(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
2017 年 3 月 2 日 (02.03.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/032242 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/095522

(22) 国际申请日: 2016 年 8 月 16 日 (16.08.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510531892.2 2015 年 8 月 26 日 (26.08.2015) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人; 及

(71) 申请人 (仅对美国): 安勍 (AN, Qing) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 付颖芳 (FU, Yingfang) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (CN)。

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

(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,

[见续页]

(54) Title: KEY GENERATION METHOD AND APPARATUS

(54) 发明名称 : 密钥生成方法及装置

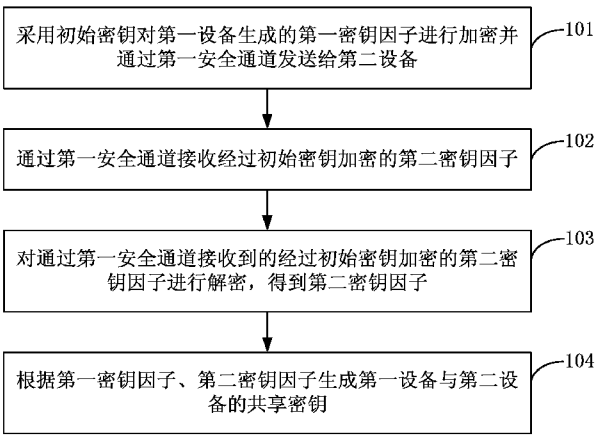

图 1

101 Encrypt, by means of an initial key, a first key factor generated by a first device, and send the encrypted first key factor to a second device by means of a first secure channel

102 Receive, by means of the first secure channel, a second key factor encrypted by the initial key

103 Decrypt the second key factor that is received by means of the first secure channel and is encrypted by the initial key, so as to obtain the second key factor

104 Generate a shared key between the first device and the second device according to the first key factor and the second key factor

(57) Abstract: The present application provides a key generation method and apparatus. The key generation method comprises: encrypting, by using an initial key, a first key factor generated by a first device, and sending the encrypted first key factor to a second device by means of a first secure channel, the initial key being a pre-set key between the first device and the second device; receiving, by means of the first secure channel, a second key factor encrypted by the initial key, the second key factor being generated by the second device; decrypting the second key factor that is received by means of the first secure channel and is encrypted by the initial key, so as to obtain the second key factor; and generating a shared key between the first device and the second device according to the first key factor and the second key factor. According to the technical solution of the present invention, a gateway device cannot acquire a shared key negotiated between a first device and a second device, such that it is ensured that data is more securely transmitted between the first device and the second device, thereby reducing the risk of illegally capturing the data in the transmission process.

(57) 摘要:

[见续页]

WO 2017/032242 A1

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))。

本申请提供一种密钥生成方法及装置，该密钥生成方法包括：采用初始密钥对第一设备生成的第一密钥因子进行加密并通过第一安全通道发送给第二设备，其中，初始密钥为第一设备与第二设备之间预设的密钥；通过第一安全通道接收经过初始密钥加密的第二密钥因子，其中，第二密钥因子由第二设备生成；对通过第一安全通道接收到的经过初始密钥加密的第二密钥因子进行解密，得到第二密钥因子；根据第一密钥因子、第二密钥因子生成第一设备与第二设备的共享密钥。在本发明的技术方案可以使网关设备无法获取第一设备与第二设备协商的共享密钥，确保数据在第一设备与第二设备之间更加安全的传输，进一步降低数据在传输过程中被非法截获的风险。

密钥生成方法及装置

技术领域

本申请涉及网络安全技术领域，尤其涉及一种密钥生成方法及装置。

背景技术

为了确保数据在终端设备与网关设备之间、网关设备与公网服务器之间的安全传输，通常会在终端设备与网关设备之间、网关设备与公网服务器分别建立安全传输通道，网关设备将数据从一个安全通道转发至另一个安全通道，从而实现数据转发的功能，而网关设备在转发数据的过程中，需要用与终端设备的共享密钥解密经过终端设备加密的数据，再用与服务器的共享密钥加密后转发给服务器，因此网关设备会存在泄露数据信息的风险。

发明内容

有鉴于此，本申请提供一种新的技术方案，可以使网关设备无法获取到两设备之间的共享密钥,从而降低数据在网络传输过程中被非法截获的风险。

为实现上述目的，本申请提供技术方案如下:

根据本申请的第一方面，提出了一种密钥生成方法，应用在第一设备上，包括:

采用初始密钥对所述第一设备生成的第一密钥因子进行加密并通过第一安全通道发送给第二设备，其中，所述初始密钥为所述第一设备与所述第二设备之间预设的密钥;

通过所述第一安全通道接收经过所述初始密钥加密的第二密钥因子，其中，所述第二密钥因子由所述第二设备生成;

对通过所述第一安全通道接收到的经过所述初始密钥加密的所述第二密钥因子进行解密，得到所述第二密钥因子;

根据所述第一密钥因子、所述第二密钥因子生成所述第一设备与第二设

备的共享密钥。

根据本申请的第二方面，提出了一种密钥生成方法，应用在第二设备上，包括：

通过第二安全通道接收来自第一设备的经过初始密钥加密的第一密钥因子，其中，所述初始密钥为所述第一设备与所述第二设备之间预设的密钥；

对经过所述初始密钥加密的所述第一密钥因子进行解密，得到所述第一加密因子；

根据所述第一密钥因子、所述第二设备生成的第二密钥因子生成所述第一设备与第二设备的共享密钥。

根据本申请的第三方面，提出了一种密钥生成装置，应用在第一设备上，包括：

第一加密模块，用于采用初始密钥对所述第一设备生成的第一密钥因子进行加密并通过第一安全通道发送给第二设备，其中，所述初始密钥为所述第一设备与所述第二设备之间预设的密钥；

第一接收模块，用于通过所述第一安全通道接收经过所述初始密钥加密的第二密钥因子，其中，所述第二密钥因子由所述第二设备生成；

第一解密模块，用于对通过所述第一接收模块通过所述第一安全通道接收到的经过所述初始密钥加密的所述第二密钥因子进行解密，得到所述第二密钥因子；

第一密钥生成模块，用于根据所述第一密钥因子、所述第一解密模块解密得到的所述第二密钥因子生成所述第一设备与第二设备的共享密钥。

根据本申请的第四方面，提出了一种密钥生成装置，应用在第二设备上，包括：

第三接收模块，用于通过第二安全通道接收来自第一设备的经过初始密钥加密的第一密钥因子，其中，所述初始密钥为所述第一设备与所述第二设备之间预设的密钥；

第三解密模块，用于对经过所述初始密钥加密的所述第一密钥因子进行

解密，得到所述第一加密因子；

第二密钥生成模块，用于根据所述第一密钥因子、所述第二设备生成的第二密钥因子生成所述第一设备与第二设备的共享密钥。

由以上技术方案可见，由于第一密钥因子与第二密钥因子在网关设备的转发过程中都经过初始密钥加密，而初始密钥为第一设备与第二设备之间预设的密钥，因此网关设备并不能获知第一密钥因子与第二密钥因子；通过第一密钥因子与第二密钥因子生成第一设备与第二设备之间的共享密钥，可以实现最终协商的共享密钥只对第一设备和第二设备可知，网关设备仍无法获取协商的共享密钥，因此可以确保数据在第一设备与第二设备之间更加安全的传输，进一步降低数据在传输过程中被非法截获的风险。

附图说明

图 1 示出了根据本发明的一示例性实施例一的密钥生成方法的流程示意图；

图 2 示出了根据本发明的一示例性实施例二的密钥生成方法的流程示意图；

图 3 示出了根据本发明的一示例性实施例三的密钥生成方法的流程示意图；

图 4 示出了根据本发明的一示例性实施例四的密钥生成方法的流程示意图；

图 5 示出了根据本发明的一示例性实施例五的密钥生成方法的流程示意图；

图 6 示出了根据本发明的一示例性实施例六的密钥生成方法的流程示意图；

图 7 示出了根据本发明的一示例性实施例七的密钥生成方法的流程示意图；

图 8 示出了根据本发明的一示例性实施例所适用的终端设备与服务器之

间密钥协商的信令示意图；

图 9 示出了根据本发明的一示例性实施例所适用的终端设备与服务器之间进行数据传输的信令示意图；

图 10 示出了根据本发明的一示例性实施例的终端设备的结构示意图；

图 11 示出了根据本发明的一示例性实施例的服务器的结构示意图；

图 12 示出了根据本发明的一示例性实施例的密钥生成装置的结构示意图；

图 13 示出了根据本发明的又一示例性实施例的密钥生成装置的结构示意图；

图 14 示出了根据本发明的再一示例性实施例的密钥生成装置的结构示意图；

图 15 示出了根据本发明的另一示例性实施例的密钥生成装置的结构示意图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼

此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

为对本申请进行进一步说明，提供下列实施例：

根据本申请一个实施例，由于第一密钥因子与第二密钥因子在网关设备的转发过程中都经过初始密钥加密，而初始密钥为第一设备与第二设备之间预设的密钥，因此网关设备并不能获知第一密钥因子与第二密钥因子；通过第一密钥因子与第二密钥因子生成第一设备与第二设备之间的共享密钥，可以实现最终协商的共享密钥只对第一设备和第二设备可知，网关设备仍无法获取协商的共享密钥，因此可以确保数据在第一设备与第二设备之间更加安全的传输，进一步降低数据在传输过程中被非法截获的风险。

图 1 示出了根据本发明的一示例性实施例一的密钥生成方法的流程示意图；在一实施例中，第一设备可以为终端设备，第二设备可以为服务器，可替换地，第一设备可以为服务器，第二设备可以为终端设备，本实施例以应用在终端设备上为例进行示例性说明，如图 1 所示，密钥生成方法包括如下步骤：

步骤 101，采用初始密钥对第一设备生成的第一密钥因子进行加密并通过第一安全通道发送给第二设备，其中，初始密钥为第一设备与第二设备之间预设的密钥；

步骤 102，通过第一安全通道接收经过初始密钥加密的第二密钥因子，其中，第二密钥因子由第二设备生成；

步骤 103，对通过第一安全通道接收到的经过初始密钥加密的第二密钥因子进行解密，得到第二密钥因子；

步骤 104，根据第一密钥因子、第二密钥因子生成第一设备与第二设备的共享密钥。

在步骤 101 中，在一实施例中，初始密钥 K_{basic} 可以在第一设备投入使用前，第二设备预先将 K_{basic} 颁发给第一设备，可以通过硬件写入的方式颁发给

第一设备。在一实施例中，第一设备与第二设备之间通过网关设备转发相关数据信息，其中，第一安全通道可以由第一设备与网关设备协商建立，并通过第一安全通道传输相关数据信息，第二安全通道可以由服务器与网关设备协商建立，并通过第二安全通道传输相关数据信息。本领域技术人员可以理解的是，第一安全通道和第二安全通道的建立过程可以参见现有技术的相关描述，例如，可以采用安全套接字层（Secure Socket Layer，简称 SSL）、安全传输层协议（Transport Layer Security，简称 TLS）的密钥协商机制。

在一实施例中，在第一设备需要向第二设备发起密钥协商流程时，通过伪随机函数生成第一密钥因子，采用初始密钥对第一密钥因子进行加密，得到第一次加密后的第一密钥因子，采用第一安全通道的第一加密密钥对第一次加密后的第一密钥因子进行加密，得到第二次加密后的第一密钥因子。通过对第一密钥因子进行双重加密，可以使第一密钥因子在网关设备处不可知，避免第一密钥因子在网关设备侧被非法截获的风险。

在步骤 103 中，采用第一加密密钥对经过双重加密的第二密钥因子进行解密，得到第一次解密后的第二密钥因子，采用初始密钥对第一次解密后的第二密钥因子进行解密，得到第二密钥因子。由于第二密钥因子在第二设备处已经进行了双重加密，因此第二密钥因子在网关设备处不可知，避免第二密钥因子在网关设备侧被非法截获的风险。

