

(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
2018 年 5 月 3 日 (03.05.2018)



(10) 国际公布号
WO 2018/076289 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2016/103812

(22) 国际申请日: 2016 年 10 月 28 日 (28.10.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 美的智能家居科技有限公司 (MIDEA SMART TECHNOLOGY CO., LTD.) [CN/CN]; 中国广东省深圳市南山区前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518000 (CN)。美的集团股份有限公司 (MIDEA GROUP CO., LTD.) [CN/CN]; 中国广东省佛山市顺德区北滘镇美的大道 6 号美的总部大楼 B 区 26-28 楼, Guangdong 528311 (CN)。

(72) 发明人: 刘复鑫 (LIU, Fuxin); 中国广东省深圳市南山区前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518000 (CN)。

(74) 代理人: 北京清亦华知识产权代理事务所 (普通合伙) (TSINGYIHUA INTELLECTUAL PROPERTY LLC); 中国北京市海淀区清华园清华大学照澜院商业楼 301 室, Beijing 100084 (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, DJ, 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, 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,

(54) Title: KEY NEGOTIATION METHOD AND DEVICE

(54) 发明名称: 密钥协商方法及装置

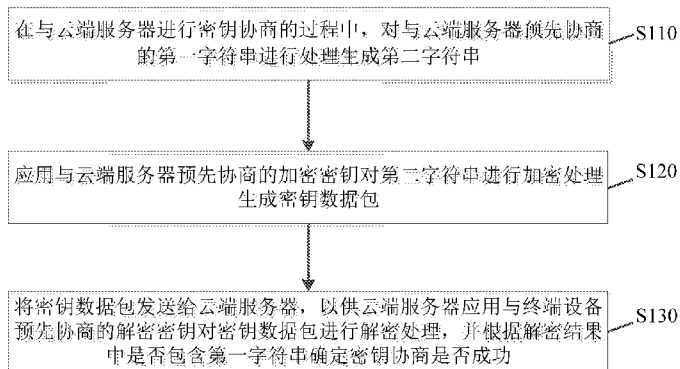


图 2

S110 DURING THE PROCESS OF KEY NEGOTIATION WITH A CLOUD SERVER, PROCESSING A FIRST CHARACTER STRING NEGOTIATED WITH THE CLOUD SERVER IN ADVANCE TO GENERATE A SECOND CHARACTER STRING
S120 ENCRYPTING THE SECOND CHARACTER STRING USING AN ENCRYPTION KEY NEGOTIATED WITH THE CLOUD SERVER IN ADVANCE SO AS TO GENERATE A KEY DATA PACKET
S130 SENDING THE KEY DATA PACKET TO THE CLOUD SERVER, SO THAT THE CLOUD SERVER DECRYPTS THE KEY DATA PACKET USING A DECRYPTION KEY NEGOTIATED WITH A TERMINAL DEVICE IN ADVANCE, AND DETERMINING WHETHER KEY NEGOTIATION IS SUCCESSFUL DEPENDING ON WHETHER A DECRYPTION RESULT INCLUDES THE FIRST CHARACTER STRING

(57) Abstract: Disclosed are a key negotiation method and device. The method comprises: during the process of key negotiation with a cloud server, processing a first character string negotiated with the cloud server in advance to generate a second character string; encrypting the second character string using an encryption key negotiated with the cloud server in advance so as to generate a key data packet; and sending the key data packet to the cloud server, so that the cloud server decrypts the key data packet using a decryption key negotiated with a terminal device in advance, and determining whether key negotiation is successful depending on whether a decryption

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, 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))。

result includes the first character string. Therefore, by processing a character string negotiated in advance to generate a key data packet with no regulation, the complexity of a ciphertext increases, and the security of key negotiation is improved.

(57) 摘要: 本申请公开了一种密钥协商方法及装置。其中, 该方法包括: 在与云端服务器进行密钥协商的过程中, 对与云端服务器预先协商的第一字符串进行处理生成第二字符串; 应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包; 将密钥数据包发送给云端服务器, 以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理, 并根据解密结果中是否包含第一字符串确定密钥协商是否成功。由此, 通过对预先协商的字符串进行处理, 以生成无规律可循的密钥数据包, 增加了密文的复杂性, 提高了密钥协商的安全性。

密钥协商方法及装置

技术领域

5 本申请涉及信息安全技术领域，尤其涉及一种密钥协商方法及装置。

背景技术

通常，终端设备与服务器进行通信时需要考虑到数据传输的安全性问题。为了保证传输数据的安全性，不被泄露。一般通过非对称算法先协商出通信密钥，然后用对称算法用
10 协商出来的密钥进行加密解密。

然而，上述密钥协商的过程中，使用固定的字符串作为密钥协商的确认包，存在一定的规律性，安全性低。

发明内容

15 本申请的目的旨在至少在一定程度上解决相关技术中的技术问题之一。

为此，本申请的第一个目的在于提出一种密钥协商方法，该方法通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

