(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 12 月 5 日 (05.12.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/231392 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *G06F 21/31* (2013.01)
H04L 9/14 (2006.01) *H04L 29/06* (2006.01)
H04L 9/28 (2006.01)

(21) 国际申请号: PCT/SG2018/050266

(22) 国际申请日: 2018 年 5 月 30 日 (30.05.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为国际有限公司 (**HUAWEI INTERNATIONAL PTE. LTD.**) [SG/SG]; 新加坡, Singapore 486066 (SG)。

(72) 发明人: 朋特其旺·大卫 (**POINTCHEVAL, David**); 法国, Thiais 94320 (FR)。 王贵林(**WANG, Guilin**); 新加坡, Singapore 117674 (SG)。

(74) 代理人: 艾伦格禧有限责任合伙律师事务所 (**ALLEN & GLEDHILL LLP**); 新加坡一号滨海林荫道#28-00, Singapore 018989 (SG)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,

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

(54) 发明名称: 一种密钥协商系统、方法及装置

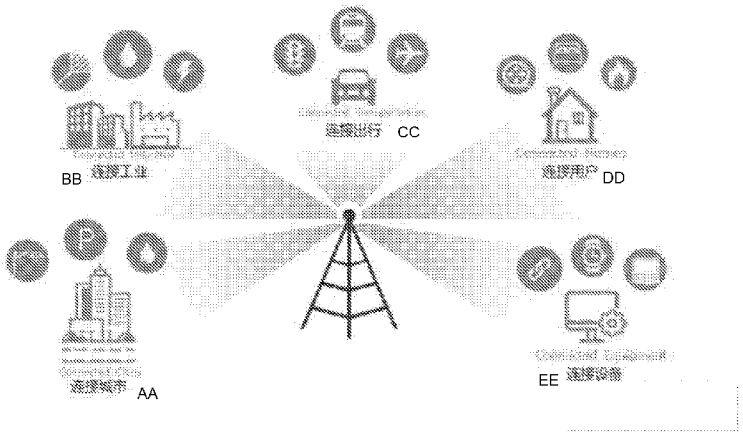


图 1

AA ... Connected cities
BB ... Connected industries
CC ... Connected transportation
DD ... Connected users
EE ... Connected devices

(57) **Abstract:** The present application provides a key exchange system, method, and apparatus. The method comprises: a first device generating a public-private key pair, sending, to a second device, the public key of the public-private key pair, and receiving ciphertext and a promise value; the first device acquiring a first result, acquiring an original key according to the private key of the public-private key pair and the ciphertext, determining a second bit string according to part of bits in the original key, calculating a second result according to the second bit string and the first result, and sending the second result to the second device; and the first device receiving an opening value, and acquiring, according to the opening value and the promise value, an authentication result of the second device, and generating a session key for communicating with the second device. The method provided by the present application can be used to significantly improve exchange efficiency while guaranteeing a certain degree of security and is easy to implement.

WO 2019/231392 A1

[见续页]

NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。
- 黑白；提交的国际申请包含彩色或灰度，并且可通过PATENTSCOPE下载

(57) 摘要: 本申请提供一种密钥协商系统、方法及装置，该方法包括：第一设备生成一个公私钥对，向第二设备发送公私钥对中的公钥，接收密文和承诺值。第一设备获取第一结果，根据公私钥对中的私钥和密文获得原始密钥，并根据原始密钥中的部分比特确定第二比特串，根据第二比特串和第一结果计算得到第二结果，向第二设备发送第二结果。第一设备接收打开值，第一设备根据打开值和承诺值对第二设备得到认证结果并生成用于与第二设备通信的会话密钥。因此，采用本申请提供的方法可以在一定程度保证安全的情况下实现协商效率的明显提高，且该方法实施简便。

一种密钥协商系统、方法及装置

技术领域

本申请涉及量子安全技术领域，特别涉及一种密钥协商系统、方法及装置。

背景技术

密钥协商，或者更准确地说是认证密钥协商(Authenticated Key Exchange，AKE)，可以使得两个通信主体安全地协商出一个共同的会话密钥，用于随后的安全通信。

传统的AKE协议使用公私钥对、口令等作为密钥协商和认证的材料，通信双方在公开的非安全信道上协商出一个共同的安全会话密钥。但这些协议，比如加密密钥交换(Encrypted Key Exchange，EKE)协议、简单的基于口令加密密钥交换 (Simple Password-based encrypted key exchange，SPAKE)协议、基于验证值的双基口令指数密钥交换 (Verifier-based Two-Basis Password Exponential Key Exchange，VTBPEKE)协议，本质都以迪菲-赫尔曼（Diffie-Hellman，DH）密钥交换技术作为基础。但该DH密钥交换技术基于离散对数问题，该问题已被证明是可以破解的，因此DH密钥交换技术就在量子计算下不再安全。

与此相比较，现有的量子安全AKE协议都比较复杂，且效率不高。比如凯伯（Kyber）协议需要通信双方共执行6次密钥封装（Key Encapsultation Mechanism，KEM）加解密操作，虽然有其他科研人员提出了将系统参数进行优化的量子协议，但还是需要通信双方共执行2次KEM加解密操作和4次数字签名相关操作。

由上可知，现有的量子安全AKE协议比较复杂，效率不高。

发明内容

本申请实施例提供一种密钥协商系统、方法及装置，用以实现简便高效的量子安全密钥协商。

第一方面，本申请实施例提供一种密钥协商系统，包括第一设备和第二设备，其中：

所述第一设备用于采用密钥生成算法生成一个公私钥对，向所述第二设备发送所述公私钥对中的公钥；所述第二设备用于根据接收到的所述公钥采用封装算法选取原始密钥，根据所述公钥和所述原始密钥采用所述封装算法获得密文，以及根据第一比特串和随机数采用承诺算法获得承诺值和打开值，向所述第一设备发送所述密文和所述承诺值，所述第一比特串为随机比特串；以及，根据所述原始密钥中的部分比特确定第二比特串，根据所述第一比特串和所述第二比特串计算得到第一结果；所述第一设备还用于根据所述公私钥对中的私钥和接收到的所述密文采用解封装算法获得所述原始密钥，并根据所述原始密钥中的所述部分比特确定所述第二比特串；根据所述第二比特串和所述第一结果计算得到第二结果，向所述第二设备发送所述第二结果；所述第二设备还用于在所述第一比特串与接收到的所述第二结果相同的情况下，向所述第一设备发送所述打开值并生成用于与所述第一设备通信的会话密钥，其中所述第一比特串与所述第二结果相同表示所述第二设备对所

述第一设备认证成功；所述第一设备还用于根据接收到的所述打开值和所述承诺值对所述第二设备进行认证，得到认证结果，所述认证结果用于指示所述第一设备对所述第二设备认证成功，并生成用于与所述第二设备通信的会话密钥。

因此，本申请实施例提供的系统只在协商时生成和使用一个临时的KEM公钥对，通信双方共执行2次KEM加解密操作，以及一些简单的承诺操作。与现有技术中提到的Kyber协议和系统参数优化后的量子协议相比，在一定程度保证安全的情况下效率提高明显，且实施简便。

在一种可能的设计中，所述第二设备具体用于采用第一算法对所述第一比特串和所述第二结果进行计算，以得到第一结果；所述第一设备具体用于采用所述第一算法对所述第二比特串和所述第一结果进行计算，以得到第二结果；所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

因此，第二设备可以采用多种可能的算法计算得到第一结果，第一设备可以采用与计算第一结果相同的算法计算得到第二结果。

在一种可能的设计中，所述第一设备还用于在所述第一设备生成用于与所述第二设备通信的会话密钥后，删除所述公私钥对；当发起与所述第二设备重新执行密钥协商，或者，当发起与第三设备执行密钥协商，重新生成一个公私钥对。

相较于现有技术中，通信主体双方需要保存公私钥对、口令等作为密钥协商和认证的材料，占用大量存储空间，在本申请实施例中，当第一设备生成用于与第二设备通信的会话密钥后，第一设备删除公私钥对，可以节省存储空间，本申请实施例提供的方法更加适用于硬件能力受限的设备。

在一种可能的设计中，所述第二设备还用于在所述第二设备生成用于与所述第一设备通信的会话密钥后，删除所述公钥；当发起与所述第一设备重新执行密钥协商，或者，当发起与第四设备执行密钥协商，生成一个公私钥对。

相较于现有技术中，通信主体双方需要保存公私钥对、口令等作为密钥协商和认证的材料，占用大量存储空间，在本申请实施例中，当第二设备生成用于与第一设备通信的会话密钥后，第二设备删除公钥，可以节省存储空间，本申请实施例提供的方法更加适用于硬件能力受限的设备。

在一种可能的设计中，所述第一设备具体用于根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第二设备通信的会话密钥；

所述第二设备具体用于根据所述一个或多个参数生成用于与所述第一设备通信的会话密钥，其中，用于与所述第二设备通信的会话密钥与用于与所述第一设备通信的会话密钥相同。

因此，会话密钥的生成可以采用多种参数组合形式以及多种函数形式，实施方式灵活方便，

第二方面，本申请实施例提供一种密钥协商方法，包括：

第一设备采用密钥生成算法生成一个公私钥对，向第二设备发送所述公私钥对中的公钥；所述第一设备接收密文和承诺值，所述密文是根据所述公钥和原始密钥采用封装算法获得的，所述原始密钥是根据所述公钥采用所述封装算法选取的，所述承诺值是根据第一比特串和随机数采用承诺算法获得的，所述第一比特串为随机比特串；所述第一设备获取

第一结果，所述第一结果是根据所述第一比特串和第二比特串计算得到的，所述第二比特串是根据所述原始密钥中的部分比特确定的；所述第一设备根据所述公私钥对中的私钥和所述密文采用解封装算法获得所述原始密钥，并根据所述原始密钥中的所述部分比特确定所述第二比特串；所述第一设备根据所述第二比特串和所述第一结果计算得到第二结果，向所述第二设备发送所述第二结果；所述第一设备接收打开值，其中，所述打开值是在所述第一比特串与所述第二结果相同的情况下所述第二设备向所述第一设备发送的，所述打开值是根据所述第一比特串和所述随机数采用所述承诺算法获得的；所述第一设备根据所述打开值和所述承诺值对所述第二设备进行认证，得到认证结果，所述认证结果用于指示所述第二设备对所述第二设备认证成功，并生成用于与所述第二设备通信的会话密钥。

因此，本申请实施例提供的方法只在协商时生成和使用一个临时的KEM公钥对，通信双方共执行2次KEM加解密操作，以及一些简单的承诺操作。与现有技术中提到的Kyber协议和系统参数优化后的量子协议相比，在一定程度保证安全的情况下效率提高明显，且实施简便。

在一种可能的设计中，在所述第一设备根据所述第二比特串和所述第一结果计算得到第二结果时，所述第一设备采用第一算法对所述第二比特串和所述第一结果进行计算，以得到第二结果，所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

