能的实现方式中，所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。

结合第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的第二种可能的实现方式，或者第五方面的第三种可能的实现方式，或者第五方面的第四种可能的实现方式，在第九种可能的实现方式中，所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；基于所述第一交换密钥生成进行四步握手过程时的主密钥。

结合第五方面的第五种可能的实现方式，在第十种可能的实现方式中，所述处理器以所述第一交换密钥解密接收到的所述配置信息后还执行:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的配置信息进行哈希消息认证运算，通过所述输出装置并向第二设备发送进行哈希消息认证运算后的信息。

结合第五方面的第六种可能的实现方式，在第十一种可能的实现方式中，所述处理器还执行:

生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对所述配置确认信息进行哈希消息认证运算，通过所述输出装置并向第二设备发送进行哈希消息认证运算后的信息。

结合第五方面的第七种可能的实现方式，在第十二种可能的实现方式中，所述处理器还执行:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的第三设备公钥运算值进行哈希消息认证运算，并通过所述输出装置向第二设备发送进行哈希消息认证运算后的信息。

第六方面，本发明实施例提供了一种网络设备，包括：输入装置、输出装置、存储器和处理器；

其中，所述存储器用于存储程序代码，所述处理器用于调用所述存储器存储的程序代码执行如下步骤:

将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；通过所述输入装置接收所述第

一设备发送的第一设备公钥信息，并根据所述第一设备公钥信息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息；通过所述输出装置向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本；根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

结合第六方面，在第一种可能的实现方式中，所述处理器通过所述输入装置接收所述第一设备发送的第一设备公钥信息之前还包括：

生成第二设备密钥信息，以供第一设备通过带外方式获取。

结合第六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，所述处理器通过所述输入装置接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

所述处理器根据所述第一设备公钥信息获取第一设备的公钥包括：利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥。

结合第六方面，或者第六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，通过所述输入装置接收的所述第一设备公钥信息为所述第一设备利用所述第二设备公钥运算值作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

所述处理器根据所述第一设备公钥信息获取第一设备的公钥包括：

利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥。

结合第六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，所述第二设备公钥信息为所述处理器利用第一设备公钥运算值对第二设备的公钥进行对称加密而得到的信息；所述第一设备公钥运算值为所述处理器将获得的第一设备的公钥进行预设算法的运算而得到的结果；或者

当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述处理器利用自身的第二设备密钥信息对第二设备的公钥进行对称

加密而得到的信息。

结合第六方面，或者第六方面的第一种可能的实现方式，或者第六方面的第二种可能的实现方式，或者第六方面的第三种可能的实现方式，或者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，所述处理器根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

通过所述输入装置接收所述第一设备发送的配置信息；所述配置信息为第一设备以第一交换密钥为加密密钥进行加密后的配置信息，所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密接收到的所述配置信息；或者

将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥；以所述第二交换密钥为加密密钥，加密配置信息后通过所述输出装置发送给所述第一设备。

结合第六方面，或者第六方面的第一种可能的实现方式，或者第六方面的第二种可能的实现方式，或者第六方面的第三种可能的实现方式，或者第六方面的第四种可能的实现方式，在第六种可能的实现方式中，所述处理器根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

通过所述输入装置接收所述第一设备发送的加密后的第三设备公钥运算值；将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程；所述加密后的第三设备公钥运算值为所述第一设备以所述第一交换密钥为加密密钥对第三设备公钥运算值进行加密而得到的结果；所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果。

结合第六方面的第五种可能的实现方式，在第七种可能的实现方式中，所

述处理器还执行:

通过所述输入装置接收第一设备发送的经过哈希消息认证运算后的信息，以第二交换密钥或第二交换密钥的衍生密钥作为哈希消息认证码运算的解密密钥，对通过所述输入装置接收到的所述经过哈希消息认证运算后的信息进行解密验证。

第七方面，本发明实施例提供了一种网络配置系统，包括第一设备和第二设备，其中

所述第一设备为第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的第二种可能的实现方式，或者第五方面的第三种可能的实现方式，或者第五方面的第四种可能的实现方式，或者第五方面的第五种可能的实现方式，或者第五方面的第六种可能的实现方式，或者第五方面的第七种可能的实现方式，或者第五方面的第八种可能的实现方式，或者第五方面的第九种可能的实现方式，或者第五方面的第十种可能的实现方式中，或者第五方面的第十一种可能的实现方式中，或者第五方面的第十二种可能的实现方式中的网络设备;

所述第二设备为第六方面，或者第六方面的第一种可能的实现方式，或者第六方面的第二种可能的实现方式，或者第六方面的第三种可能的实现方式，或者第六方面的第四种可能的实现方式，或者第六方面的第五种可能的实现方式，或者第六方面的第六种可能的实现方式，或者第六方面的第七种可能的实现方式中的网络设备。

通过实施本发明实施例，对公钥进行运算得到公钥运算值，以公钥运算值作为加密密钥来加密密钥交换的公钥，可大大提高配置过程的安全性；在配置过程的交互信息中用公钥运算值替代公钥，可以减少交互信息的内容，提高配置双方设备的带外信道利用率，并可以通过扫描多维码的配置方式完成配置，解决了现有技术中 PIN 方式比较繁琐且安全性不高，PBC 方式安全性不足，以及 NFC 普适性较低的问题，而且与对公钥进行多维码编码相比，大大减少了多维码编码内容，降低了多维码的显示、扫描以及解码的要求，并适用性高，配置效率得到了很大的提高，大大提升了用户的配置体验。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明提供的网络配置方法的第一实施例的流程示意图；

图 2 是本发明提供的网络配置方法的第二实施例的流程示意图；

图 3 是本发明提供的网络配置方法的第三实施例的流程示意图；

图 4 是本发明提供的网络配置方法的第四实施例的流程示意图；

图 5 是本发明提供的网络配置方法的第五实施例的流程示意图；

图 6 是本发明的网络配置装置的第一实施例的结构示意图；

图 7 是本发明的网络配置装置的第二实施例的结构示意图；

图 8 是本发明的网络配置装置的第三实施例的结构示意图；

图 9 是本发明实施例的第二设备公钥副本获取模块的结构示意图；

图 10 是本发明第一配置模块的第一实施例的结构示意图；

图 11 是本发明第一配置模块的第二实施例的结构示意图；

图 12 是本发明第一配置模块的第三实施例的结构示意图；

图 13 是本发明第一配置模块的第四实施例的结构示意图；

图 14 是本发明第一配置模块的第五实施例的结构示意图；

图 15 是本发明的网络配置设备的第一实施例的结构示意图；

图 16 是本发明的网络配置设备的第二实施例的结构示意图；

图 17 是本发明的接收获取模块的第一实施例的结构示意图；

图 18 是本发明的接收获取模块的第二实施例的结构示意图；

图 19 是本发明的网络配置设备的第三实施例的结构示意图；

图 20 是本发明的第二配置模块的第一实施例的结构示意图；

图 21 是本发明的第二配置模块的第二实施例的结构示意图；

图 22 是本发明的网络设备的第一实施例的结构示意图；

图 23 是本发明的网络设备的第二实施例的结构示意图；

图 24 是本发明实施例的网络配置系统的结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

参见图 1，是本发明提供的网络配置方法的第一实施例的流程示意图，该方法包括:

步骤 S100: 通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果;

具体地，第一设备与第二设备进行网络配置，例如，第一设备为智能手机，第二终端与智能平板，通过网络配置过程后使得第一设备与第二设备拥有共享密钥信息；或者，第一设备为无线接入点的配置器设备，第二设备为要接入无线接入点的无线终端，通过网络配置后，第一设备向第二设备发放接入无线接入点的信任状信息，如四步握手的主密钥等认证材料。第二设备持有自己的公私钥对，第二设备将自身的公钥进行预设算法的运算后可得到第二设备公钥运算值；该预设算法包括但不限于散列算法，散列算法可以为安全散列算法（Secure Hash Algorithm，SHA）-256，SHA-224，信息摘要算法第五版（Message Digest Algorithm，MD5）等，但不以此为限。

本发明实施例以 SHA-256 为例进行说明，SHA-256 输出 256bit 的杂凑值，该杂凑值可以直接作为公钥的运算值，其运算示例如下:

公钥 PKey 的运算值=SHA-256(PKey);

或者可以对该输出进行截取，如截取前 128 位或后 128 位作为公钥的运算值，其运算示例如下:

公钥 PKey 的运算值= SHA-256(PKey)的前 128 位

又或者，将设备的信息也加入进去进行运算，设备信息包括 MAC 地址，设备类型等，运算示例如下:

公钥 PKey 的运算值=SHA-256（PKey||MAC_address||device type）

又或者，当设备不受 UI 功能限制时，在运算公钥的运算值之前可以通过获得另一设备的设备信息，将另一设备的设备信息加入运算，设备信息包括 MAC 地址，设备类型等，运算示例如下：

公钥 PKey 的运算值=SHA-256（PKey|| 对方的 MAC_address）

此外，设备的公钥的运算值也可以通过其他方式得到，如通过直接截取公钥 PKey 的若干位得到。运算示例如下：

公钥 PKey 的运算值= PKey 的前 128 位

步骤 S100 中，第一设备可以通过多种带外方式来获取第二设备公钥运算值，包括但不限于如下 3 种获取方式：

a、第二设备将得到的公钥运算值（可以假设该供第一设备获取的第二设备公钥运算值为带外第二公钥运算值）编码于多维码，第一设备以扫描等方式获得多维码后解码得到第二设备公钥运算值。根据设备能力的不同，多维码可以为静态多维码，如标签打印的多维码，在制造出厂时被贴在设备上；或动态多维码，如由第二设备动态生成多维码显示于屏幕上；多维码码制可以为任何可以识读的一维条码、二维条码码制，例如通用产品代码（Universal Product Code，UPC）、快速响应码（Quick Response Code，QR Code）等。本发明并不以此为限。第一设备具备多维码获取和识别功能，以获得多维码并将多维码解码得到第二设备公钥运算值。

b、第一设备以近距离无线通信方式获得带外第二公钥运算值。例如，第一设备通过 NFC 接口获得带外第二公钥运算值，具体地可以通过 NFC 主动模式或 NFC 被动模式获得。或是，第二设备通过其他无线低功率通信，如低功率蓝牙或低功率 Wi-Fi 等方式，将带外第二公钥运算值在报文中发送给第一设备。

c、第一设备通过接收人机交互界面的输入而获得带外第二公钥运算值，如接收用户通过键盘输入的带外第二公钥运算值，或者接收从 USB 接口输入的带外第二公钥运算值。

步骤 S102：根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息，将所述第一设备公钥信息发送给所述第二设备；

具体地，该第一设备公钥信息可以为对用于执行密钥交换的公钥进行加密

等处理后得到的信息，那么第二设备得到该第一设备公钥信息后，进行相对应的解密等处理后得到第一设备用于执行密钥交换的公钥。

步骤 S104：获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本；

步骤 S106：对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

具体地，第一设备对第二设备的公钥副本进行运算的算法可参考步骤 S100 中描述的运算算法，这里不再赘述。第一设备将运算后的第二设备公钥运算值副本与步骤 S100 中获得的第二设备公钥运算值进行对比，若两者相等，则表明判断匹配成功，确认了接收到的消息为第二设备发送而来的消息，因此可以进一步进行配置，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

进一步地，本发明实施例中的步骤 S102 之前还可以包括：通过带外方式获取第二设备密钥信息。即可以在步骤 S100 通过带外方式获取第二设备公钥运算值的同时，获取第二设备密钥信息；具体地：

该第二设备密钥信息包括但不限于由第二设备随机生成，或者在生产过程中配置到第二设备中，又或者由用户配置到第二设备中，然后由带外方式提供给第一设备。

为了便于更好地实施本发明实施例的上述方案，下面结合图 2 示出的本发明提供的网络配置方法的第二实施例的流程示意图，以第二设备端来描述配置过程，该方法包括：

步骤 S200：将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；

具体地，第二设备持有自身的公私钥对，即第二设备私钥（假设为 Key 第二设备）和第二设备公钥（假设为 PKey 第二设备）；第二设备将自身的公钥进行的运算算法可参考图 1 实施例中的步骤 S100 描述的运算算法，这里不

再赘述；可以理解的，本发明实施例中的第二设备公钥运算值（假设为 PKey 第二设备运算值）还可以是通过上述算法运算得出的公钥运算衍生值（假设为 Pkey 第二设备运算衍生值），其衍生方式包括但不限于对公钥运算后的值进行散列、移位、反转等衍生运算。

步骤 S202：接收所述第一设备发送的第一设备公钥信息，并根据所述第一设备公钥信息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息；

步骤 S204：向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本；根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

并对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，所述第一设备接受接收到的第二设备发送的配置信息，或者生成配置信息发送给所述第二设备。

具体地，该第二设备公钥信息可以直接为第二设备的公钥，即第一设备接收到该第二设备公钥信息后直接得到了第二设备的公钥副本；也可以为对第二设备的公钥经过加密等处理后的信息，那么第一设备接收到该第二设备公钥信息后进行相应的解密等处理，得到第二设备的公钥副本，并对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

下面结合图 3 示出的本发明提供的网络配置方法的第三实施例的流程示意图，进一步说明本发明实施方案：

步骤 S300：第二设备将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；

具体地，第二设备持有自身的公私钥对，即第二设备私钥（假设为 Key

第二设备）和第二设备公钥（假设为 PKey 第二设备）；第二设备将自身的公钥进行的运算算法可参考图 1 实施例中的步骤 S100 描述的运算算法，这里不再赘述；可以理解的，本发明实施例中的第二设备公钥运算值（假设为 PKey 第二设备运算值）还可以是通过上述算法运算得出的公钥运算衍生值（假设为 Pkey 第二设备运算衍生值），其衍生方式包括但不限于对公钥运算后的值进行散列、移位、反转等衍生运算。

步骤 S302：第一设备通过带外方式获取第二设备公钥运算值和第二设备密钥信息；

具体地，获取方式可以为图 1 实施例中步骤 S100 描述的方式，这里不再赘述。

步骤 S304：第一设备利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息；

步骤 S306：将第一设备公钥信息发送给所述第二设备；

步骤 S308：第二设备利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥；

步骤 S310：向第一设备发送用于执行密钥交换的第二设备公钥副本；

步骤 S312：第一设备把接收到的第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；

可理解的，第一设备对第二设备公钥副本进行运算的算法可以参考图 1 实施例中步骤 S100 描述的运算算法，这里不再赘述；

步骤 S314：第一设备判断所述第二设备公钥运算值副本与所述第二设备公钥运算值是否匹配；

具体地，第一设备将运算后的第二设备公钥运算值副本与步骤 S302 中获得的第二设备公钥运算值进行对比，若两者相等，则表明判断匹配成功，确认了接收到的消息为第二设备发送而来的消息，执行步骤 S316，进一步进行配置；否则执行步骤 S318，终止配置过程。