在步骤 104 中如何根据第一密钥因子、第二密钥因子生成第一设备与第二设备的共享密钥的详细描述参见下述描述，在此先不详述。

由上述描述可知，由于第一密钥因子与第二密钥因子在网关设备的转发过程中都经过初始密钥加密，而初始密钥为第一设备与第二设备之间预设的密钥，因此网关设备并不能获知第一密钥因子与第二密钥因子；通过第一密钥因子与第二密钥因子生成第一设备与第二设备之间的共享密钥，可以实现最终协商的共享密钥只对第一设备和第二设备可知，网关设备仍无法获取协商的共享密钥，因此可以确保数据在第一设备与第二设备之间更加安全的传输，进一步降低数据在传输过程中被非法截获的风险。

图 2 示出了根据本发明的一示例性实施例二的密钥生成方法的流程示意图，本实施例以上述图 1 所示实施例中的步骤 105 中如何通过第一密钥因子和第二密钥因子生成第一设备与第二设备之间的共享密钥为例进行示例性说明，如图 2 所示，密钥生成方法包括如下步骤:

步骤 201，确定第一设备与第二设备之间共享的初始密钥和第一设备的设备标识;

步骤 202，将初始密钥、设备标识、第一密钥因子、第二密钥因子依次连接，得到组合字串;

步骤 203，将组合字串切分为长度相等的两个子字串;

步骤 204，对两个子字串分别进行散列运算，得到两个散列结果;

步骤 205，将两个散列结果以位进行异或运算，得到第一设备与第二设备的共享密钥。

在第一设备通过上述图 1 所示实施例中的步骤 104 得到第二密钥因子后，第一设备具有了第一密钥因子 p 和第二密钥因子 q。第一设备可以将第一密钥因子和第二密钥因子作为输入，利用共享密钥的生成算法，得到密钥 K_{AC}。其中，密钥生成算法如下:

K_{AC} = KeyGenerate（K_{basic}，“Shared Key”，p，q）;

其中，K_{basic} 为初始密钥，Shared Key 为第一设备的设备标识，该设备标识可以为第一设备的设备序列号，也可以为 MAC 地址，或者上述二者的组合，等等，只要能够使第二设备能够通过设备标识对第一设备与其它设备进行区分即可。

此外，在通过函数 KeyGenerate 生成共享密钥的过程中，可以将第一加密密钥 K_{basic} 对应的字串，“Shared Key”，p，q 依次连接，得到组合字串，将组合字串利用函数 KeyGenerate 生成共享密钥 K_{AC}。

在一实施例中，函数 KeyGenerate 所实现的过程具体可以为：将输入的组合字串切分为长度相等的两个子字串（如果组合字串的长度为奇数，则在组合字串的最后一位补 1），之后对两个子字串分别进行散列运算（例如，

MD5），将得到的两个计算结果以位进行异或运算，得到的结果即是共享密钥 K_{AC}。

以 MD5 为例进行示例性说明，由于 MD5 可以将任意长度的输入转化为 128 位长度的结果，因此共享密钥 K_{AC} 的长度为 128 位，简化了共享密钥计算的复杂度。由于共享密钥 K_{AC} 的计算采用 MD5，计算量对于计算能力受限的第一设备而言可以承受。

本实施例中，通过第一密钥因子、第二密钥因子、初始密钥和第一设备的设备标识生成共享密钥 K_{AC}，因此实现了在第一设备与第二设备之间是通过安全协商并共享该共享密钥 K_{AC}，且该共享密钥 K_{AC} 对作为中间节点的网关设备不可知，因此可以确保第一设备可以利用该共享密钥 K_{AC} 对发送至第二设备的数据进行加密，确保数据在网络传输过程中的安全性。

图 3 示出了根据本发明的一示例性实施例三的密钥生成方法的流程示意图，在上述实施例的基础上，如图 3 所示，密钥生成方法包括如下步骤：

步骤 301，确定第一设备与第二设备的共享密钥的更换周期；

步骤 302，根据更换周期重新确定第一加密因子和第二加密因子；

步骤 303，根据重新确定的第一加密因子和第二加密因子更换第一设备与第二设备的共享密钥。

在一实施例中，第一设备与第二设备可以约定共享密钥 K_{AC} 的更换周期，当共享密钥 K_{AC} 使用了更换周期对应的时长后，第一设备与第二设备之间重新发起生成共享密钥 K_{AC} 的流程，从而可以进一步保证共享密钥 K_{AC} 的及数据在网络传输过程中的安全性，进一步降低该共享密钥 K_{AC} 被破解的可能。

图 4 示出了根据本发明的一示例性实施例四的密钥生成方法的流程示意图，在上述图 1 所示实施例生成共享密钥后，可以通过共享密钥对第一设备待传输的数据加密，并传输给第二设备，如图 4 所示，对待传输的数据进行加密并传输的过程包括如下步骤：

步骤 401，确定第一设备需要向第二设备发送的待传输的数据；

步骤 402，采用共享密钥对待传输的数据进行加密，并通过第一安全通

道发送给第二设备;

步骤 403，通过第一安全通过接收第二设备在接收到待传输的数据生成的响应数据，响应数据已经经过共享密钥加密;

步骤 404，采用共享密钥对经过共享密钥加密的响应数据进行解密，得到响应数据。

在步骤 401 中，待传输的数据可以为第一设备上的传感器获取到的物联网数据。

步骤 402 和步骤 403 中的第一安全通道的相关描述可以参见上述图 1 所示实施例的相关描述，在此不再详述。

在步骤 404 中，在通过第一安全通道接收到经过共享密钥加密的响应数据时，可以先通过第一安全通道的第一加密密钥对经过共享密钥加密的响应数据进行解密，然后通过共享密钥对响应数据进行第二次解密，从而得到原始的响应数据。

本实施例中，由于待传输的数据在网关设备的转发过程中都经过共享密钥加密，而共享密钥为第一设备与第二设备之间共同协商的密钥，因此网关设备并不能获知共享密钥，因此可以确保待传输的数据在第一设备与第二设备之间更加安全的传输，进一步降低数据在传输过程中被非法截获的风险。

图 5 示出了根据本发明的一示例性实施例五的密钥生成方法的流程示意图，本实施例中，第一设备可以为终端设备，第二设备可以为服务器，本实施例可以应用在第二设备上，如图 5 所示，密钥生成方法包括如下步骤:

步骤 501，通过第二安全通道接收来自第一设备的经过初始密钥加密的第一密钥因子，其中，初始密钥为第一设备与第二设备之间预设的密钥;

步骤 502，对经过初始密钥加密的第一密钥因子进行解密，得到第一加密因子;

步骤 503，根据第一密钥因子、第二设备生成的第二密钥因子生成第一设备与第二设备的共享密钥。

步骤 501 中的第二安全通道的相关描述请参见上述图 1 所示实施例的相

关描述，在此不再详述。

在步骤 502 中，在通过第二安全通道接收到经过初始密钥加密的第一密钥因子后，可以先通过第二安全通道的第二加密密钥对经过初始密钥加密的第一密钥因子进行解密，然后通过初始密钥对第一密钥因子进行第二次解密，从而得到原始的第一密钥因子。

步骤 503 中如何根据第一密钥因子、第二密钥因子生成第一设备与第二设备的共享密钥的详细描述可以参见上述图 2 所示实施例的描述，在此不再详述。

由上述描述可知，由于第一密钥因子与第二密钥因子在网关设备的转发过程中都经过初始密钥加密，而初始密钥为第一设备与第二设备之间预设的密钥，因此网关设备并不能获知第一密钥因子与第二密钥因子；通过第一密钥因子与第二密钥因子生成第一设备与第二设备之间的共享密钥，可以实现最终协商的共享密钥只对第一设备和第二设备可知，网关设备仍无法获取协商的共享密钥，因此可以确保数据在第一设备与第二设备之间更加安全的传输，进一步降低数据在传输过程中被非法截获的风险。

图 6 示出了根据本发明的一示例性实施例六的密钥生成方法的流程示意图，如图 6 所示，密钥生成方法包括如下步骤：

步骤 601，采用初始密钥对第二设备生成的第二密钥因子进行加密；

步骤 602，通过第二安全通道将经过初始密钥加密后的第二密钥因子发送给第一设备。

本实施例中，采用第二安全通道的第二加密密钥对经过初始密钥加密后的第二密钥因子进行第二次加密，从而可以使在发送至第一设备的过程中经由网关设备转发时第二密钥因子对网关设备是可不知的，避免第二密钥因子在网关设备侧被非法截获的风险。

图 7 示出了根据本发明的一示例性实施例七的密钥生成方法的流程示意图，如图 7 所示，密钥生成方法包括如下步骤：

步骤 701，通过第二安全通道接收来自第一设备的经过共享密钥加密的

待传输的数据；

步骤 702，采用共享密钥对待传输的数据进行解密；

步骤 703，在接收到待传输的数据后，生成响应数据；

步骤 704，通过共享密钥对响应数据进行加密；

步骤 705，通过第二安全通道向第一设备发送经过共享密钥加密的响应数据。

步骤 701 中的第二安全通道的相关描述可以参见上述图 1 所示实施例的相关描述，在此不再详述。

在步骤 704 中，在通过第二安全通道接收到来自第一设备的待传输的数据后，通过共享密钥对待传输的数据经过共享密钥解密后得到原始的数据，在需要对第一设备做出响应时，可以先通过第二安全通道的第二加密密钥对经过共享密钥加密的响应数据进行加密，从而使网关设备在转发响应数据的过程中不能够获取到原始的响应数据。

本实施例中，由于待传输的数据在网关设备的转发过程中都经过共享密钥加密，而共享密钥为第一设备与第二设备之间共同协商的密钥，因此网关设备并不能获知共享密钥，因此可以确保待传输的数据在第一设备与第二设备之间更加安全的传输，进一步降低数据在传输过程中被非法截获的风险。

通过上述实施例，可以基于第一设备和第二设备之间预置的初始密钥，在各自对应的本地通过密钥生成算法生成共享密钥，最后利用共享密钥对待传输的数据进行加密，从而可以使网关设备在网络中转发数据时无法查看到原始的数据，从而达到了安全传输数据的目的。

图 8 示出了根据本发明的一示例性实施例所适用的终端设备与服务器之间密钥协商的信令示意图，以第一设备为终端设备，第二设备为服务器为例进行示例性说明，其中，终端设备在接入到网络前，服务器需要预先为终端设备颁发初始密钥（K_{basic}），可以通过硬件写入等方式颁发给终端设备，如图 8 所示，终端设备和服务器之间进行密钥协商包括如下步骤：

步骤 801，终端设备与网关设备协商第一安全通道的第一加密密钥（K_{AB}），并建立终端设备与网关设备之间的第一安全通道。该第一安全通道的建立方法可以参见现有技术的相关描述。

步骤 802，网关设备与服务器协商第二安全通道的第二加密密钥（K_{BC}），并建立第二安全通道。与上述步骤 801 类似，第二安全通道的建立过程可以参见现有技术的相关描述，同样可以采用 SSL、TLS 的密钥协商机制。本领域技术人员可以理解的是，步骤 801 和步骤 802 的顺序可以互换，可以根据实际执行的需求设定执行顺序。

步骤 803，终端设备准备发起与服务器的密钥协商流程，终端设备生成第一密钥因子（p），该第一密钥因子用于生成终端设备与服务器的共享密钥。同时，利用初始密钥（K_{basic}）加密第一密钥因子，得到 K_{basic}（p），再采用第一加密密钥 K_{AB} 加密，得到 $K_{AB}[K_{basic}(p)]$。

步骤 804，终端设备通过第一安全通道向网关设备发送经过双重加密的第一密钥因子 $K_{AB}[K_{basic}(p)]$。

步骤 805，网关设备在接收到经过双重加密的第一密钥因子 $K_{AB}[K_{basic}(p)]$ 后，采用第一安全通道的第一加密密钥 K_{AB} 对经过双重加密的第一密钥因子 $K_{AB}[K_{basic}(p)]$ 进行解密，得到 $K_{basic}(p)$，之后再采用第二安全通道的第三加密密钥 K_{BC} 进行加密，得到双重加密的 $K_{BC}[K_{basic}(p)]$。

