(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114362946 B
(45)授权公告日 2022.06.07

(21)申请号 202210232964.3
(22)申请日 2022.03.10
(65)同一申请的已公布的文献号
申请公布号 CN 114362946 A
(43)申请公布日 2022.04.15
(73)专利权人 北京得瑞领新科技有限公司
地址 100192 北京市海淀区西小口路66号中关村东升科技园·北领地B-6号楼A座9层A905室
(72)发明人 赵连讯 薛红军
(74)专利代理机构 北京慧智兴达知识产权代理有限公司 11615
专利代理师 李丽颖
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
WO 2018076365 A1,2018.05.03
US 2016344561 A1,2016.11.24
CN 107925578 A,2018.04.17
WO 2021022406 A1,2021.02.11
WO 2021203853 A1,2021.10.14

审查员 郭海波

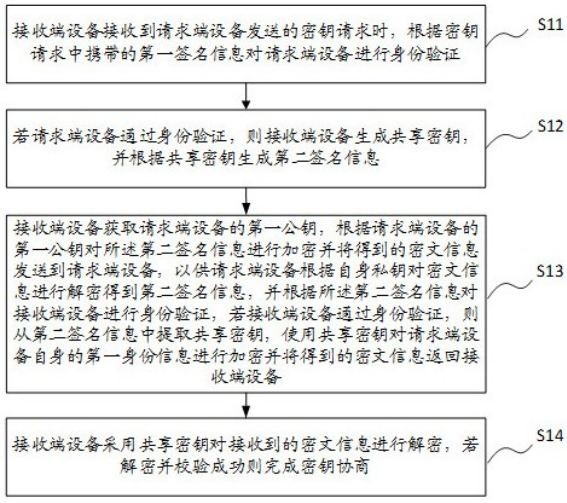
权利要求书2页 说明书7页 附图2页

(54)发明名称

密钥协商方法及系统

(57)摘要

本发明提供一种密钥协商方法及系统，该方法包括：根据请求端设备发送的密钥请求中携带的第一签名信息对请求端设备进行身份验证；若通过身份验证，则生成共享密钥，并根据共享密钥生成第二签名信息；获取请求端设备的公钥，根据请求端设备的公钥对第二签名信息进行加密并将密文信息发送到请求端设备，请求端设备根据自身私钥对密文信息进行解密得到第二签名信息，并根据第二签名信息对接收端设备进行身份验证，若通过身份验证，则通过共享密钥对请求端设备的身份信息进行加密并将密文信息返回接收端设备，接收端设备采用共享密钥对接收到的密文信息进行解密。本发明能同时完成密钥协商和双方身份认证，在保证密钥安全的同时，保证协商效率。



CN 114362946 B

1.一种密钥协商方法,其特征在于,所述方法包括:

接收端设备接收到请求端设备发送的密钥请求时,根据密钥请求中携带的第一签名信息对请求端设备进行身份验证,接收端设备中存储支持密钥协商的对方的公钥信息表供查询使用,请求端设备中存储支持所有分发密钥的对方的公钥信息表;

若请求端设备通过身份验证,则接收端设备生成共享密钥,并根据共享密钥生成第二签名信息;

接收端设备获取请求端设备的第一公钥,根据请求端设备的第一公钥对所述第二签名信息进行加密并将得到的密文信息发送到请求端设备,以供请求端设备根据自身私钥对密文信息进行解密得到第二签名信息,并根据所述第二签名信息对接收端设备进行身份验证,若接收端设备通过身份验证,则从第二签名信息中提取共享密钥,使用共享密钥对请求端设备自身的第一身份信息进行加密并将得到的密文信息返回接收端设备;

接收端设备采用共享密钥对接收到的密文信息进行解密,若解密并校验成功则完成密钥协商;

其中,所述接收端设备生成共享密钥,并根据共享密钥生成第二签名信息,包括:接收端设备生成随机数,将所述随机数作为共享密钥;接收端设备采用自身的私钥对接收端设备的第二身份信息和共享密钥的组合数据进行签名后得到的第二签名值;将所述第二身份信息、共享密钥和第二签名值进行组合,生成第二签名信息。

2.根据权利要求1所述的方法,其特征在于,所述第一签名信息包括请求端设备的第一身份信息和第一签名值,所述第一签名值是请求端设备采用自身的私钥对第一身份信息签名后得到的签名值。