本申请的第二个目的在于提出另一种密钥协商方法。

20 本申请的第三个目的在于提出一种密钥协商装置。

本申请的第四个目的在于提出另一种密钥协商装置。

本发明的第五个目的在于提出一种设备。

本发明的第六个目的在于提出另一种设备。

本发明的第七个目的在于提出一种非易失性计算机存储介质。

25 本发明的第八个目的在于提出另一种非易失性计算机存储介质。

为达上述目的，根据本申请第一方面实施例提出的一种密钥协商方法，包括：在与云端服务器进行密钥协商的过程中，对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串；应用与所述云端服务器预先协商的加密密钥对所述第二字符串进行加密处理生成密钥数据包；将所述密钥数据包发送给所述云端服务器，以供所述云端服务器应用
30 与终端设备预先协商的解密密钥对所述密钥数据包进行解密处理，并根据解密结果中是否包含所述第一字符串确定密钥协商是否成功。

本申请实施例的密钥协商方法，首先在与云端服务器进行密钥协商的过程中，对与云

端服务器预先协商的第一字符串进行处理生成第二字符串，接着应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，最后将密钥数据包发送给云端服务器，以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理，并根据解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

另外，根据本申请上述实施例的密钥协商方法还可以具有如下附加的技术特征：

在本申请的一个实施例中，所述对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串，包括：按照预设周期通过随机数发生器生成预设长度的随机数；将所述随机数与所述第一字符串进行拼接处理生成第二字符串。

在本申请的一个实施例中，所述对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串，包括：应用预设算法获取与所述第一字符串对应的参考字符；将所述参考字符与所述第一字符串进行拼接处理生成第二字符串。

为达上述目的，根据本申请第二方面实施例提出的另一种密钥协商方法，包括：在与终端设备进行密钥协商的过程中，接收所述终端设备发送的密钥数据包，其中，所述密钥数据包是所述终端设备应用与所述云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，所述第二字符串是所述终端设备对与云端服务器预先协商的第一字符串进行处理生成的；应用与所述终端设备预先协商的解密密钥对所述密钥数据包进行解密处理获取解密结果；检测所述解密结果中是否包含所述第一字符串确定密钥协商是否成功。

本申请实施例的密钥协商方法，首先在与终端设备进行密钥协商的过程中，接收终端设备发送的密钥数据包，其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的，接着应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理获取解密结果，最后检测解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

另外，根据本申请上述实施例的密钥协商方法还可以具有如下附加的技术特征：

在本申请的一个实施例中，所述的方法，还包括：如果检测获知所述解密结果中包含所述第一字符串，则应用与所述终端设备协商的密钥信息对交互信息进行加密或解密处理。

为达上述目的，根据本申请第三方面实施例提出的一种密钥协商装置，包括：第一处理模块，用于在与云端服务器进行密钥协商的过程中，对与所述云端服务器预先协商的第

一字符串进行处理生成第二字符串；加密模块，用于应用与所述云端服务器预先协商的加密密钥对所述第二字符串进行加密处理生成密钥数据包；发送模块，用于将所述密钥数据包发送给所述云端服务器，以供所述云端服务器应用与终端设备预先协商的解密密钥对所述密钥数据包进行解密处理，并根据解密结果中是否包含所述第一字符串确定密钥协商是否成功。

本申请实施例的密钥协商装置，首先在与云端服务器进行密钥协商的过程中，对与云端服务器预先协商的第一字符串进行处理生成第二字符串，接着应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，最后将密钥数据包发送给云端服务器，以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理，并根据解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

另外，根据本申请上述实施例的密钥协商装置还可以具有如下附加的技术特征：

在本申请的一个实施例中，所述第一处理模块用于：按照预设周期通过随机数发生器生成预设长度的随机数；将所述随机数与所述第一字符串进行拼接处理生成第二字符串。

在本申请的一个实施例中，所述第一处理模块还用于：应用预设算法获取与所述第一字符串对应的参考字符；将所述参考字符与所述第一字符串进行拼接处理生成第二字符串。

为达上述目的，根据本申请第四方面实施例提出的一种密钥协商装置，包括：接收模块，用于在与终端设备进行密钥协商的过程中，接收所述终端设备发送的密钥数据包，其中，所述密钥数据包是所述终端设备应用与所述云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，所述第二字符串是所述终端设备对与云端服务器预先协商的第一字符串进行处理生成的；解密模块，用于应用与所述终端设备预先协商的解密密钥对所述密钥数据包进行解密处理获取解密结果；检测模块，用于检测所述解密结果中是否包含所述第一字符串确定密钥协商是否成功。

本申请实施例的密钥协商装置，首先在与终端设备进行密钥协商的过程中，接收终端设备发送的密钥数据包，其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的，接着应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理获取解密结果，最后检测解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

另外，根据本申请上述实施例的密钥协商装置还可以具有如下附加的技术特征：

在本申请的一个实施例中，所述的装置，还包括：第二处理模块，用于在检测获知所述解密结果中包含所述第一字符串时，应用与所述终端设备协商的密钥信息对交互信息进行加密或解密处理。