步骤 806，将经过初始密钥和第二加密密钥双重加密的第一密钥因子 $K_{BC}[K_{basic}(p)]$ 通过第二安全通道发送给服务器。

步骤 807，服务器接收到经过双重加密的第一密钥因子后，采用第二安全通道的第二加密密钥 K_{BC} 对经过双重加密的第一密钥因子进行解密，得到 $K_{basic}(p)$，之后利用初始密钥 K_{basic} 对 $K_{basic}(p)$ 进行解密，得到第一密钥因子 p。

步骤 808，服务器通过伪随机函数生成第二密钥因子（q），该第二密钥因子 q 将与第一密钥因子 p 共同作为参数生成共享密钥 K_{AC}。

步骤 809，服务器采用初始密钥 K_{basic} 加密第二加密因子 q，得到 K_{basic}

（q），再采用第二加密密钥 K_{BC} 对 K_{basic}（q）加密，得到 $K_{BC}[K_{basic}$（q）]。

步骤 810，服务器通过第二安全通道向网关设备发送经过双重加密的第二密钥因子 $K_{BC}[K_{basic}$（q）]。

步骤 811，网关设备接收到经过双重加密的第二密钥因子 $K_{BC}[K_{basic}$（q）]后，采用第二安全通道的第二加密密钥 K_{BC} 对经过双重加密的第二加密因子进行解密，得到 K_{basic}（q），之后利用第一安全通道的第一加密密钥 K_{AB} 进行加密，得到 $K_{AB}[K_{basic}$（q）]，之后将经过双重加密的第二加密因子通过第一安全通道发送至终端设备。

步骤 812，终端设备接收到该经过双重加密的第二加密因子后，采用第一安全通道的第一加密密钥 K_{AB} 对经过双重加密的第二加密因子进行解密，得到 K_{basic}（q），之后利用第一加密密钥 K_{basic} 对第一次解密后的 K_{basic}（q）进行二次解密，得到第二密钥因子 q。

步骤 813，终端设备与服务器均共享了第一密钥因子 p 和第二密钥因子 q，终端设备与服务器均将第一密钥因子和第二密钥因子作为输入，采用密钥生成算法，得到终端设备和服务器之间的共享密钥 K_{AC}。其中，密钥生成算法的详细描述可以参见上述图 2 所示实施例的相关描述，在此不再详述。

本实施例中，由此实现了共享密钥 K_{AC} 在终端设备与公网服务器间的安全协商和共享，且该共享密钥对作为中间节点的网关设备不可知，之后终端设备可以利用该共享密钥，对发往公网服务器的物联网数据进行加密，从而保证了数据传输的安全性。

为了进一步保证共享密钥及数据传输的安全性，终端设备可以与服务器之间周期性地进行密钥协商流程来更换共享密钥 K_{AC}，从而可以进一步降低该共享密钥被破解的可能。

图 9 示出了根据本发明的一示例性实施例一的数据传输方法的流程示意图，在通过上述图 8 所示实施例生成共享秘钥后，终端设备如果需要向服务器发送物联网数据（data），如图 9 所示，数据传输方法包括如下步骤：

步骤 901，使用共享密钥 K_{AC} 对物联网数据进行一次加密，得到密文 K_{AC}

（data），之后使用第一安全通道的第一加密密钥 K_{AB} 二次加密，得到密文 $K_{AB}[K_{AC}（data）]$。

步骤 902，终端设备通过第一安全通道向网关设备发送密文 $K_{AB}[K_{AC}（data）]$。

步骤 903，网关设备收到密文 $K_{AB}[K_{AC}（data）]$后，使用第一安全密钥 K_{AB} 解密，得到 $K_{AC}（data）$，然后使用第二加密密钥 K_{BC} 进行加密，得到密文 $K_{BC}[K_{AC}（data）]$。

步骤 904，网关设备通过第二安全通道向服务器发送密文 $K_{BC}[K_{AC}（data）]$。

步骤 905，服务器接收到经过双重加密的密文 $K_{BC}[K_{AC}（data）]$后，使用第二加密密钥 K_{BC} 解密，得到 $K_{AC}（data）$，然后使用共享密钥 K_{AC} 解密，得到原始的物联网数据 data。

步骤 906，服务器在得到原始的物联网数据后，生成响应数据（res），利用共享密钥 K_{AC} 对响应数据加密，得到密文 $K_{AC}（res）$，再使用第二加密密钥 K_{BC} 进行二次加密，得到 $K_{BC}[K_{AC}（res）]$。

步骤 907，服务器通过第二安全通道向网关设备发送经过双重加密的密文 $K_{BC}[K_{AC}（res）]$。

步骤 908，网关设备收到经过双重加密的密文 $K_{BC}[K_{AC}（res）]$后，使用第二加密密钥 K_{BC} 解密，得到 $K_{AC}（res）$，然后使用第一加密密钥 K_{AB} 进行加密，得到密文 $K_{AB}[K_{AC}（res）]$。

步骤 909，网关设备通过第一安全通道向终端设备发送经过双重加密的密文 $K_{AB}[K_{AC}（res）]$。

步骤 910，终端设备接收到经过双重加密的密文 $K_{AB}[K_{AC}（res]$后，使用第一加密密钥 K_{AB} 解密，得到 $K_{AC}（res）$，然后使用共享密钥 K_{AC} 解密，得到原始的响应数据（res）。

本实施例中，实现了终端设备通过中间节点的网关设备与服务器间的跨网域的密钥协商与共享，共享密钥对网关设备不可知，确保了物联网数据在

终端设备与服务器间的端到端的安全传输；此外，除了保证终端设备与网关设备间的数据安全传输和网关设备与公网服务器间的数据安全传输，数据在传输路径上的网关设备内的转发过程也受到安全保护，即使网关设备被非法入侵，经由网关设备转发的物联网数据也依然由于被共享密钥加密而受到保护，避免物联网数据被非法截取。

对应于上述的密钥生成方法，本申请还提出了图 10 所示的根据本申请的一示例性实施例的终端设备的示意结构图。请参考图 10，在硬件层面，该网络服务器包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成密钥生成装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

对应于上述的密钥生成方法，本申请还提出了图 11 所示的根据本申请的一示例性实施例的服务器的示意结构图。请参考图 11，在硬件层面，该网络服务器包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成密钥生成装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

图 12 示出了根据本发明的一示例性实施例的密钥生成装置的结构示意图；如图 12 所示，该密钥生成装置可以包括：第一加密模块 1201、第一接收模块 1202、第一解密模块 1203、第一密钥生成模块 1204。其中：

第一加密模块 1201，用于采用初始密钥对第一设备生成的第一密钥因子进行加密并通过第一安全通道发送给第二设备，其中，初始密钥为第一设备与第二设备之间预设的密钥；

第一接收模块 1202，用于通过第一安全通道接收经过初始密钥加密的第二密钥因子，其中，第二密钥因子由第二设备生成；

第一解密模块 1203，用于对通过第一接收模块 1202 通过第一安全通道接收到的经过初始密钥加密的第二密钥因子进行解密，得到第二密钥因子；

第一密钥生成模块 1204，用于根据第一密钥因子、第一解密模块 1203 解密得到的第二密钥因子生成第一设备与第二设备的共享密钥。

图 13 示出了根据本发明的又一示例性实施例的密钥生成装置的结构示意图；如图 13 所示，在上述图 12 所示实施例的基础上，第一加密模块 1201 可包括：

第一因子生成单元 12011，用于在第一设备需要向第二设备发起密钥协商流程时，通过伪随机函数生成第一密钥因子；

第一加密单元 12012，用于采用初始密钥对第一因子生成单元 12011 生成的第一密钥因子进行加密，得到第一次加密后的第一密钥因子；

第二加密单元 12013，用于采用第一安全通道的第一加密密钥对第一加密单元 12012 第一次加密后的第一密钥因子进行加密，得到第二次加密后的第一密钥因子。

在一实施例中，第一解密模块 1203 包括：

第一解密单元 12031，用于采用第一加密密钥对经过双重加密的第二密钥因子进行解密，得到第一次解密后的第二密钥因子；

第二加密单元 12032，用于采用初始密钥对第一解密单元 12031 第一次解密后的第二密钥因子进行解密，得到第二密钥因子。

在一实施例中，第一密钥生成模块 1204 可包括：

第一确定单元 12041，用于确定第一设备与第二设备之间共享的第一加密密钥和第一设备的设备标识；

第一因子生成单元 12042，用于根据第一加密密钥、第一确定单元 12041 确定的设备标识、第一密钥因子、第一解密模块 1203 得到的第二密钥因子生成第一设备与第二设备的共享密钥。

在一实施例中，第一因子生成单元具体用于：

将第一加密密钥、设备标识、第一密钥因子、第二密钥因子依次连接，得到组合字串；

将组合字串切分为长度相等的两个子字串；

对两个子字串分别进行散列运算，得到两个散列结果；

将两个散列结果以位进行异或运算，得到第一设备与第二设备的共享密钥。

在一实施例中，装置还可包括：

第一确定模块 1205，用于确定第一设备与第二设备的共享密钥的更换周期；

第二确定模块 1206，用于根据第一确定模块 1205 确定的更换周期重新确定第一加密因子和第二加密因子；

第一更换模块 1207，用于根据第二确定模块 1206 重新确定的第一加密因子和第二加密因子更换第一设备与第二设备的共享密钥。

在一实施例中，装置还可包括：

第三确定模块 1208，用于确定第一设备需要向第二设备发送的待传输的数据；

数据加密模块 1209，用于采用共享密钥对第三确定模块 1208 确定的待传输的数据进行加密，并通过第一安全通道发送给第二设备。

在一实施例中，装置还可包括：

第二接收模块 1210，用于通过第一安全通过接收第二设备在接收到待传输的数据生成的响应数据，响应数据已经经过共享密钥加密；

第二解密模块 1211，用于采用共享密钥对经过共享密钥加密的响应数据进行解密，得到响应数据。

图 14 示出了根据本发明的再一示例性实施例的密钥生成装置的结构示意图；如图 14 所示，该密钥生成装置可以包括：第三接收模块 1401、第三解密模块 1402、第二密钥生成模块 1403。其中：

第三接收模块 1401，用于通过第二安全通道接收来自第一设备的经过初始密钥加密的第一密钥因子，其中，初始密钥为第一设备与第二设备之间预设的密钥；

第三解密模块 1402，用于对经过初始密钥加密的第一密钥因子进行解密，得到第一加密因子；

第二密钥生成模块 1403，用于根据第一密钥因子、第二设备生成的第二密钥因子生成第一设备与第二设备的共享密钥

图 15 示出了根据本发明的另一示例性实施例的密钥生成装置的结构示意图；如图 15 所示，在上述图 14 所示实施例的基础上，第二密钥生成模块 1403 具体用于：

将第一加密密钥、第一设备的设备标识、第一密钥因子、第二密钥因子依次连接，得到组合字串；

将组合字串切分为长度相等的两个子字串；

对两个子字串分别进行散列运算，得到两个散列结果；

将两个散列结果以位进行异或运算，得到第一设备与第二设备的共享密钥。

在一实施例中，装置还可包括：

第二加密模块 1404，用于采用初始密钥对第二设备生成的第二密钥因子进行加密；

第一发送模块 1405，用于通过第二安全通道将经过初始密钥加密后的第二密钥因子发送给第一设备。

在一实施例中，装置还可包括：

第三确定模块 1406，用于确定第一设备与第二设备的共享密钥的更换周期；

第四确定模块 1407，用于根据更换周期重新确定第一加密因子和第二加密因子；

第二更换模块 1408，用于根据重新确定的第一加密因子和第二加密因子

更换第一设备与第二设备的共享密钥。

在一实施例中，装置还可包括:

第四接收模块 1409，用于通过第二安全通道接收来自第一设备的经过共享密钥加密的待传输的数据;

第四解密模块 1410，用于采用共享密钥对待传输的数据进行解密。

在一实施例中，装置还可包括:

响应数据生成模块 1411，用于在接收到待传输的数据后，生成响应数据;

第三加密模块 1412，用于通过共享密钥对响应数据进行加密;