3.根据权利要求2所述的方法,其特征在于,所述根据密钥请求中携带的第一签名信息对请求端设备进行身份验证包括:

接收端设备查询预设的请求端设备公钥信息表,以获取与所述第一身份信息匹配的请求端设备的第一公钥;

接收端设备根据所述第一公钥对所述第一签名值进行验证,若验证通过,则请求端设备通过身份验证。

4.根据权利要求3所述的方法,其特征在于,所述接收端设备查询预设的请求端设备公钥信息表,以获取与所述第一身份信息匹配的请求端设备的第一公钥,包括:

接收端设备根据所述第一身份信息查询预设的请求端设备公钥信息表,所述请求端设备公钥信息表中包括有设备公钥与设备身份信息之间的对应关系;或

接收端设备计算所述第一身份信息的Hash值,根据所述第一身份信息的Hash值查询预设的请求端设备公钥信息表,所述请求端设备公钥信息表中包括有设备公钥与设备身份信息的Hash值之间的对应关系。

5.根据权利要求1所述的方法,其特征在于,所述请求端设备根据所述第二签名信息对接收端设备进行身份验证,包括:

请求端设备查询预设的接收端设备公钥信息表,以获取与所述第二身份信息匹配的接收端设备的第二公钥;

请求端设备根据所述第二公钥对所述第二签名信息进行完整性验证,若验证通过,则接收端设备通过身份验证。

6.根据权利要求5所述的方法,其特征在于,所述请求端设备查询预设的接收端设备公钥信息表,以获取与所述第二身份信息匹配的接收端设备的第二公钥,包括:

请求端设备根据所述第二身份信息查询预设的接收端设备公钥信息表,所述接收端设备公钥信息表中包括有设备公钥与设备身份信息之间的对应关系;或

请求端设备计算所述第二身份信息的Hash值,根据所述第二身份信息的Hash值查询预设的接收端设备公钥信息表,所述接收端设备公钥信息表中包括有设备公钥与设备身份信息的Hash值之间的对应关系。

7.根据权利要求1所述的方法,其特征在于,所述请求端设备使用共享密钥对请求端设备自身的第一身份信息进行加密并将得到的密文信息返回接收端设备,包括:

请求端设备使用共享密钥对第一身份信息和共享密钥的组合数据进行加密,并将得到的密文信息发送到接收端设备;或

请求端设备计算第一身份信息和共享密钥的组合数据的Hash值;使用共享密钥对组合数据的Hash值进行加密,并将得到的密文信息发送到接收端设备。

8.根据权利要求7所述的方法,其特征在于,所述接收端设备采用共享密钥对接收到的密文信息进行解密,若解密并校验成功则完成密钥协商,包括:

接收端设备采用共享密钥对接收到的密文信息进行解密;

若解密成功,则验证解密后的数据是否为请求端设备的第一身份信息和共享密钥的组合数据,或请求端设备的第一身份信息和共享密钥的组合数据的Hash值;

若验证成功,则判定请求端设备接收到所述共享密钥,完成密钥协商。

9.一种密钥协商系统,其特征在于,所述系统包括请求端设备和接收端设备,所述请求端设备和接收端设备通过如权利要求1-8任一项所述密钥协商方法实现密钥协商。

密钥协商方法及系统

技术领域

[0001] 本发明涉及通信技术领域,尤其涉及一种密钥协商方法及系统。

背景技术

[0002] 随着通信技术的发展,信息网络环境日益复杂,通信环境中的设备之间信息交互越来越多。在通信过程中,通信的参与方保证通信信息安全,也越来越重要。通信双方建立一个共享密钥(Key),真正通信时使用共享密钥通信,是保证信息安全的前提。

[0003] 密钥协商(Key Agreement)是建立共享密钥的基本方式,密钥协商分为两种方案,第一种是隐式密钥方案,该方案以明文形式交互参数信息,然后通信双方基于参数计算得到共同的密钥,密钥信息不在通信链路上传输。第二种是显式密钥方案,该方案中密钥在一侧产生,以密文形式发送到另外一端。