因此，第一设备可以采用多种可能的算法计算第二结果。

在一种可能的设计中，所述第一算法为异或运算；

在所述第一设备采用第一算法对所述第二比特串和所述第一结果进行计算，以得到第二结果时，所述第一设备采用异或算法对所述第二比特串和所述第一结果进行计算，得到异或结果作为第二结果。

因此，第一设备可以采用异或运算计算得到异或结果作为第二结果。

在一种可能的设计中，在所述第一设备生成用于与所述第二设备通信的会话密钥后，所述第一设备删除所述公私钥对；当所述第一设备发起与所述第二设备重新执行密钥协商，或者，当所述第一设备发起与第三设备执行密钥协商，所述第一设备重新生成一个公私钥对。

相较于现有技术中，通信主体双方需要保存公私钥对、口令等作为密钥协商和认证的材料，占用大量存储空间，在本申请实施例中，当第一设备生成用于与第二设备通信的会话密钥后，第一设备删除公私钥对，可以节省存储空间，本申请实施例提供的方法更加适用于硬件能力受限的设备。

在一种可能的设计中，在所述第一设备生成用于与所述第二设备通信的会话密钥时，所述第一设备根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第二设备通信的会话密钥。可见，第一设备可以采用多种参数组合形式以及多种函数形式生成会话密钥，实施方式灵活方便。

第三方面，本申请实施例提供一种密钥协商方法，包括：

第二设备接收公钥，所述公钥为采用密钥生成算法生成的一个公私钥对中的公钥；

所述第二设备根据所述公钥采用所述封装算法选取原始密钥，根据所述公钥和所述原始密钥采用所述封装算法获得密文，以及根据第一比特串和随机数采用承诺算法获得承诺

值和打开值，向所述第一设备发送所述密文和所述承诺值，所述第一比特串为随机比特串；所述第二设备根据所述原始密钥中的部分比特确定第二比特串，根据所述第一比特串和所述第二比特串计算得到第一结果；所述第二设备接收第二结果，所述第二结果是根据所述第二比特串和所述第一结果计算得到的；所述第二设备在所述第一比特串与所述第二结果相同的情况下，向所述第一设备发送所述打开值，并生成用于与所述第一设备通信的会话密钥，其中所述第一比特串与所述第二结果相同表示所述第二设备对所述第一设备认证成功。

因此，本申请实施例提供的方法只在协商时生成和使用一个临时的KEM公钥对，通信双方共执行2次KEM加解密操作，以及一些简单的承诺操作。因此，与现有技术中提到的Kyber协议和系统参数优化后的量子协议相比，在一定程度保证安全的情况下效率提高明显，且实施简便。

在一种可能的设计中，在所述第二设备根据所述第一比特串和所述第二比特串计算得到第一结果时，所述第二设备采用第一算法对所述第一比特串和所述第二比特串进行计算，以得到第一结果；所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。第二设备可以采用多种可能的算法计算第一结果，使实施方式更灵活方便。

在一种可能的设计中，所述第一算法为异或运算；在所述第二设备采用第一算法对所述第一比特串和所述第二比特串进行计算，以得到第一结果时，所述第二设备采用异或运算对所述第一比特串和所述第二比特串进行计算，得到异或结果作为第一结果。

在一种可能的设计中，在所述第二设备生成用于与所述第一设备通信的会话密钥后，所述第二设备删除所述公钥；当所述第二设备重新发起与所述第一设备执行密钥协商，或者，当所述第二设备发起与第三设备执行密钥协商，所述第二设备生成一个公私钥对。

相较于现有技术中，通信主体双方需要保存公私钥对、口令等作为密钥协商和认证的材料，占用大量存储空间，在本申请实施例中，当第二设备生成用于与第一设备通信的会话密钥后，第二设备删除公钥，可以节省存储空间，本申请实施例提供的方法更加适用于硬件能力受限的设备。

在一种可能的设计中，在所述第二设备生成用于与所述第二设备通信的会话密钥时，所述第二设备根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第一设备通信的会话密钥。

相较于现有技术中，通信主体双方需要保存公私钥对、口令等作为密钥协商和认证的材料，占用大量存储空间，在本申请实施例中，当第二设备生成用于与第二设备通信的会话密钥后，第二设备删除公钥，可以节省存储空间，本申请实施例提供的方法更加适用于硬件能力受限的设备。

第四方面，本申请实施例提供一种密钥协商装置，该装置可以为第一设备，也可以为第一设备内的芯片。该装置可以包括处理单元和收发单元。当该装置是第一设备时，该处理单元可以是处理器，该收发单元可以是收发器，该第一设备还可以包括存储单元，该存储单元可以是存储器，该存储单元用于存储指令，该处理单元执行该存储单元所存储的指令，以使该第一设备执行第二方面或第二方面任意一种可能的设计中的方法。当该装置是第一设备内的芯片时，该处理单元可以是处理器，该收发单元可以是输入/输出接口、管脚

或电路等；该处理单元执行存储单元所存储的指令，该存储单元用于存储指令，该存储单元可以是该芯片内的存储单元（例如，寄存器、缓存等），也可以是该第一设备内的位于该芯片外部的存储单元（例如，只读存储器、随机存取存储器等），以使该第一设备执行第二方面或第二方面任意一种可能的设计中的方法。

第五方面，本申请实施例提供一种密钥协商装置，该装置可以为第二设备，也可以为第二设备内的芯片。该装置可以包括处理单元和收发单元。当该装置是第二设备时，该处理单元可以是处理器，该收发单元可以是收发器，该第二设备还可以包括存储单元，该存储单元可以是存储器，该存储单元用于存储指令，该处理单元执行该存储单元所存储的指令，以使该第二设备执行第三方面或第三方面任意一种可能的设计中的方法。当该装置是第二设备内的芯片时，该处理单元可以是处理器，该收发单元可以是输入/输出接口、管脚或电路等；该处理单元执行存储单元所存储的指令，该存储单元用于存储指令，该存储单元可以是该芯片内的存储单元（例如，寄存器、缓存等），也可以是该第二设备内的位于该芯片外部的存储单元（例如，只读存储器、随机存取存储器等），以使该第二设备执行第三方面或第三方面任意一种可能的设计中的方法。

第六方面，本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，当该计算机程序在计算机上运行时，使得计算机执行上述第一方面和/或第二方面所述的方法。

第七方面，本申请实施例还提供一种包含程序的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第一方面和/或第二方面所述的方法。

附图说明

图1为本申请实施例中IoT应用场景的示意图；

图2为本申请实施例中密钥协商方法的概述流程图；

图3为本申请实施例中设备A与设备B执行密钥协商的具体流程示意图；

图4为本申请实施例中LPN KEM参数图表；

图5为本申请实施例中基于DH KEM的密钥协商方法的具体流程示意图；

图6为本申请实施例中密钥协商装置的结构示意图之一；

图7为本申请实施例中密钥协商装置的结构示意图之二；

图8为本申请实施例中通信设备的结构示意图。

具体实施方式

下面结合附图，对本申请的实施例进行描述。

本申请实施例所提供的密钥协商方法可以应用于设备硬件能力受限的场景，比如智能家居、车辆网等物联网（Internet of Things，IoT）场景。

本申请实施例中涉及的通信主体可以为在计算、存储、通信和能耗等某一方面或多方面硬件能力受限的设备，具体可以是任何硬件实现的设备，或者软件实现的程序、应用，或其他组合实现的主体。且本申请中的通信主体需具有简单的输入、输出端口(I/O)，具体来说，设备输入端口可以是简单的键盘或按钮等，设备输出端口可以是简单的显示屏、灯

光颜色或灯光闪烁等。

本申请中的一种可能的应用场景为IoT场景。IoT是一种面向机器间通信（MTC, Machine-Type Communications）的网络，如图1所示，可以用来实现连接工业、连接出行、连续用户、连接城市以及连接设备等，未来可以主要应用在智能抄表、医疗检测监控、物流检测、工业检测监控、汽车联网、智能社区以及可穿戴设备等领域。本申请中涉及的通信主体可以为IoT终端，例如，IoT终端为通常安装在室内甚至地下室的电表水表，或者为了检测土壤湿度实现自动灌溉设置于土壤中的传感器，又或者为了监控奶牛健康状况佩戴在奶牛身上的检测仪器。因此，上述这类通信主体一般需要大规模部署，为了降低成本，这类通信主体的硬件配置一般不高，例如，某些IoT终端是通过电池来供电的，为了保证IoT终端的使用时间不需要经常更换电池，这就要求IoT终端能够以极低的电力消耗来工作，因此，其计算能力、存储能力等一般不高。

下面首先介绍本申请需要使用到的两个基本密码工具：KEM和承诺方案(Commitment Scheme)。

KEM可以包含如下三个算法：

（1）密钥生成算法KeyGen()：运行该算法可生成一对KEM公私钥对 (sk; pk)，其中，sk表示私钥，pk表示公钥。

（2）封装算法Encaps(pk)：对某个给定的KEM公钥pk，运行该算法输出(C,k)，其中k是一个原始密钥，而C是对k加密后的密文。

（3）解封装算法Decaps(sk; C)：对密文C和KEM私钥sk运行该算法，解密出原始密钥k。

更为详细的对KEM的解释和安全性定义，可参见ISO国际标准文档，这里不再过多赘述。

承诺方案可以包含如下两个算法：

（1）承诺算法Commit(m; r)：对输入消息m，该算法选择随机数r，然后运行该算法可以输出(F, t)，其中，F是对m的承诺值，而t是验证该承诺值的打开值(opening value)；

（2）打开算法Open(F; t)：运行该算法可以输出m，对所给的(F, t, m)，该算法可以验证承诺值F是否为对消息m关于打开值t的承诺。

另外，更为详细的对承诺方案的解释和安全性定义，可参见具体科研论文。

另外，本申请中的承诺方案还可以使用于哈希算法替换，其中，哈希算法是指密码意义上安全的哈希函数（hash function）。例如，可以用H(m, r)来代替上述承诺方案。也就是说，将m作为输入消息，选择随机数r，计算承诺值F=H(m, r)，并置打开值t=r。由于已有标准化的Hash函数，因此工程实现上更为方便。进一步地，会话密钥的生成也可以使用Hash函数，可以采用不同的Hash函数，也可以采用相同的Hash函数，这样更便于工程实现。

以下以两个通信主体包括第一设备和第二设备为例进行描述，第一设备和第二设备可以是任意两个需要进行密钥协商的设备，其中，第一设备发起与第二设备执行密钥协商。参阅图2所示，本申请实施例提供一种密钥协商方法，用以实现简便高效的量子安全密钥协商，该方法包括：

步骤201：第一设备采用密钥生成算法生成一个公私钥对。

一种可实现的方案中，第一设备可以采用KEM中包含的密钥生成算法生成该公私钥对。KEM可以为环上的带错误学习（Ring Learning With Error，RLWE）KEM，带噪音的学习奇偶（Learning Parity with Noise, LPN）KEM、我们数论家（Number Theorist aRe Us, NTRU）