第二发送模块 1413，用于通过第二安全通道向第一设备发送经过共享密钥加密的响应数据。

上述实施例可见，由于第一密钥因子与第二密钥因子在网关设备的转发过程中都经过初始密钥加密，而初始密钥为第一设备与第二设备之间预设的密钥，因此网关设备并不能获知第一密钥因子与第二密钥因子；通过第一密钥因子与第二密钥因子生成第一设备与第二设备之间的共享密钥，可以实现最终协商的共享密钥只对第一设备和第二设备可知，网关设备仍无法获取协商的共享密钥，因此可以确保数据在第一设备与第二设备之间更加安全的传输，进一步降低数据在传输过程中被非法截获的风险。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中

还存在另外的相同要素。

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

5

权 利 要 求 书

1、一种密钥生成方法，应用在第一设备上，其特征在于，所述方法包括：

采用初始密钥对所述第一设备生成的第一密钥因子进行加密并通过第一安全通道发送给第二设备，其中，所述初始密钥为所述第一设备与所述第二设备之间预设的密钥；

通过所述第一安全通道接收经过所述初始密钥加密的第二密钥因子，其中，所述第二密钥因子由所述第二设备生成；

对通过所述第一安全通道接收到的经过所述初始密钥加密的所述第二密钥因子进行解密，得到所述第二密钥因子；

根据所述第一密钥因子、所述第二密钥因子生成所述第一设备与第二设备的共享密钥。

2、根据权利要求 1 所述的方法，其特征在于，所述采用初始密钥对所述第一设备生成的第一密钥因子进行加密，包括：

在所述第一设备需要向第二设备发起密钥协商流程时，通过伪随机函数生成第一密钥因子；

采用初始密钥对所述第一密钥因子进行加密，得到第一次加密后的所述第一密钥因子；

采用第一安全通道的第一加密密钥对所述第一次加密后的所述第一密钥因子进行加密，得到第二次加密后的所述第一密钥因子。

3、根据权利要求 1 所述的方法，其特征在于，所述对通过所述第一安全通道接收到的经过所述第一加密密钥加密的所述第二密钥因子进行解密，包括：

采用所述第一加密密钥对经过双重加密的所述第二密钥因子进行解密，得到第一次解密后的所述第二密钥因子；

采用所述初始密钥对所述第一次解密后的所述第二密钥因子进行解密，得到所述第二密钥因子。

4、根据权利要求 1 所述的方法，其特征在于，所述根据所述第一密钥因子、所述第二密钥因子生成所述第一设备与第二设备的共享密钥，包括:

确定所述第一设备与所述第二设备之间共享的初始密钥和所述第一设备的设备标识;

根据所述初始密钥、所述设备标识、所述第一密钥因子、所述第二密钥因子生成所述第一设备与第二设备的共享密钥。

5、根据权利要求 4 所述的方法，其特征在于，所述根据所述设备标识、所述第一加密密钥、所述第一密钥因子、所述第二密钥因子生成所述第一设备与第二设备的共享密钥，包括:

将所述第一加密密钥、所述设备标识、所述第一密钥因子、所述第二密钥因子依次连接，得到组合字串;

将所述组合字串切分为长度相等的两个子字串;

对所述两个子字串分别进行散列运算，得到两个散列结果;

将所述两个散列结果以位进行异或运算，得到所述第一设备与第二设备的共享密钥。

6、根据权利要求 1 所述的方法，其特征在于，所述方法还包括:

确定所述第一设备与所述第二设备的共享密钥的更换周期;

根据所述更换周期重新确定所述第一加密因子和所述第二加密因子;

根据重新确定的所述第一加密因子和所述第二加密因子更换所述第一设备与所述第二设备的共享密钥。

7、根据权利要求 1-6 任一所述的方法，其特征在于，所述方法还包括:

确定所述第一设备需要向所述第二设备发送的待传输的数据;

采用所述共享密钥对所述待传输的数据进行加密，并通过所述第一安全通道发送给所述第二设备。

8、根据权利要求 7 所述的方法，其特征在于，所述方法还包括:

通过所述第一安全通过接收所述第二设备在接收到所述待传输的数据生成的响应数据，所述响应数据已经经过所述共享密钥加密;

采用所述共享密钥对所述经过所述共享密钥加密的所述响应数据进行解密，得到所述响应数据。

9、一种密钥生成方法，应用在第二设备上，其特征在于，所述方法包括:

通过第二安全通道接收来自第一设备的经过初始密钥加密的第一密钥因子，其中，所述初始密钥为所述第一设备与所述第二设备之间预设的密钥;

对经过所述初始密钥加密的所述第一密钥因子进行解密，得到所述第一加密因子;

根据所述第一密钥因子、所述第二设备生成的第二密钥因子生成所述第一设备与第二设备的共享密钥。

10、根据权利要求 9 所述的方法，其特征在于，所述根据所述第一密钥因子、所述第二设备生成的第二密钥因子生成所述第一设备与第二设备的共享密钥，包括:

将所述第一加密密钥、所述第一设备的设备标识、所述第一密钥因子、所述第二密钥因子依次连接，得到组合字串;

将所述组合字串切分为长度相等的两个子字串;

对所述两个子字串分别进行散列运算，得到两个散列结果;

将所述两个散列结果以位进行异或运算，得到所述第一设备与第二设备的共享密钥。

11、根据权利要求 9 所述的方法，其特征在于，所述方法还包括:

采用所述初始密钥对所述第二设备生成的第二密钥因子进行加密;

通过所述第二安全通道将所述经过所述初始密钥加密后的所述第二密钥因子发送给所述第一设备。

12、根据权利要求 9 所述的方法，其特征在于，所述方法还包括:

确定所述第一设备与所述第二设备的共享密钥的更换周期;

根据所述更换周期重新确定所述第一加密因子和所述第二加密因子;

根据重新确定的所述第一加密因子和所述第二加密因子更换所述第一设备与所述第二设备的共享密钥。

13、根据权利要求 9-12 任一所述的方法，其特征在于，所述方法还包括：

通过第二安全通道接收来自所述第一设备的经过所述共享密钥加密的待传输的数据；

采用所述共享密钥对所述待传输的数据进行解密。

14、根据权利要求 13 所述的方法，其特征在于，所述方法还包括：

在接收到所述待传输的数据后，生成响应数据；

通过所述共享密钥对所述响应数据进行加密；

通过所述第二安全通道向所述第一设备发送经过所述共享密钥加密的响应数据。

15、一种密钥生成装置，应用在第一设备上，其特征在于，所述装置包括：

第一加密模块，用于采用初始密钥对所述第一设备生成的第一密钥因子进行加密并通过第一安全通道发送给第二设备，其中，所述初始密钥为所述第一设备与所述第二设备之间预设的密钥；

第一接收模块，用于通过所述第一安全通道接收经过所述初始密钥加密的第二密钥因子，其中，所述第二密钥因子由所述第二设备生成；

第一解密模块，用于对通过所述第一接收模块通过所述第一安全通道接收到的经过所述初始密钥加密的所述第二密钥因子进行解密，得到所述第二密钥因子；

第一密钥生成模块，用于根据所述第一密钥因子、所述第一解密模块解密得到的所述第二密钥因子生成所述第一设备与第二设备的共享密钥。

16、根据权利要求 15 所述的装置，其特征在于，所述第一加密模块包括：

第一因子生成单元，用于在所述第一设备需要向第二设备发起密钥协商流程时，通过伪随机函数生成第一密钥因子；

第一加密单元，用于采用初始密钥对所述第一因子生成单元生成的所述第一密钥因子进行加密，得到第一次加密后的所述第一密钥因子；

第二加密单元，用于采用第一安全通道的第一加密密钥对所述第一加密

单元第一次加密后的所述第一密钥因子进行加密，得到第二次加密后的所述第一密钥因子。

17、根据权利要求 15 所述的装置，其特征在于，所述第一解密模块包括：

第一解密单元，用于采用所述第一加密密钥对经过双重加密的所述第二密钥因子进行解密，得到第一次解密后的所述第二密钥因子；

第二加密单元，用于采用所述初始密钥对所述第一解密单元第一次解密后的所述第二密钥因子进行解密，得到所述第二密钥因子。

18、根据权利要求 15 所述的装置，其特征在于，所述第一密钥生成模块包括：

第一确定单元，用于确定所述第一设备与所述第二设备之间共享的第一加密密钥和所述第一设备的设备标识；

第一因子生成单元，用于根据所述第一加密密钥、所述第一确定单元确定的所述设备标识、所述第一密钥因子、所述第一解密模块得到的所述第二密钥因子生成所述第一设备与第二设备的共享密钥。