[0004] 但是对于一些特殊的应用场景,例如,在一些嵌入式设备启动场景中,设备处于信息孤岛状态,当第一次与外部主机连接时,如何识别外部主机的身份并与外部主机完成密钥协商建立共享Key,是当前亟待解决的技术问题。现有技术中提出了一种能够在完成密钥协商的同时,也会完成双方身份验证的方案,但是双方身份验证的基础必须是通信双方彼此共享一段秘密信息。

发明内容

[0005] 鉴于上述问题,提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的密钥协商方法及系统。

[0006] 本发明的一个方面,提供了一种密钥协商方法,所述方法包括:

[0007] 接收端设备接收到请求端设备发送的密钥请求时,根据密钥请求中携带的第一签名信息对请求端设备进行身份验证;

[0008] 若请求端设备通过身份验证,则接收端设备生成共享密钥,并根据共享密钥生成第二签名信息;

[0009] 接收端设备获取请求端设备的第一公钥,根据请求端设备的第一公钥对所述第二签名信息进行加密并将得到的密文信息发送到请求端设备,以供请求端设备根据自身私钥对密文信息进行解密得到第二签名信息,并根据所述第二签名信息对接收端设备进行身份验证,若接收端设备通过身份验证,则从第二签名信息中提取共享密钥,使用共享密钥对请求端设备自身的第一身份信息进行加密并将得到的密文信息返回接收端设备;

[0010] 接收端设备采用共享密钥对接收到的密文信息进行解密,若解密并校验成功则完成密钥协商。

[0011] 进一步地,所述第一签名信息包括请求端设备的第一身份信息和第一签名值,所述第一签名值是请求端设备采用自身的私钥对第一身份信息签名后得到的签名值。

[0012] 进一步地,所述根据密钥请求中携带的第一签名信息对请求端设备进行身份验证包括:

[0013] 接收端设备查询预设的请求端设备公钥信息表，以获取与所述第一身份信息匹配的请求端设备的第一公钥；

[0014] 接收端设备根据所述第一公钥对所述第一签名值进行验证，若验证通过，则请求端设备通过身份验证。

[0015] 进一步地，所述接收端设备查询预设的请求端设备公钥信息表，以获取与所述第一身份信息匹配的请求端设备的第一公钥，包括：

[0016] 接收端设备根据所述第一身份信息查询预设的请求端设备公钥信息表，所述请求端设备公钥信息表中包括有设备公钥与设备身份信息之间的对应关系；或

[0017] 接收端设备计算所述第一身份信息的Hash值，根据所述第一身份信息的Hash值查询预设的请求端设备公钥信息表，所述请求端设备公钥信息表中包括有设备公钥与设备身份信息的Hash值之间的对应关系。

[0018] 进一步地，所述接收端设备生成共享密钥，并根据共享密钥生成第二签名信息，包括：

[0019] 接收端设备生成随机数，将所述随机数作为共享密钥；

[0020] 接收端设备采用自身的私钥对接收端设备的第二身份信息和共享密钥的组合数据进行签名后得到的第二签名值；

[0021] 将所述第二身份信息、共享密钥和第二签名值进行组合，生成第二签名信息。

[0022] 进一步地，所述请求端设备根据所述第二签名信息对接收端设备进行身份验证，包括：

[0023] 请求端设备查询预设的接收端设备公钥信息表，以获取与所述第二身份信息匹配的接收端设备的第二公钥；

[0024] 请求端设备根据所述第二公钥对所述第二签名信息进行完整性验证，若验证通过，则接收端设备通过身份验证。

[0025] 进一步地，所述请求端设备查询预设的接收端设备公钥信息表，以获取与所述第二身份信息匹配的接收端设备的第二公钥，包括：

[0026] 请求端设备根据所述第二身份信息查询预设的接收端设备公钥信息表，所述接收端设备公钥信息表中包括有设备公钥与设备身份信息之间的对应关系；或

[0027] 请求端设备计算所述第二身份信息的Hash值，根据所述第二身份信息的Hash值查询预设的接收端设备公钥信息表，所述接收端设备公钥信息表中包括有设备公钥与设备身份信息的Hash值之间的对应关系。