5 本发明第五方面实施例提供了一种设备，包括：一个或者多个处理器；存储器；一个或者多个程序，所述一个或者多个程序存储在所述存储器中，当被所述一个或者多个处理器执行时，执行以下步骤：在与云端服务器进行密钥协商的过程中，对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串；应用与所述云端服务器预先协商的加密密钥对所述第二字符串进行加密处理生成密钥数据包；将所述密钥数据包发送给所述云端服务器，以供所述云端服务器应用与终端设备预先协商的解密密钥对所述密钥数据包进行
10 解密处理，并根据解密结果中是否包含所述第一字符串确定密钥协商是否成功。

本申请实施例的设备，首先在与云端服务器进行密钥协商的过程中，对与云端服务器预先协商的第一字符串进行处理生成第二字符串，接着应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，最后将密钥数据包发送给云端服务器，以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理，并根据
15 解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

本发明第六方面实施例提供了一种设备，包括：一个或者多个处理器；存储器；一个或者多个程序，所述一个或者多个程序存储在所述存储器中，当被所述一个或者多个处理器
20 器执行时，执行以下步骤：在与终端设备进行密钥协商的过程中，接收所述终端设备发送的密钥数据包，其中，所述密钥数据包是所述终端设备应用与所述云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，所述第二字符串是所述终端设备对与云端服务器预先协商的第一字符串进行处理生成的；应用与所述终端设备预先协商的解密密钥对所述密钥数据包进行解密处理获取解密结果；检测所述解密结果中是否包
25 含所述第一字符串确定密钥协商是否成功。

本申请实施例的设备，首先在与终端设备进行密钥协商的过程中，接收终端设备发送的密钥数据包，其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的，接着应用与终端设备预先协商的解密密钥对密钥数
30 据包进行解密处理获取解密结果，最后检测解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

本发明第七方面实施例提供了一种非易失性计算机存储介质，所述计算机存储介质存储有一个或者多个程序，当所述一个或者多个程序被一个设备执行时，使得所述设备执行以下步骤：在与云端服务器进行密钥协商的过程中，对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串；应用与所述云端服务器预先协商的加密密钥对所述第二字符串进行加密处理生成密钥数据包；将所述密钥数据包发送给所述云端服务器，以供所述云端服务器应用与终端设备预先协商的解密密钥对所述密钥数据包进行解密处理，并根据解密结果中是否包含所述第一字符串确定密钥协商是否成功。

本申请实施例的非易失性计算机存储介质，首先在与云端服务器进行密钥协商的过程中，对与云端服务器预先协商的第一字符串进行处理生成第二字符串，接着应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，最后将密钥数据包发送给云端服务器，以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理，并根据解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

本发明第八方面实施例提供了一种非易失性计算机存储介质，所述计算机存储介质存储有一个或者多个程序，当所述一个或者多个程序被一个设备执行时，使得所述设备执行以下步骤：在与终端设备进行密钥协商的过程中，接收所述终端设备发送的密钥数据包，其中，所述密钥数据包是所述终端设备应用与所述云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，所述第二字符串是所述终端设备对与云端服务器预先协商的第一字符串进行处理生成的；应用与所述终端设备预先协商的解密密钥对所述密钥数据包进行解密处理获取解密结果；检测所述解密结果中是否包含所述第一字符串确定密钥协商是否成功。

本申请实施例的非易失性计算机存储介质，首先在与终端设备进行密钥协商的过程中，接收终端设备发送的密钥数据包，其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的，接着应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理获取解密结果，最后检测解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

本申请附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本申请的实践了解到。

附图说明

本申请的上述和/或附加的方面和优点从结合下面附图对实施例的描述中将变得明显和容易理解，其中：

图 1 是根据本申请一个实施例的终端设备与云端服务器数据传输的示意图；

5 图 2 是根据本申请一个实施例的密钥协商方法的流程图；

图 3 是根据本申请另一个实施例的密钥协商方法的流程图；

图 4 是根据本申请一个实施例的密钥协商装置的结构示意图；

图 5 是根据本申请另一个实施例的密钥协商装置的结构示意图。

10 具体实施方式

下面详细描述本申请的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本申请，而不能理解为对本申请的限制。

下面参考附图描述本申请实施例的密钥协商方法及装置。

15 通常，通过非对称算法先协商出通信密钥，然后用对称算法用协商出来的密钥进行加密解密，以保证终端设备与云端服务器进行通信时传输数据的安全性。

其中，非对称密钥协商是在终端设备与云端服务器使用非对称密钥进行密钥协商之后，终端设备和云端服务器会对一串双方都已知的字符串进行加密、解密。通过解密之后的明文的比对来确认协商的密钥是否正确。

20 图 1 是根据本申请一个实施例的终端设备与云端服务器数据传输的示意图。

如图 1 所示，终端设备发起密钥协商请求，接着云端服务器对密钥协商响应，最后终端设备对密钥协商进行确认后，两者进行数据的安全传输。举例说明如下：

具体地，终端设备与云端服务器之间约定对“OK”的密文和明文操作作为密钥协商的确认。在密钥协商的最后一次终端设备与云端服务器交互的时候，终端设备使用协商出来的密钥对“OK”进行加密，然后将密文发送给云端服务器，云端服务器使用协商出来的密
25 钥对密文进行解密，如果解密出来的明文是“OK”，则确认密钥协商完成。