步骤 S316：根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息；

步骤 S318：终止配置过程。

下面结合图 4 示出的本发明提供的网络配置方法的第四实施例的流程示意图，进一步说明本发明实施方案：

步骤 S400：第二设备将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；

具体地，可以参考图 3 实施例中的步骤 S300，这里不再赘述。

步骤 S402：第一设备通过带外方式获取第二设备公钥运算值和第二设备密钥信息；

具体地，获取方式可以为图 1 实施例中步骤 S100 描述的方式，这里不再赘述。

步骤 S404：第一设备利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息；

步骤 S406：将第一设备公钥信息发送给所述第二设备；

步骤 S408：第二设备利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥；

步骤 S410：第二设备利用自身的第二设备密钥信息作为对称加密密钥对用于执行密钥交换的第二设备公钥副本进行对称加密运算后得到第二设备公钥信息，发送给第一设备；

步骤 S412：第一设备接收该第二设备公钥信息后，利用步骤 S402 获得的第二设备密钥信息进行解密得到第二设备公钥副本，并将第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；

可理解的，第一设备对第二设备公钥副本进行运算的算法可以参考图 1 实施例中步骤 S100 描述的运算算法，这里不再赘述；

步骤 S414：第一设备判断所述第二设备公钥运算值副本与所述第二设备公钥运算值是否匹配；

具体地，第一设备将运算后的第二设备公钥运算值副本与步骤 S402 中获

得的第二设备公钥运算值进行对比，若两者相等，则表明判断匹配成功，确认了接收到的消息为第二设备发送而来的消息，执行步骤 S416，进一步进行配置；否则执行步骤 S418，终止配置过程。

步骤 S416：根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息；

步骤 S418：终止配置过程。

需要说明的是，本发明实施例可以不涉及第二设备密钥信息来实现，具体如图 5 示出的本发明提供的网络配置方法的第五实施例的流程示意图，进一步说明本发明实施方案：

步骤 S500：第二设备将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；

步骤 S502：第一设备通过带外方式获取第二设备公钥运算值；

具体地，获取方式可以为图 1 实施例中步骤 S100 描述的方式，这里不再赘述。

步骤 S504：第一设备利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息；

步骤 S506：将所述第一设备公钥信息发送给所述第二设备；

步骤 S508：第二设备利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥；

步骤 S510：第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到第二设备公钥信息，发送给第一设备；

具体地，第二设备将解密得到的第一设备的公钥进行运算得出第一设备公钥运算值，其中运算的算法可以参考图 1 实施例中步骤 S100 描述的运算算法，这里不再赘述；

步骤 S512：第一设备接收该第二设备公钥信息后，利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本，并将所述第二设备公钥副本进行预设算法的运算而得到第二设备公钥运算值副

本;

具体地，第一设备将自身的公钥进行预设算法的运算而得到第一设备公钥运算值副本，然后利用该第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本；可理解的，预设的运算算法可以参考图 1 实施例中步骤 S100 描述的运算算法，这里不再赘述;

步骤 S514：第一设备判断所述第二设备公钥运算值副本与所述第二设备公钥运算值是否匹配;

具体地，第一设备将运算后的第二设备公钥运算值副本与步骤 S502 中获得的第二设备公钥运算值进行对比，若两者相等，则表明判断匹配成功，确认了接收到的消息为第二设备发送而来的消息，执行步骤 S516，进一步进行配置；否则执行步骤 S518，终止配置过程。

步骤 S516：根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息;

步骤 S518：终止配置过程。

进一步地，本发明实施例中步骤 S316、S416 和 S516 中根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息的步骤，具体可以包括：由第一设备生成配置信息发送给第二设备，也可以由第二设备生成配置信息发送给第一设备。具体地:

当第一设备生成配置信息发送给第二设备时，可以包括：将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；以所述第一交换密钥为加密密钥，加密配置信息后发送给所述第二设备。

可以理解的，第一设备生成第一交换密钥可以利用 Diffie-Hellman（DH）密钥交换算法进行，计算方式可以为：第一交换密钥=第二设备公钥副本^第一设备私钥；但本发明实施例不限于用 DH 密钥交换算法来进行运算。

再进一步地，本发明实施例中在步骤 S316、S416 和 S516 之前、或者在步骤 S316、S416 和 S516 之后、或者与步骤 S316、S416 和 S516 同时还可以包括：第一设备以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证

码（Hash-based Message Authentication Code，HMAC）运算的输入密钥，对加密后的配置信息进行HMAC运算，并向第二设备发送进行HMAC运算后的信息；以使第二设备接收到经过HMAC运算后的信息后，以第二交换密钥或第二交换密钥的衍生密钥作为 HMAC 运算的解密密钥，对接收到的所述经过HMAC运算后的信息进行解密验证，验证消息是否被篡改。

当第二设备生成配置信息发送给第一设备时，第一设备接受接收到的第二设备发送的配置信息可以包括:

接收所述第二设备发送的配置信息；所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息；所述第二交换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果；将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；以所述第一交换密钥解密接收到的所述配置信息。

可以理解的，第二设备生成第二交换密钥可以利用 Diffie-Hellman（DH）密钥交换算法进行，计算方式可以为：第二交换密钥=第一设备公钥^第二设备私钥；但本发明实施例不限于用 DH 密钥交换算法来进行运算。

再进一步地，本发明实施例中在第一设备以所述第一交换密钥解密接收到的所述配置信息后还可以包括：第一设备生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为 HMAC 运算的输入密钥，对所述配置确认信息进行HMAC运算，并向第二设备发送进行HMAC运算后的信息；以使第二设备接收到经过 HMAC 运算后的信息后，以第二交换密钥或第二交换密钥的衍生密钥作为HMAC运算的解密密钥，对接收到的所述经过HMAC运算后的信息进行解密验证，验证消息是否被篡改。

需要说明的是，第二设备接收到第一设备发送的配置信息后，根据不同的应用场景，可以通过以下方式建立第一设备与第二设备之间的网络:

（1）、当第一设备与第二设备为点对点网络（Peer to Peer，P2P）连接时，第一设备发送的配置信息包括第一设备与第二设备连接的信任状，用于第一设备与第二设备在连接过程中进行四步握手过程中的验证过程，验证成功后，第一设备与第二设备建立 P2P 连接;

（2）当第一设备为终端，第二设备为支持 802.11 协议的接入点（Access

Point，AP）时，第一设备发送的配置信息包括第一设备与第二设备连接的信任状，用于第一设备与第二设备在连接过程中进行四步握手过程中的验证过程，验证成功后，第一设备与第二设备建立连接，第一设备加入第二设备所在的网络；

（3）当第一设备为 AP，第二设备为终端时，第一设备可由外部设备获得第二设备公钥运算值，第一设备发送的配置信息包括第一设备与第二设备连接的信任状，用于第一设备与第二设备在连接过程中进行四步握手过程中的验证过程，验证成功后，第一设备与第二设备建立连接，第二设备加入第一设备所在的网络。

可理解的是，配置信息可以由第一设备或第二设备发起，本实施例仅以第一设备发放配置信息为例。当由第二设备发放配置信息时，第二设备同样可以通过第二交换密钥或其衍生密钥加密配置信息，可以同上述的发送自己公钥的消息（即第二消息）一起过去，也可以等待第一设备发送触发消息后，向第一设备发送配置信息。本发明实施例中的配置信息可以为包含信任状的信息或配置信息为包含认证密钥的信息。

再进一步地，在一些配置场景下，两设备均为 UI 受限设备时，一设备无法安全获得另一设备的公钥运算值，那么此时，需要通过第三方的设备来协助配置连接该两个待配置连接的设备；具体地：

假设上述图 1 至图 5 实施例中的第一设备为第三方的设备，那么第一设备生成配置信息发送给第二设备时，可以包括：

将所述第二设备公钥副本与第一设备的私钥进行运算得到第一交换密钥；以所述第一交换密钥为加密密钥，加密第三设备公钥运算值；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；将加密后的第三设备公钥运算值发送给所述第二设备；以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

再进一步地，本发明实施例还可以包括：第一设备以第一交换密钥或第一交换密钥的衍生密钥作为 HMAC 运算的输入密钥，对加密后的第三设备公钥

运算值进行 HMAC 运算，并向第二设备发送进行 HMAC 运算后的信息。以使第二设备接收到经过 HMAC 运算后的信息后，以第二交换密钥或第二交换密钥的衍生密钥作为 HMAC 运算的解密密钥，对接收到的所述经过 HMAC 运算后的信息进行解密验证，验证消息是否被篡改。

再进一步地，在一些配置场景下，该第三方设备还可以通过本发明图 1 至图 5 任一实施例，分别与该两个待配置设备进行网络配置连接交互，并分别发放连接或配置的验证信息；具体地，通过本发明图 1 至图 5 任一实施例，第三方设备分别与两个待配置设备进行发现、鉴权、关联及安全密钥交换后，该第三方设备分别向两个待配置设备发送配置信息。配置信息为该两个待配置设备用于四步握手验证的信息，或两个待配置设备用于再次进行配置过程的验证信息。

还需要说明的是，第一设备通过带外方式获取第二设备的信息，比如通过扫描多维码来获取第二设备的信息，除了获取到第二设备公钥运算值和第二设备密钥信息外，还可以获取到第二设备的设备信息，如 MAC 地址、设备类型，以及优先信道等；

再进一步地，本发明实施例中的步骤 S316、步骤 S416 和步骤 S516 还可以具体为：将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。即，第一设备与第二设备可以无需进行四步握手过程，将该第一交换密钥作为加密数据的会话密钥，以保护双方设备之间业务数据的安全传输。

本发明实施例中的步骤 S316、步骤 S416 和步骤 S516 还可以具体为：将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；基于所述第一交换密钥生成进行四步握手过程时的主密钥。即，第一设备可以在进行四步握手的过程中，把该第一交换密钥作为主密钥（pairwise master key，PMK），通过 PMK 生成会话密钥保护数据传输。

可以理解的，本发明实施例中的对称算法包括但不限于 AES(Advanced Encryption Standard,高级加密标准)。通常，AES 加密算法的加密密钥为 128 位，192 位或 256 位，本发明实施例中，可以选取 128 位长度。同时，为进一步保

证消息完整性，可以对交互的消息进行完整性校验运算，以确认消息是否被篡改。

可以理解的，本发明实施例中通过HMAC-SHA-256运算得出的是256位的消息摘要，可选地，本发明实施例可以但不限于取前64位作为当前消息的消息摘要，带在当前消息中，用于给对方设备接收后进行消息完整性校验，以确认消息是否被篡改。

实施本发明实施例，通过对公钥进行运算得到公钥运算值，以公钥运算值或者预设的密钥信息作为加密密钥来加密密钥交换的公钥，可大大提高配置过程的安全性；在配置过程的交互信息中用公钥运算值替代公钥，可以减少交互信息的内容，提高配置双方设备的带外信道利用率，并可以通过扫描多维码的配置方式完成配置，解决了现有技术中PIN方式比较繁琐且安全性不高，PBC方式安全性不足，以及NFC普适性较低的问题，而且与对公钥进行多维码编码相比，大大减少了多维码编码内容，降低了多维码的显示、扫描以及解码的要求，并适用性高，配置效率得到了很大的提高，大大提升了用户的配置体验。

为了便于更好地实施本发明实施例的上述方案，本发明还提供了用于配合实施上述方案的相关装置。下面结合图6示出的本发明的网络配置装置的第一实施例的结构示意图，进行详细说明：

网络配置装置60包括：第一获取模块600、第一设备公钥信息生成模块602、第一发送模块604、第二设备公钥副本获取模块606和第一配置模块608，其中

第一获取模块600用于通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；

第一设备公钥信息生成模块602用于根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息；

第一发送模块604用于将所述第一设备公钥信息发送给所述第二设备，以使所述第二设备根据所述第一设备公钥信息获取第一设备的公钥；

第二设备公钥副本获取模块606用于获取所述第二设备发送的用于执行

密钥交换的第二设备公钥副本;

第一配置模块 608 用于对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

进一步地，结合图 7 示出的本发明的网络配置装置的第二实施例的结构示意图，网络配置装置 60 包括第一获取模块 600、第一设备公钥信息生成模块 602、第一发送模块 604、第二设备公钥副本获取模块 606 和第一配置模块 608 外，还可以包括第二获取模块 6010，其中

第二获取模块 6010 用于通过带外方式获取第二设备密钥信息;

第一设备公钥信息生成模块 602 还可以包括第一加密单元 6020，用于利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息;

再进一步地，结合图 8 示出的本发明的网络配置装置的第三实施例的结构示意图，网络配置装置 60 中的第一设备公钥信息生成模块 602 还可以包括第二加密单元 6022，用于利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

再进一步地，如图 9 示出的本发明实施例的第二设备公钥副本获取模块的结构示意图，第二设备公钥副本获取模块 606 还可以包括第一接收单元 6060 和第一解密得到单元 6062，和/或第二接收单元 6064 和第二解密得到单元 6066，本发明实施例中以都包含第一接收单元 6060、第一解密得到单元 6062、第二接收单元 6064 和第二解密得到单元 6066 为例进行说明，其中

第一接收单元 6060 用于接收所述第二设备发送的第二设备公钥信息，所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息;

第一解密得到单元 6062 用于利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本；所述第一设备公钥运算值

为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；所述第一设备公钥运算值副本为将自身的公钥进行预设算法的运算而得到的结果；

第二接收单元 6064 用于接收所述第二设备发送的第二设备公钥信息；当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；

第二解密得到单元 6066 用于利用第一设备获取的第二设备密钥信息解密所述第二设备公钥信息，得到第二设备公钥副本。

再进一步地，如图 10 示出的本发明第一配置模块的第一实施例的结构示意图，第一配置模块 608 可以包括：第一运算单元 6080 和配置信息加密单元 6082，其中