[0028] 进一步地，所述请求端设备使用共享密钥对请求端设备自身的第一身份信息进行加密并将得到的密文信息返回接收端设备，包括：

[0029] 请求端设备使用共享密钥对第一身份信息和共享密钥的组合数据进行加密，并将得到的密文信息发送到接收端设备；或

[0030] 请求端设备计算第一身份信息和共享密钥的组合数据的Hash值；使用共享密钥对组合数据的Hash值进行加密，并将得到的密文信息发送到接收端设备。

[0031] 进一步地，所述接收端设备采用共享密钥对接收到的密文信息进行解密，若解密并校验成功则完成密钥协商，包括：

[0032] 接收端设备采用共享密钥对接收到的密文信息进行解密；

[0033] 若解密成功,则验证解密后的数据是否为请求端设备的第一身份信息和共享密钥的组合数据,或请求端设备的第一身份信息和共享密钥的组合数据的Hash值;

[0034] 若验证成功,则判定请求端设备接收到所述共享密钥,完成密钥协商。

[0035] 本发明的另一方面,还提供了一种密钥协商系统,所述系统包括请求端设备和接收端设备,所述请求端设备和接收端设备采用如上所述密钥协商方法实现密钥协商。

[0036] 本发明实施例提供的密钥协商方法及系统,无需通信双方共享一段秘密信息,只需要经过两次密文数据交换就能同时完成密钥协商和双方身份认证。在保证密钥安全的同时,也保证了协商效率,达到与隐式密钥协商方案相同的效果。

[0037] 上述说明仅是本发明技术方案的概述,为了能够更清楚了解本发明的技术手段,而可依照说明书的内容予以实施,并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂,以下特举本发明的具体实施方式。

附图说明

[0038] 通过阅读下文优选实施方式的详细描述,各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的,而并不认为是对本发明的限制。而且在整个附图中,用相同的参考符号表示相同的部件。在附图中:

[0039] 图1为本发明实施例提供的密钥协商方法的流程图;

[0040] 图2为本发明实施例提供的密钥协商方法的整体交互流程框图。

具体实施方式

[0041] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例,然而应当理解,可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反,提供这些实施例是为了能够更透彻地理解本公开,并且能够将本公开的范围完整的传达给本领域的技术人员。

[0042] 本技术领域技术人员可以理解,除非特意声明,这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是,本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件,但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。

[0043] 本技术领域技术人员可以理解,除非另外定义,这里使用的所有术语(包括技术术语和科学术语),具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是,诸如通用字典中定义的那些术语,应该被理解为具有与现有技术的上下文中的意义一致的意义,并且除非被特定定义,否则不会用理想化或过于正式的含义来解释。

[0044] 图1示意性示出了本发明一个实施例的密钥协商方法的流程图。参照图1,本发明实施例的密钥协商方法具体包括以下步骤:

[0045] S11、接收端设备接收到请求端设备发送的密钥请求时,根据密钥请求中携带的第一签名信息对请求端设备进行身份验证。

[0046] 本实施例中,设定通信双方为设备A和设备B,其中,设备A为接收端,设备B为请求端,实现接收端设备A对请求端设备B之间的密钥协商和身份相互认证。A中存储支持密钥协商的对方的公钥信息表(Public Key Table)供查询使用。B中存储支持所有分发密钥的对

方的公钥信息表(Public Key Table)。

[0047] S12、若请求端设备B通过身份验证,则接收端设备A生成共享密钥,并根据共享密钥生成第二签名信息。

[0048] S13、接收端设备A获取请求端设备B的第一公钥,根据请求端设备B的第一公钥对所述第二签名信息进行加密并将得到的密文信息发送到请求端设备B,以供请求端设备B根据自身私钥对密文信息进行解密得到第二签名信息,并根据所述第二签名信息对接收端设备A进行身份验证,若接收端设备A通过身份验证,则从第二签名信息中提取共享密钥,使用共享密钥对请求端设备B自身的第一身份信息进行加密并将得到的密文信息返回接收端设备A。

[0049] S14、接收端设备A采用共享密钥对接收到的密文信息进行解密,若解密并校验成功则完成密钥协商。

[0050] 本实施例中,接收端设备A采用共享密钥对接收到的密文信息进行解密并对请求端设备B的身份信息进行校验,若解密并校验成功则完成密钥协商。

[0051] 本发明实施例提供的密钥协商方法,无需通信双方共享一段秘密信息,只需要经过两次密文数据交换就能同时完成密钥协商和双方身份认证。在保证密钥安全的同时,也保证了协商效率,达到与隐式密钥协商方案相同的效果。