然而，上述密钥协商的过程中，使用固定的字符串作为密钥协商的确认包，存在一定的规律性，安全性低。

为了解决上述问题，本申请实施例提出的密钥协商方法，通过对预先协商的字符串进
30 行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。具体如下：

图 2 是根据本申请一个实施例的密钥协商方法的流程图。

如图 2 所示, 本申请实施例的密钥协商方法包括:

步骤 110, 在与云端服务器进行密钥协商的过程中, 对与云端服务器预先协商的第一字符串进行处理生成第二字符串。

具体地, 在终端设备发起密钥协商请求, 接着云端服务器对密钥协商响应, 最后终端设备对密钥协商进行确认。通过对终端设备与云端服务器预先协商的第一字符串进行处理以生成第二字符串。

其中, 第一字符串可以是字母、数字和特殊符号等中的一种或者多种。

其中, 对与云端服务器预先协商的第一字符串进行处理生成第二字符串的方式有很多种, 可以根据需要进行选择。举例说明如下:

10 第一种示例, 首先按照预设周期通过随机数发生器生成预设长度的随机数, 接着将随机数与第一字符串进行拼接处理生成第二字符串。

其中, 预设周期可以根据需要进行设置, 例如 10 分钟、20 分钟等。

其中, 预设长度可以根据需要进行设置, 例如 5 个字符串、10 个字符串等。

其中, 随机数可以是字母、数字和特殊符号等中的一种或者多种。

15 需要说明的是, 拼接处理可以理解为“随机数+第一字符串”、也可以理解为“第一字符串+随机数”、还可以理解为随机数任意插入第一字符串的各个字符之间等。

举例而言, 第一字符串为 4 位字符, 在其后面拼接上随机数发生器生成的 12 位的随机数组成第二字符串。

20 第二种示例, 首先应用预设算法获取与第一字符串对应的参考字符, 接着将参考字符与第一字符串进行拼接处理生成第二字符串。

具体地, 通过在终端设备中预先设置一种算法, 通过应用预设算法获取与第一字符串对应的参考字符。

其中, 参考字符可以是字母、数字和特殊符号等中的一种或者多种。

25 需要说明的是, 拼接处理可以理解为“参考字符+第一字符串”、也可以理解为“第一字符串+参考字符”、还可以理解为参考字符任意插入第一字符串的各个字符之间等。

步骤 120, 应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包。

30 步骤 130, 将密钥数据包发送给云端服务器, 以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理, 并根据解密结果中是否包含第一字符串确定密钥协商是否成功。

具体地, 可以通过例如 MD5 加密算法、DES 加密算法和 RSA 加密算法等, 应用与云端服务器预先协商的加密密钥对第二字符串进行加密得到的结果作为密钥数据包。

进一步，将密钥数据包发送给云端服务器，云端服务器会利用相应的解密算法，应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理。

进一步地，判断解密结果中是否包含第一字符串以确定终端设备与服务器协商是否成功。

5 可以理解的是，在解密结果找到第一字符串，表示终端设备与云端服务器之间是可以建立连接以进行数据传输。进一步提高密钥协商的安全性。

可以理解的是，在解密结果没有找到第一字符串，表示终端设备与云端服务器之间是不可以建立连接，不能进行数据传输。进一步提高密钥协商的安全性。

本申请实施例的密钥协商方法，首先在与云端服务器进行密钥协商的过程中，对与云端服务器预先协商的第一字符串进行处理生成第二字符串，接着应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，最后将密钥数据包发送给云端服务器，以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理，并根据解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

10 15

图 3 是根据本申请另一个实施例的密钥协商方法的流程图。

如图 3 所示，本申请实施例的密钥协商方法包括：

步骤 210，在与终端设备进行密钥协商的过程中，接收终端设备发送的密钥数据包，其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的。

20

具体地，在终端设备发起密钥协商请求，接着云端服务器对密钥协商响应，最后终端设备对密钥协商进行确认。首先接收终端设备发送的密钥数据包。

其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包。第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的。

25

需要说明的是，如何根据与云端服务器预先协商的第一字符串进行处理生成的第二字符串以及如何根据与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包的具体过程可以参见步骤 110。此处不再详述。

步骤 220，应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理获取解密结果。

30

步骤 230，检测解密结果中是否包含第一字符串确定密钥协商是否成功。

具体地，在接收到数据包后应用于加密算法对应的解密算法，利用与终端设备预先协商的解密密钥对密钥数据包进行解密处理获取解密结果，并进一步检测解密结果中是否包含第一字符串。

进一步，将密钥数据包发送给云端服务器，云端服务器会利用相应的解密算法，应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理。

进一步地，判断解密结果中是否包含第一字符串以确定终端设备与服务器协商是否成功。

需要说明的是，在检测获知解密结果中包含第一字符串时应用与终端设备协商的密钥信息对交互信息进行加密或解密处理。即在密钥协商结束以后，可以利用与终端设备协商的密钥信息对交互信息进行处理，可以是加密、解密等一种或者多种。