KEM或DH KEM 中的任意一种。

步骤202：第一设备向第二设备发送公私钥对中的公钥。第一设备可以通过公开信道将该公钥发送给第二设备

步骤203：第二设备根据接收到的公钥采用封装算法选取原始密钥，根据原始密钥和公钥采用封装算法获得密文，根据第一比特串和随机数采用承诺算法获得承诺值和打开值，以及根据原始密钥中的部分比特确定第二比特串，根据第一比特串和第二比特串计算得到第一结果。

一种可实现的方案中，第二设备根据公钥采用KEM中包含的封装算法选取原始密钥，进一步根据原始密钥和公钥采用KEM中包含的封装算法获得密文。应理解的是，这里第二设备采用的封装算法与步骤201中第一设备采用的密钥生成算法属于相同的KEM。

第二设备可以随机生成第一比特串，将第一比特串作为输入消息，选择随机数，运行承诺算法获得承诺值和打开值；或者，第二设备选择随机数，对第一比特串和随机数运行哈希算法，得到承诺值，将随机数作为打开值。应理解的是，在本申请实施例的具体实施过程中，通信主体双方可以事先预定或预配置至少一种承诺方案或者至少一种哈希算法，且通信主体双方在进行密钥协商通信时采用相同的承诺方案或者哈希算法。

第二设备可以根据原始密钥中的部分比特确定第二比特串。其中，第二设备生成的第一比特串可以为长度为L比特的随机比特串，L可以在20-30范围之间。第二比特串的长度与第一比特串的长度相同，第二比特串为原始密钥中任意L位构成的比特串，例如，处于原始密钥中较高比特位上的连续L比特，或者处于原始密钥中较低比特位上的连续L比特，或者原始密钥中不连续的L比特，本申请实施例对第二比特串的确定方式不做限定。

第二设备可以根据第一比特串与第二比特串采用第一算法计算得到第一结果，第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。例如，第一算法为异或运算，第二设备可以根据第一比特串与第二比特串采用异或运算计算得到异或结果作为第一结果。应理解的是，第二设备还可通过上述所列第一算法外的算法将第一比特串和第二比特串“混合”起来，得到第一结果，本申请实施例对此不作限定。以下仅以对第一比特串与第二比特串采用异或运算得到异或结果作为第一结果为例进行说明。

步骤204：第二设备向第一设备发送密文和承诺值。第二设备这里可以通过公开信道将密文和承诺值发送给第一设备。

步骤205：第一设备获取第一结果。具体的，第一设备获取第一结果可以采用但不限于以下方案：

方案A：工作人员将步骤203中第二设备计算得到的第一结果，输入到第一设备上。例如，工作人员以人工的方式从第二设备上通过读、看或听等方式获取第一结果，然后在第一设备上输入该第一结果。这里要求第二设备具有简单的输出端口，而第一设备具有简单的输入端口。设备输出端口可以是简单的显示屏、灯光颜色、灯光闪烁或声音等，而设备输入端口可以是简单的键盘或按钮等。在一种可能的设计中，当第一比特串的长度为20~30比特，第二比特串的长度与第一比特串的长度相同，第一结果为第二设备根据第一比特串与第二比特串采用异或运算计算得到的异或结果，则第一结果的长度与第一比特串的长度相同，也为20~30比特，因此，工作人员进行输入操作并不繁琐，具有较好的可用性。

方案B：工作人员用第一设备扫描第二设备在步骤203中确定的第一结果所对应的二维

码或者其他标识，以使第一设备获取第一结果。

方案C：第一设备扫描第二设备在步骤203确定的第一结果对应的二维码或者其他标识。例如，第一设备可以自动移动至第二设备附近，利用第一设备上的摄像头采集第二设备的显示屏上显示的第一结果，或，第一结果对应的二维码或者其他标识，以使第一设备获取第一结果。

应理解的是，上述各个方案仅为举例，不作为本申请实施例的限定。本申请中假设第一设备获取第一结果的过程是较安全的，即攻击者无法获得第一结果。

步骤206：第一设备根据公私钥对中的私钥和接收到的密文采用解封装算法获得原始密钥，根据原始密钥中的部分比特确定第二比特串，以及根据第二比特串和第一结果计算得到第二结果。

一种可实现的方案中，第一设备可以根据公私钥对中的私钥和密文采用KEM中包含的解封装算法获得原始密钥。同理，第一设备采用的解封装算法，与步骤203中第二设备采用的封装算法，以及步骤201中第一设备采用的密钥生成算法属于相同的KEM。在本申请实施例的具体实施过程中，通信主体双方可以事先预定或预配置至少一种KEM，且通信主体双方在进行密钥协商通信时选择相同的KEM。例如，设备A采用 LPN KEM中的密钥生成算法生成一个公私钥对，并将该公私钥对中的公钥发送给设备B。设备B在接收到设备A发送的公钥后，采用LPN KEM中包含的封装算法，根据公钥选取原始密钥，并根据公钥和原始密钥获得密文，将密文发送给设备A。设备A在接收到设备B发送的密文后，采用LPN KEM中包含的解封装算法，根据密文和公私钥对中的私钥获得原始密钥。

应理解的是，为了保证第二设备确定的第二比特串与第一设备确定的第二比特串相同，第一设备确定第二比特串的方式与第二设备确定第二比特串的方式相同。进一步地，第一设备可以根据第二比特串与第一结果采用第二设备计算第一结果时采用的算法计算第二结果，例如，第二设备根据第一比特串和第二比特串采用异或运算计算得到第一结果，则第一设备根据第二比特串和第一结果采用异或运算计算得到第二结果。

步骤207：第一设备向第二设备发送第二结果。第一设备可以通过公开信道将第二结果发送给第二设备。

步骤208：第二设备从在第一比特串与第二结果相同的情况下，第二设备对第一设备认证成功。在第一比特串与第二结果不相同的情况下，第二设备对第一设备认证失败。此时，第一设备需要与第二设备重新执行密钥协商，第一设备可以重新生成一个公私钥对，重复执行上述步骤直至步骤208中第二设备对第一设备认证成功为止。

步骤209：第二设备向第一设备发送打开值。第二设备可以通过公开信道将打开值发送给第一设备。这里的打开值为上述步骤203中获得的打开值。

步骤210：第二设备生成用于与第一设备通信的会话密钥。第二设备可以根据第一设备的身份标识符、第二设备的身份标识符、公钥、密文、承诺值、打开值、原始密钥、第二结果中的一个或多个参数生成用于与第一设备通信的会话密钥，例如，第二设备可以根据第一设备的身份标识符、第二设备的身份标识符、公钥和原始密钥生成用于与第一设备通信的会话密钥。又例如，第二设备可以根据第一设备的身份标识符、第二设备的身份标识符、公钥、密文、承诺值、打开值、原始密钥、第二结果采用Hash函数生成用于与第一设备通信的会话密钥。

此外，在第二设备生成用于与第一设备通信的会话密钥后，第二设备可以删除公钥，

以节省第二设备的存储空间。当第二设备重新发起与第一设备执行密钥协商时，或者，当第二设备发起与第三设备执行密钥协商时，第二设备重新生成一个公私钥对，其中，第三设备为除第一设备外的任一设备。相较于现有技术中，通信主体双方需要保存公私钥对、口令等作为密钥协商和认证的材料，占用大量存储空间，在本申请实施例中，当第二设备生成用于与第一设备通信的会话密钥后，第二设备删除公钥，可以节省存储空间，因此，本申请实施例提供的方法更加适用于硬件能力受限的设备。

应理解的是，步骤209和步骤210的顺序可以调换或者两个步骤同时进行，本申请不限定这两个步骤的执行顺序。

步骤211：第一设备根据接收到的打开值和承诺值对第二设备进行认证，得到认证结果，认证结果用于指示第一设备对第二设备认证成功，并生成用于与第二设备通信的会话密钥。

若承诺值和打开值是第二设备根据第一比特串和随机数获得，则第一设备采用打开算法根据打开值和承诺值获得第三结果（即采用打开算法根据打开值和承诺值解出第一比特串），当第一设备确定第三结果与第二结果相同（即第一设备确定第一比特串与第二结果相同）时，则第一设备确定对第二设备认证成功。应理解的是，第二设备采用的承诺算法与第二设备采用的打开算法属于相同的承诺方案。

或者，若承诺值是第二设备采用哈希算法根据第一比特串和随机数获得，打开值为该随机数，则第一设备采用哈希算法根据打开值和第二结果生成第四结果（即重新生成一个承诺值），当第一设备确定第四结果与承诺值相同时（即第一设备确定两个承诺值相同），则第一设备确定对第二设备认证成功。应理解的是，第二设备采用的哈希算法与第一设备采用的哈希算法相同。

此外，第一设备生成的用于与第二设备通信的会话密钥，与第二设备生成的用于与第一设备通信的会话密钥相同，即两者采用相同的参数利用相同的函数生成相同的密钥。

在第一设备生成用于与第二设备通信的会话密钥后，第一设备也可以删除公私钥对。当第一设备发起与第二设备重新执行密钥协商时，第一设备重新生成一个公私钥对，采用新生成的公私钥对与第二设备进行密钥协商，以节省第一设备的存储空间。或者，当第一设备发起与第三设备执行密钥协商时，第一设备重新生成一个公私钥对，其中，第三设备为除第一设备外的任一设备。相较于现有技术中，通信主体双方需要保存公私钥对、口令等作为密钥协商和认证的材料占用大量存储空间，在本申请实施例中，当第一设备不保存公私钥对，可以节省存储空间，因此，本申请实施例提供的方法更加适用于硬件能力受限的设备。

下面以设备A与设备B的密钥协商过程为例，说明如图2所示实施例提供的密钥协商方法，具体如图3所示。

设备A可以采用KEM中包含的密钥生成算法生成随机的公私钥对(sk, pk),并可以通过公开信道将公钥pk发送给设备B，设备A保存私钥sk。

设备B可可以采用KEM中包含的封装算法根据公钥pk选取原始密钥k，根据原始密钥k和公钥pk计算得到密文C，并将原始密钥k的高比特上的连续L比特记为第二比特串K，计算第二比特串K与第一比特串S（长度为L的随机比特串）的异或结果作为第一结果E，其中，$E = K \oplus S$。工作人员可以通过从设备B读取第一结果E，然后在设备A上输入第一结果

E。同时，设备B计算采用承诺方案中包含的承诺算法，对第一比特串S执行承诺，选择随机数r，得到承诺值F和打开值t。设备B可以通过公开信道将密文C和承诺值F发送给设备A。

设备A可以根据私钥sk和密文C采用KEM中包含的解封装算法得到原始密钥k，并确定原始密钥k的高比特上的连续L比特作为第二比特串K，然后将第二比特串K和第一结果E进行异或运算得到第二结果S'，其中，$S' = K \oplus E$。设备A可以通过公开信道将第二结果S'发送给设备B。

设备B检查第二结果S'是否等于第一比特串S：若不相等，则可以确定对设备A认证失败，不再继续执行密钥协商；若相等，则可以确定对设备A认证成功，设备B可以通过公开信道将打开值t发送给设备A。