第一运算单元 6080 用于将所述第二设备公钥副本与第一设备的私钥进行运算得到第一交换密钥；

配置信息加密单元 6082 用于以所述第一交换密钥为加密密钥，加密配置信息后发送给所述第二设备。

再进一步地，如图 11 示出的本发明第一配置模块的第二实施例的结构示意图，第一配置模块 608 可以包括：配置信息接收单元 6084、第二运算单元 6086 和解密单元 6088，其中

配置信息接收单元 6084 用于接收所述第二设备发送的配置信息；所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息；所述第二交换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果；

第二运算单元 6086 用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；

解密单元 6088 用于以所述第一交换密钥解密接收到的所述配置信息。

再进一步地，如图 12 示出的本发明第一配置模块的第三实施例的结构示意图，第一配置模块 608 可以包括：第三运算单元 60810、公钥运算值加密单元 60812 和发送单元 60814，其中

第三运算单元 60810 将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

公钥运算值加密单元 60812 用于以所述第一交换密钥为加密密钥，加密第三设备公钥运算值; 所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果;

发送单元 60814 用于将加密后的第三设备公钥运算值发送给所述第二设备; 以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

再进一步地，如图 13 示出的本发明第一配置模块的第四实施例的结构示意图，第一配置模块 608 可以包括: 第四运算单元 60816 和会话密钥生成单元 60818，其中

第四运算单元 60816 用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

会话密钥生成单元 60818 用于基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。

再进一步地，如图 14 示出的本发明第一配置模块的第五实施例的结构示意图，第一配置模块 608 可以包括: 第五运算单元 60820 和主密钥生成单元 60822，其中

第五运算单元 60820 用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

主密钥生成单元 60822 用于基于所述第一交换密钥生成进行四步握手过程时的主密钥。

再进一步地，网络配置装置 60 还可以包括: 第一哈希运算模块，用于以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的配置信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

再进一步地，网络配置装置 60 还可以包括: 第二哈希运算模块，用于当解密单元 6088 解密接收到的所述配置信息后，生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对

所述配置确认信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

再进一步地，网络配置装置 60 还可以包括：第三哈希运算模块，用于以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的第三设备公钥运算值进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

需要说明的是，本发明实施例中的网络配置装置 60 中各功能模块的功能可根据上述方法实施例中的方法具体实现，即，具体可以参考上述图 1 至图 5 中第一设备的方法项实施例，这里不再赘述。

为了便于更好地实施本发明实施例的上述方案，本发明还提供了用于配合实施上述方案的相关装置。下面结合图 15 示出的本发明的网络配置设备的第一实施例的结构示意图，进行详细说明：

网络配置设备 150 包括：第二设备公钥运算值生成模块 1500、接收获取模块 1502、第二设备公钥信息发送模块 1504 和第二配置模块 1506，其中

第二设备公钥运算值生成模块 1500 用于将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；

接收获取模块 1502 用于接收所述第一设备发送的第一设备公钥信息，并根据所述第一设备公钥信息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息；

第二设备公钥信息发送模块 1504 用于向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本；

第二配置模块 1506 用于根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

进一步地，如图 16 示出的本发明的网络配置设备的第二实施例的结构示意图，网络配置设备 150 包括第二设备公钥运算值生成模块 1500、接收获取

模块 1502、第二设备公钥信息发送模块 1504 和第二配置模块 1506 外，还可以包括随机密钥生成模块 1508，用于生成第二设备密钥信息，以供第一设备通过带外方式获取。

进一步地，如图 17 示出的本发明的接收获取模块的第一实施例的结构示意图，接收获取模块 1502 可以包括第一解密单元 15020，具体地：

接收获取模块 1502 接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；第一解密单元 15020 用于利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥；

进一步地，如图 18 示出的本发明的接收获取模块的第二实施例的结构示意图：接收获取模块 1502 可以包括第二解密单元 15022，其中

接收获取模块 1502 接收的所述第一设备公钥信息为所述第一设备利用所述第二设备公钥运算值作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；第二解密单元 15022 用于利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥。

进一步地，如图 19 示出的本发明的网络配置设备的第三实施例的结构示意图，网络配置设备 150 包括第二设备公钥运算值生成模块 1500、接收获取模块 1502、第二设备公钥信息发送模块 1504、第二配置模块 1506 和随机密钥生成模块 1508 外，还可以包括公钥信息第一生成模块 15010 和公钥信息第二生成模块 15012，其中

公钥信息第一生成模块 15010 用于利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到第二设备公钥信息；所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；或者

公钥信息第二生成模块 15012 用于当第一设备通过带外方式获取了第二设备密钥信息时，利用自身的第二设备密钥信息对第二设备的公钥进行对称加密而得到第二设备公钥信息。

进一步地，如图 20 示出的本发明的第二配置模块的第一实施例的结构示意图，第二配置模块 1506 包括配置信息接收解密单元 15060 和/或配置信息发

送单元 15062，图中以都包含为例进行说明，其中

配置信息接收解密单元 15060 用于接收所述第一设备发送的配置信息；所述配置信息为第一设备以第一交换密钥为加密密钥进行加密后的配置信息，所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密接收到的所述配置信息；和/或

配置信息发送单元 15062 用于将所述第一设备的公钥与第二设备用于执行密钥交换的私钥进行运算得到第二交换密钥；以所述第二交换密钥为加密密钥，加密配置信息后发送给所述第一设备。

进一步地，如图 21 示出的本发明的第二配置模块的第二实施例的结构示意图，第二配置模块 1506 包括第三设备公钥运算值接收解密单元 15064 和配置子单元 15066，其中

第三设备公钥运算值接收解密单元 15064 用于接收所述第一设备发送的加密后的第三设备公钥运算值，将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密所述第三设备公钥运算值；所述加密后的第三设备公钥运算值为所述第一设备以所述第一交换密钥为加密密钥对第三设备公钥运算值进行加密而得到的结果；所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；

配置子单元 15066 用于利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

再进一步地，本发明实施例的网络配置设备 150 还可以包括：哈希运算验证模块，用于接收第一设备发送的经过哈希消息认证运算后的信息，以第二交换密钥或第二交换密钥的衍生密钥作为哈希消息认证码运算的解密密钥，对接收到的所述经过哈希消息认证运算后的信息进行解密验证。

需要说明的是，本发明实施例中的网络配置设备 150 中各功能模块的功能可根据上述方法实施例中的方法具体实现，即，具体可以参考上述图 1 至图 5

中第二设备的方法项实施例，这里不再赘述。

为了便于更好地实施本发明实施例的上述方案，本发明还提供了用于配合实施上述方案的相关设备。下面结合图 22 示出的本发明的网络设备的第一实施例的结构示意图，进行详细说明：

网络设备 220 包括：输入装置 2200、输出装置 2202、存储器 2204 和处理器 2206（网络设备中的处理器 2206 的数量可以一个或多个，图 22 中以一个处理器为例）。在本发明的一些实施例中，输入装置 2200、输出装置 2202、存储器 2204 和处理器 2206 可通过总线或者其它方式连接，其中，图 22 中以通过总线连接为例。

其中，存储器 2204 用于存储程序代码，处理器 2206 用于调用存储器 2204 存储的程序代码执行如下步骤：

由输入装置 2200 通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息，通过输出装置 2202 将所述第一设备公钥信息发送给所述第二设备，以使所述第二设备根据所述第一设备公钥信息获取第一设备的公钥；通过输入装置 2200 获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本；对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

具体地，处理器 2206 根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息之前还执行：

由输入装置 2200 通过带外方式获取第二设备密钥信息。

再具体地，处理器 2206 根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括：

利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

再具体地，处理器 2206 根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括:

利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

再具体地，处理器 2206 通过输入装置 2200 获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本包括:

通过输入装置 2200 接收所述第二设备发送的第二设备公钥信息，所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本；所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；所述第一设备公钥运算值副本为将自身的公钥进行预设算法的运算而得到的结果；或者

通过输入装置 2200 接收所述第二设备发送的第二设备公钥信息；当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；利用第一设备获取的第二设备密钥信息解密所述第二设备公钥信息，得到第二设备公钥副本。

再具体地，处理器 2206 根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；以所述第一交换密钥为加密密钥，加密配置信息后发送给所述第二设备。

再具体地，处理器 2206 根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

通过输入装置 2200 接收所述第二设备发送的配置信息；所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息；所述第二交

换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果; 将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥; 以所述第一交换密钥解密接收到的所述配置信息。

再具体地，处理器 2206 根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥; 以所述第一交换密钥为加密密钥，加密第三设备公钥运算值; 所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果; 将加密后的第三设备公钥运算值发送给所述第二设备; 以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

再具体地，处理器 2206 根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥; 基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。

再具体地，处理器 2206 根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥; 基于所述第一交换密钥生成进行四步握手过程时的主密钥。

再具体地，处理器 2206 以所述第一交换密钥解密接收到的所述配置信息后还执行:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的配置信息进行哈希消息认证运算，通过输出装置 2202

并向第二设备发送进行哈希消息认证运算后的信息。

再具体地，处理器 2206 还执行:

生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对所述配置确认信息进行哈希消息认证运算，通过输出装置 2202 并向第二设备发送进行哈希消息认证运算后的信息。

再具体地，处理器 2206 还执行:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的第三设备公钥运算值进行哈希消息认证运算，并通过输出装置 2202 向第二设备发送进行哈希消息认证运算后的信息。

本发明实施例的网络设备 220 例如可以是网管设备、路由器、传送节点、智能移动终端或其它网络设备。

可理解的是，网络设备 220 中各功能模块的功能可根据上述方法实施例中的方法具体实现，即，具体可以参考上述图 1 至图 5 中第一设备的方法项实施例，这里不再赘述。

为了便于更好地实施本发明实施例的上述方案，本发明还提供了用于配合实施上述方案的相关设备。下面结合图 23 示出的本发明的网络设备的第二实施例的结构示意图，进行详细说明:

网络设备 230 包括: 输入装置 2300、输出装置 2302、存储器 2304 和处理器 2306（网络设备中的处理器 2306 的数量可以一个或多个，图 23 中以一个处理器为例）。在本发明的一些实施例中，输入装置 2300、输出装置 2302、存储器 2304 和处理器 2306 可通过总线或者其它方式连接，其中，图 23 中以通过总线连接为例。

其中，存储器 2304 用于存储程序代码，处理器 2306 用于调用存储器 2304 存储的程序代码执行如下步骤:

将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；通过输入装置 2300 接收所述第一设备发送的第一设备公钥信息，并根据所述第一设备公钥信息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公

钥生成的信息；通过输出装置 2302 向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本；根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

再具体地，处理器 2306 通过输入装置 2300 接收所述第一设备发送的第一设备公钥信息之前还包括：

生成第二设备密钥信息，以供第一设备通过带外方式获取。

再具体地，处理器 2306 通过输入装置 2300 接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

处理器 2306 根据所述第一设备公钥信息获取第一设备的公钥包括：利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥。

再具体地，处理器 2306 通过输入装置 2300 接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

处理器 2306 根据所述第一设备公钥信息获取第一设备的公钥包括：利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥。

再具体地，所述第二设备公钥信息为处理器 2306 利用第一设备公钥运算值对第二设备的公钥进行对称加密而得到的信息；所述第一设备公钥运算值为处理器 2306 将获得的第一设备的公钥进行预设算法的运算而得到的结果；或者

当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为处理器 2306 利用自身的第二设备密钥信息对第二设备的公钥进行对称加密而得到的信息。

再具体地，处理器 2306 根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置

信息包括:

通过输入装置 2300 接收所述第一设备发送的配置信息; 所述配置信息为第一设备以第一交换密钥为加密密钥进行加密后的配置信息,所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果;将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥,以所述第二交换密钥解密接收到的所述配置信息; 或者

将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥; 以所述第二交换密钥为加密密钥,加密配置信息后通过输出装置 2302 发送给所述第一设备。

再具体地, 处理器 2306 根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥,以用于处理第一设备和第二设备之间的配置信息包括:

通过输入装置 2300 接收所述第一设备发送的加密后的第三设备公钥运算值;将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥,以所述第二交换密钥解密所述第三设备公钥运算值,并利用所述第三设备公钥运算值与所述第三设备进行密钥交换,并完成最终的配置过程;所述加密后的第三设备公钥运算值为所述第一设备以所述第一交换密钥为加密密钥对第三设备公钥运算值进行加密而得到的结果;所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果;所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果。

再具体地, 处理器 2306 还执行:

通过输入装置 2300 接收第一设备发送的经过哈希消息认证运算后的信息,以第二交换密钥或第二交换密钥的衍生密钥作为哈希消息认证码运算的解密密钥, 对通过输入装置 2300 接收到的所述经过哈希消息认证运算后的信息进行解密验证。

本发明实施例的网络设备 230 例如可以是网管设备、路由器、传送节点、智能移动终端或其它网络设备。

可理解的是,网络设备 230 中各功能模块的功能可根据上述方法实施例中

的方法具体实现，即，具体可以参考上述图 1 至图 5 中第二设备的方法项实施例，这里不再赘述。

为了便于更好地实施本发明实施例的上述方案，本发明还提供了用于配合实施上述方案的相关系统。下面结合图 24 示出的本发明实施例的网络配置系统的结构示意图，进行详细说明：

网络配置系统 240 包括第一设备 2400 和第二设备 2402，其中，

第一设备 2400 参考上述图 22 实施例中的网络设备 220，这里不再赘述；

第二设备 2402 参考上述图 23 实施例中的网络设备 230，这里不再赘述。

需要说明的是，在一些配置场景下，两设备均为 UI 受限设备时，一设备无法安全获得另一设备的公钥运算值，那么此时，需要通过第三方的设备来协助配置连接该两个待配置连接的设备；即，网络配置系统 240 还可以包括第三设备，其中第一设备 2400 为第三方设备，第二设备 2402 和第三设备可以均为 UI 受限设备，需要通过第一设备 2400 来协助配置连接，详细配置连接方式可参考上述方法实施例中的实现方式，这里不再赘述。

综上所述，实施本发明实施例，通过对公钥进行运算得到公钥运算值，以公钥运算值或者预设的密钥信息作为加密密钥来加密密钥交换的公钥，可大大提高配置过程的安全性；在配置过程的交互信息中用公钥运算值替代公钥，可以减少交互信息的内容，提高配置双方设备的带外信道利用率，并可以通过扫描多维码的配置方式完成配置，解决了现有技术中 PIN 方式比较繁琐且安全性不高，PBC 方式安全性不足，以及 NFC 普适性较低的问题，而且与对公钥进行多维码编码相比，大大减少了多维码编码内容，降低了多维码的显示、扫描以及解码的要求，并适用性高，配置效率得到了很大的提高，大大提升了用户的配置体验。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