本申请实施例的密钥协商方法，首先在与终端设备进行密钥协商的过程中，接收终端设备发送的密钥数据包，其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的，接着应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理获取解密结果，最后检测解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

为了实现本申请还提出一种密钥协商装置。

图 4 是根据本申请一个实施例的密钥协商装置的结构示意图。

如图 4 所示，该密钥协商包括：第一处理模块 41、加密模块 42 和发送模块 43。

其中，第一处理模块 41 用于在与云端服务器进行密钥协商的过程中，对与云端服务器预先协商的第一字符串进行处理生成第二字符串。

加密模块 42 用于应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包。

发送模块 43 用于将密钥数据包发送给云端服务器，以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理，并根据解密结果中是否包含第一字符串确定密钥协商是否成功。

其中，在本申请的一个实施例中，第一处理模块 41 用于：按照预设周期通过随机数发生器生成预设长度的随机数；将随机数与所述第一字符串进行拼接处理生成第二字符串。

其中，在本申请的一个实施例中，第一处理模块 41 还用于：应用预设算法获取与第一字符串对应的参考字符；将参考字符与第一字符串进行拼接处理生成第二字符串。

本发明实施例提供的密钥协商装置与上述第一方面实施例提供的密钥协商方法相对应，因此在前述密钥协商方法的实施方式也适用于本实施例提供的密钥协商装置，在本实施例中不再详细描述。

5 本申请实施例的密钥协商装置，首先在与云端服务器进行密钥协商的过程中，对与云端服务器预先协商的第一字符串进行处理生成第二字符串，接着应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，最后将密钥数据包发送给云端服务器，以供云端服务器应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理，并根据解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

图 5 是根据本申请另一个实施例的密钥协商装置的结构示意图。

如图 5 所示，该密钥协商装置包括：接收模块 51、解密模块 52 和检测模块 53。

其中，接收模块 51 用于在与终端设备进行密钥协商的过程中，接收终端设备发送的密钥数据包，其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的。

解密模块 52 用于应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理获取解密结果。

检测模块 53 用于检测解密结果中是否包含第一字符串确定密钥协商是否成功。

20 其中，在本申请的一个实施例中，该密钥协商装置还包括第二处理模块 54。

其中，第二处理模块 54 用于在检测获知解密结果中包含第一字符串时，应用与终端设备协商的密钥信息对交互信息进行加密或解密处理。

25 本发明实施例提供的密钥协商装置与上述第二一方面实施例提供的密钥协商方法相对应，因此在前述密钥协商方法的实施方式也适用于本实施例提供的密钥协商装置，在本实施例中不再详细描述。

30 本申请实施例的密钥协商装置，首先在与终端设备进行密钥协商的过程中，接收终端设备发送的密钥数据包，其中，密钥数据包是终端设备应用与云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，第二字符串是终端设备对与云端服务器预先协商的第一字符串进行处理生成的，接着应用与终端设备预先协商的解密密钥对密钥数据包进行解密处理获取解密结果，最后检测解密结果中是否包含第一字符串确定密钥协商是否成功。由此，通过对预先协商的字符串进行处理，以生成无规律可循的密钥数据包，增加了密文的复杂性，提高了密钥协商的安全性。

此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本申请的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

5 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本申请的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本申请的实施例所属技术领域的技术人员所理解。

10 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

15

 尽管上面已经示出和描述了本申请的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本申请的限制，本领域的普通技术人员在本申请的范围内可以对上述实施例进行变化、修改、替换和变型。

20

权利要求书

1、一种密钥协商方法，其特征在于，包括以下步骤：

在与云端服务器进行密钥协商的过程中，对与所述云端服务器预先协商的第一字符串
5 进行处理生成第二字符串；

应用与所述云端服务器预先协商的加密密钥对所述第二字符串进行加密处理生成密钥数据包；

将所述密钥数据包发送给所述云端服务器，以供所述云端服务器应用与终端设备预先
10 协商的解密密钥对所述密钥数据包进行解密处理，并根据解密结果中是否包含所述第一字符串确定密钥协商是否成功。

2、如权利要求 1 所述的方法，其特征在于，所述对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串，包括：

按照预设周期通过随机数发生器生成预设长度的随机数；

将所述随机数与所述第一字符串进行拼接处理生成第二字符串。

3、如权利要求 1 所述的方法，其特征在于，所述对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串，包括：

应用预设算法获取与所述第一字符串对应的参考字符；

将所述参考字符与所述第一字符串进行拼接处理生成第二字符串。

4、一种密钥协商方法，其特征在于，包括以下步骤：

在与终端设备进行密钥协商的过程中，接收所述终端设备发送的密钥数据包，其中，
20 所述密钥数据包是所述终端设备应用与所述云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，所述第二字符串是所述终端设备对与云端服务器预先协商的第一字符串进行处理生成的；

应用与所述终端设备预先协商的解密密钥对所述密钥数据包进行解密处理获取解密结
25 果；

检测所述解密结果中是否包含所述第一字符串确定密钥协商是否成功。

5、如权利要求 4 所述的方法，其特征在于，还包括：

如果检测获知所述解密结果中包含所述第一字符串，则应用与所述终端设备协商的密钥信息对交互信息进行加密或解密处理。

6、一种密钥协商装置，其特征在于，包括：

第一处理模块，用于在与云端服务器进行密钥协商的过程中，对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串；