设备A在收到打开值t后，可以根据承诺值F和打开值t采用承诺方案中包含的打开算法得到第三结果S''。进一步地，设备A检查第三结果S''是否等于第二结果S'：若相等，则可以确定对设备B认证成功；若不相等，则可以确定对设备B认证失败。

若设备A和设备B都认证成功，最后双方计算出会话密钥SK=H(A||B||pk||C||F||S''||t||k)，其中，A和B分别表示设备A的身份标识符和设备B的身份标识符。A||B||pk||C||F||S''||t||k可视为会话识别号 (Session ID)。

另外，可以用Hash函数H(S, r)来代替上述承诺方案。具体的，设备B对第一比特串S进行承诺时，选择随机数r后计算承诺值F=H(S, r)，并置打开值t=r，而设备A收到打开值t后，若确定打开值t满足F=H(S', t)，或者计算第四结果F'=H(S', t)，确定F'=F，则可以确定对设备B认证成功。

下面结合具体KEM说明如图2和图3所示实施例的具体实施过程。

应理解的是，下面4个实施例仅对两个通信主体（以设备A和设备B为例）使用具体KEM的过程进行详细描述，其他过程与上述实施例类似，此处不再进行描述。

实施例1：KEM为RLWE KEM。

其中，该KEM为CRYSTALS提出的具体KEM 。CRYSTALS是美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）后量子密码竞赛的一个候选算法套件，包括加密、签名和密钥协商机制，该KEM是典型的格密码方案。

RLWE KEM工作在多项式环$R_q = Z_q[x]/(x^n + 1)$上，其中，q是一个素数，n是一个整数，x是多项式变量，Z_p表示模一个素数p的所有剩余类，即$Z_p = \{0,1,2,\dots,p-1\}$。$R_q$中每个元素是一个次数不超过n-1的多项式。另外，用χ表示R_q上的离散高斯分布(discrete Gaussian distribution)。RLWE KEM具体算法和使用描述如下：

密钥生成：设备A可以随机选取$s, e \in \chi^k$，并计算$b = As + e$，其中，k是一个正整数，而$A \in R_q^{kxk}$是一个k行k列的矩阵。设备A将s作为KEM私钥存储，将KEM公钥(A, b)发给设备B。

封装过程：设备B在收到KEM公钥(A, b)后，可以随机选取$t, f \in \chi^k$，并计算$c = A^T t + f$，将密文c发给设备A。这里密文c是对原始密钥$b^T t$的加密，$b^T t \in R_q$作为一个n-1次多项式，其每个系数的奇偶性就表示原始密钥的一个比特。

解封装过程：设备A在收到密文c后，可以使用KEM私钥s计算$s^T c \in R_q$，并将$s^T c$作为原始密钥。

上述KEM实现的一个关键问题是，$b^T t$和$s^T c$并不绝对相等，应理解的是，只要相关参数和向量选择合适，二者就可以非常接近。设备A在解封装时，需对密文和解密后的原始密钥进行适当的调和(reconciliation)，即一些近似和编码操作，从而可保证KEM解封装失败

的可能性非常低。

另外，为减少传输数据，在一种可能的设计中，KEM公钥(A, b)中包含的多项式矩阵A可以由一个256比特的随机种子按既定方法计算出来，这样设备A只需要给设备B发送随机数和b即可，而不必发送完整的矩阵A。

下面是NIST后量子密码算法标准化候选算法CRYSTALS给出的参数，可以作为本申请实施例的一种具体实现:

系统参数：n=256, q=7681=2^{13}-2^9+1, k=3。

对于上述系统参数，KEM公钥为1088字节(Bytes), KEM私钥为2400字节，密文为1184字节，原始密钥长度为256比特，解封装失败率为2^{-142}。

此外，上述设备A和设备B使用的KEM公私钥对是临时产生的、只用一次。所以，与现有技术中解密失败可能造成部分泄露私钥信息不同，这里KEM解封装失败只意味着通信双方需要再次产生并使用另一对KEM公私钥。因此，可以对上述系统参数进行优化，以适当增大解封装失败率为代价，减小KEM公私密钥及密文的大小，进而提高计算效率和通信效率。

实施例2：KEM为LPN KEM。

LPN KEM工作在二元域Z_2上。参数n, q, N, L, D均为正整数。参数n和q的选择需要适当保证LPN问题是困难的，n决定了密文的大小。N是纠错码C[N, L, D]码字的比特长度，也是编码后被封装信息的比特长度，其中，纠错码C[N, L, D]表示将长度为L比特的信息编码为N比特的码字，各有效码字间的海明距离(Hamming distance)至少是D，记Ber_τ为具有参数τ的贝努利分布(Bernouilli distribution)，即该分布以τ的概率输出1，而以1-τ的概率输出0。K是编码前信息的比特长度。对于所给的贝努利分布参数τ，参数D决定封装后的消息有多少错误可以被纠正。这里推荐可被纠错的错误不超过10%。具体LPN KEM算法和使用描述如下：

密钥生成：设备A可以随机选取矩阵$S \in Z_2^{n\times N}$、$A \in Z_2^{q\times n}$和$E \in \mathrm{Ber}_\tau^{q\times N}$，计算$B = AS + E$。随后，设备A将S作为KEM私钥存储，将KEM公钥(A, B)发送给设备B。

封装过程:设备B在收到KEM公钥(A, B)后，设备B可以选择随机向量$f \in \mathrm{Ber}_\tau^{q}$，将$f^TB \in Z_2^{1\times N}$作为原始密钥，计算并发送密文$u^T = f^TA$给设备A。

解封装过程：设备在A收到密文u^T后，可以根据KEM私钥S计算$u^TS \in Z_2^{1\times N}$，并将其作为原始密钥。

同样地，上述LPN KEM实现的一个关键问题是，u^TS和f^TB并不绝对相等。应理解的是，只要选择合适的相关参数，E和f分别为噪音矩阵和噪音向量，故而u^TS和f^TB二者的比特值非常接近的概率很大。事实上，$f^TB - u^TS = f^TE$的平均海明重量(Hamming weight)为$Nq\tau^2$，只要$Nq\tau^2 < D/2$，设备A计算得到的u^TS就能以高概率与设备B持有的原始密钥f^TB相同。

具体来讲，对于i比特的真正原始密钥c，设备B可以将其分成j块，每块长度为L比特（对最后一块进行填充）。这里，$(j-1)N < i \leq jN$。然后对每块使用纠错码C[N, L, D]将L比特编码为N比特的码字，将每个码字视为一个属于$Z_2^{1\times N}$的一行N列的行向量(即上述方案中的f^TB)，设备B可以使用上述KEM公钥将其封装后发送设备A。在收到所有j块封装信息后，设备A可以使用上述KEM私钥对所有j块进行解封装，然后利用纠错码C[N, L, D]解码各块，最后恢复出i比特长的真正原始密钥c。这里的关键是，需要选择合适参数使得封装和解封装的误差(即$f^TB - u^TS$)能够被纠错码C[N, L, D]将其视为错误后能以高概率纠正过来。

下面推荐两种方案能够实现正确纠错的概率至少为90%（也就是说，解封装失败率不超过10%）。

方案一：使用Golay码[23, 12, 7]传送140比特的真正原始密钥c。

首先，设备B可以将140比特的真正原始密钥c，拆分成12个块，每个块12比特(使用适当的方式填充最后一个块的4比特)。

随后，设备B可以将每个12比特的块使用Golay码[23, 12, 7]编码为23比特的码字，这样一共产生12个码字。

设备B再将这12个码字使用上述 KEM公钥分别进行封装，然后将所得到封装后的结果发给设备A。

设备A可以将收到的12个封装块先使用上述 KEM私钥进行解封装，然后对得到的结果按Golay码[23, 12, 7]进行解码、纠错，即可恢复出140比特的真正原始密钥c。

为保证设备A能正确纠错，即可恢复出正确的真正原始密钥c，推荐使用的LPN KEM参数(q, τ)见图4中的第一栏和第二栏。

若使用参数$(q = 512, \tau = 0.0029)$, n=512, 则传送140比特真正原始密钥相关性能指标如下：公钥为34240字节，私钥为1472字节，密文为64字节，解封装失败率为10%。

在一种可能的设计中，为了减少KEM公钥(A, B)中的A大小，设备B可以选择由一256比特的随机数种子生成A。这时，KEM公钥的变小为1504字节。

方案2：使用级联码(Concatenated Code)进行编码，传送140比特的真正原始密钥c。比如，可使用Reed-Solomon [15, 7, 9]作为外码和具有单比特纠错能力的Hamming [7, 4]作为内码。

首先，设备B可以将140比特的真正原始密钥c拆分成5个块，每个块28比特。

随后，设备B可以将每个28比特的块使用外码Reed-Solomon [15, 7, 9]进行编码。也就是说，将28比特视为7个4比特，每个4比特当作Reed-Solomon [15, 7, 9]的一个字母。这样，一个28比特的块将被编码为一个15x4=60比特的Reed-Solomon [15, 7, 9]码字。5个块一共编码为5个码字，长度为5x60=300比特。

接下来，设备B使用内码Hamming [7, 4]对上一步得到的5个Reed-Solomon码字中的每个字母(长度为4比特)进行编码，即将每个4比特的字母编码为7比特的Hamming [7, 4]码字。这样，5个块一共得到5x15=75个Hamming [7, 4]码字。

之后，设备B使用上述 KEM公钥，对这75个Hamming [7, 4]码字（共计5x15x7=525比特）进行封装，并将所得到的封装结果发给设备A。

设备A在收到上述封装结果后，可以先使用 KEM私钥进行解封装，然后对所得到的结果按内码Hamming [7, 4]进行解码、纠错，再按外码Reed-Solomon [15, 7, 9]进行解码、纠错，以恢复出140比特的真正原始密钥c。

为保证设备A能以不低于90%的概率正确纠错以复出正确的真正原始密钥c，推荐使用的LPN KEM参数(q, τ)见图3中的第一栏和第三栏。

若使用参数$(q = 512, \tau = 0.0063$, n=512, N=105, L=28), 则传送140比特真正原始密钥相关性能指标如下：KEM公钥为39488字节，KEM私钥为6720字节，密文为128字节，解封装失败率为10%。

实施例3：KEM为NTRU KEM。

其中，NTRU已经在IEEE 1394标准化，目前在IETF进行推标，同时也是NIST后量子标准化项目的一个候选算法。与RLWE KEM类似，NTRU也工作在多项式环$R_q = Z_q[x]/(x^n + 1)$上，其中q是一个素数，是系统参数，是已知和公开的，整数n表示待封装密钥或消息的比特长度。另外，用$R_{q,S}$表示R_q中所有小系数的多项式。NTRU KEM算法和使用如下：

密钥生成：设备A可以随机选取小系数多项式$g \in R_{q,S}$作为KEM私钥，计算$h = f/g \in R_q$为KEM公钥并将其发送给设备B，其中$f \in R_{q,S}$是另一个随机的小系数多项式。