[0052] 本发明实施例中,第一签名信息包括请求端设备B的第一身份信息和第一签名值,所述第一签名值是请求端设备B采用自身的私钥对第一身份信息签名后得到的签名值。具体的,请求端设备B对自己的身份信息(B_User_ID)即第一身份信息签名后得到第一签名值(Signature1),并将全部内容作为第一身份信息(B_User_ID,Signature1)发送给接收端设备A。

[0053] 本实施例中,所述的根据密钥请求中携带的第一签名信息对请求端设备B进行身份验证具体实现过程如下:接收端设备A查询预设的请求端设备公钥信息表,以获取与所述第一身份信息匹配的请求端设备B的第一公钥;接收端设备A根据所述第一公钥对所述第一签名值进行验证,若验证通过,则请求端设备B通过身份验证。进一步地,接收端设备A获取请求端设备B的第一公钥,可通过以下两种实现方式获取:

[0054] 第一种方式,接收端设备A根据所述第一身份信息查询预设的请求端设备公钥信息表,所述请求端设备公钥信息表中包括有设备公钥与设备身份信息之间的对应关系。

[0055] 第二种方式,接收端设备A计算第一身份信息即请求端设备B的身份信息B_User_ID的Hash值,根据第一身份信息的Hash值查询预设的请求端设备公钥信息表,所述请求端设备公钥信息表中包括有设备公钥与设备身份信息的Hash值之间的对应关系。

[0056] 本发明的密钥协商方法的整体交互流程如图2所示。具体的,以第二种方式为例进行说明,接收端设备A收到请求端设备B的密钥请求消息后,首先使用B的身份信息(B_User_ID)计算Hash值。使用Hash结果查询Public Key Table得到请求端设备B的公钥(B Public Key)即第一公钥。使用请求端设备B的B Public key验证第一身份信息(B_User_ID,Signature1)中的签名。验证签名通过时,表示接收端设备A收到的消息确实是请求端设备B发送的密钥请求,开始密钥协商。验证签名失败时,表示这条消息不是请求端设备B发送的密钥协商请求,接收端设备A忽略此次请求,密钥协商失败。

[0057] 本发明实施例中,第二签名信息包括接收端设备A的第二身份信息、接收端设备生

成的共享密钥Key和第二签名值，第二签名值是接收端设备A采用自身的私钥(A Private Key)对第二身份信息(A_User_ID)和共享密钥Key的组合数据(A_User_ID,Key)进行签名后得到签名值。

[0058] 本实施例中，所述的接收端设备A生成共享密钥，并根据共享密钥生成第二签名信息，具体实现方式如下：接收端设备A生成随机数，将所述随机数作为共享密钥；接收端设备A采用自身的私钥对接收端设备A的第二身份信息和共享密钥的组合数据进行签名后得到的第二签名值；将所述第二身份信息、共享密钥和第二签名值进行组合，生成第二签名信息。

[0059] 如图2所示，具体的，接收端设备A产生一个随机数作为共享密钥Key，并使用自己的私钥(A Private Key)对(A_User_ID,Key)的值计算签名值得到第二签名值(Signature2)，并将全部内容作为第二签名信息(A_User_ID,Key,Signature2)。

[0060] 本实施例中，请求端设备B根据所述第二签名信息对接收端设备A进行身份验证的具体实现方式如下：请求端设备B查询预设的接收端设备A公钥信息表，以获取与所述第二身份信息匹配的接收端设备A的第二公钥；请求端设备B根据所述第二公钥对所述第二签名信息进行完整性验证，若验证通过，则接收端设备A通过身份验证。进一步地，请求端设备B获取接收端设备A的第二公钥，可通过以下两种实现方式获取：

[0061] 第一种方式、请求端设备B根据所述第二身份信息查询预设的接收端设备公钥信息表，所述接收端设备公钥信息表中包括有设备公钥与设备身份信息之间的对应关系。

[0062] 第二种方式、请求端设备B计算所述第二身份信息的Hash值，根据所述第二身份信息的Hash值查询预设的接收端设备公钥信息表，所述接收端设备公钥信息表中包括有设备公钥与设备身份信息的Hash值之间的对应关系。