19、根据权利要求 18 所述的装置，其特征在于，所述第一因子生成单元具体用于：

将所述第一加密密钥、所述设备标识、所述第一密钥因子、所述第二密钥因子依次连接，得到组合字串；

将所述组合字串切分为长度相等的两个子字串；

对所述两个子字串分别进行散列运算，得到两个散列结果；

将所述两个散列结果以位进行异或运算，得到所述第一设备与第二设备的共享密钥。

20、根据权利要求 15 所述的装置，其特征在于，所述装置还包括：

第一确定模块，用于确定所述第一设备与所述第二设备的共享密钥的更换周期；

第二确定模块，用于根据所述第一确定模块确定的所述更换周期重新确定所述第一加密因子和所述第二加密因子；

第一更换模块，用于根据所述第二确定模块重新确定的所述第一加密因子和所述第二加密因子更换所述第一设备与所述第二设备的共享密钥。

21、根据权利要求 15-20 任一所述的装置，其特征在于，所述装置还包括：

第三确定模块，用于确定所述第一设备需要向所述第二设备发送的待传输的数据；

数据加密模块，用于采用所述共享密钥对所述第三确定模块确定的所述待传输的数据进行加密，并通过所述第一安全通道发送给所述第二设备。

22、根据权利要求 21 所述的装置，其特征在于，所述装置还包括：

第二接收模块，用于通过所述第一安全通过接收所述第二设备在接收到所述待传输的数据生成的响应数据，所述响应数据已经经过所述共享密钥加密；

第二解密模块，用于采用所述共享密钥对所述经过所述共享密钥加密的所述响应数据进行解密，得到所述响应数据。

23、一种密钥生成装置，应用在第二设备上，其特征在于，所述装置包括：

第三接收模块，用于通过第二安全通道接收来自第一设备的经过初始密钥加密的第一密钥因子，其中，所述初始密钥为所述第一设备与所述第二设备之间预设的密钥；

第三解密模块，用于对经过所述初始密钥加密的所述第一密钥因子进行解密，得到所述第一加密因子；

第二密钥生成模块，用于根据所述第一密钥因子、所述第二设备生成的第二密钥因子生成所述第一设备与第二设备的共享密钥。

24、根据权利要求 23 所述的装置，其特征在于，所述第二密钥生成模块具体用于：

将所述第一加密密钥、所述第一设备的设备标识、所述第一密钥因子、所述第二密钥因子依次连接，得到组合字串；

将所述组合字串切分为长度相等的两个子字串；

对所述两个子字串分别进行散列运算，得到两个散列结果；

将所述两个散列结果以位进行异或运算，得到所述第一设备与第二设备的共享密钥。

25、根据权利要求 24 所述的装置，其特征在于，所述装置还包括：

第二加密模块，用于采用所述初始密钥对所述第二设备生成的第二密钥因子进行加密；

第一发送模块，用于通过所述第二安全通道将所述经过所述初始密钥加密后的所述第二密钥因子发送给所述第一设备。

26、根据权利要求 25 所述的装置，其特征在于，所述装置还包括：

第三确定模块，用于确定所述第一设备与所述第二设备的共享密钥的更换周期；

第四确定模块，用于根据所述更换周期重新确定所述第一加密因子和所述第二加密因子；

第二更换模块，用于根据重新确定的所述第一加密因子和所述第二加密因子更换所述第一设备与所述第二设备的共享密钥。

27、根据权利要求 23-26 任一所述的装置，其特征在于，所述装置还包括：

第四接收模块，用于通过第二安全通道接收来自所述第一设备的经过所述共享密钥加密的待传输的数据；

第四解密模块，用于采用所述共享密钥对所述待传输的数据进行解密。

28、根据权利要求 27 所述的装置，其特征在于，所述装置还包括：

响应数据生成模块，用于在接收到所述待传输的数据后，生成响应数据；

第三加密模块，用于通过所述共享密钥对所述响应数据进行加密；

第二发送模块，用于通过所述第二安全通道向所述第一设备发送经过所述共享密钥加密的响应数据。

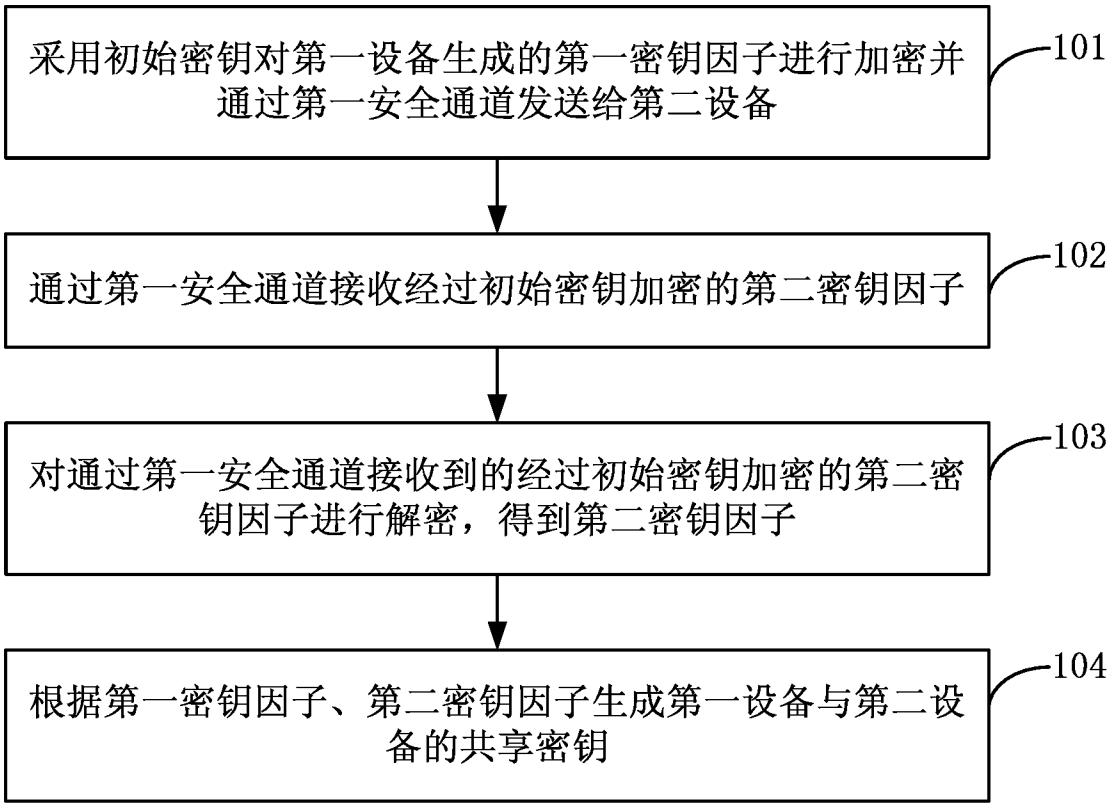
采用初始密钥对第一设备生成的第一密钥因子进行加密并通过第一安全通道发送给第二设备
101
通过第一安全通道接收经过初始密钥加密的第二密钥因子
102
对通过第一安全通道接收到的经过初始密钥加密的第二密钥因子进行解密，得到第二密钥因子
103
根据第一密钥因子、第二密钥因子生成第一设备与第二设备的共享密钥
104

图 1

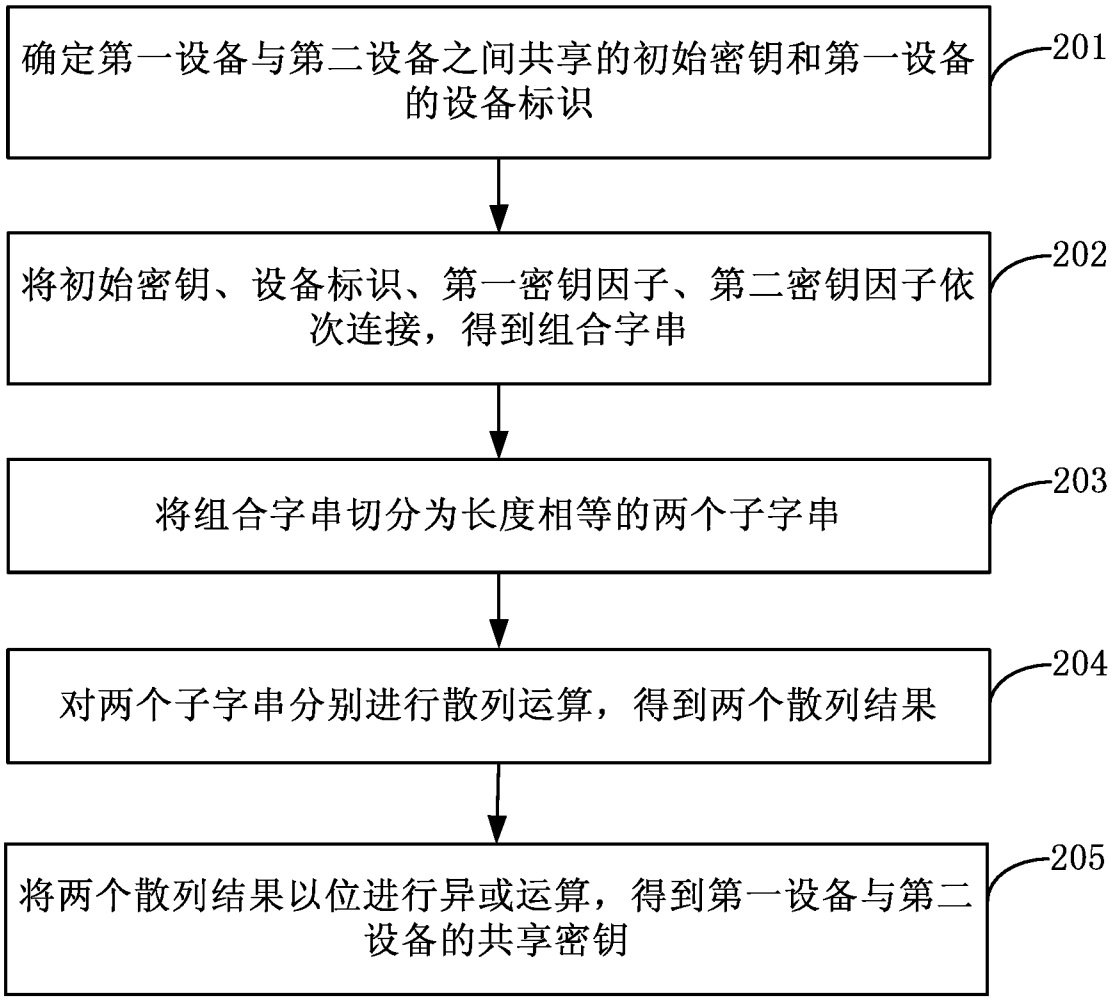
确定第一设备与第二设备之间共享的初始密钥和第一设备的设备标识
201
将初始密钥、设备标识、第一密钥因子、第二密钥因子依次连接，得到组合字串
202
将组合字串切分为长度相等的两个子字串
203
对两个子字串分别进行散列运算，得到两个散列结果
204
将两个散列结果以位进行异或运算，得到第一设备与第二设备的共享密钥
205

图 2

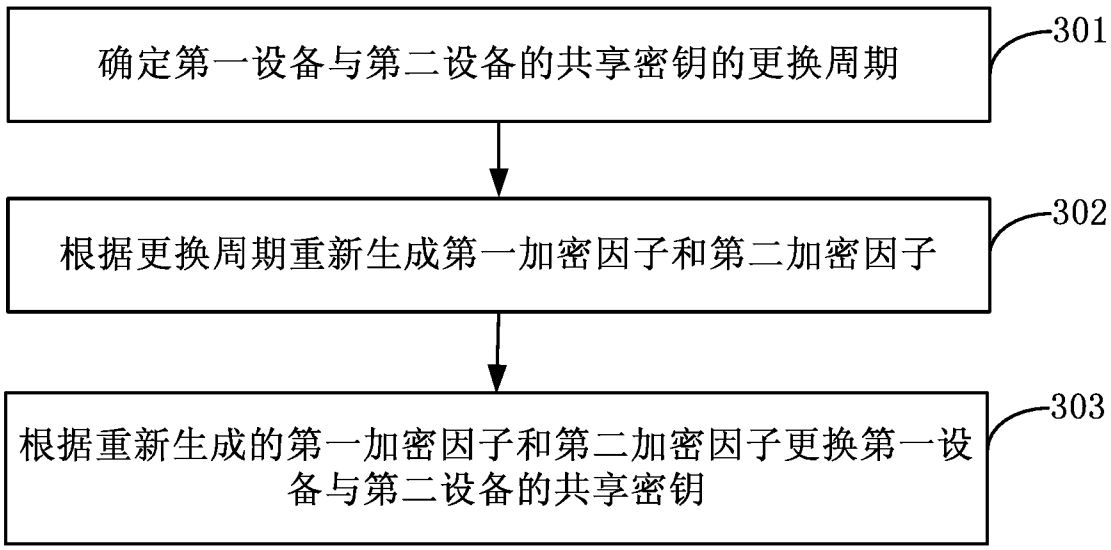
确定第一设备与第二设备的共享密钥的更换周期
301
根据更换周期重新生成第一加密因子和第二加密因子
302
根据重新生成的第一加密因子和第二加密因子更换第一设备与第二设备的共享密钥
303

图 3

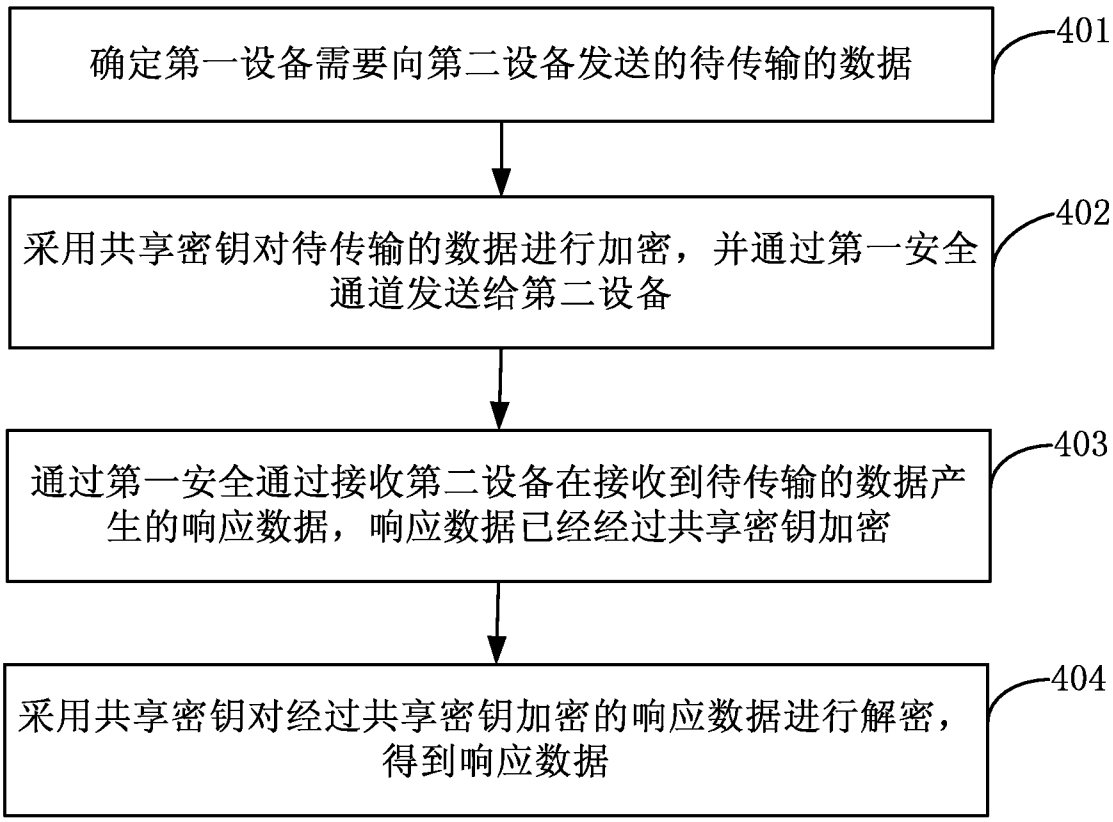
确定第一设备需要向第二设备发送的待传输的数据
401
采用共享密钥对待传输的数据进行加密，并通过第一安全通道发送给第二设备
402
通过第一安全通过接收第二设备在接收到待传输的数据产生的响应数据，响应数据已经经过共享密钥加密
403
采用共享密钥对经过共享密钥加密的响应数据进行解密，得到响应数据
404