以上所揭露的仅为本发明一种较佳实施例而已，当然不能以此来限定本发明之权利范围，本领域普通技术人员可以理解实现上述实施例的全部或部分流程，并依本发明权利要求所作的等同变化，仍属于发明所涵盖的范围。

权 利 要 求

1、一种网络配置方法，其特征在于，包括:

通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果;

根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息，将所述第一设备公钥信息发送给所述第二设备，以使所述第二设备根据所述第一设备公钥信息获取第一设备的公钥;

获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本;

对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本; 当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

2、如权利要求 1 所述的方法，其特征在于，所述根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息之前还包括:

通过带外方式获取第二设备密钥信息。

3、如权利要求 2 所述的方法，其特征在于，所述根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括:

利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

4、如权利要求 1 或 2 所述的方法，其特征在于，所述根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括:

利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

5、如权利要求 4 所述的方法，其特征在于，所述获取所述第二设备发送

的用于执行密钥交换的第二设备公钥副本包括:

接收所述第二设备发送的第二设备公钥信息,所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息;利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息,得到第二设备公钥副本;所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果;所述第一设备公钥运算值副本为将自身的公钥进行预设算法的运算而得到的结果;或者

接收所述第二设备发送的第二设备公钥信息;当第一设备通过带外方式获取了第二设备密钥信息时,所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息;利用第一设备获取的第二设备密钥信息解密所述第二设备公钥信息,得到第二设备公钥副本。

6、如权利要求 1-5 任一项所述的方法,其特征在于,所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥,以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

以所述第一交换密钥为加密密钥,加密配置信息后发送给所述第二设备。

7、如权利要求 1-5 任一项所述的方法,其特征在于,所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥,以用于处理第一设备和第二设备之间的配置信息包括:

接收所述第二设备发送的配置信息;所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息;所述第二交换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果;

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

以所述第一交换密钥解密接收到的所述配置信息。

8、如权利要求 1-5 任一项所述的方法，其特征在于，所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；

以所述第一交换密钥为加密密钥，加密第三设备公钥运算值；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；

将加密后的第三设备公钥运算值发送给所述第二设备；以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

9、如权利要求 1-5 任一项所述的方法，其特征在于，所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；

基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。

10、如权利要求 1-5 任一项所述的方法，其特征在于，所述根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；

基于所述第一交换密钥生成进行四步握手过程时的主密钥。

11、如权利要求 6 所述的方法，其特征在于，所述方法还包括:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的配置信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

12、如权利要求 7 所述的方法，其特征在于，所述以所述第一交换密钥解密接收到的所述配置信息后还包括:

生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对所述配置确认信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

13、如权利要求 8 所述的方法，其特征在于，所述方法还包括:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的第三设备公钥运算值进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

14、一种网络配置方法，其特征在于，包括:

将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取;

接收所述第一设备发送的第一设备公钥信息，并根据所述第一设备公钥信息获取第一设备的公钥; 所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息;

向所述第一设备发送第二设备公钥信息; 以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本;

根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

15、如权利要求 14 所述的方法，其特征在于，所述接收所述第一设备发送的第一设备公钥信息之前还包括:

生成第二设备密钥信息，以供第一设备通过带外方式获取。

16、如权利要求 15 所述的方法，其特征在于，接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

所述根据所述第一设备公钥信息获取第一设备的公钥包括：

利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥。

17、如权利要求 14 或 15 所述的方法，其特征在于，接收的所述第一设备公钥信息为所述第一设备利用所述第二设备公钥运算值作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息；

所述根据所述第一设备公钥信息获取第一设备的公钥包括：

利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥。

18、如权利要求 17 所述的方法，其特征在于，所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；或者

当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息。

19、如权利要求 14-18 任一项所述的方法，其特征在于，所述根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

接收所述第一设备发送的配置信息；所述配置信息为第一设备以第一交换密钥为加密密钥进行加密后的配置信息，所述第一交换密钥为所述第一设备以

所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密接收到的所述配置信息；或者

将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥；以所述第二交换密钥为加密密钥，加密配置信息后发送给所述第一设备。

20、如权利要求 14-18 任一项所述的方法，其特征在于，所述根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息包括：

接收所述第一设备发送的加密后的第三设备公钥运算值；将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程；

所述加密后的第三设备公钥运算值为所述第一设备以所述第一交换密钥为加密密钥对第三设备公钥运算值进行加密而得到的结果；所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果。

21、如权利要求 19 或 20 所述的方法，其特征在于，所述方法还包括：

接收第一设备发送的经过哈希消息认证运算后的信息，以第二交换密钥或第二交换密钥的衍生密钥作为哈希消息认证码运算的解密密钥，对接收到的所述经过哈希消息认证运算后的信息进行解密验证。

22、一种网络配置装置，其特征在于，包括：

第一获取模块，用于通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；

第一设备公钥信息生成模块，用于根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息；

第一发送模块，用于将所述第一设备公钥信息发送给所述第二设备，以使所述第二设备根据所述第一设备公钥信息获取第一设备的公钥；

第二设备公钥副本获取模块，用于获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本；

第一配置模块，用于对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

23、如权利要求 22 所述的装置，其特征在于，所述装置还包括：

第二获取模块，用于通过带外方式获取第二设备密钥信息。

24、如权利要求 23 所述的装置，其特征在于，所述第一设备公钥信息生成模块包括：

第一加密单元，用于利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

25、如权利要求 22 或 23 所述的装置，其特征在于，所述第一设备公钥信息生成模块包括：

第二加密单元，用于利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

26、如权利要求 25 所述的装置，其特征在于，所述第二设备公钥副本获取模块包括：

第一接收单元和第一解密得到单元，其中，所述第一接收单元用于接收所述第二设备发送的第二设备公钥信息，所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；所述第一解密得到单元用于利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本；所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果；所述第一设备公钥运算值副本为将自身的公钥进行预设算法的运算而得到的结果；和/或

第二接收单元和第二解密得到单元，其中，所述第二接收单元用于接收所述第二设备发送的第二设备公钥信息；当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息；所述第二解密得到单元用于利用第一设备获取的第二设备密钥信息解密所述第二设备公钥信息，得到第二设备公钥副本。

27、如权利要求 22-26 任一项所述的装置，其特征在于，所述第一配置模块包括：

第一运算单元，用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥；

配置信息加密单元，用于以所述第一交换密钥为加密密钥，加密配置信息后发送给所述第二设备。

28、如权利要求 22-26 任一项所述的装置，其特征在于，所述第一配置模块包括：

配置信息接收单元，用于接收所述第二设备发送的配置信息；所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息；所述第二交换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果；

第二运算单元，用于将所述第二设备公钥副本与第一设备用于执行密钥交

换的私钥进行运算得到第一交换密钥;

解密单元，用于以所述第一交换密钥解密接收到的所述配置信息。

29、如权利要求 22-26 任一项所述的装置，其特征在于，所述第一配置模块包括:

第三运算单元，将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

公钥运算值加密单元，用于以所述第一交换密钥为加密密钥，加密第三设备公钥运算值;所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果;

发送单元，用于将加密后的第三设备公钥运算值发送给所述第二设备;以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

30、如权利要求 22-26 任一项所述的装置，其特征在于，所述第一配置模块包括:

第四运算单元，用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

会话密钥生成单元，用于基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。

31、如权利要求 22-26 任一项所述的装置，其特征在于，所述第一配置模块包括:

第五运算单元，用于将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;

主密钥生成单元，用于基于所述第一交换密钥生成进行四步握手过程时的主密钥。

32、如权利要求 27 所述的装置，其特征在于，所述装置还包括:

第一哈希运算模块，用于以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的配置信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

33、如权利要求 28 所述的装置，其特征在于，所述装置还包括：

第二哈希运算模块，用于当所述解密单元解密接收到的所述配置信息后，生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对所述配置确认信息进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

34、如权利要求 29 所述的装置，其特征在于，所述装置还包括：

第三哈希运算模块，用于以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的第三设备公钥运算值进行哈希消息认证运算，并向第二设备发送进行哈希消息认证运算后的信息。

35、一种网络配置设备，其特征在于，包括：

第二设备公钥运算值生成模块，用于将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；

接收获取模块，用于接收所述第一设备发送的第一设备公钥信息，并根据所述第一设备公钥信息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息；

第二设备公钥信息发送模块，用于向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本；

第二配置模块，用于根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

36、如权利要求 35 所述的网络配置设备，其特征在于，所述网络配置设备还包括:

随机密钥生成模块，用于生成第二设备密钥信息，以供第一设备通过带外方式获取。

37、如权利要求 36 所述的网络配置设备，其特征在于，所述接收获取模块接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息;

所述接收获取模块包括:

第一解密单元，用于利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥。

38、如权利要求 35 或 36 所述的网络配置设备，其特征在于，所述接收获取模块接收的所述第一设备公钥信息为所述第一设备利用所述第二设备公钥运算值作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息;

所述接收获取模块包括:

第二解密单元，用于利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥。

39、如权利要求 38 所述的网络配置设备，其特征在于，所述网络配置设备还包括:

公钥信息第一生成模块，用于利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到第二设备公钥信息; 所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果; 或者

公钥信息第二生成模块，用于当第一设备通过带外方式获取了第二设备密钥信息时，利用自身的第二设备密钥信息对第二设备的公钥进行对称加密而得

到第二设备公钥信息。

40、如权利要求 35-39 任一项所述的网络配置设备，其特征在于，所述第二配置模块还包括:

配置信息接收解密单元，用于接收所述第一设备发送的配置信息；所述配置信息为第一设备以第一交换密钥为加密密钥进行加密后的配置信息，所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密接收到的所述配置信息；和/或

配置信息发送单元，用于将所述第一设备的公钥与第二设备用于执行密钥交换的私钥进行运算得到第二交换密钥；以所述第二交换密钥为加密密钥，加密配置信息后发送给所述第一设备。

41、如权利要求 35-39 任一项所述的网络配置设备，其特征在于，所述第二配置模块包括:

第三设备公钥运算值接收解密单元，用于接收所述第一设备发送的加密后的第三设备公钥运算值，将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密所述第三设备公钥运算值；所述加密后的第三设备公钥运算值为所述第一设备以所述第一交换密钥为加密密钥对第三设备公钥运算值进行加密而得到的结果；所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果；所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；

配置子单元，用于利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

42、如权利要求 40 或 41 所述的网络配置设备，其特征在于，所述网络配置设备还包括:

哈希运算验证模块，用于接收第一设备发送的经过哈希消息认证运算后的信息，以第二交换密钥或第二交换密钥的衍生密钥作为哈希消息认证码运算的解密密钥，对接收到的所述经过哈希消息认证运算后的信息进行解密验证。

43、一种网络设备，其特征在于，包括：输入装置、输出装置、存储器和处理器；

其中，所述存储器用于存储程序代码，所述处理器用于调用所述存储器存储的程序代码执行如下步骤：

由所述输入装置通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果；根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息，通过所述输出装置将所述第一设备公钥信息发送给所述第二设备，以使所述第二设备根据所述第一设备公钥信息获取第一设备的公钥；通过所述输入装置获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本；对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息。

44、如权利要求 43 所述的网络设备，其特征在于，所述处理器根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息之前还执行：

由所述输入装置通过带外方式获取第二设备密钥信息。

45、如权利要求 44 所述的网络设备，其特征在于，所述处理器根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括：

利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息。

46、如权利要求 43 或 44 所述的网络设备，其特征在于，所述处理器根据

第一设备用于执行密钥交换的公钥生成第一设备公钥信息包括:

利用所述第二设备公钥运算值作为对称加密密钥,对所述第一设备用于执行密钥交换的公钥进行对称加密运算,生成第一设备公钥信息。

47、如权利要求 46 所述的网络设备,其特征在于,所述处理器通过所述输入装置获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本包括:

通过所述输入装置接收所述第二设备发送的第二设备公钥信息,所述第二设备公钥信息为所述第二设备利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息;利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息,得到第二设备公钥副本;所述第一设备公钥运算值为所述第二设备将获得的第一设备的公钥进行预设算法的运算而得到的结果;所述第一设备公钥运算值副本为将自身的公钥进行预设算法的运算而得到的结果;或者

通过所述输入装置接收所述第二设备发送的第二设备公钥信息;当第一设备通过带外方式获取了第二设备密钥信息时,所述第二设备公钥信息为所述第二设备利用自身的第二设备密钥信息作为对称加密密钥对第二设备的公钥进行对称加密运算而得到的信息;利用第一设备获取的第二设备密钥信息解密所述第二设备公钥信息,得到第二设备公钥副本。

48、如权利要求 43-47 任一项所述的网络设备,其特征在于,所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥,以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥;以所述第一交换密钥为加密密钥,加密配置信息后发送给所述第二设备。

49、如权利要求 43-47 任一项所述的网络设备,其特征在于,所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一

交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

通过所述输入装置接收所述第二设备发送的配置信息; 所述第二设备发送的配置信息为利用第二交换密钥作为加密密钥加密的配置信息; 所述第二交换密钥为所述第二设备将得到的第一设备的公钥与自身第二设备的私钥进行运算得到的结果; 将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥; 以所述第一交换密钥解密接收到的所述配置信息。

50、如权利要求 43-47 任一项所述的网络设备，其特征在于，所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥; 以所述第一交换密钥为加密密钥，加密第三设备公钥运算值; 所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果; 将加密后的第三设备公钥运算值发送给所述第二设备; 以使所述第二设备能安全获取所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程。

51、如权利要求 43-47 任一项所述的网络设备，其特征在于，所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算得到第一交换密钥; 基于所述第一交换密钥生成用于保护第一设备与第二设备之间业务数据传输的会话密钥。

52、如权利要求 43-47 任一项所述的网络设备，其特征在于，所述处理器根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

将所述第二设备公钥副本与第一设备用于执行密钥交换的私钥进行运算

得到第一交换密钥；基于所述第一交换密钥生成进行四步握手过程时的主密钥。

53、如权利要求 48 所述的网络设备，其特征在于，所述处理器以所述第一交换密钥解密接收到的所述配置信息后还执行:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的配置信息进行哈希消息认证运算，通过所述输出装置并向第二设备发送进行哈希消息认证运算后的信息。