[0063] 如图2所示，具体的，以第二种方式为例进行说明，接收端设备A在根据共享密钥生成第二签名信息之后，使用请求端设备B的Public Key对第二签名信息(A_User_ID,Key,Signature2)加密，得到密文信息。接收端设备A将密文信息发送给请求端设备B。请求端设备B收到密文后，使用自身的私钥B Private Key解密得到(A_User_ID,Key,Signature)明文。请求端设备B通过计算接收端设备A的A_User_ID即第二身份信息的Hash值查询Public Key Table，得到接收端设备A的APublic Key即第二公钥。请求端设备B使用接收端设备A的APublic Key验证(A_User_ID,Key,Signature)消息的完整性。如果消息完整，则认为Key是用户A发送的合法共享密钥，继续协商密钥。如果消息验签失败则请求端设备B认为不是用户A回复的有效消息，拒绝使用Key，密钥协商失败。本实施例中，接收端设备A采用请求端设备B的Public Key加密(A_User_ID,Key,Signature)消息，既可以验证请求端设备B的身份信息，又传递了Key，并且也让请求端设备B验证了A的身份信息，有效提高安全性。

[0064] 本实施例中，请求端设备B使用共享密钥Key对请求端设备B自身的第一身份信息B_User_ID等信息处理后进行加密并将得到的密文信息返回接收端设备A的具体实现方式包括如下两种：

[0065] 第一种方式，请求端设备B使用共享密钥对第一身份信息和共享密钥的组合数据(B_User_ID,Key)进行加密，并将得到的密文信息发送到接收端设备A。

[0066] 第二种方式，请求端设备B计算第一身份信息和共享密钥的组合数据(B_User_ID,Key)的Hash值；使用共享密钥对组合数据的Hash值进行加密，并将得到的密文信息发送到

接收端设备A。

[0067] 本实施例中，接收端设备A采用共享密钥对接收到的密文信息进行解密，若解密并校验成功则完成密钥协商的具体实现方式如下：接收端设备A采用共享密钥对接收到的密文信息进行解密；若解密成功，则验证解密后的数据是否为请求端设备的第一身份信息和共享密钥的组合数据，或请求端设备的第一身份信息和共享密钥的组合数据的Hash值；若验证成功，则判定请求端设备B接收到所述共享密钥，完成密钥协商。其中，解密后的数据的具体内容需要根据加密时的数据内容确定。

[0068] 如图2所示，具体的，以第二种方式为例进行说明，接收端设备A收到密文后，使用共享密钥Key解密，并验证接收端设备A解密后的明文是否等于(B_User_ID,Key)的Hash值。校验成功时，表示接收端设备A知道了请求端设备B正确接收到了共享密钥Key，密钥协商成功。校验失败时，则表示本次密钥协商失败。密钥协商成功后，接收端设备A使用Key与请求端设备B进行交互信息。本实施例中，接收端设备A需要确认请求端设备B是否收到了秘钥信息，所以请求端设备B要返回一个ACK消息。ACK消息格式采用(B_User_ID,Key)的Hash值的密文，这里将待加密的消息中融入Key值，并且传递的是Key的Hash值，增加了第三方破解的难度，提高了协商方案的安全性。

[0069] 本发明实施例提供的密钥协商方法具有以下有益的技术效果，分析如下：

[0070] 1、防止窃听。接收端设备A端发送的(A_User_ID,Key,Signature)是密文，是接收端设备A使用请求端设备B的Public Key加密的，窃听者拿到的是密文。没有请求端设备B的私钥信息，无法正常解密。请求端设备B端发送的是(B_User_ID,Key)的Hash的密文。只有用户B拥有正确的Key，其他用户无法正确解密这段密文。

[0071] 2、防止篡改。请求端设备B发送的是带签名的信息，其他用户修改信息后，接收端设备A验签失败。若其他用户修改密文信息，导致解密得到错误的明文，明文的完整性验证会失败。

[0072] 3、防止身份冒充。如果第三者C冒充请求端设备B，由于C没有B的私钥信息，则无法正确解密得到正确的Key。直接导致无法得到正确的(B_User_ID,Key)Hash值，接收端设备A校验信息失败，导致密钥协商失败。如果第三者C冒充A，则C没有A的Private Key，则无法对消息生成第二签名值。B在验证第二签名消息(A_User_ID,Key,Signature)时会失败，导致本次秘钥协商终止。