封装过程：设备B在收到KEM公钥$h \in R_q$后，对于一个n比特的原始密钥$m \in Z_2^n$，将其各个比特视为系数为0或1的一个小系数多项式，设备B可以选取两随机多项式$r, e \in R_{q,S}$使得$m = e \bmod 2$,然后计算$c = 2hr + e \in R_q$并将c发给设备A。这里密文c即是对原始密钥m的加密。

解封装过程：设备A在收到c后，可以使用KEM私钥g计算$((cg \bmod q) \bmod 2)/g \in R_q$，并将该结果作为原始密钥。

同样的，上述NTRU KEM实现的一个关键问题是，$((cg \bmod q) \bmod 2)/g$和$e \bmod 2$并总是相等。应理解的是，只要相关参数选择合适，$g, f, r, e \in R_{q,S}$足够小，二者相等的概率就非常大。也就是说，经过适当的调和(reconciliation)，上述NTRU KEM解封装失败的可能性可以非常低。

根据NTRU所推荐的系统参数，对于128比特量子安全，上述NTRU KEM可使用如下参数：

系统参数：n=512, q=12289 (14比特)；小系数选取集合$\{0, \pm 1, \pm 2, \cdots, \pm 12\}$中的元素。

对于上述系统参数，KEM公钥为896字节，KEM私钥为320字节，密文为896字节，而被封装的原始密钥长度为512比特，解封装失败率小于2^{-30}。其中，128比特量子安全是密码强度的概念，相当于要破解这个密码系统，需要做2的128次方个密码操作。

若原始密钥的长度更长，也可以在上述系统参数中将n设置为1024。

实施例4：KEM是DH (Diffie-Hellman) KEM。

与上述三个实施例不同，由于DH问题在量子计算下不再安全，所以采用DH KEM的密钥协商方法不是量子安全的。但该方法仍具有现实意义。具体的现实意义可以包括但不限于以下方面：第一，在量子计算机成为现实前，该方法是安全的，所以可在合适的场景使用。第二，与上述三个基于格密码的实施例相比，采用DH KEM的密钥协商方法对应的KEM公私钥长度都会大幅度降低，变为格密码的1/4到1/30，通信效率显著提升。

其中，令p为素数，G是某p阶乘法群，$g \in G$为群G的一个生成元。H()为一安全的hash函数，其输出为κ比特。基于DH KEM的密钥协商方法如图5所示，具体描述如下：

设备A可以随机选取$x \in Z_p$作为KEM私钥，计算KEM公钥$X = g^x \in G$并通过公开信道将X发送给设备B，设备A保存KEM私钥x。

设备B在接收到KEM公钥X后，可以随机选取$y \in Z_p$，置原始密钥为$k = H(X^y)$，计算密钥封装值$C = Y = g^y \in G$。设备B确定k的高比特l位K和长度为l比特的随机比特串S的异或结果E (即E=K⊕S) 。设备A获取E（具体可以采用步骤105提供的任一方案）。设备B可以选择随机数$r \in \{0,1\}^{4\kappa}$，计算$F = H(S, r)$作为对S的承诺值，并通过公开信道将(Y, F)发送给设备A。

设备A使用KEM私钥x解密Y得到k，即$k = H(Y^x)$，根据k得到K，然后将K和E进行异或

运算得到S’(即S'=K⊕E)，将S’发送给设备B。

设备B检查S’是否等于S：若不相等，则不再继续执行密钥协商；若相等，即对设备A认证成功，并将承诺打开值r发送给设备A。

设备A在收到检查r后，检查F是否等于H(S′,r)：若相等，则设备A对设备B认证成功；若不相等，则设备A对设备B认证失败。

若设备A和设备B都认证成功，最后双方计算出会话密钥SK=H(A||B||X||Y||F||S’||r||k)。与常规基于离散对数问题的密码系统(比如数字签名算法标准(Digital Signature Algorithm，DSA)标准签名，施诺（Schnorr）签名，艾伽马（ElGamal）加密)类似，上述DH KEM有两种典型参数选择：剩余类群和椭圆曲线上的群。具体来说，上述方案中的群G可选为有限域Z_q的一个p阶乘法子群，其中p和q都是素数，且p|q-1。p的比特长度一般可选择1024，1536或2048，q的比特长度可为128或256。或者，G可以是基于256比特的椭圆曲线群，而q的比特长度可为128或256。

由上述各个实施例可知，本申请实施例提供的方法只在协商时生成和使用一个临时的KEM公钥对，通信双方共执行2次KEM加解密操作，以及一些简单的承诺操作。因此，与现有技术中提到的Kyber协议和系统参数优化后的量子协议相比，在一定程度保证安全的情况下效率提高明显，且实施简便。

本申请实施例提供的方法具有严格的可证明安全性。具体来说，如果其中所使用的KEM和承诺方案都是安全的，则本申请实施例提供的方法在标准模型下是安全的；如果其中所使用的KEM和Hash函数都是安全的，则本申请实施例提供的方法在随机预言模型(random oracle)下是安全的。另外，若所使用的KEM还是量子安全的，则本申请实施例提供的方法是量子安全的。

基于以上实施例，本申请实施例提供一种密钥协商装置600，在一种示例下，所述密钥协商装置600可以被包括于密钥协商系统中的第一设备中，如图6所示，该装置600包括：

处理单元610，用于采用密钥生成算法生成一个公私钥对；

收发单元620，用于向第二设备发送所述公私钥对中的公钥，接收密文和承诺值，所述密文是根据所述公钥和原始密钥采用封装算法获得的，所述原始密钥是根据所述公钥采用所述封装算法选取的，所述承诺值是根据第一比特串和随机数采用承诺算法获得的，所述第一比特串为随机比特串；

所述收发单元620，还用于获取第一结果，所述第一结果是根据所述第一比特串和第二比特串计算得到的，所述第二比特串是根据所述原始密钥中的部分比特确定的；

所述处理单元610，还用于根据所述公私钥对中的私钥和所述密文采用解封装算法获得所述原始密钥，并根据所述原始密钥中的所述部分比特确定所述第二比特串；根据所述第二比特串和所述第一结果计算得到第二结果；

所述收发单元620，还用于向所述第二设备发送所述第二结果；接收打开值，其中，所述打开值是在所述第一比特串与所述第二结果相同的情况下所述第二设备向所述第一设备发送的，所述打开值是根据所述第一比特串和所述随机数采用所述承诺算法获得的；

所述处理单元610，还用于根据所述打开值和所述承诺值对所述第二设备进行认证，得到认证结果，所述认证结果用于指示所述第二设备对所述第二设备认证成功，并生成用于与所述第二设备通信的会话密钥。

在一种可能的设计中，所述处理单元610，具体用于：

采用第一算法对所述第二比特串和所述第一结果进行计算，以得到第二结果；

所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

在一种可能的设计中，所述处理单元610，还用于：

在生成用于与所述第二设备通信的会话密钥后，删除所述公私钥对；当发起与所述第二设备重新执行密钥协商，或者，当发起与第三设备执行密钥协商，重新生成一个公私钥对。

在一种可能的设计中，所述处理单元610，具体用于：

根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第二设备通信的会话密钥。

基于以上实施例，本申请实施例提供一种密钥协商装置700，在一种示例下，所述密钥协商装置700可以被包括于密钥协商系统中的第二设备中，如图7所示，该装置700包括：

收发单元710，用于接收公钥，所述公钥为采用密钥生成算法生成的一个公私钥对中的公钥；

处理单元720，用于根据所述公钥采用所述封装算法选取原始密钥，根据所述公钥和所述原始密钥采用所述封装算法获得密文，以及根据第一比特串和随机数采用承诺算法获得承诺值和打开值；所述收发单元710，还用于向所述第一设备发送所述密文和所述承诺值，所述第一比特串为随机比特串；

所述处理单元720，还用于根据所述原始密钥中的部分比特确定第二比特串，根据所述第一比特串和所述第二比特串计算得到第一结果；

所述收发单元710，还用于：接收第二结果，所述第二结果是根据所述第二比特串和所述第一结果计算得到的；

所述处理单元720，还用于：在所述第一比特串与所述第二结果相同的情况下，生成用于与所述第一设备通信的会话密钥，其中所述第一比特串与所述第二结果相同表示所述第二设备对所述第一设备认证成功；所述收发单元710，还用于向所述第一设备发送所述打开值。

在一种可能的设计中，所述处理单元720，具体用于：

采用第一算法对所述第一比特串和所述第二比特串进行计算，以得到第一结果；

所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

在一种可能的设计中，所述处理单元720，还用于：

在生成用于与所述第一设备通信的会话密钥后，删除所述公钥；当发起与所述第一设备重新执行密钥协商，或者，当发起与第三设备执行密钥协商，生成一个公私钥对。

在一种可能的设计中，所述处理单元720，具体用于：

根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第一设备通信的会话密钥。

可以理解的，关于图6和图7的密钥协商装置包括的功能模块的具体实现方式及相应的有益效果，可参考前述图2所示实施例的具体介绍，这里不赘述。

应理解以上各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。且这些单元可以全部以软件通过处理元件调用的形式实现；也可以全部以硬件的形式实现，还可以部分单元以软件通过处理元件调用的形式实现，部分单元以硬件的形式实现。在实现过程中，上述方法的各步骤或以上各个单元可以通过处理器元件中的硬件的集成逻辑电路或者软件形式的指令完成。

例如，以上这些单元可以是被配置成实施以上方法的一个或多个集成电路，例如：一个或多个特定集成电路（Application Specific Integrated Circuit，ASIC），或，一个或多个微处理器（digital signal processor，DSP），或，一个或者多个现场可编程门阵列（Field Programmable Gate Array，FPGA）等。再如，当以上某个单元通过处理元件调度程序的形式实现时，该处理元件可以是通用处理器，例如中央处理器（Central Processing Unit，CPU）或其它可以调用程序的处理器。再如，这些单元可以集成在一起，以片上系统（system-on-a-chip，SOC）的形式实现。

作为另一种可选的变形，本申请实施例提供一种密钥协商装置，示例性地，可以为一种芯片，该装置包括处理器和接口，该接口可以为输入/输出接口。其中，处理器完成上述图6中处理单元610，接口完成上述图6中收发单元620。或处理器完成上述图7中处理单元720的功能，接口完成上述图7中收发单元710的功能。该装置还可以包括存储器，存储器用于存储可在处理器上运行的程序，处理器执行该程序时实现上述如图2所示实施例的方法。

基于以上实施例，本申请实施例还提供了一种通信设备，参阅图8所示，该通信设备800中包括：收发器801、处理器802、存储器803。其中，存储器803用于存储计算机程序；处理器802调用存储器803存储的计算机程序，通过收发器801执行上述如图2所示的方法实施例中第一设备的步骤或第二设备的步骤。其中，处理器可以是CPU，网络处理器（network processor，NP），硬件芯片或者其任意组合。存储器可以包括易失性存储器（volatile memory），例如随机存取存储器（random access memory，RAM），也可以包括非易失性存储器（non-volatile memory），例如只读存储器（read-only memory，ROM），快闪存储器（flash memory），硬盘（hard disk drive，HDD）或固态硬盘（solid-state drive，SSD），存储器还可以包括上述种类的存储器的组合。