54、如权利要求 49 所述的网络设备，其特征在于，所述处理器还执行:

生成配置确认信息，并以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对所述配置确认信息进行哈希消息认证运算，通过所述输出装置并向第二设备发送进行哈希消息认证运算后的信息。

55、如权利要求 50 所述的网络设备，其特征在于，所述处理器还执行:

以第一交换密钥或第一交换密钥的衍生密钥作为哈希消息认证码运算的输入密钥，对加密后的第三设备公钥运算值进行哈希消息认证运算，并通过所述输出装置向第二设备发送进行哈希消息认证运算后的信息。

56、一种网络设备，其特征在于，包括：输入装置、输出装置、存储器和处理器;

其中，所述存储器用于存储程序代码，所述处理器用于调用所述存储器存储的程序代码执行如下步骤:

将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取；通过所述输入装置接收所述第一设备发送的第一设备公钥信息，并根据所述第一设备公钥信息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息；通过所述输出装置向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的

第二设备公钥副本; 根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息。

57、如权利要求 56 所述的网络设备，其特征在于，所述处理器通过所述输入装置接收所述第一设备发送的第一设备公钥信息之前还包括:

生成第二设备密钥信息，以供第一设备通过带外方式获取。

58、如权利要求 57 所述的网络设备，其特征在于，所述处理器通过所述输入装置接收的所述第一设备公钥信息为所述第一设备利用所述第二设备密钥信息作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息;

所述处理器根据所述第一设备公钥信息获取第一设备的公钥包括: 利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥。

59、如权利要求 56 或 57 所述的网络设备，其特征在于，通过所述输入装置接收的所述第一设备公钥信息为所述第一设备利用所述第二设备公钥运算值作为对称加密密钥对所述第一设备用于执行密钥交换的公钥进行对称加密运算而得到的信息;

所述处理器根据所述第一设备公钥信息获取第一设备的公钥包括:

利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥。

60、如权利要求 59 所述的网络设备，其特征在于，所述第二设备公钥信息为所述处理器利用第一设备公钥运算值对第二设备的公钥进行对称加密而得到的信息; 所述第一设备公钥运算值为所述处理器将获得的第一设备的公钥进行预设算法的运算而得到的结果; 或者

当第一设备通过带外方式获取了第二设备密钥信息时，所述第二设备公钥信息为所述处理器利用自身的第二设备密钥信息对第二设备的公钥进行对称

加密而得到的信息。

61、如权利要求 56-60 任一项所述的网络设备，其特征在于，所述处理器根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

通过所述输入装置接收所述第一设备发送的配置信息; 所述配置信息为第一设备以第一交换密钥为加密密钥进行加密后的配置信息，所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果; 将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密接收到的所述配置信息; 或者

将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥; 以所述第二交换密钥为加密密钥，加密配置信息后通过所述输出装置发送给所述第一设备。

62、如权利要求 56-60 任一项所述的网络设备，其特征在于，所述处理器根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息包括:

通过所述输入装置接收所述第一设备发送的加密后的第三设备公钥运算值; 将第二设备用于执行密钥交换的私钥和获取的第一设备公钥进行运算得到第二交换密钥，以所述第二交换密钥解密所述第三设备公钥运算值，并利用所述第三设备公钥运算值与所述第三设备进行密钥交换，并完成最终的配置过程; 所述加密后的第三设备公钥运算值为所述第一设备以所述第一交换密钥为加密密钥对第三设备公钥运算值进行加密而得到的结果; 所述第一交换密钥为所述第一设备以所述第二设备公钥副本与第一设备的私钥进行运算而得到的结果; 所述第三设备公钥运算值为将所述第三设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果。

63、如权利要求 61 或 62 所述的方法，其特征在于，所述处理器还执行:

通过所述输入装置接收第一设备发送的经过哈希消息认证运算后的信息，

以第二交换密钥或第二交换密钥的衍生密钥作为哈希消息认证码运算的解密密钥，对通过所述输入装置接收到的所述经过哈希消息认证运算后的信息进行解密验证。

64、一种网络配置系统，其特征在于，包括第一设备和第二设备，其中
所述第一设备如权利要求 43-55 任一项所述的网络设备；
所述第二设备如权利要求 56-63 任一项所述的网络设备。

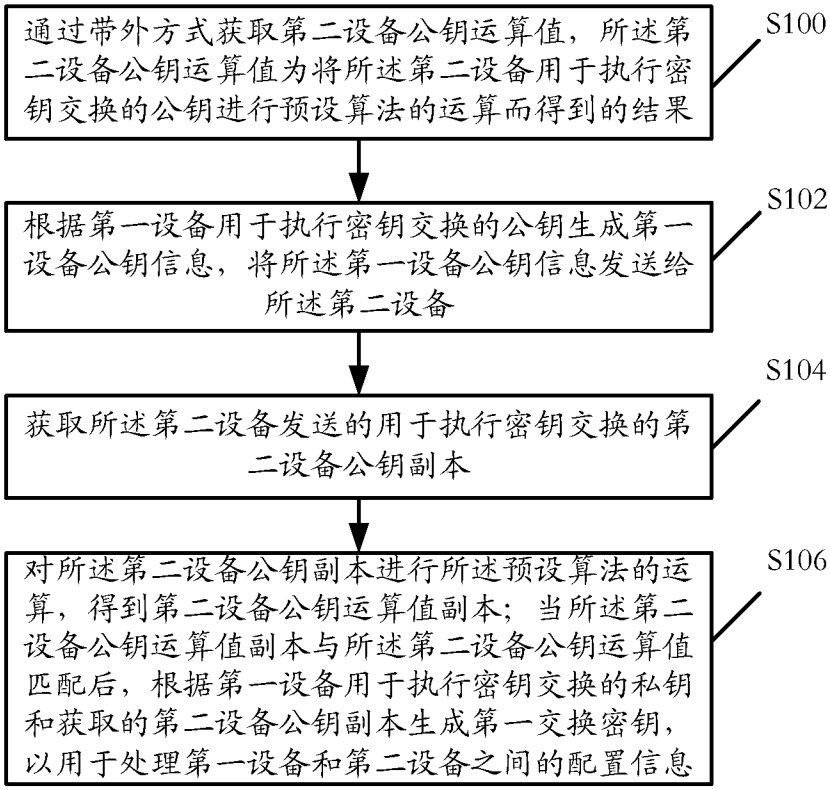
通过带外方式获取第二设备公钥运算值，所述第二设备公钥运算值为将所述第二设备用于执行密钥交换的公钥进行预设算法的运算而得到的结果
S100
根据第一设备用于执行密钥交换的公钥生成第一设备公钥信息，将所述第一设备公钥信息发送给所述第二设备
S102
获取所述第二设备发送的用于执行密钥交换的第二设备公钥副本
S104
对所述第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本；当所述第二设备公钥运算值副本与所述第二设备公钥运算值匹配后，根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理第一设备和第二设备之间的配置信息
S106

图 1

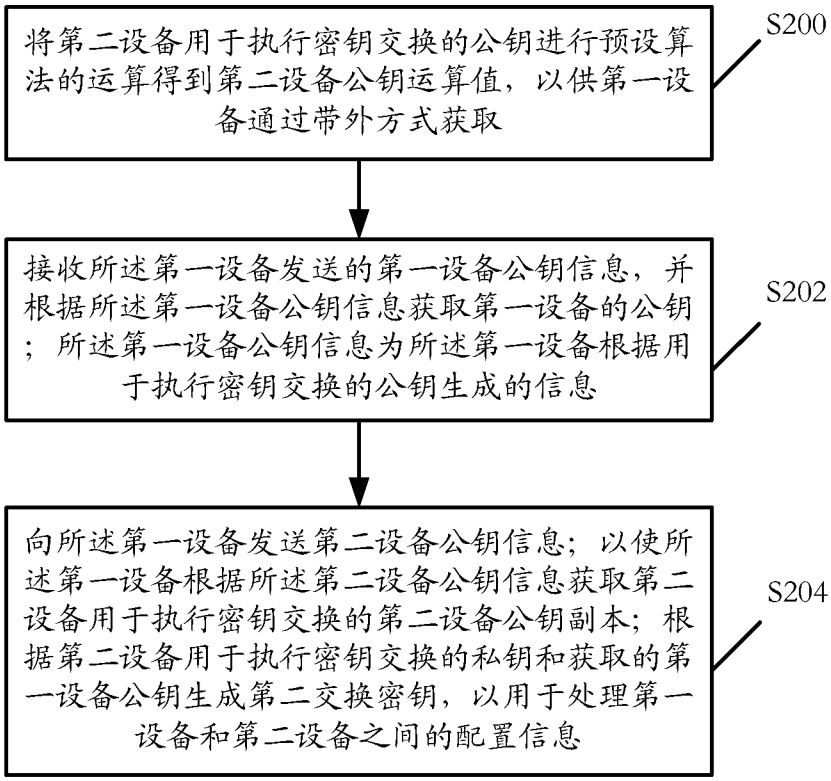
将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取
S200
接收所述第一设备发送的第一设备公钥信息，并根据所述第一设备公钥信息获取第一设备的公钥；所述第一设备公钥信息为所述第一设备根据用于执行密钥交换的公钥生成的信息
S202
向所述第一设备发送第二设备公钥信息；以使所述第一设备根据所述第二设备公钥信息获取第二设备用于执行密钥交换的第二设备公钥副本；根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理第一设备和第二设备之间的配置信息
S204

图 2

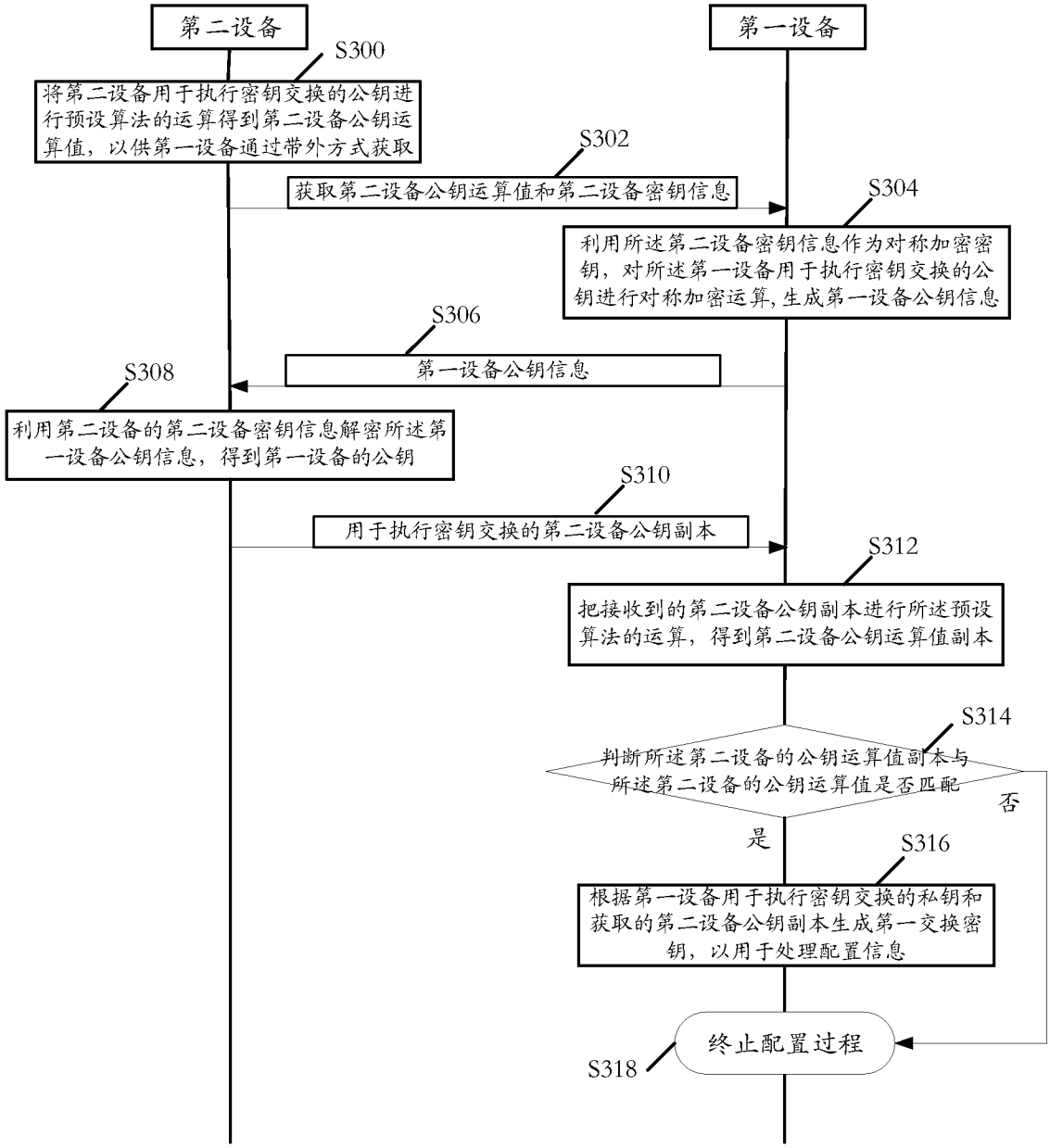
第二设备
第一设备
S300
将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取
S302
获取第二设备公钥运算值和第二设备密钥信息
S304
利用所述第二设备密钥信息作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息
S306
第一设备公钥信息
S308
利用第二设备的第二设备密钥信息解密所述第一设备公钥信息，得到第一设备的公钥
S310
用于执行密钥交换的第二设备公钥副本
S312
把接收到的第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本
S314
判断所述第二设备的公钥运算值副本与所述第二设备的公钥运算值是否匹配
否
是
S316
根据第一设备用于执行密钥交换的私钥和获取的第二设备公钥副本生成第一交换密钥，以用于处理配置信息
终止配置过程
S318