[0073] 本发明的另一实施例还提供了一种密钥协商系统，所述系统包括请求端设备和接收端设备，所述请求端设备和接收端设备采用如上任一实施例所述密钥协商方法实现密钥协商。

[0074] 本发明实施例提供的密钥协商方法及系统，无需通信双方共享一段秘密信息，只需要经过两次密文数据交换就能同时完成密钥协商和双方身份认证。在保证密钥安全的同时，也保证了协商效率，达到与隐式密钥协商方案相同的效果。

[0075] 此外，本领域的技术人员能够理解，尽管在此的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0076] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管

参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

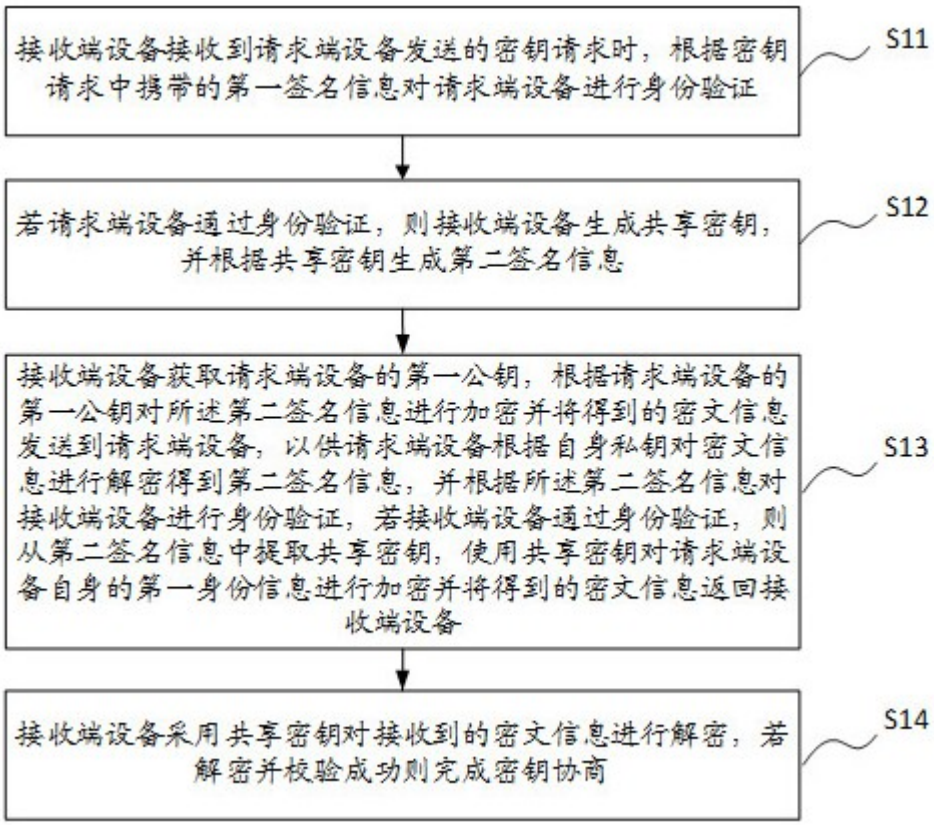

接收端设备接收到请求端设备发送的密钥请求时，根据密钥请求中携带的第一签名信息对请求端设备进行身份验证
S11
若请求端设备通过身份验证，则接收端设备生成共享密钥，并根据共享密钥生成第二签名信息
S12
接收端设备获取请求端设备的第一公钥，根据请求端设备的第一公钥对所述第二签名信息进行加密并将得到的密文信息发送到请求端设备，以供请求端设备根据自身私钥对密文信息进行解密得到第二签名信息，并根据所述第二签名信息对接收端设备进行身份验证，若接收端设备通过身份验证，则从第二签名信息中提取共享密钥，使用共享密钥对请求端设备自身的第一身份信息进行加密并将得到的密文信息返回接收端设备
S13
接收端设备采用共享密钥对接收到的密文信息进行解密，若解密并校验成功则完成密钥协商
S14