可以理解的，上述图6或图7所示实施例中的装置可以以图8所示的通信设备800实现。具体的，图6中处理单元610可以由处理器802实现，收发单元620可以由收发器801实现。图7中处理单元720可以由处理器802实现，收发单元710可以由收发器801实现。通信结构800的结构并不构成对本申请实施例的限定。

本申请实施例提供一种密钥协商系统，包括第一设备和第二设备。示例性地，该系统可以包括两个如图8所示的通信设备，其中，一个设备用于执行上述如图2所示的方法实施例中第一设备的步骤，另一个设备用于执行上述如图2所示的方法实施例中第二设备的步骤。

本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，当该计算机程序在计算机上运行时，使得计算机执行上述如图2所示实施例的方法。

综上所述，本申请实施例提供的方法只在协商时生成和使用一个临时的KEM公钥对，

通信双方共执行2次KEM加解密操作，以及一些简单的承诺操作。因此，与现有技术中提到的Kyber协议和系统参数优化后的量子协议相比，在一定程度保证安全的情况下效率提高明显，且实施简便。

另外，目前量子安全的密码系统公私钥尺寸都比较大，这些量子安全AKE需要通信双方持有长期使用的量子安全公私密钥对，对设备的存储能力也是一个挑战。但本申请实施例提供的方法不需要存储公私密钥对，每次密钥协议所用到的KEM公私密钥对都是临时的，一次使用完后即可删除，可以有效节省设备的存储空间。

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

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

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

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

显然，本领域的技术人员可以对本申请实施例进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权利要求

1、一种密钥协商系统，其特征在于，包括第一设备和第二设备，其中：

所述第一设备用于采用密钥生成算法生成一个公私钥对，向所述第二设备发送所述公私钥对中的公钥；

所述第二设备用于根据接收到的所述公钥采用封装算法选取原始密钥，根据所述公钥和所述原始密钥采用所述封装算法获得密文，以及根据第一比特串和随机数采用承诺算法获得承诺值和打开值，向所述第一设备发送所述密文和所述承诺值，所述第一比特串为随机比特串；以及，根据所述原始密钥中的部分比特确定第二比特串，根据所述第一比特串和所述第二比特串计算得到第一结果；

所述第一设备还用于根据所述公私钥对中的私钥和接收到的所述密文采用解封装算法获得所述原始密钥，并根据所述原始密钥中的所述部分比特确定所述第二比特串；根据所述第二比特串和所述第一结果计算得到第二结果，向所述第二设备发送所述第二结果；

所述第二设备还用于在所述第一比特串与接收到的所述第二结果相同的情况下，向所述第一设备发送所述打开值并生成用于与所述第一设备通信的会话密钥，其中所述第一比特串与所述第二结果相同表示所述第二设备对所述第一设备认证成功；

所述第一设备还用于根据接收到的所述打开值和所述承诺值对所述第二设备进行认证，得到认证结果，所述认证结果用于指示所述第一设备对所述第二设备认证成功，并生成用于与所述第二设备通信的会话密钥。

2、如权利要求1所述的系统，其特征在于，所述第二设备具体用于采用第一算法对所述第一比特串和所述第二结果进行计算，以得到第一结果；

所述第一设备具体用于采用所述第一算法对所述第二比特串和所述第一结果进行计算，以得到第二结果；

所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

3、如权利要求1或2所述的系统，其特征在于，所述第一设备还用于在所述第一设备生成用于与所述第二设备通信的会话密钥后，删除所述公私钥对；当发起与所述第二设备重新执行密钥协商，或者，当发起与第三设备执行密钥协商，重新生成一个公私钥对。

4、如权利要求1-3任一项所述的系统，其特征在于，所述第二设备还用于在所述第二设备生成用于与所述第一设备通信的会话密钥后，删除所述公钥；当发起与所述第一设备重新执行密钥协商，或者，当发起与第四设备执行密钥协商，生成一个公私钥对。

5、如权利要求1-4任一项所述的系统，其特征在于，所述第一设备具体用于根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第二设备通信的会话密钥；

所述第二设备具体用于根据所述一个或多个参数生成用于与所述第一设备通信的会话密钥，其中，用于与所述第二设备通信的会话密钥与用于与所述第一设备通信的会话密钥相同。

6、一种密钥协商方法，其特征在于，包括：

第一设备采用密钥生成算法生成一个公私钥对，向第二设备发送所述公私钥对中的公钥；

所述第一设备接收密文和承诺值，所述密文是根据所述公钥和原始密钥采用封装算法获得的，所述原始密钥是根据所述公钥采用所述封装算法选取的，所述承诺值是根据第一比特串和随机数采用承诺算法获得的，所述第一比特串为随机比特串；

所述第一设备获取第一结果，所述第一结果是根据所述第一比特串和第二比特串计算得到的，所述第二比特串是根据所述原始密钥中的部分比特确定的；

所述第一设备根据所述公私钥对中的私钥和所述密文采用解封装算法获得所述原始密钥，并根据所述原始密钥中的所述部分比特确定所述第二比特串；

所述第一设备根据所述第二比特串和所述第一结果计算得到第二结果，向所述第二设备发送所述第二结果；

所述第一设备接收打开值，其中，所述打开值是在所述第一比特串与所述第二结果相同的情况下所述第二设备向所述第一设备发送的，所述打开值是根据所述第一比特串和所述随机数采用所述承诺算法获得的；

所述第一设备根据所述打开值和所述承诺值对所述第二设备进行认证，得到认证结果，所述认证结果用于指示所述第二设备对所述第二设备认证成功，并生成用于与所述第二设备通信的会话密钥。

7、如权利要求6所述的方法，其特征在于，所述第一设备根据所述第二比特串和所述第一结果计算得到第二结果，包括：

所述第一设备采用第一算法对所述第二比特串和所述第一结果进行计算，以得到第二结果；

所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

8、如权利要求6或7所述的方法，其特征在于，在所述第一设备生成用于与所述第二设备通信的会话密钥后，还包括：

所述第一设备删除所述公私钥对；

当所述第一设备发起与所述第二设备重新执行密钥协商，或者，当所述第一设备发起与第三设备执行密钥协商，所述第一设备重新生成一个公私钥对。

9、如权利要求6-8任一项所述的方法，其特征在于，所述第一设备生成用于与所述第二设备通信的会话密钥，包括：

所述第一设备根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第二设备通信的会话密钥。

10、一种密钥协商方法，其特征在于，包括：

第二设备接收公钥，所述公钥为采用密钥生成算法生成的一个公私钥对中的公钥；

所述第二设备根据所述公钥采用所述封装算法选取原始密钥，根据所述公钥和所述原始密钥采用所述封装算法获得密文，以及根据第一比特串和随机数采用承诺算法获得承诺值和打开值，向所述第一设备发送所述密文和所述承诺值，所述第一比特串为随机比特串；

所述第二设备根据所述原始密钥中的部分比特确定第二比特串，根据所述第一比特串和所述第二比特串计算得到第一结果；

所述第二设备接收第二结果，所述第二结果是根据所述第二比特串和所述第一结果计算得到的；

所述第二设备在所述第一比特串与所述第二结果相同的情况下，向所述第一设备发送所述打开值，并生成用于与所述第一设备通信的会话密钥，其中所述第一比特串与所述第二结果相同表示所述第二设备对所述第一设备认证成功。

11、如权利要求10所述的方法，其特征在于，所述第二设备根据所述第一比特串和所述第二比特串计算得到第一结果，包括：

所述第二设备采用第一算法对所述第一比特串和所述第二比特串进行计算，以得到第一结果；

所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

12、如权利要求10或11所述的方法，其特征在于，在所述第二设备生成用于与所述第一设备通信的会话密钥后，还包括：

所述第二设备删除所述公钥；

当所述第二设备发起与所述第一设备重新执行密钥协商，或者，当所述第二设备发起与第三设备执行密钥协商，所述第二设备生成一个公私钥对。

13、如权利要求10-12任一项所述的方法，其特征在于，所述第二设备生成用于与所述第二设备通信的会话密钥，包括：

所述第二设备根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第一设备通信的会话密钥。

14、一种密钥协商装置，其特征在于，包括：

处理单元，用于采用密钥生成算法生成一个公私钥对；

收发单元，用于向第二设备发送所述公私钥对中的公钥，接收密文和承诺值，所述密文是根据所述公钥和原始密钥采用封装算法获得的，所述原始密钥是根据所述公钥采用所述封装算法选取的，所述承诺值是根据第一比特串和随机数采用承诺算法获得的，所述第一比特串为随机比特串；

所述收发单元，还用于获取第一结果，所述第一结果是根据所述第一比特串和第二比特串计算得到的，所述第二比特串是根据所述原始密钥中的部分比特确定的；

所述处理单元，还用于根据所述公私钥对中的私钥和所述密文采用解封装算法获得所述原始密钥，并根据所述原始密钥中的所述部分比特确定所述第二比特串；根据所述第二比特串和所述第一结果计算得到第二结果；

所述收发单元，还用于向所述第二设备发送所述第二结果；接收打开值，其中，所述打开值是在所述第一比特串与所述第二结果相同的情况下所述第二设备向所述第一设备发送的，所述打开值是根据所述第一比特串和所述随机数采用所述承诺算法获得的；

所述处理单元，还用于根据所述打开值和所述承诺值对所述第二设备进行认证，得到认证结果，所述认证结果用于指示所述第二设备对所述第二设备认证成功，并生成用于与所述第二设备通信的会话密钥。

15、如权利要求14所述的方法，其特征在于，所述处理单元具体用于：

采用第一算法对所述第二比特串和所述第一结果进行计算，以得到第二结果；

所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

16、如权利要求14或15所述的装置，其特征在于，所述处理单元，还用于：

在生成用于与所述第二设备通信的会话密钥后，删除所述公私钥对；当发起与所述第二设备重新执行密钥协商，或者，当发起与第三设备执行密钥协商，重新生成一个公私钥对。

17、如权利要求14-16任一项所述的装置，其特征在于，所述处理单元，具体用于：

根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第二设备通信的会话密钥。

18、一种密钥协商装置，其特征在于，包括：

收发单元，用于接收公钥，所述公钥为采用密钥生成算法生成的一个公私钥对中的公钥；

处理单元，用于根据所述公钥采用所述封装算法选取原始密钥，根据所述公钥和所述原始密钥采用所述封装算法获得密文，以及根据第一比特串和随机数采用承诺算法获得承诺值和打开值；所述收发单元，还用于向所述第一设备发送所述密文和所述承诺值，所述第一比特串为随机比特串；