图 3

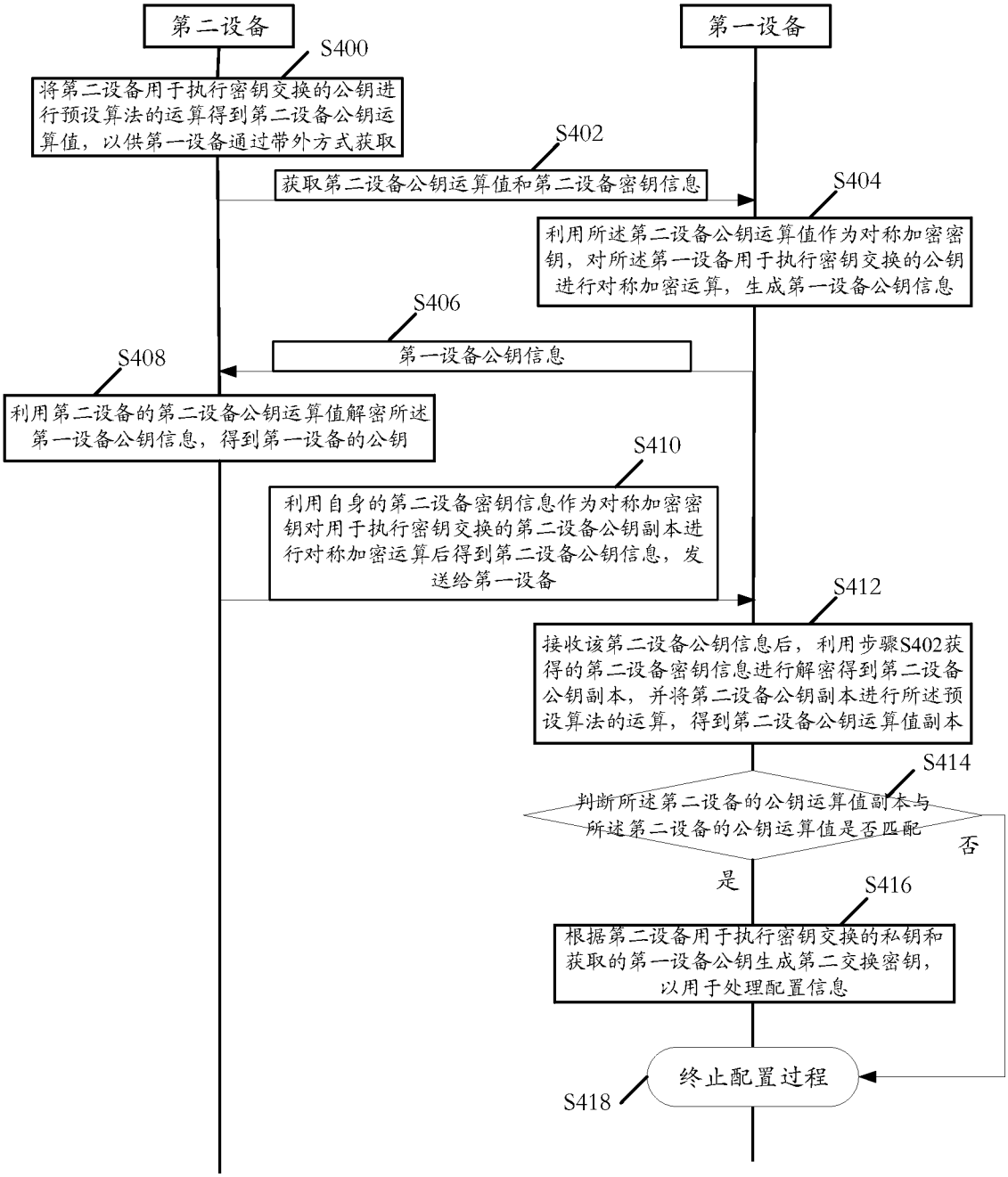
第二设备
第一设备
S400
将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取
S402
获取第二设备公钥运算值和第二设备密钥信息
S404
利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息
S406
第一设备公钥信息
S408
利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥
S410
利用自身的第二设备密钥信息作为对称加密密钥对用于执行密钥交换的第二设备公钥副本进行对称加密运算后得到第二设备公钥信息，发送给第一设备
S412
接收该第二设备公钥信息后，利用步骤S402获得的第二设备密钥信息进行解密得到第二设备公钥副本，并将第二设备公钥副本进行所述预设算法的运算，得到第二设备公钥运算值副本
S414
判断所述第二设备的公钥运算值副本与所述第二设备的公钥运算值是否匹配
否
是
S416
根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理配置信息
终止配置过程
S418

图 4

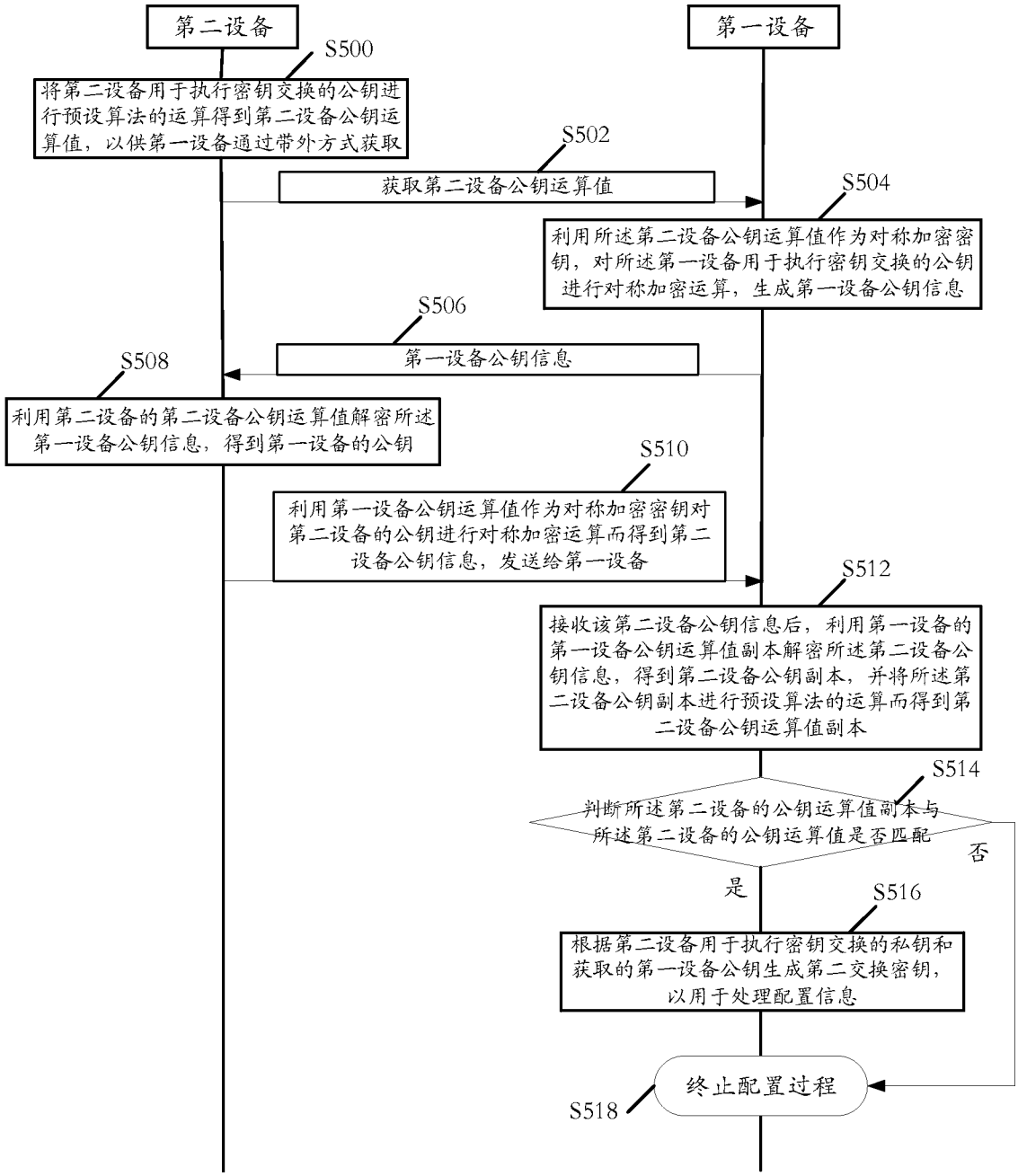
第二设备
第一设备
S500
将第二设备用于执行密钥交换的公钥进行预设算法的运算得到第二设备公钥运算值，以供第一设备通过带外方式获取
S502
获取第二设备公钥运算值
S504
利用所述第二设备公钥运算值作为对称加密密钥，对所述第一设备用于执行密钥交换的公钥进行对称加密运算，生成第一设备公钥信息
S506
第一设备公钥信息
S508
利用第二设备的第二设备公钥运算值解密所述第一设备公钥信息，得到第一设备的公钥
S510
利用第一设备公钥运算值作为对称加密密钥对第二设备的公钥进行对称加密运算而得到第二设备公钥信息，发送给第一设备
S512
接收该第二设备公钥信息后，利用第一设备的第一设备公钥运算值副本解密所述第二设备公钥信息，得到第二设备公钥副本，并将所述第二设备公钥副本进行预设算法的运算而得到第二设备公钥运算值副本
S514
判断所述第二设备的公钥运算值副本与所述第二设备的公钥运算值是否匹配
否
是
S516
根据第二设备用于执行密钥交换的私钥和获取的第一设备公钥生成第二交换密钥，以用于处理配置信息
终止配置过程
S518

图 5

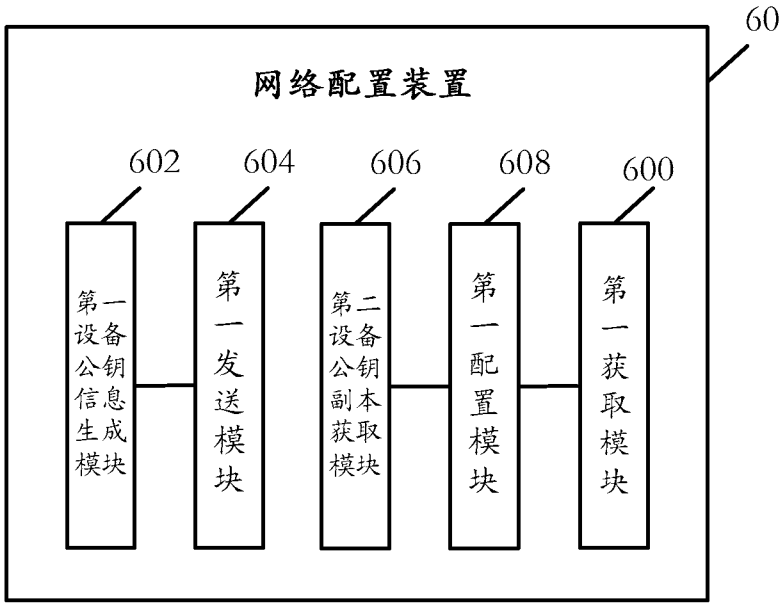
60
网络配置装置
602
604
606
608
600
第一备钥息成块
第一发送模块
第二备钥本取块
第一配置模块
第一获取模块

图 6

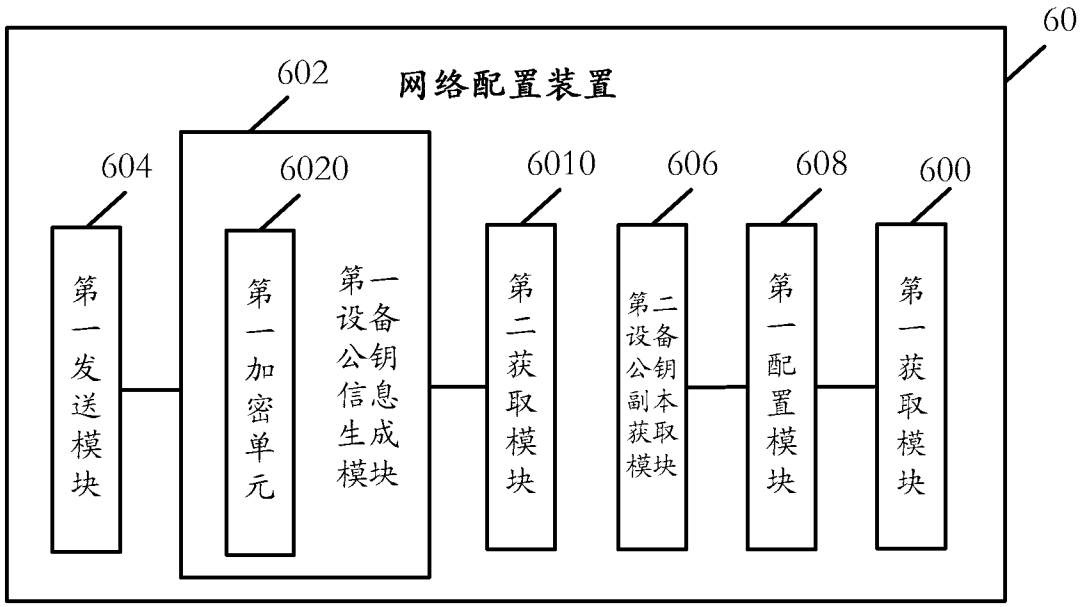
60
网络配置装置
602
604
6020
6010
606
608
600
第一发送模块
第一加密单元
第一备钥息成块
第二获取模块
第二备钥本取块
第一配置模块
第一获取模块

图 7

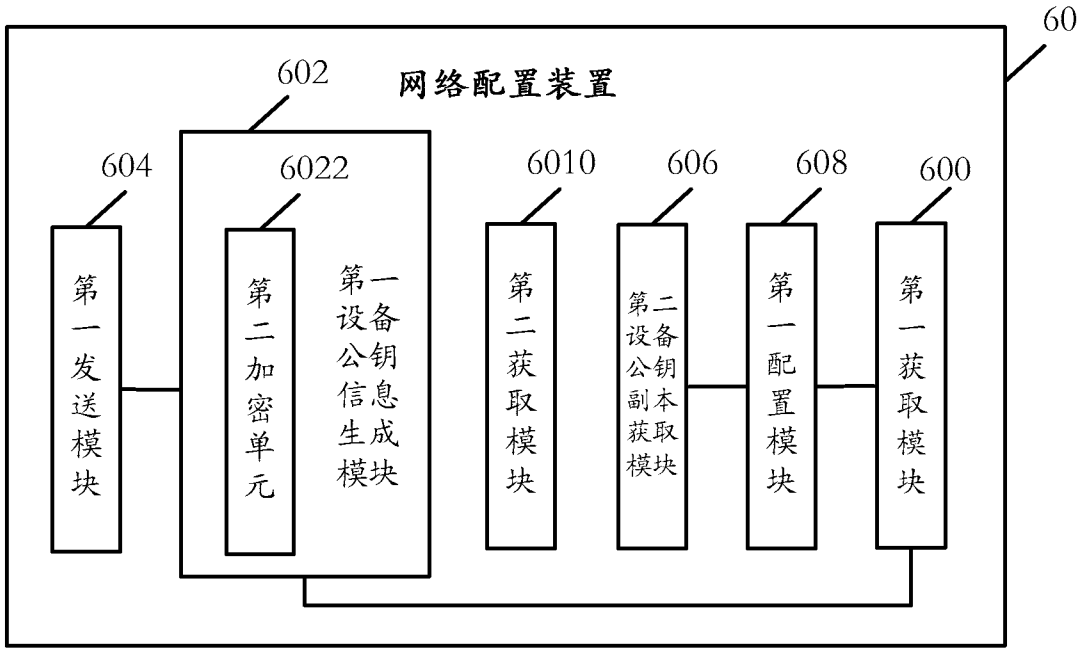
60
网络配置装置
602
604
6022
6010
606
608
600
第一发送模块
第二加密单元
第一备设公钥信息生成模块
第二获取模块
第二备设公钥副本获取模块
第一配置模块
第一获取模块