图1

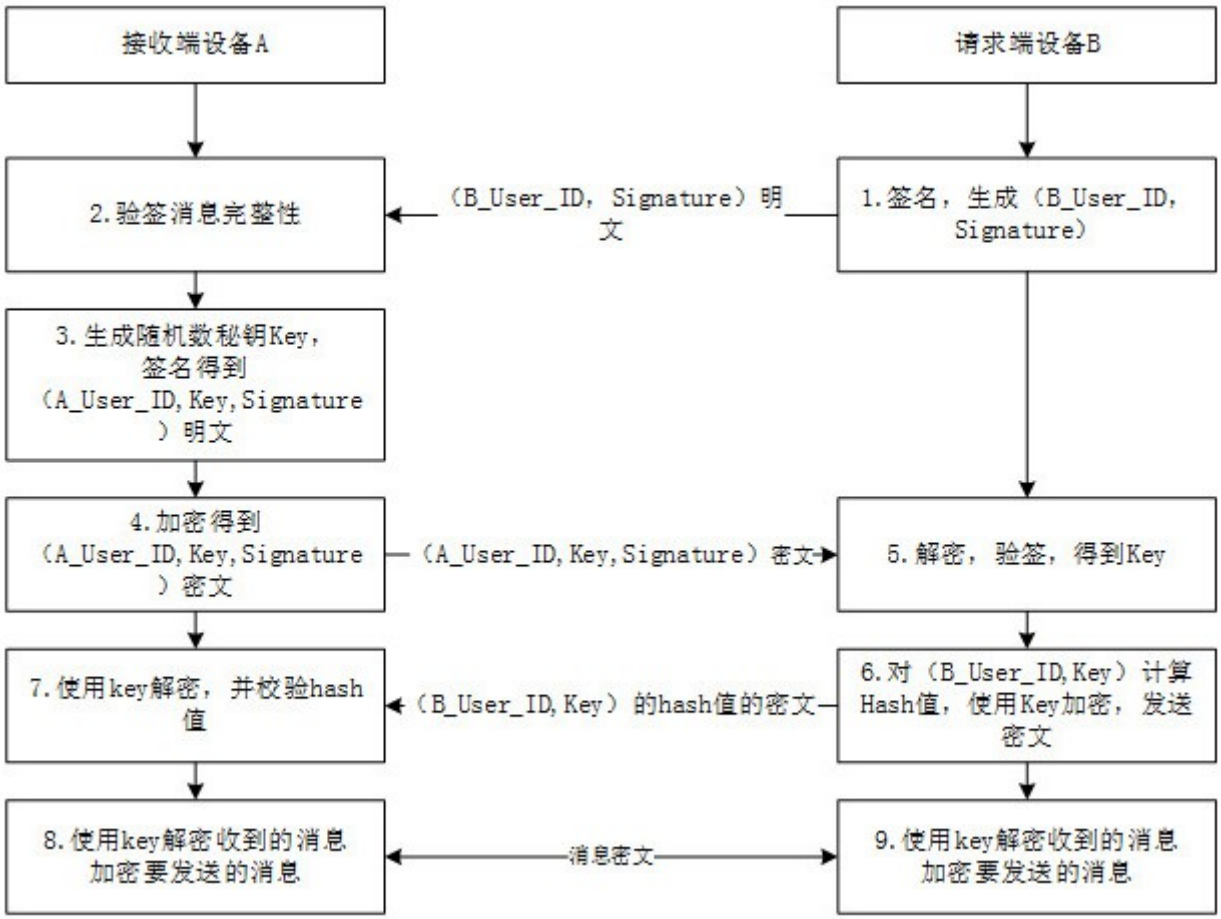

接收端设备A
请求端设备B
2.验签消息完整性
（B_User_ID，Signature）明文
1.签名，生成（B_User_ID，Signature）
3.生成随机数秘钥Key，签名得到（A_User_ID,Key,Signature）明文
4.加密得到（A_User_ID,Key,Signature）密文
（A_User_ID,Key,Signature）密文
5.解密，验签，得到Key
7.使用key解密，并校验hash值
（B_User_ID,Key）的hash值的密文
6.对（B_User_ID,Key）计算Hash值，使用Key加密，发送密文
8.使用key解密收到的消息加密要发送的消息
消息密文
9.使用key解密收到的消息加密要发送的消息

图2