所述处理单元，还用于根据所述原始密钥中的部分比特确定第二比特串，根据所述第一比特串和所述第二比特串计算得到第一结果；

所述收发单元，还用于：接收第二结果，所述第二结果是根据所述第二比特串和所述第一结果计算得到的；

所述处理单元，还用于：在所述第一比特串与所述第二结果相同的情况下，生成用于与所述第一设备通信的会话密钥，其中所述第一比特串与所述第二结果相同表示所述第二设备对所述第一设备认证成功；所述收发单元，还用于向所述第一设备发送所述打开值。

19、如权利要求18所述的装置，其特征在于，所述处理单元，具体用于：

采用第一算法对所述第一比特串和所述第二比特串进行计算，以得到第一结果；

所述第一算法为异或运算、模加法运算、模减法运算、模乘法运算中的任意一种运算或多种运算的组合。

20、如权利要求18或19所述的装置，其特征在于，所述处理单元，还用于：

在生成用于与所述第一设备通信的会话密钥后，删除所述公钥；当发起与所述第一设备重新执行密钥协商，或者，当发起与第三设备执行密钥协商，生成一个公私钥对。

21、如权利要求18-20任一项所述的装置，其特征在于，所述处理单元，具体用于：

根据所述第一设备的身份标识符、所述第二设备的身份标识符、所述公钥、所述密文、所述承诺值、所述打开值、所述原始密钥、所述第二结果中的一个或多个参数生成用于与所述第一设备通信的会话密钥。

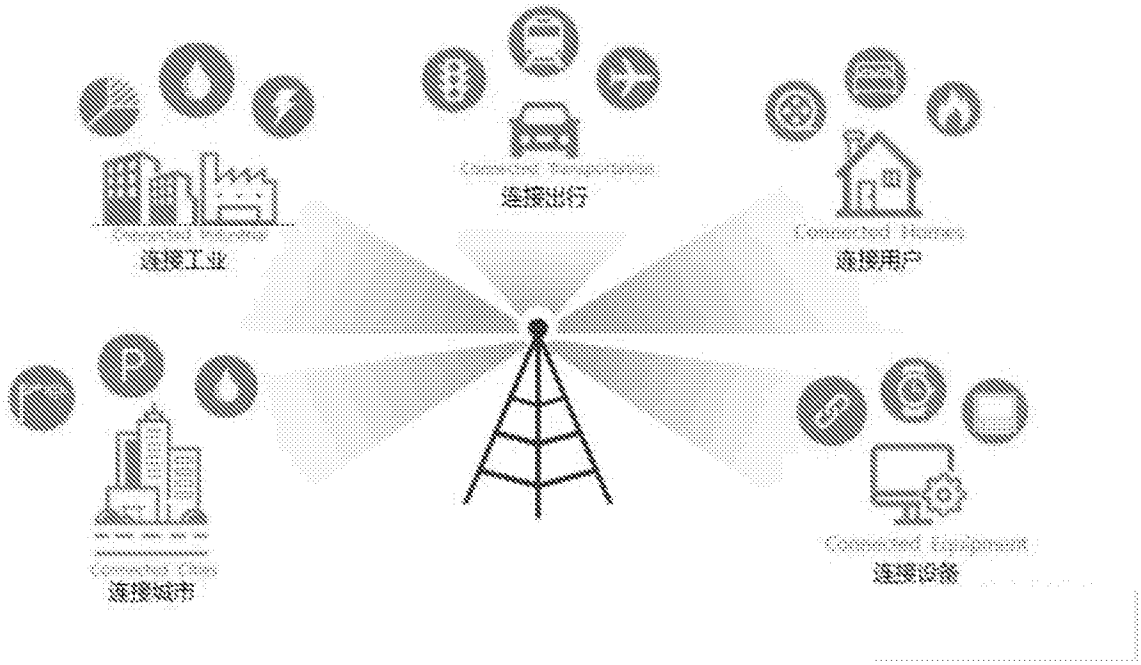


图 1

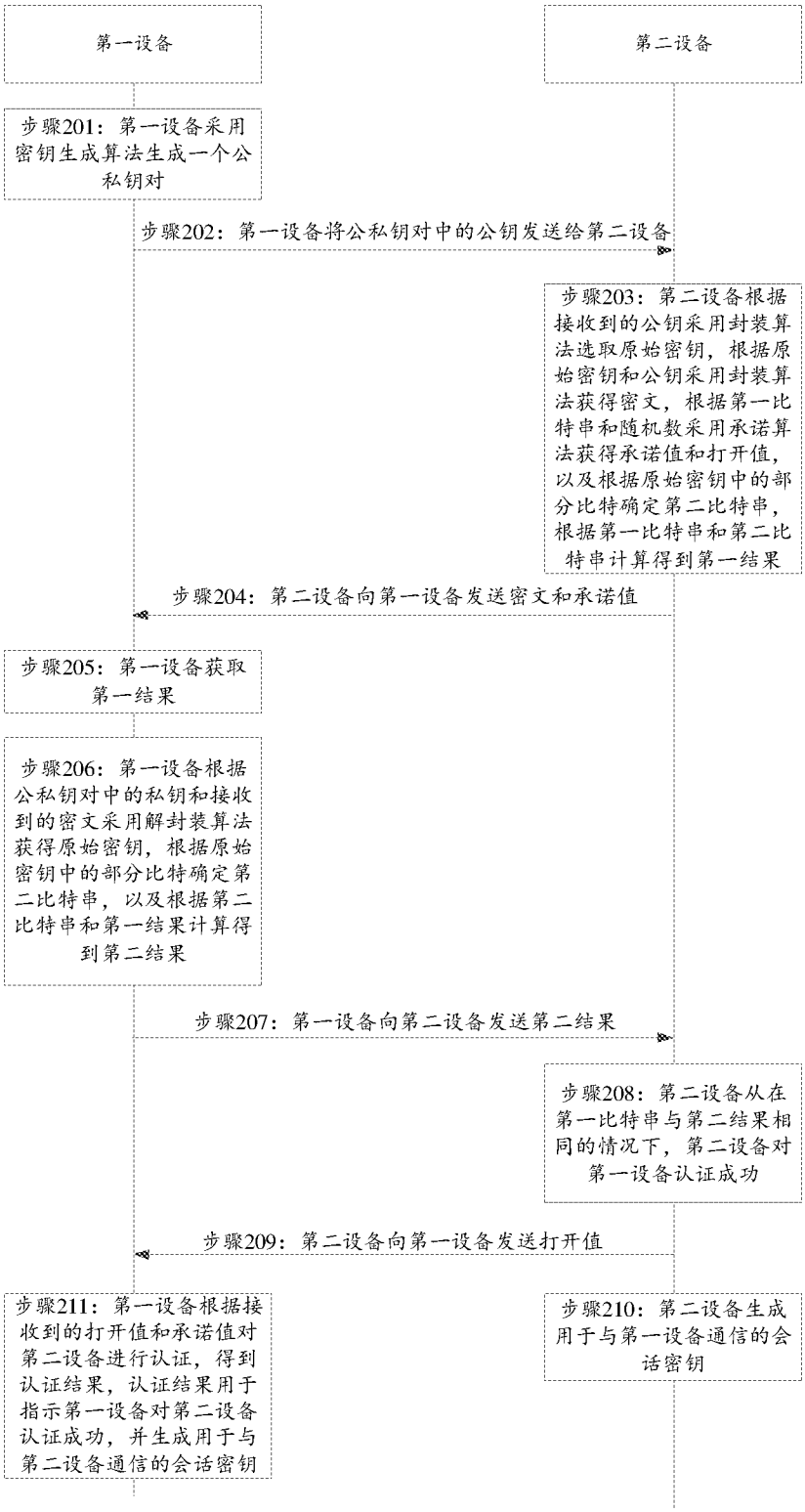

第一设备
第二设备
步骤201：第一设备采用密钥生成算法生成一个公私钥对
步骤202：第一设备将公私钥对中的公钥发送给第二设备
步骤203：第二设备根据接收到的公钥采用封装算法选取原始密钥，根据原始密钥和公钥采用封装算法获得密文，根据第一比特串和随机数采用承诺算法获得承诺值和打开值，以及根据原始密钥中的部分比特确定第二比特串，根据第一比特串和第二比特串计算得到第一结果
步骤204：第二设备向第一设备发送密文和承诺值
步骤205：第一设备获取第一结果
步骤206：第一设备根据公私钥对中的私钥和接收到的密文采用解封装算法获得原始密钥，根据原始密钥中的部分比特确定第二比特串，以及根据第二比特串和第一结果计算得到第二结果
步骤207：第一设备向第二设备发送第二结果
步骤208：第二设备从在第一比特串与第二结果相同的情况下，第二设备对第一设备认证成功
步骤209：第二设备向第一设备发送打开值
步骤211：第一设备根据接收到的打开值和承诺值对第二设备进行认证，得到认证结果，认证结果用于指示第一设备对第二设备认证成功，并生成用于与第二设备通信的会话密钥
步骤210：第二设备生成用于与第一设备通信的会话密钥

图 2

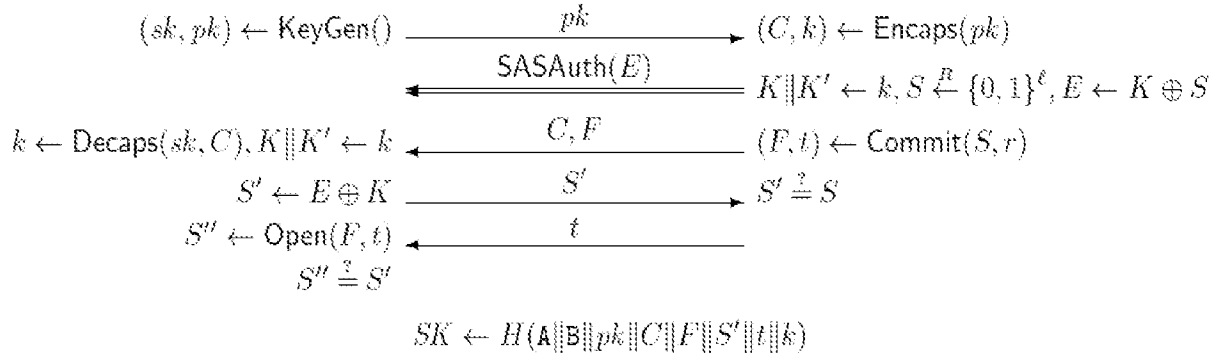


图 3

q	τ	
	Golay Code	Hamming+RS
512	0.0029	0.0063
1024	0.0021	0.0044
2048	0.0015	0.0031
4096	0.0011	0.0022
8192	0.00074	0.0016