加密模块，用于应用与所述云端服务器预先协商的加密密钥对所述第二字符串进行加密处理生成密钥数据包；

发送模块，用于将所述密钥数据包发送给所述云端服务器，以供所述云端服务器应用与终端设备预先协商的解密密钥对所述密钥数据包进行解密处理，并根据解密结果中是否包含所述第一字符串确定密钥协商是否成功。

7、如权利要求6所述的装置，其特征在于，所述第一处理模块用于：

按照预设周期通过随机数发生器生成预设长度的随机数；

将所述随机数与所述第一字符串进行拼接处理生成第二字符串。

8、如权利要求6所述的装置，其特征在于，所述第一处理模块还用于：

应用预设算法获取与所述第一字符串对应的参考字符；

将所述参考字符与所述第一字符串进行拼接处理生成第二字符串。

9、一种密钥协商装置，其特征在于，包括：

接收模块，用于在与终端设备进行密钥协商的过程中，接收所述终端设备发送的密钥数据包，其中，所述密钥数据包是所述终端设备应用与所述云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，所述第二字符串是所述终端设备对与云端服务器预先协商的第一字符串进行处理生成的；

解密模块，用于应用与所述终端设备预先协商的解密密钥对所述密钥数据包进行解密处理获取解密结果；

检测模块，用于检测所述解密结果中是否包含所述第一字符串确定密钥协商是否成功。

10、如权利要求9所述的装置，其特征在于，还包括：

第二处理模块，用于在检测获知所述解密结果中包含所述第一字符串时，应用与所述终端设备协商的密钥信息对交互信息进行加密或解密处理。

11、一种设备，其特征在于，包括：

一个或者多个处理器；

存储器；

一个或者多个程序，所述一个或者多个程序存储在所述存储器中，当被所述一个或者多个处理器执行时，执行以下步骤：

在与云端服务器进行密钥协商的过程中，对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串；

应用与所述云端服务器预先协商的加密密钥对所述第二字符串进行加密处理生成密钥数据包；

将所述密钥数据包发送给所述云端服务器，以供所述云端服务器应用与终端设备预先

协商的解密密钥对所述密钥数据包进行解密处理，并根据解密结果中是否包含所述第一字符串确定密钥协商是否成功。

12、一种设备，其特征在于，包括：

一个或者多个处理器；

5 存储器；

一个或者多个程序，所述一个或者多个程序存储在所述存储器中，当被所述一个或者多个处理器执行时，执行以下步骤：

在与终端设备进行密钥协商的过程中，接收所述终端设备发送的密钥数据包，其中，所述密钥数据包是所述终端设备应用与所述云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，所述第二字符串是所述终端设备对与云端服务器预先协商的第一字符串进行处理生成的；

应用与所述终端设备预先协商的解密密钥对所述密钥数据包进行解密处理获取解密结果；

检测所述解密结果中是否包含所述第一字符串确定密钥协商是否成功。

15 13、一种非易失性计算机存储介质，其特征在于，所述计算机存储介质存储有一个或者多个程序，当所述一个或者多个程序被一个设备执行时，使得所述设备执行以下步骤：

在与云端服务器进行密钥协商的过程中，对与所述云端服务器预先协商的第一字符串进行处理生成第二字符串；

应用与所述云端服务器预先协商的加密密钥对所述第二字符串进行加密处理生成密钥数据包；

将所述密钥数据包发送给所述云端服务器，以供所述云端服务器应用与终端设备预先协商的解密密钥对所述密钥数据包进行解密处理，并根据解密结果中是否包含所述第一字符串确定密钥协商是否成功。

25 14、一种非易失性计算机存储介质，其特征在于，所述计算机存储介质存储有一个或者多个程序，当所述一个或者多个程序被一个设备执行时，使得所述设备执行以下步骤：

在与终端设备进行密钥协商的过程中，接收所述终端设备发送的密钥数据包，其中，所述密钥数据包是所述终端设备应用与所述云端服务器预先协商的加密密钥对第二字符串进行加密处理生成密钥数据包，其中，所述第二字符串是所述终端设备对与云端服务器预先协商的第一字符串进行处理生成的；

