(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111404674 B
(45)授权公告日 2023.06.27

(21)申请号 201910002534.0
(22)申请日 2019.01.02
(65)同一申请的已公布的文献号
申请公布号 CN 111404674 A
(43)申请公布日 2020.07.10
(73)专利权人 中国移动通信有限公司研究院
地址 100032 北京市西城区金融大街29号19层
专利权人 中国移动通信集团有限公司
(72)发明人 刘福文 马冰柯 阎军智
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
专利代理师 郭润湘
(51)Int.Cl.
H04L 9/08(2006.01)

审查员 李晓

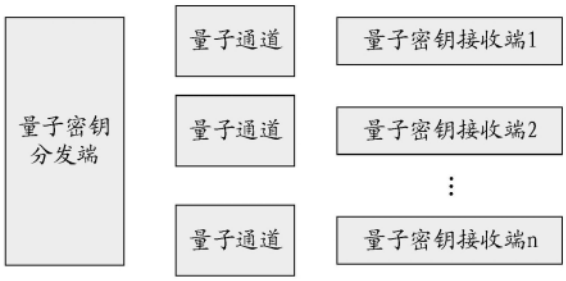
权利要求书1页 说明书10页 附图4页

(54)发明名称

一种会话密钥的生成和接收方法及设备

(57)摘要

本发明公开了一种会话密钥的生成和接收方法及设备，用于解决量子通信易受干扰的问题。该方法包括：生成至少一个随机数S；通过与每个随机数S对应的量子通道传输对应的随机数S，以使接收方利用哈希函数对接收的随机数S与预设密钥进行哈希运算生成会话密钥Ks；接收量子密钥分发端通过至少两个量子通道传输的对应随机数S；利用哈希函数对接收的随机数S和预设密钥进行哈希运算，生成会话密钥Ks。用于在量子通信中长距离传输量子密钥以及量子密钥的抗干扰传输。



CN 111404674 B

1.一种会话密钥的生成方法,其特征在于,该方法包括:

生成至少两个随机数;

通过与每个随机数对应的一个量子通道传输对应的随机数,以使接收方利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥;其中一个随机数对应一个量子通道;

收到接收方反馈的确认消息,确定被接收方成功接收的随机数;

利用哈希函数对所述被接收方成功接收的随机数S和预设密钥进行哈希运算,生成会话密钥。

2.根据权利要求1所述的方法,其特征在于,通过与所述随机数对应的量子通道传输对应的随机数,包括:

通过量子通信中继网络中与每个随机数对应的量子通道传输对应的随机数。

3.根据权利要求1所述的方法,其特征在于,所述哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

4.一种会话密钥的接收方法,其特征在于,该方法包括:

接收量子密钥分发端通过至少两个量子通道传输的对应随机数;成功接收到随机数后,向分发端反馈确认消息;

利用哈希函数对接收的随机数和预设密钥进行哈希运算,生成会话密钥Ks。

5.根据权利要求4所述的方法,其特征在于,接收量子密钥分发端通过至少两个量子通道传输的对应随机数,包括:

接收量子通信中继网络中至少两个量子通道传输的对应随机数。

6.根据权利要求4所述的方法,其特征在于,所述哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

7.一种会话密钥的生成设备,其特征在于,该设备包括:处理器以及存储器,其中,所述存储器存储有程序代码,当所述程序代码被所述处理器执行时,使得所述处理器执行权利要求1～3任一所述方法的步骤。

8.一种会话密钥的接收设备,其特征在于,该设备包括:处理器以及存储器,其中,所述存储器存储有程序代码,当所述程序代码被所述处理器执行时,使得所述处理器执行权利要求4～6任一所述方法的步骤。

一种会话密钥的生成和接收方法及设备

技术领域

[0001] 本发明涉及量子密钥分发，尤其涉及一种会话密钥的生成和接收方法及设备。

背景技术

[0002] 由于量子计算技术的快速发展，许多经典密码算法的安全性面临日益严峻的挑战。量子计算技术对非对称密码算法和对称密码算法有不同影响。现有的对称密码算法，只要其密钥长度增加一倍，就可以保证其在量子计算条件下的安全。而量子计算技术将使现在普遍使用的基于计算复杂性的非对称算法，如RSA、DH全都失效。因为大多数系统的数据保护使用对称密钥算法，但其使用的密钥依赖于非对称算法来生成，所以量子计算技术对现在的安全系统将造成严重威胁。