图 8

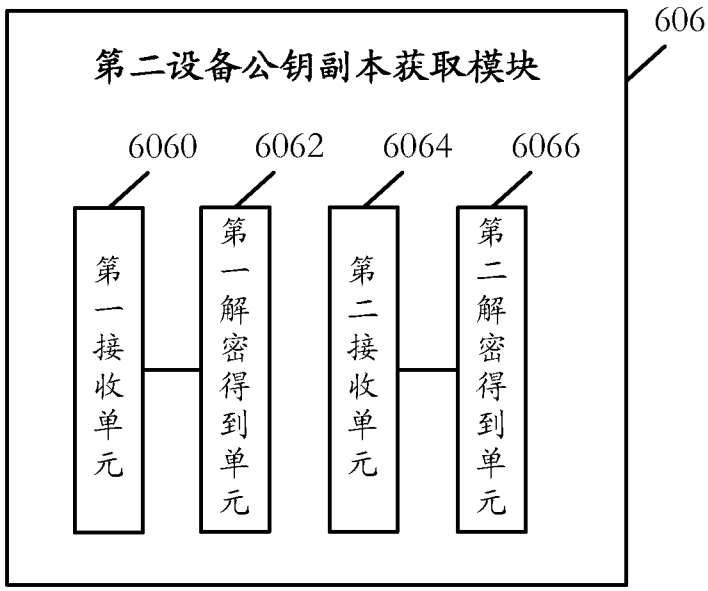
606
第二设备公钥副本获取模块
6060
6062
6064
6066
第一接收单元
第一解密得到单元
第二接收单元
第二解密得到单元

图 9

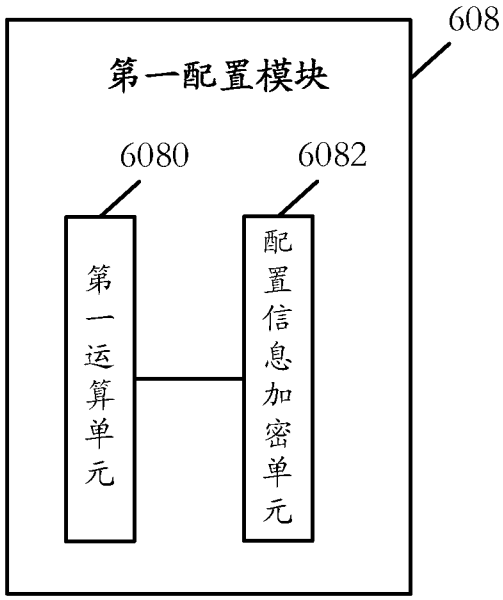
608
第一配置模块
6080
6082
第一运算单元
配置信息加密单元

图 10

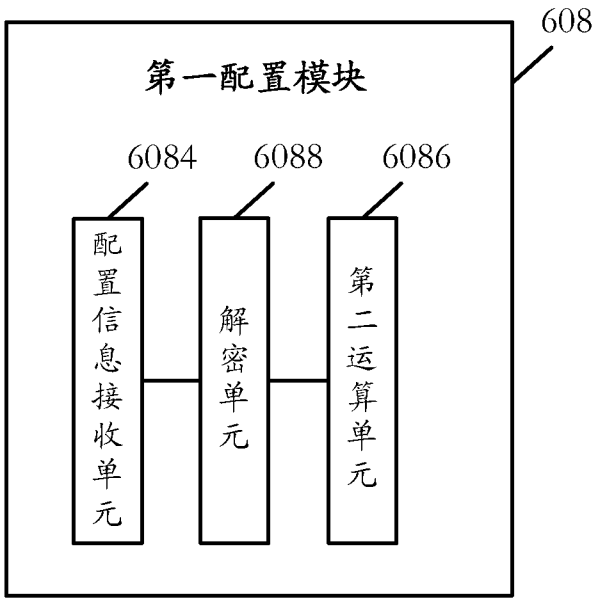
608
第一配置模块
6084
6088
6086
配置信息接收单元
解密单元
第二运算单元

图 11

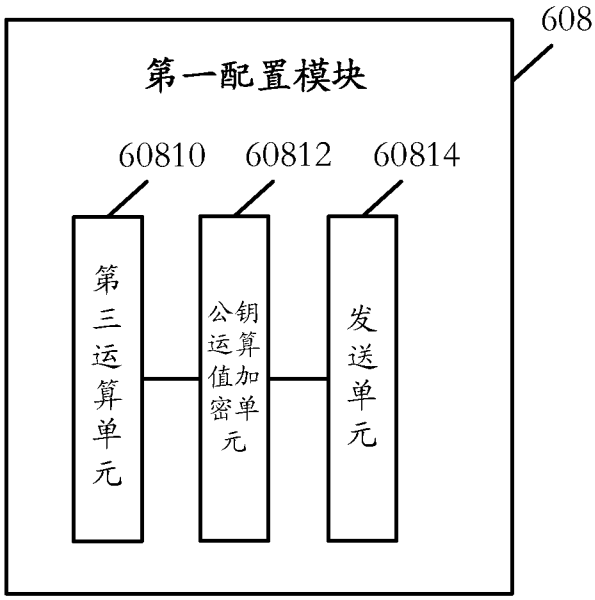
608
第一配置模块
60810
60812
60814
第三运算单元
公钥运算加密值单元
发送单元

图 12

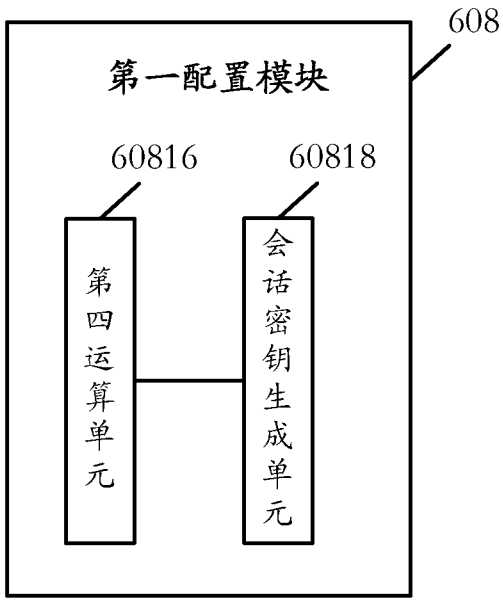
608
第一配置模块
60816
60818
第四运算单元
会话密钥生成单元

图 13

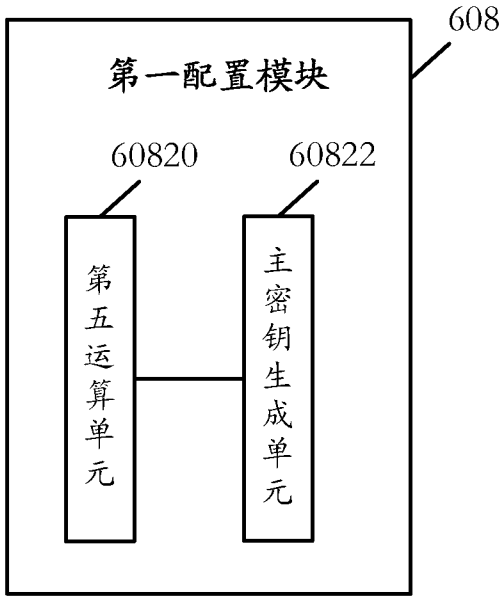
608
第一配置模块
60820
60822
第五运算单元
主密钥生成单元

图 14

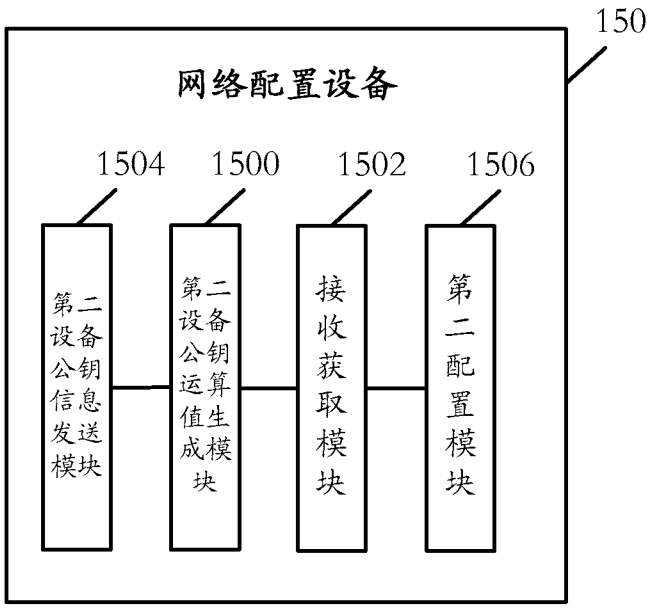
150
网络配置设备
1504
1500
1502
1506
第二备份密钥公信息发送模块
第二备份密钥公共运算值生成模块
接收获取模块
第二配置模块

图 15

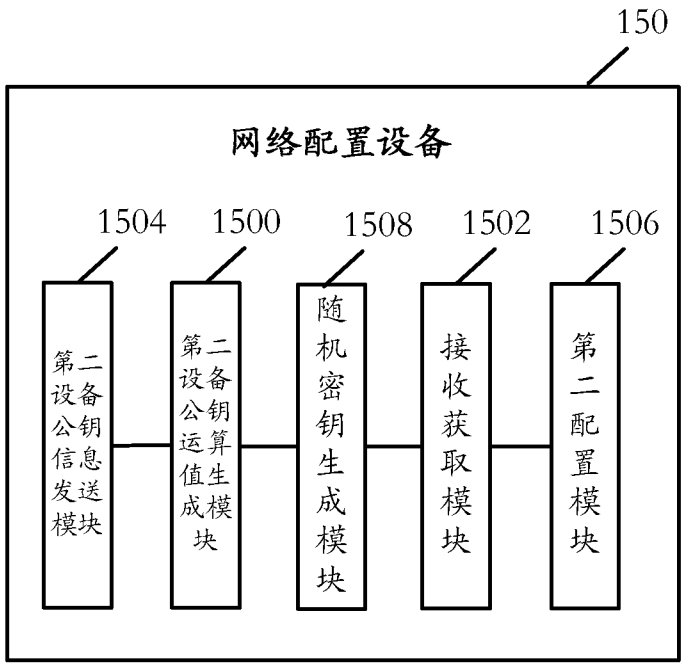
150
网络配置设备
1504
1500
1508
1502
1506
第二设备公钥信息发送模块
第二设备公钥运算生成模块
随机密钥生成模块
接收获取模块
第二配置模块