30 应用与所述终端设备预先协商的解密密钥对所述密钥数据包进行解密处理获取解密结果；

检测所述解密结果中是否包含所述第一字符串确定密钥协商是否成功。

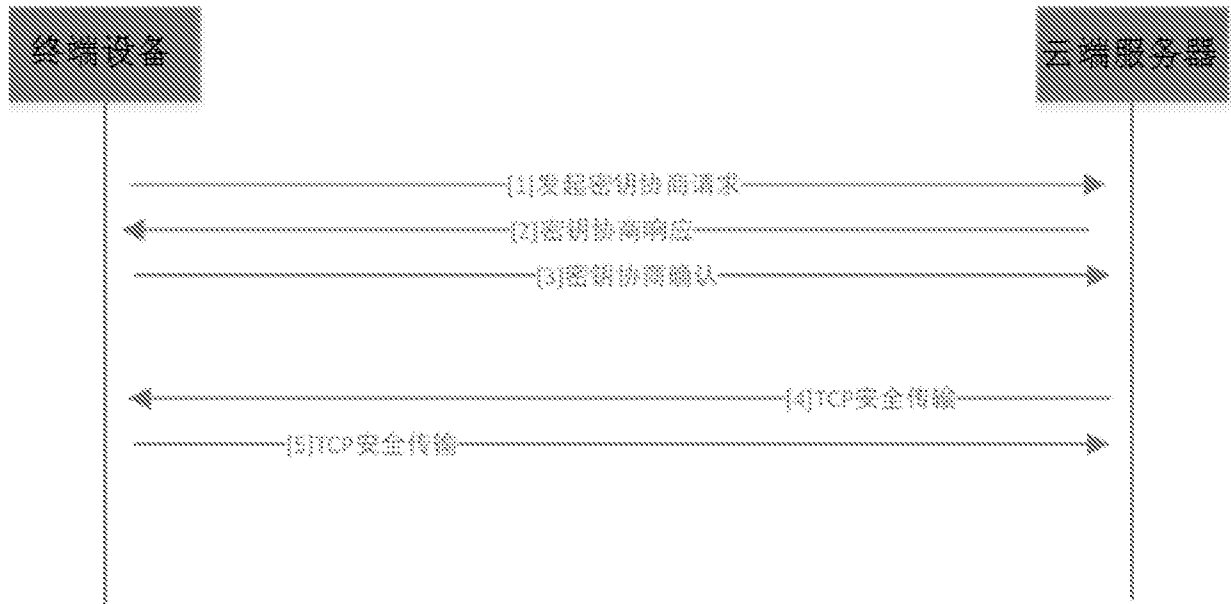


图 1

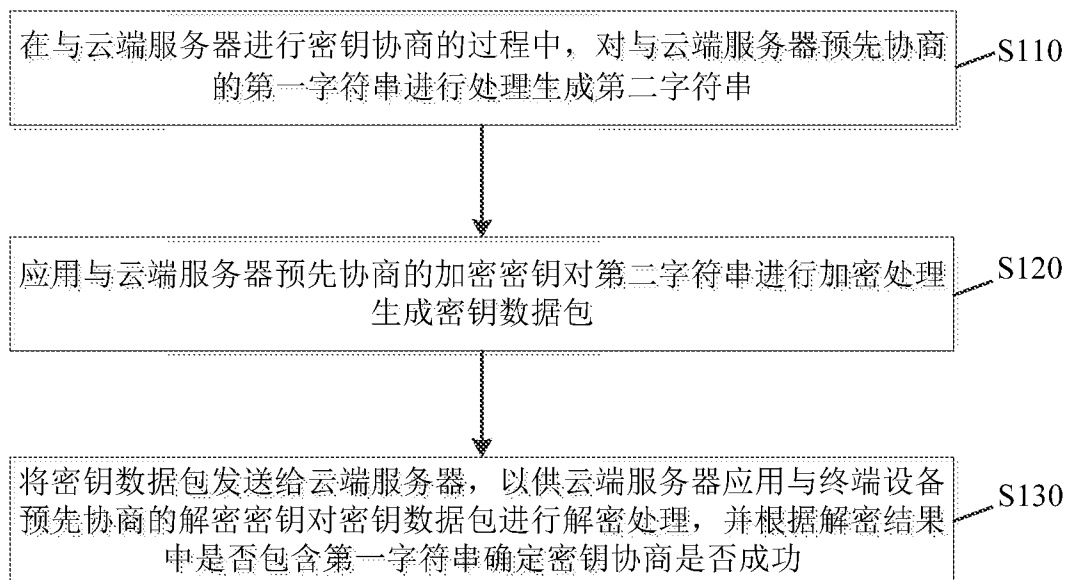


图 2

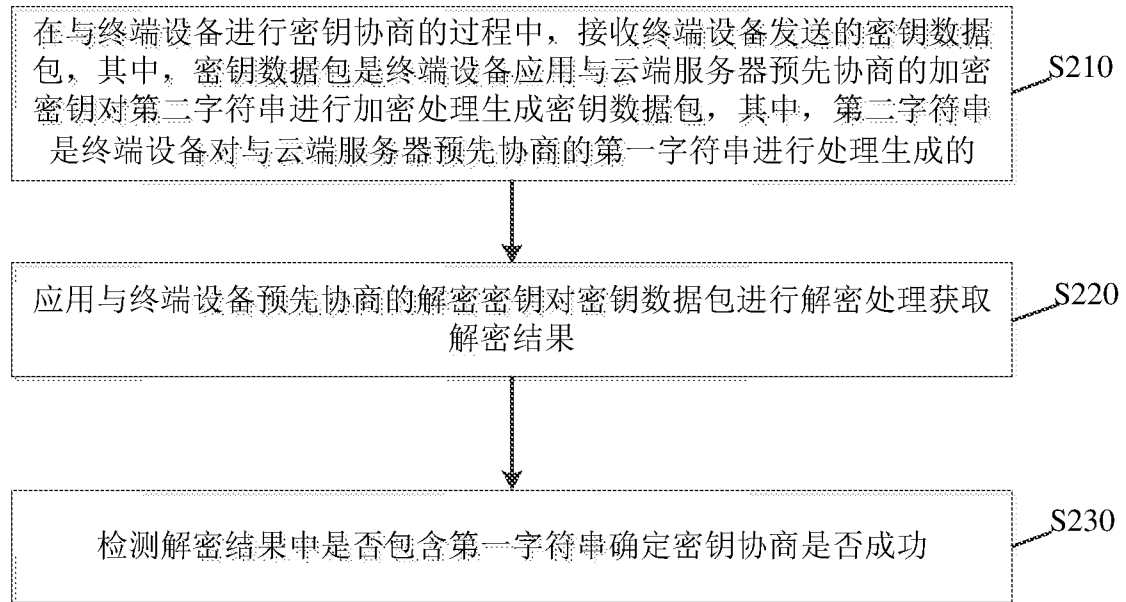


图 3



图 4

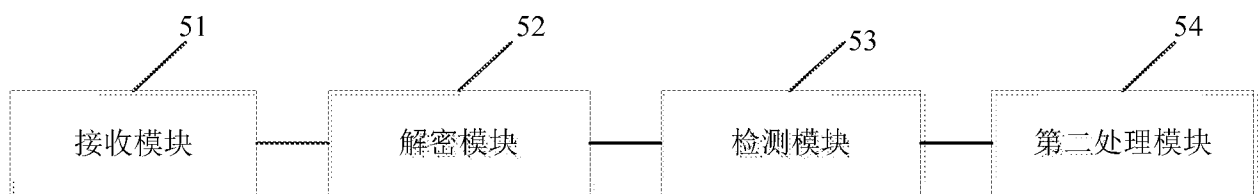


图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/103812

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; WOTXT; USTXT; EPTXT: 密钥, 协商, 加密, 解密, 随机, 串, key, negotiat+, encrypt+, decrypt+, random, string, H04L63/061/CPC, H04L29/06714/CPC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101378320 A (UNITEND TECHNOLOGIES INC.) 04 March 2009 (04.03.2009), description, page 1, lines 20-23, page 4, line 7 to page 8, line 8 and page 10, line 1 to page 12, line 10, and figures 2 and 4	1-14
X	CN 102594823 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 18 July 2012 (18.07.2012), description, paragraphs [0022]-[0032] and [0035]-[0045]	1-14
A	US 2016261566 A1 (SSH COMMUNICATIONS SECURITY OYJ) 08 September 2016 (08.09.2016), entire document	1-14
A	US 2016294783 A1 (AT & T IP I, L.P.) 06 October 2016 (06.10.2016), entire document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 14 June 2017	Date of mailing of the international search report 29 June 2017
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 REN, Ling Telephone No. (86-10) 62088423

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/103812

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101378320 A	04 March 2009	CN 101378320 B	28 September 2011