[0003] 基于量子力学定律的不可再分、测不准、不可复制以及理想随机等特性，并不依赖于任何对计算复杂性的要求和假设，量子密钥分发(Quantum Key Distribution)是一种在量子时代能保证密钥安全分发的关键技术。它替代现有的非对称算法实现密钥协商，可以使现在的安全系统在量子时代仍能继续使用。虽然它有广阔的应用前景，但有以下缺点：

[0004] 在量子通信过程中，量子被测量时会发生状态的突变，通信双方一旦发现状态有变就会停止通信。因此敌方任何形式的入侵行为，不管是窃听、复制还是干扰，都会阻挠通信。

发明内容

[0005] 本发明提供一种会话密钥的生成和接收方法及设备，可以解决量子通信易受干扰的问题。

[0006] 第一方面，本发明提供一种会话密钥的生成方法，该方法包括：

[0007] 生成至少一个随机数；

[0008] 通过与所述随机数对应的量子通道传输对应的随机数，以使接收方利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥。

[0009] 第二方面，本发明提供一种会话密钥的接收方法，该方法包括：

[0010] 接收量子密钥分发端通过至少两个量子通道传输的对应随机数；

[0011] 利用哈希函数对接收的随机数和预设密钥进行哈希运算，生成会话密钥。

[0012] 第三方面，本发明提供一种会话密钥的生成设备，该设备包括：处理器以及存储器，其中，所述存储器存储有程序代码，当所述程序代码被所述处理器执行时，使得所述处理器执行以下步骤：

[0013] 生成至少一个随机数；

[0014] 通过与所述随机数对应的量子通道传输对应的随机数，以使接收方利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥。

[0015] 第四方面，本发明提供一种会话密钥的接收设备，该设备包括：处理器以及存储器，其中，所述存储器存储有程序代码，当所述程序代码被所述处理器执行时，使得所述处

理器执行以下步骤：

[0016] 接收量子密钥分发端通过至少两个量子通道传输的对应随机数；

[0017] 利用哈希函数对接收的随机数和预设密钥进行哈希运算，生成会话密钥。

[0018] 本发明提供的一种会话密钥的生成和接收方法及设备，具有以下有益效果：

[0019] 根据预置密钥和随机数基于哈希函数生成会话密钥，能够保证会话密钥的安全性不依赖于量子网络的中继站是否可信，从而能够在利用中继站远距离传输量子密钥时，量子通信不易受阻挠，能够满足用户对会话密钥安全性的要求；

[0020] 并且，采用多量子通道密钥分发时，能够保证在一个量子通道受到干扰时，整个量子通信系统仍然不受影响，提高了量子通信的抗干扰能力。

附图说明

[0021] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0022] 图1为一种会话密钥的生成和接收系统图；

[0023] 图2为单量子通道密钥生成系统图；

[0024] 图3为两个量子通道密钥生成系统图；

[0025] 图4为多个量子通道密钥生成系统图；

[0026] 图5为一种会话密钥的生成方法图；

[0027] 图6为一种会话密钥的接收方法图。

具体实施方式

[0028] 为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

[0029] 实施例一

[0030] 本发明实施例提供一种会话密钥的生成和接收系统，如图1所示，该系统包括量子密钥分发端、至少一个量子密钥接收端、至少两个量子通道，其中：

[0031] 量子密钥分发端，用于生成至少一个随机数S，通过至少两个量子通道将生成的上述随机数S发送给至少一个量子密钥接收端；

[0032] 量子密钥接收端，接收量子密钥分发端通过至少两个量子通道传输的对应随机数S，利用哈希函数将接收到的随机数S与预设密钥K进行哈希运算后生成会话密钥Ks。

[0033] 因为哈希函数是一种把任意长度的数据通过散列算法压缩到某一个固定长度的单向散列函数，因此，即使攻击者获取了量子通道传输的随机数S，因不知道通信用户双方预设的密钥，也无法获取上述会话密钥Ks，保证了量子通信的可靠性，保障了生成会话密钥的安全性。