图 4

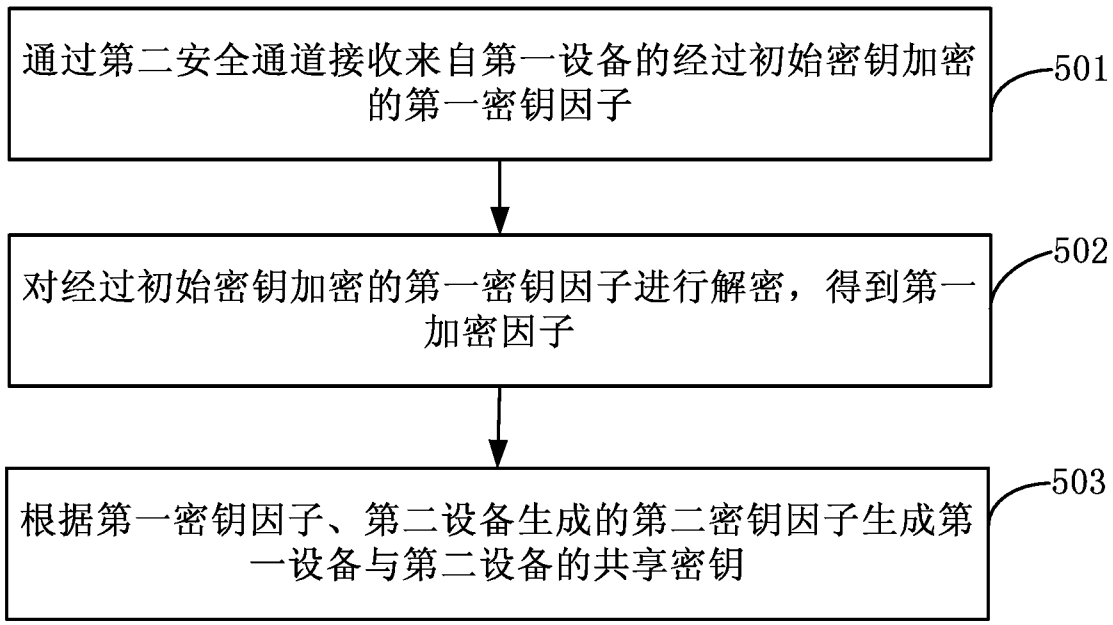
通过第二安全通道接收来自第一设备的经过初始密钥加密的第一密钥因子
501
对经过初始密钥加密的第一密钥因子进行解密，得到第一加密因子
502
根据第一密钥因子、第二设备生成的第二密钥因子生成第一设备与第二设备的共享密钥
503

图 5

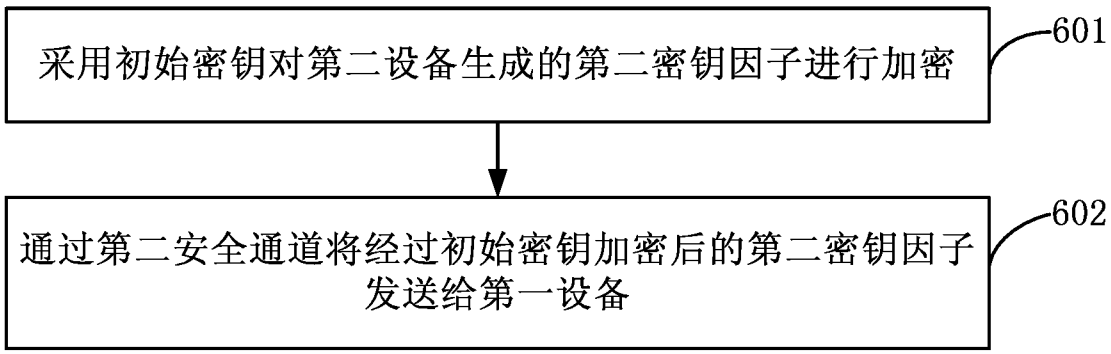
采用初始密钥对第二设备生成的第二密钥因子进行加密
601
通过第二安全通道将经过初始密钥加密后的第二密钥因子发送给第一设备
602

图 6

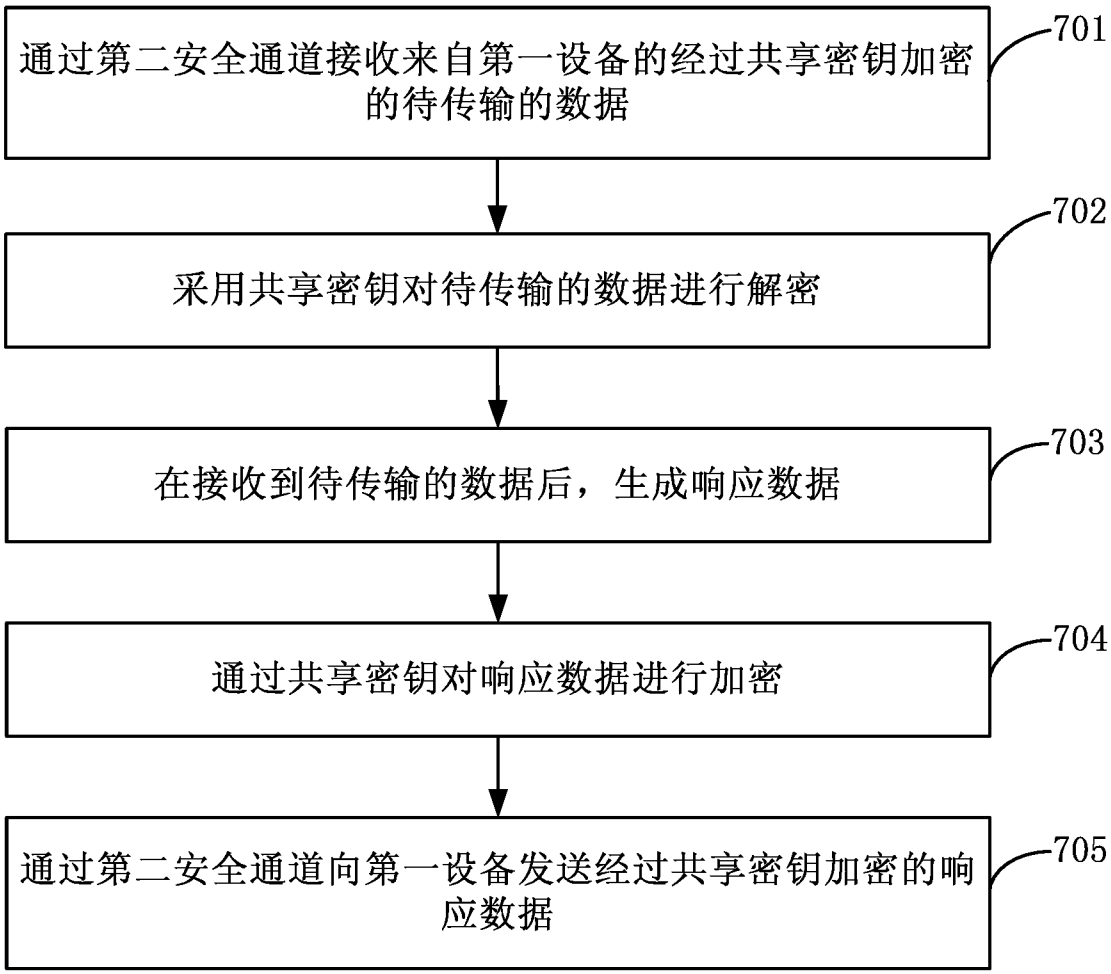
通过第二安全通道接收来自第一设备的经过共享密钥加密的待传输的数据
701
采用共享密钥对待传输的数据进行解密
702
在接收到待传输的数据后，生成响应数据
703
通过共享密钥对响应数据进行加密
704
通过第二安全通道向第一设备发送经过共享密钥加密的响应数据
705

图 7

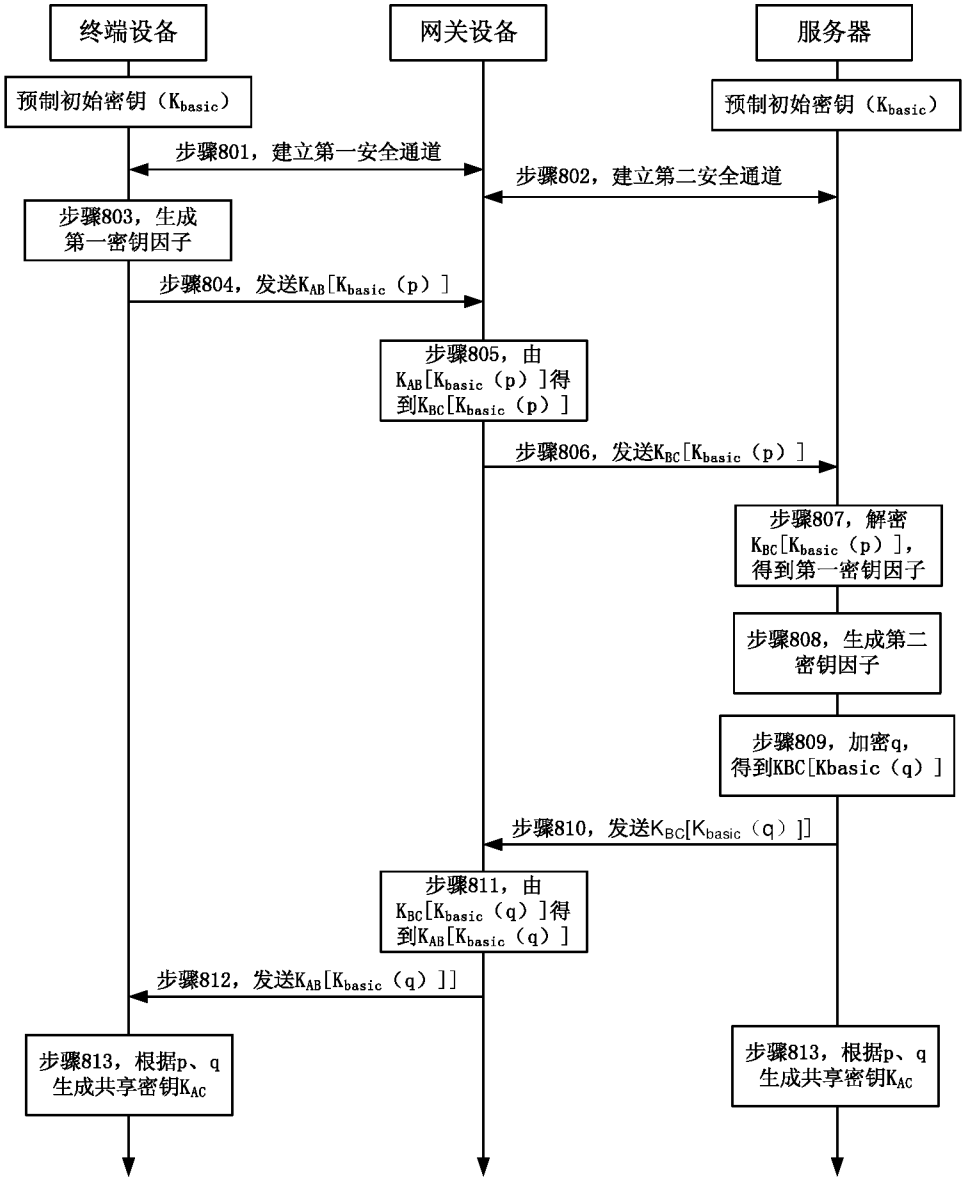
终端设备
网关设备
服务器
预制初始密钥（K_{basic}）
预制初始密钥（K_{basic}）
步骤801，建立第一安全通道
步骤802，建立第二安全通道
步骤803，生成第一密钥因子
步骤804，发送$K_{AB}[K_{basic}（p）]$
步骤805，由$K_{AB}[K_{basic}（p）]$得到$K_{BC}[K_{basic}（p）]$
步骤806，发送$K_{BC}[K_{basic}（p）]$
步骤807，解密$K_{BC}[K_{basic}（p）]$，得到第一密钥因子
步骤808，生成第二密钥因子
步骤809，加密q，得到KBC[Kbasic（q）]
步骤810，发送$K_{BC}[K_{basic}（q）]]$
步骤811，由$K_{BC}[K_{basic}（q）]$得到$K_{AB}[K_{basic}（q）]$
步骤812，发送$K_{AB}[K_{basic}（q）]]$
步骤813，根据p、q生成共享密钥K_{AC}
步骤813，根据p、q生成共享密钥K_{AC}