CN 102594823 A	18 July 2012	CN 102594823 B	22 October 2014
US 2016261566 A1	08 September 2016	None	
US 2016294783 A1	06 October 2016	US 9667600 B2	30 May 2017

国际检索报告

国际申请号

PCT/CN2016/103812

A. 主题的分类

H04L 9/32 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNABS; CNTXT; CNKI; VEN; WOTXT; USTXT; EPTXT: 密钥, 协商, 加密, 解密, 随机, 串, key, negotiat+, encrypt+, decrypt+, random, string, H04L63/061/CPC, H04L29/06714/CPC

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 101378320 A (北京数字太和科技有限责任公司) 2009年 3月 4日 (2009 - 03 - 04) 说明书第1页第20-23行、第4页第7行到第8页第8行、第10页第1行到第12页第10行, 图2、4	1-14
X	CN 102594823 A (南京邮电大学) 2012年 7月 18日 (2012 - 07 - 18) 说明书第22-32、35-45段	1-14
A	US 2016261566 A1 (SSH COMMUNICATIONS SECURITY OYJ) 2016年 9月 8日 (2016 - 09 - 08) 全文	1-14
A	US 2016294783 A1 (AT & T IP I, L.P.) 2016年 10月 6日 (2016 - 10 - 06) 全文	1-14

☐ 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

2017年 6月 14日

国际检索报告邮寄日期

2017年 6月 29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)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10) 62019451

受权官员

任玲

电话号码 (86-10) 62088423

国际申请号	PCT/CN2016/103812
-------	-------------------

检索报告引用的专利文件			公布日 (年/月/日)	同族专利		公布日 (年/月/日)
CN	101378320	A	2009年 3月 4日	CN	101378320 B	2011年 9月 28日
CN	102594823	A	2012年 7月 18日	CN	102594823 B	2014年 10月 22日
US	2016261566	A1	2016年 9月 8日	无		
US	2016294783	A1	2016年 10月 6日	US	9667600 B2	2017年 5月 30日

表 PCT/ISA/210 (同族专利附件) (2009年7月)