图 16

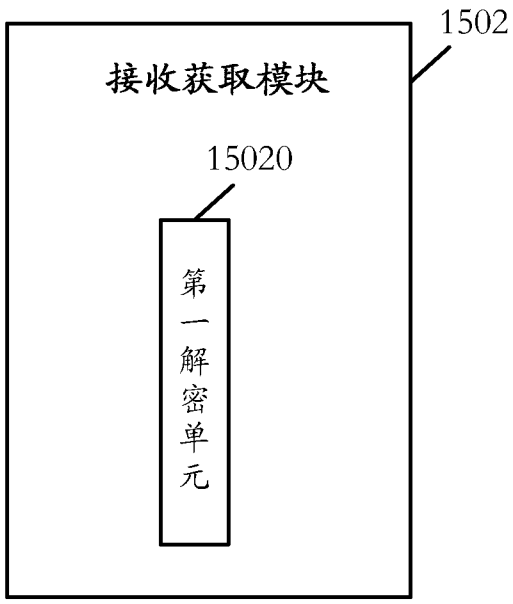
1502
接收获取模块
15020
第一解密单元

图 17

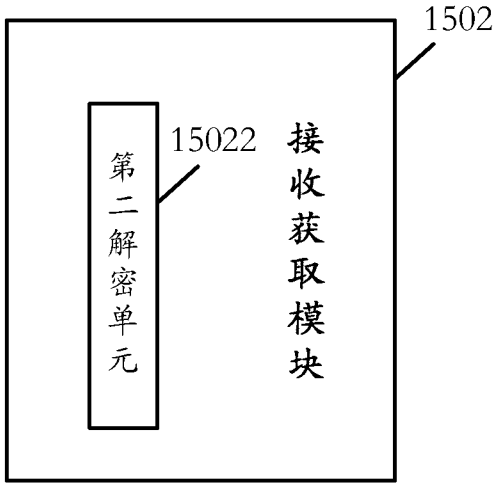
1502
15022
第二解密单元
接收获取模块

图 18

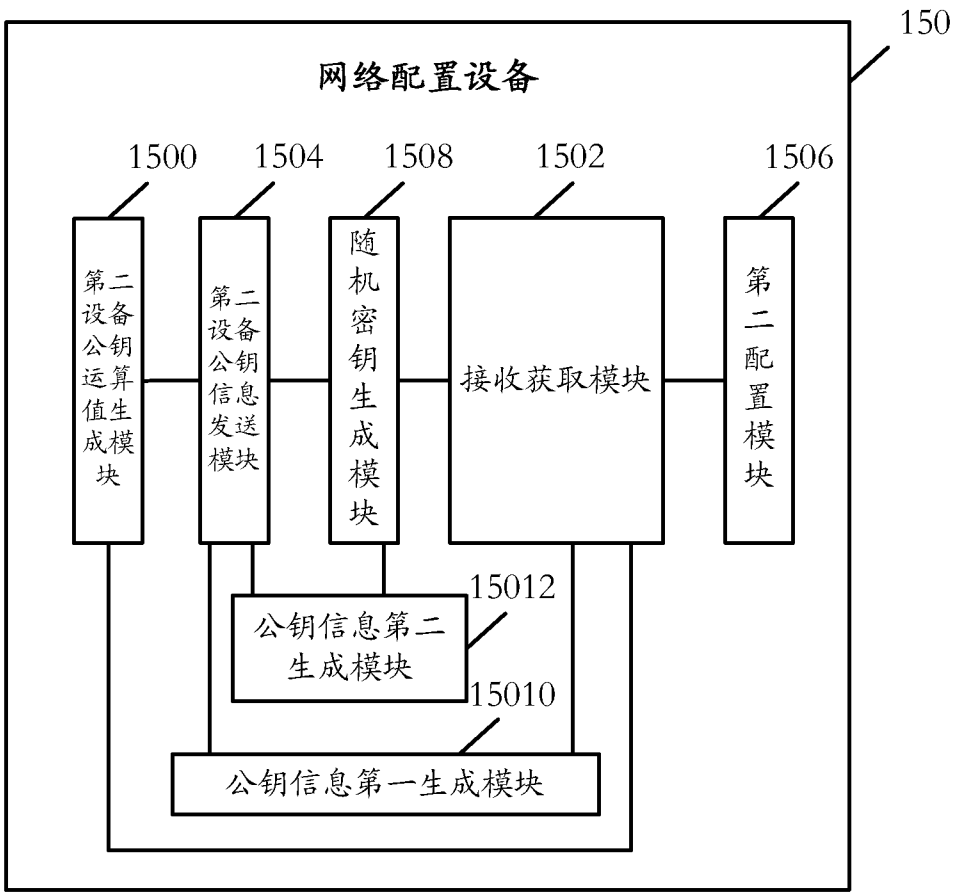
150
网络配置设备
1500
1504
1508
1502
1506
第二备用公钥运算生成模块
第二备用公钥信息发送模块
随机密钥生成模块
接收获取模块
第二配置模块
15012
公钥信息第二生成模块
15010
公钥信息第一生成模块

图 19

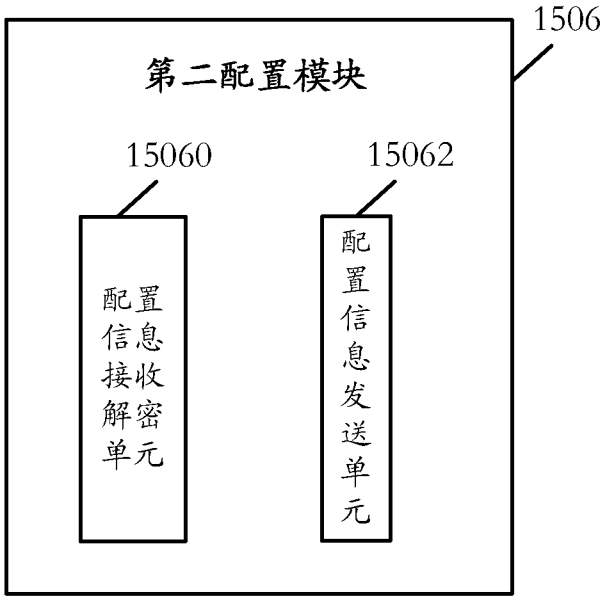
1506
第二配置模块
15060
配置信息接收解密单元
15062
配置信息发送单元

图 20

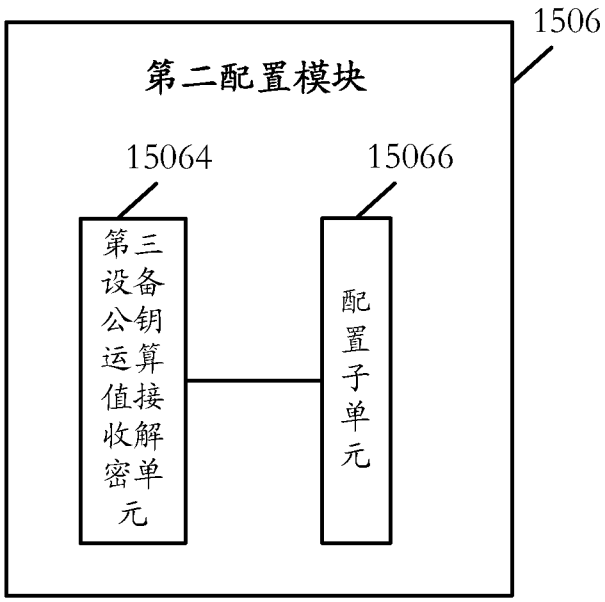
1506
第二配置模块
15064
第三设备公钥运算接收解密单元
15066
配置子单元

图 21

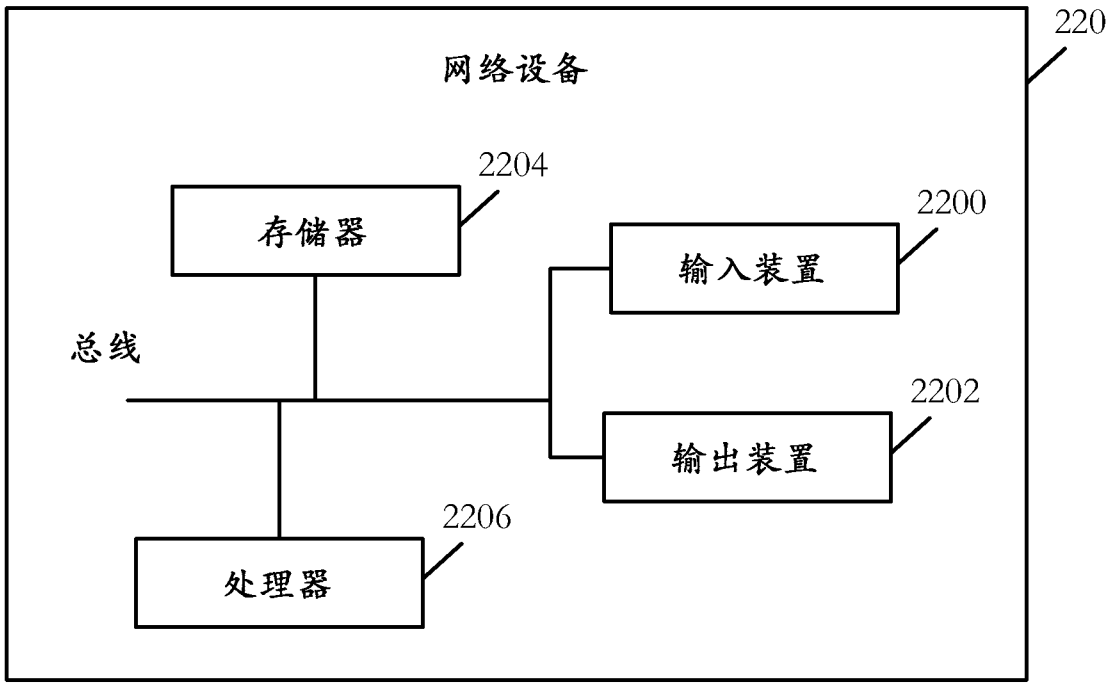
网络设备
220
2204
存储器
2200
输入装置
总线
2202
输出装置
2206
处理器

图 22

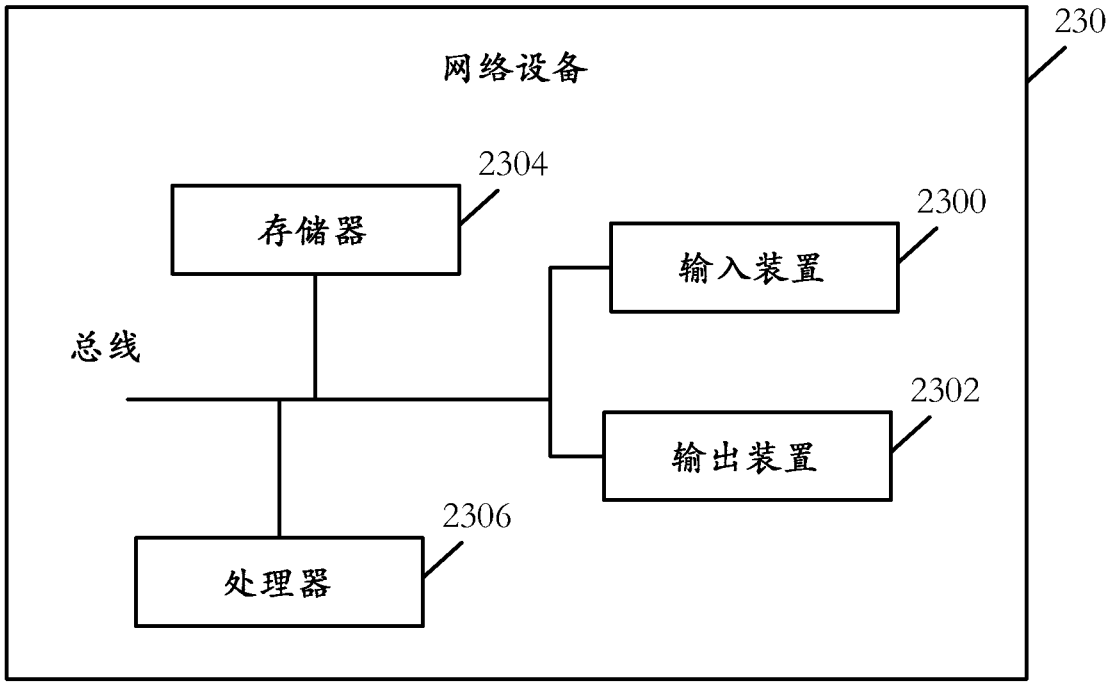
网络设备
230
2304
存储器
2300
输入装置
总线
2302
输出装置
2306
处理器

图 23

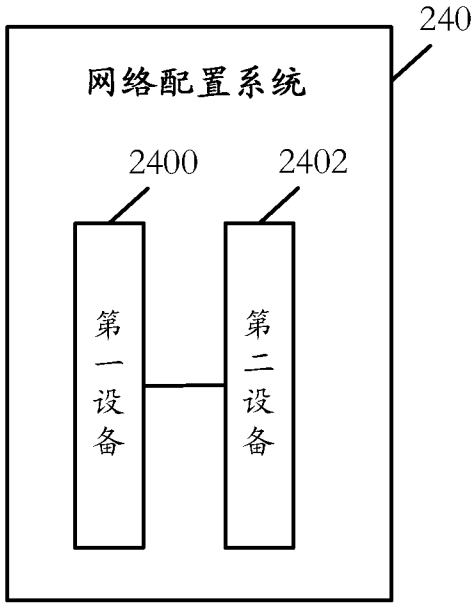

图 24

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/091236

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; 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; CNKI; VEN: in-band, key, configure, setting, out of band, public key, calculate, algorithm, exchange

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101150849 A (HUAWEI TECHNOLOGIES CO., LTD.), 26 March 2008 (26.03.2008), description, page 8, line 14 to page 10, line 27	14-21, 35-42, 56-63
A	CN 101150849 A (HUAWEI TECHNOLOGIES CO., LTD.), 26 March 2008 (26.03.2008), description, page 8, line 14 to page 10, line 27	1-13, 22-34, 43-55, 64
A	CN 102195930 A (HUAWEI TECHNOLOGIES CO., LTD.), 21 September 2011 (21.09.2011), description, paragraphs [0034]-[0083]	1-64
A	CN 1661959 A (MICROSOFT CORPORATION), 31 August 2005 (31.08.2005), description, page 2, line 4 to page 5, line 6, and claim 1	1-64

☐ 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
28 August 2014 (28.08.2014)	**26 September 2014 (26.09.2014)**
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 **GAO, Lijun** Telephone No.: (86-10) **62411224**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/091236

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101150849 A	26 March 2008	WO 2008034368 A1	27 March 2008
		CN 101150849 B	08 September 2010
CN 102195930 A	21 September 2011	WO 2011107013 A1	09 September 2011
		EP 2544397 A1	09 January 2013
		EP 2544397 A4	24 April 2013
		US 2012331538 A1	27 December 2012
CN 1661959 A	31 August 2005	KR 20060042262 A	12 May 2006
		JP 2005244988 A	08 September 2005
		EP 1569382 A1	31 August 2005
		US 2005193203 A1	01 September 2005
		US 7778422 B2	17 August 2010

国际检索报告

国际申请号
PCT/CN2013/091236

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; 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;CNKI;VEN:配置,设置,带外,带内,公钥,密钥,运算,算法,交换,configure, setting, out of band, public key, calculate, algorithm, exchange

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 101150849 A (华为技术有限公司) 2008年 3月 26日 (2008-03-26) 说明书第8页第14行-第10页第27行	14-21，35-42，56-63
A	CN 101150849 A (华为技术有限公司) 2008年 3月 26日 (2008-03-26) 说明书第8页第14行-第10页第27行	1-13，22-34，43-55，64
A	CN 102195930 A (华为技术有限公司) 2011年 9月 21日 (2011-09-21) 说明书第[0034]-[0083]段	1-64
A	CN 1661959 A (微软公司) 2005年 8月 31日 (2005-08-31) 说明书第2页第4行-第5页第6行，权利要求1	1-64

☐ 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
2014年 8月 28日	2014年 9月 26日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	受权官员 高利军 电话号码 (86-10)62411224

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/091236

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	101150849	A	2008年 3月 26日	WO	2008034368	A1	2008年 3月 27日
				CN	101150849	B	2010年 9月 08日
CN	102195930	A	2011年 9月 21日	WO	2011107013	A1	2011年 9月 09日
				EP	2544397	A1	2013年 1月 09日
				EP	2544397	A4	2013年 4月 24日
				US	2012331538	A1	2012年 12月 27日
CN	1661959	A	2005年 8月 31日	KR	20060042262	A	2006年 5月 12日
				JP	2005244988	A	2005年 9月 08日
				EP	1569382	A1	2005年 8月 31日
				US	2005193203	A1	2005年 9月 01日
				US	7778422	B2	2010年 8月 17日