图 8

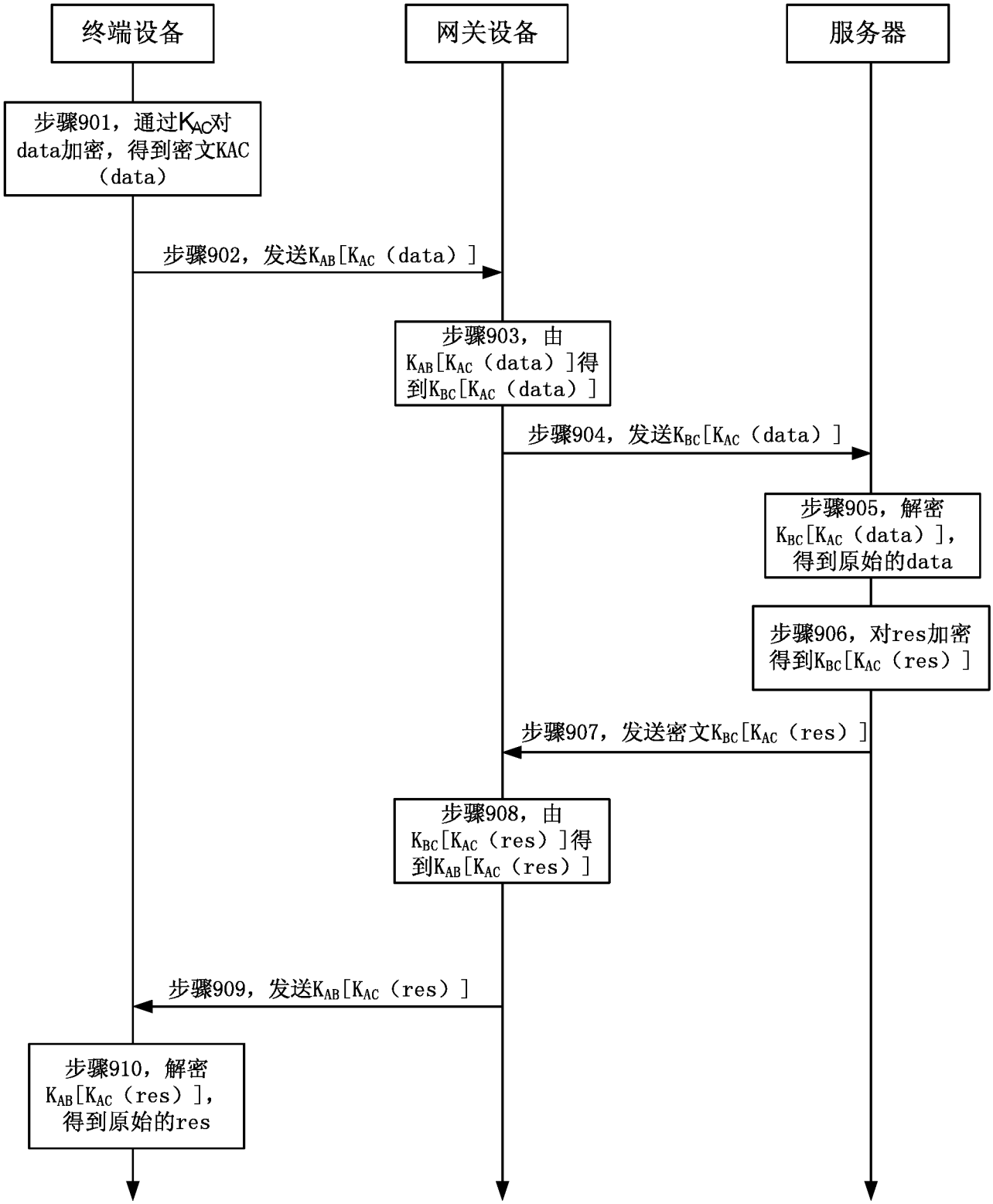
终端设备
网关设备
服务器
步骤901，通过K_{AC}对data加密，得到密文KAC（data）
步骤902，发送$K_{AB}[K_{AC}（data）]$
步骤903，由$K_{AB}[K_{AC}（data）]$得到$K_{BC}[K_{AC}（data）]$
步骤904，发送$K_{BC}[K_{AC}（data）]$
步骤905，解密$K_{BC}[K_{AC}（data）]$，得到原始的data
步骤906，对res加密得到$K_{BC}[K_{AC}（res）]$
步骤907，发送密文$K_{BC}[K_{AC}（res）]$
步骤908，由$K_{BC}[K_{AC}（res）]$得到$K_{AB}[K_{AC}（res）]$
步骤909，发送$K_{AB}[K_{AC}（res）]$
步骤910，解密$K_{AB}[K_{AC}（res）]$，得到原始的res

图 9

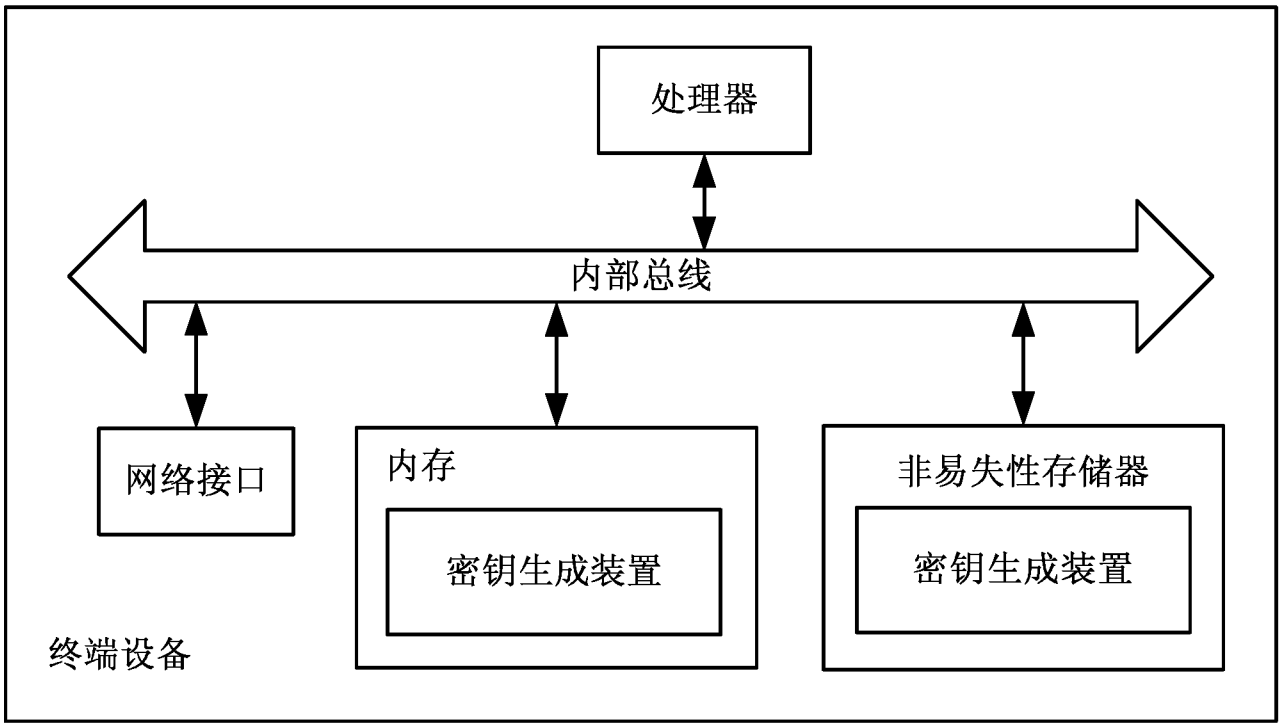
处理器
内部总线
网络接口
内存
密钥生成装置
非易失性存储器
密钥生成装置
终端设备

图 10

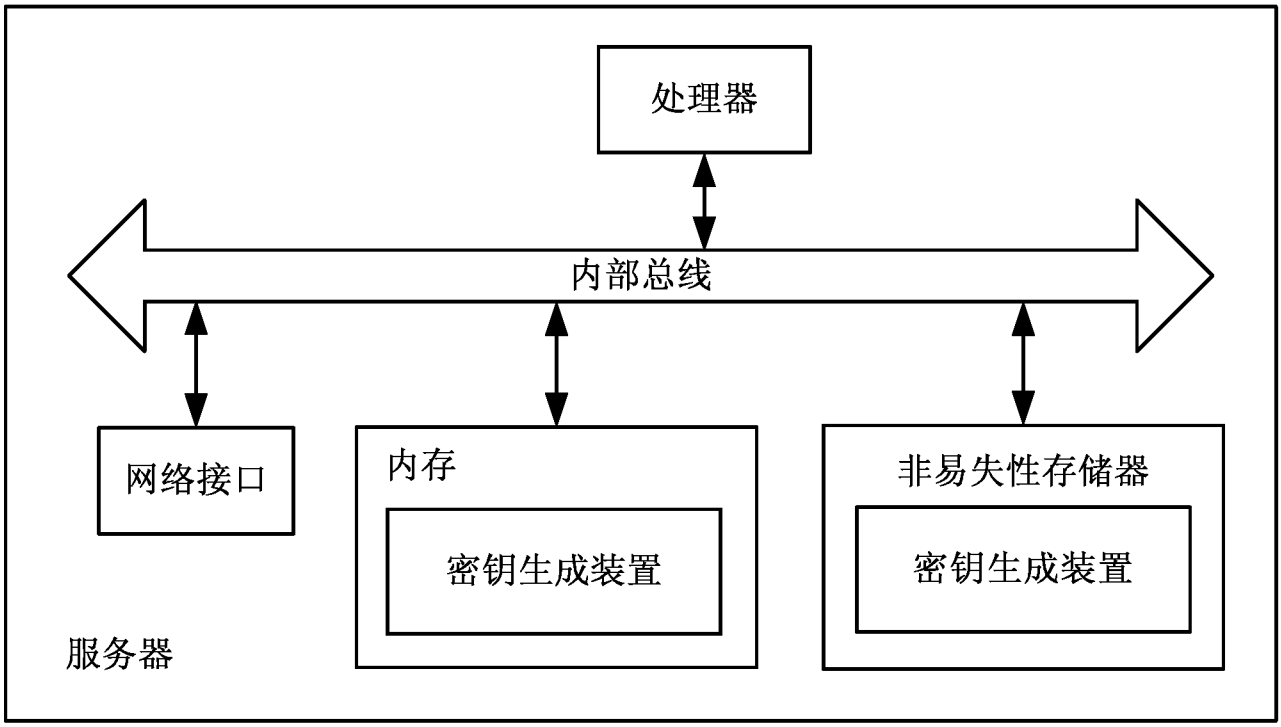
处理器
内部总线
网络接口
内存
密钥生成装置
非易失性存储器
密钥生成装置
服务器