图 4

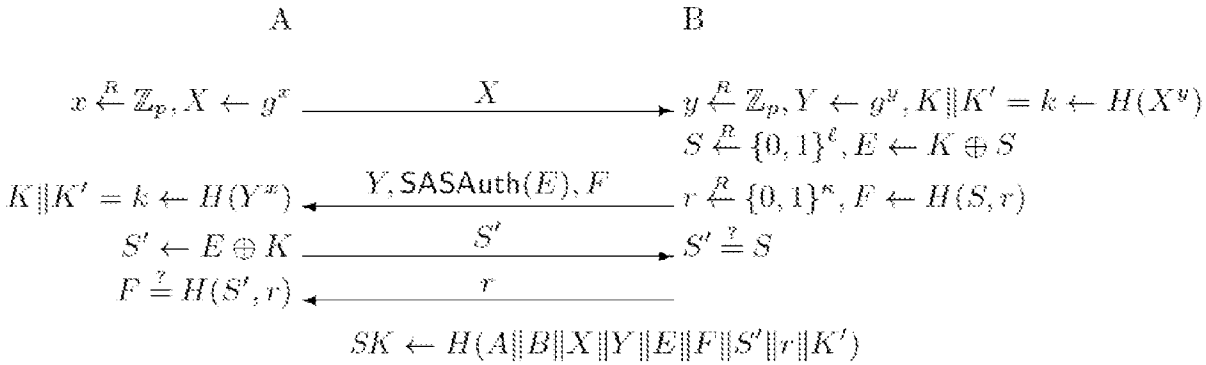


图 5

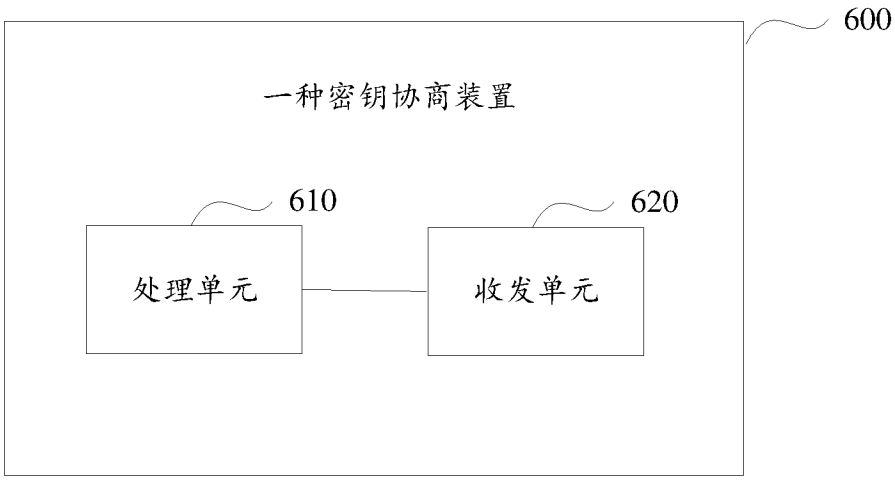

600
一种密钥协商装置
610
620
处理单元
收发单元

图 6

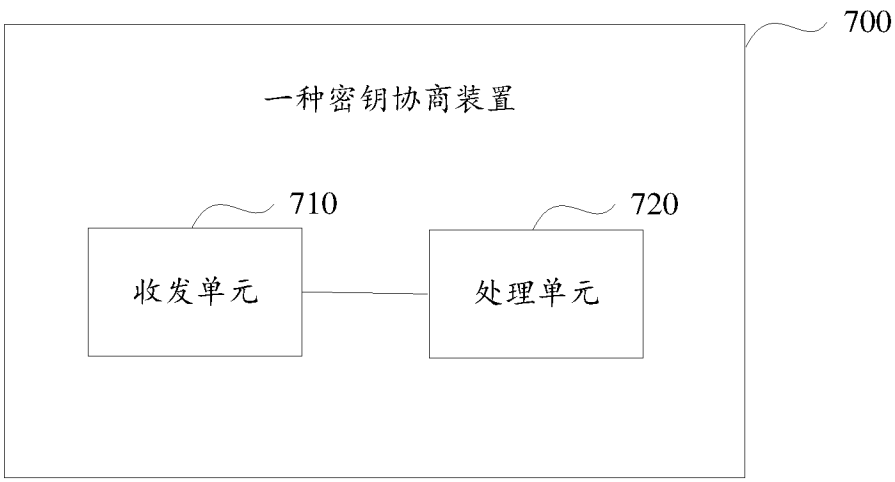

700
一种密钥协商装置
710
720
收发单元
处理单元

图 7

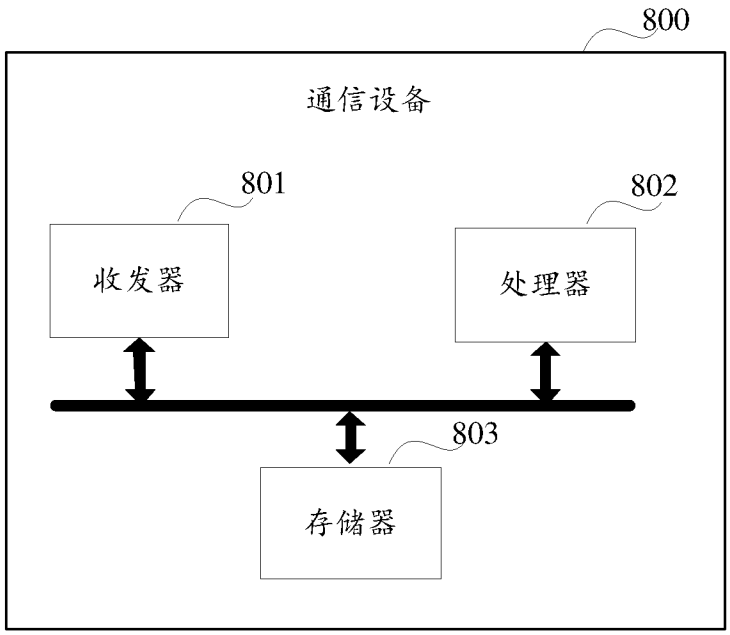


图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2018/050266

A. CLASSIFICATION OF SUBJECT MATTER

SEE EXTRA BOX

According to International Patent Classification (IPC)

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

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)

FAMPAT, INCOPAT, IEEE: key, password, exchange, distribution, negotiation, authentication, validation, match, compare, public key, private, key, commitment, encapsulate, bit string, same, consistent, identical, quantum, mutual, XOR, hash, mod, random, open value, 密钥, 协商, 交换, 公钥, 私钥, 封装, 承诺, 打开, 比特串, 随机数, 认证, 匹配, 配对, 相互, 互相, 双向, 相同, 一样, 符合, and other relevant key terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 107948189 A (GLOBAL DIGITAL CYBERSECURITY AUTHORITY CO., LTD.), 20 April 2018, original document, figure 8, and paragraphs [0042], [0064]-[0066], [0071]-[0075], [0141]-[0144] and [0192]-[0196]	1-21
A	US 2010/0017602 A1 (BUSSARD, L. et al.), 21 January 2010, entire document	

☒ 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 the issuance of the international search report
27 August 2018 *(day/month/year)*	04 September 2018 *(day/month/year)*

Name and mailing address of the ISA/SG

IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE
Intellectual Property Office of Singapore
No. 51, Bras Basah Road
Manulife Centre#01 01
Singapore 189554
E-mail: pct@ipos.gov.sg

Authorized officer

HONG, Lei (doctor)

IPOS Telephone No. (+65) 6339 8616

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2018/050266

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 106603485 A (MIDEA SMART TECHNOLOGY CO., LTD.), 26 April 2017, entire original document	
A	CN 104980928 A (HUAWEI DEVICE CO., LTD.), 14 October 2015, entire original document	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2018/050266

EXTRA BOX

(CLASSIFICATION OF SUBJECT MATTER)

International Class Number:

H04L 9/32 (2006.01)

H04L 9/14 (2006.01)

H04L 9/28 (2006.01)

G06F 21/31 (2013.01)

H04L 29/06 (2006.01)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG2018/050266

Note: related known patent family members of the patent documents referred to by this international search report are listed in this annex. This authority only provides information on the related patent family members, and assumes no responsibility for the details of the patents.

Patent Documents referred in the Report	Publication Date/Announcement Date (day/month/year)	Patent Family	Publication Date/Announcement Date (day/month/year)
CN 107948189 A	20/04/2018	None	
US 2010/0017602 A1	21/01/2010	None	
CN 106603485 A	26/04/2017	None	
CN 104980928 A	14/10/2015	EP 3119119 A1 WO 2015/149723 A1 US 2017/0026174 A1	18/01/2017 08/10/2015 26/01/2017

国际检索报告

国际申请号

PCT/SG2018/050266

A. 主题的分类

请参照附加栏

按照国际专利分类(IPC)

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; G06F

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))

FAMPAT, INCOPAT, IEEE: key, password, exchange, distribution, negotiation, authentication, validation, match, compare, public key, private, key, commitment, encapsulate, bit string, same, consistent, identical, quantum, mutual, XOR, hash, mod, random, open value, 密钥, 协商, 交换, 公钥, 私钥, 封装, 承诺, 打开, 比特串, 随机数, 认证, 匹配, 配对, 相互, 互相, 双向, 相同, 一样, 符合, 以及其他相关关键词

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
A	CN 107948189 A (数安时代科技股份有限公司) 2018 年 04 月 20 日 原文中的图 8 及段落 [0042], [0064]-[0066], [0071]-[0075], [0141]-[0144], [0192]-[0196]	1-21
A	US 2010/0017602 A1 (BUSSARD L. ET AL.) 2010 年 01 月 21 日 全文	

☒ 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	国际检索报告发文日
2018 年 08 月 27 日	04/09/2018
ISA/SG 的名称和邮寄地址 **新加坡知识产权局** IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE 勿拉士巴沙路 51 号 宏利中心#01-01 新加坡 189554 电子邮件账号: pct@ipos.gov.sg	受权官员 洪 磊 (博士) IPOS 客服电话号码: (+65) 6339 8616

国际检索报告

国际申请号

PCT/SG2018/050266

C (续). 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
A	CN 106603485 A (美的智慧家居科技有限公司) 2017 年 04 月 26 日 原文全文	
A	CN 104980928 A (华为终端有限公司) 2015 年 10 月 14 日 原文全文	

国 际 检 索 报 告

国际申请号

PCT/SG2018/050266

附加栏

(主题的分类)

国际分类号：

H04L 9/32 (2006.01)

H04L 9/14 (2006.01)

H04L 9/28 (2006.01)

G06F 21/31 (2013.01)

H04L 29/06 (2006.01)

国际检索报告

关于同族专利的信息

国际申请号

PCT/SG2018/050266

备注: 此附件列出了本国际检索报告引用的专利文件的相关已知同族专利。本单位仅提供相关同族专利的信息，并不对专利的详情承担任何责任。

检索报告中引用的专利文件	公布日或公告日	同族专利	公布日或公告日
CN 107948189 A	20/04/2018	无	
US 2010/0017602 A1	21/01/2010	无	
CN 106603485 A	26/04/2017	无	
CN 104980928 A	14/10/2015	EP 3119119 A1 WO 2015/149723 A1 US 2017/0026174 A1	18/01/2017 08/10/2015 26/01/2017