图 11

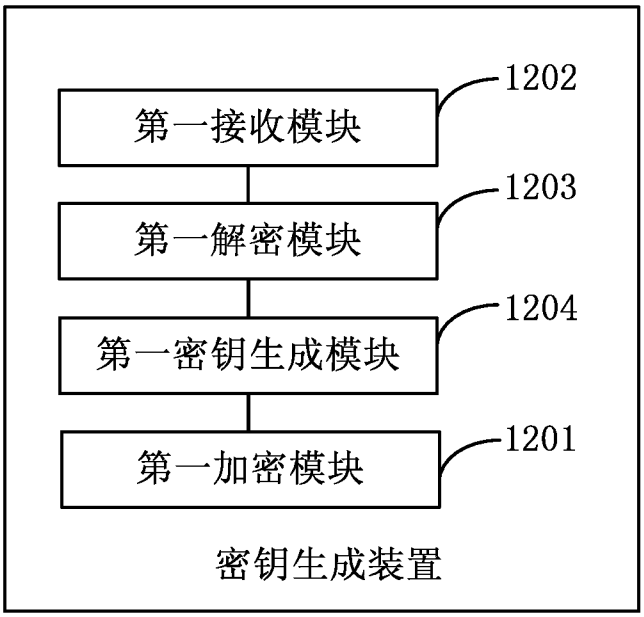
第一接收模块
1202
第一解密模块
1203
第一密钥生成模块
1204
第一加密模块
1201
密钥生成装置

图 12

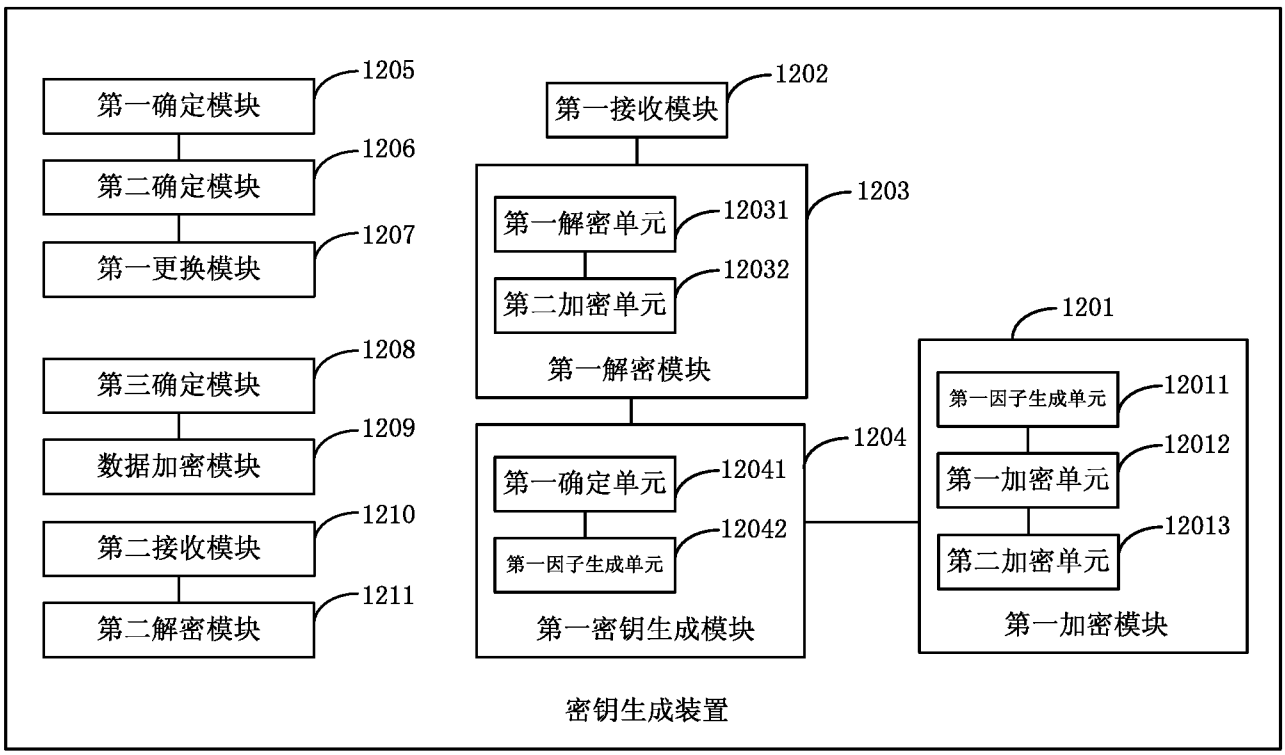
第一确定模块
1205
第二确定模块
1206
第一更换模块
1207
第三确定模块
1208
数据加密模块
1209
第二接收模块
1210
第二解密模块
1211
第一接收模块
1202
第一解密单元
12031
第二加密单元
12032
第一解密模块
1203
第一确定单元
12041
第一因子生成单元
12042
第一密钥生成模块
1204
第一因子生成单元
12011
第一加密单元
12012
第二加密单元
12013
第一加密模块
1201
密钥生成装置

图 13

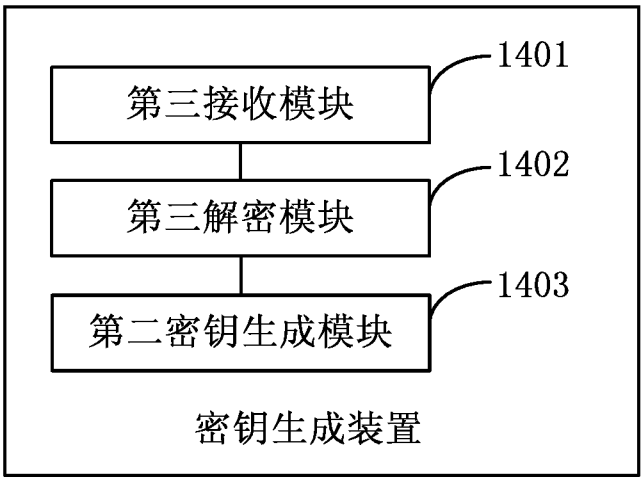
1401
第三接收模块
1402
第三解密模块
1403
第二密钥生成模块
密钥生成装置

图 14

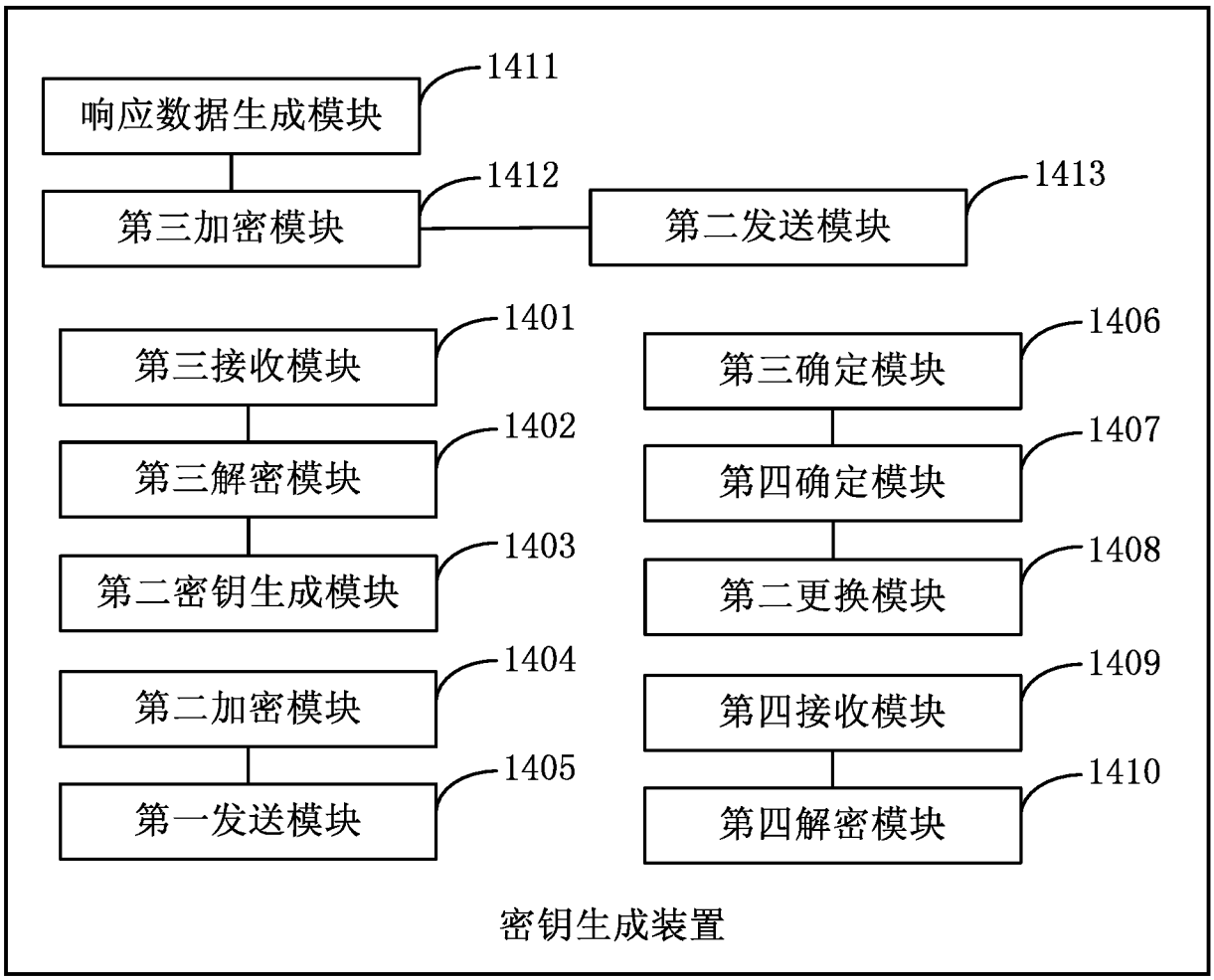
1411
响应数据生成模块
1412
第三加密模块
1413
第二发送模块
1401
第三接收模块
1402
第三解密模块
1403
第二密钥生成模块
1404
第二加密模块
1405
第一发送模块
1406
第三确定模块
1407
第四确定模块
1408
第二更换模块
1409
第四接收模块
1410
第四解密模块
密钥生成装置

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/095522

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

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)

CNTXT; CNABS; VEN; CNKI: key, terminal, device, server, gateway, encrypt, generate, negotiate, 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 103209075 A (NANJING EST ELECTRIC POWER TECHNOLOGY CO., LTD.) 17 July 2013 (17.07.2013) description, paragraphs [0003] and [0004], [0007] to [0011]	1-28
A	CN 104753682 A (CLOUDSEC CENTURY CO., LTD.) 01 July 2015 (01.07.2015) the whole document	1-28
A	WO 2013089725 A1 (INTEL CORP. et al.) 20 June 2013 (20.06.2013) the whole document	1-28

☐ 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 October 2016	09 November 2016
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer ZOU, Ting Telephone No. (86-10) 62089393

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/095522

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103209075 A	17 July 2013	None	
CN 104753682 A	01 July 2015	None	
WO 2013089725 A1	20 June 2013	US 2015039890 A1	05 February 2015
		CN 104170312 A	26 November 2014
		EP 2792100 A1	22 October 2014
		TW 201332331 A	01 August 2013

国际检索报告

国际申请号
PCT/CN2016/095522

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

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）)

CNTXT;CNABS;VEN;CNKI:密钥，终端，设备，服务器，网关，加密，生成，协商，交换，key， terminal， device， server， gateway， encrypt， generate， negotiate， 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 103209075 A (南京易司拓电力科技股份有限公司) 2013年 7月 17日 (2013 - 07 - 17) 说明书第0003-0004，0007-0011段	1-28
A	CN 104753682 A (北京云安世纪科技有限公司) 2015年 7月 1日 (2015 - 07 - 01) 全文	1-28
A	WO 2013089725 A1 (英特尔公司等) 2013年 6月 20日 (2013 - 06 - 20) 全文	1-28

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 10月 28日	2016年 11月 9日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	邹婷
传真号 (86-10)62019451	电话号码 (86-10)62089393

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/CN2016/095522

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	103209075	A	2013年 7月 17日	无			
CN	104753682	A	2015年 7月 1日	无			
WO	2013089725	A1	2013年 6月 20日	US	2015039890	A1	2015年 2月 5日
				CN	104170312	A	2014年 11月 26日
				EP	2792100	A1	2014年 10月 22日
				TW	201332331	A	2013年 8月 1日