[0034] 另外，在量子通信过程中，基于量子通道的特性，能够保证发送的消息和接收消息

的一致性，攻击者无法修改随机数S，而且，量子被测量时会发生状态的突变，通信双方一旦发现状态有变就会停止通信，而本实施例提供的使用多个量子通道传输随机数S，能够保证即使一个量子通道受到干扰时，通信双方也不会停止通信，依然可以利用未被干扰的量子通道中传输的随机数S生成会话密钥。

[0035] 作为一种可选的实施方式，上述哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

[0036] 作为一种可选的实施方式，上述随机数S表示单个随机数值，也可以表示一个随机数流。

[0037] 根据随机数S和量子通道的个数不同，上述通过至少两个量子通道将生成的上述随机数S发送给至少一个量子密钥接收端有以下几种情况：

[0038] 情况一：随机数S表示单个随机数值时，单个随机数S对应使用一个量子通道A传输上述单个随机数S；

[0039] 情况二：随机数S表示一个随机数流时，一个随机数流S对应使用一个量子通道A传输上述一个随机数流S；

[0040] 情况三：n(n为正整数且大于等于2)个随机数值S表示n个随机数值$S_1S_2\cdots S_n$时，每个随机数值对应使用一个量子通道A传输上述单个随机数值S，共需使用n个量子通道传输，如，通过量子通道A_1传输随机数值S_1，通过量子通道A_2传输随机数值S_2，同理，通过量子通道A_n传输随机数Sn。

[0041] 情况四：n(n为正整数且大于等于2)个随机数流S表示n个随机数流$S_1S_2\cdots S_n$时，每个随机数流对应使用一个量子通道A传输上述单个随机数流S，共需使用n个量子通道传输，如，通过量子通道A_1传输随机数流S_1，通过量子通道A_2传输随机数流S_2，同理，通过量子通道A_n传输随机数流S_n。

[0042] 作为一种可选的实施方式，通过与每个随机数S对应的量子通道传输对应的随机数S，包括：

[0043] 通过量子通信中继网络中与每个随机数S对应的量子通道传输对应的随机数S。

[0044] 因为量子通信使用单光子为载体，考虑到单光子在光纤信道的衰减和探测器的灵敏度，量子通信距离一般不会超过200公里，限制了量子密钥分发的使用范围，而中继网络中有多个中继站进行量子密钥的中继转发，可以实现量子通信的远距离传输。

[0045] 现有技术中，两个远距离通信用户之间至少有一个以上的中继站，每相邻两个中继站之间利用量子通道获取共享的量子密钥，并逐段利用共享的量子密钥对要传输的会话密钥进行“加密-解密-加密…解密”的中继转发操作，最终接受方获取会话密钥，实现远距离量子通信。而且现有技术中上述量子密钥传输依赖于中继站是可信中继站。

[0046] 本实施例中利用量子通信中继网络能够实现量子通信远距离传输，具体的，量子通信中继网络是由至少一个中继站组成的中继网络架构，由中继站作为中继转发，将分发端用户传输的信息转发到接收端接收。两个通信用户之间至少有一个以上的中继站，每相邻两个中继站之间通过至少一个量子通道传输对应的随机数S，经过多个中继站将上述随机数S转发操作，最终接收方获取会话密钥，实现远距离量子通信。

[0047] 因为上述中继站是对上述随机数S的中继转发操作，因此不需要求中继站是可信中继站，即使中继站不可信，攻击者获取了上述随机数，因为上述接收端利用哈希函数对接

收的随机数S与预设密钥进行哈希运算生成会话密钥Ks，基于上述哈希函数的特性，攻击者在不知道通信双方预设密钥的情况下，无法根据S获取上述会话密钥Ks，确保了利用中继网络中的量子通道传输随机数S基于哈希函数生成的会话密钥Ks的安全性。

[0048] 综上，分发端利用上述量子通信中继网络中与每个随机数S对应的量子通道传输对应的随机数S，接收方利用哈希函数对接收的随机数S与预设密钥进行哈希运算生成会话密钥Ks，不仅可以实现量子通道的远距离传输，而且可以解决量子通信易受阻挠的问题。

[0049] 作为一种可选的实施方式，分发端可以给一个接收端发送至少一个随机数S，也可以给多个接收端发送至少一个随机数S。分发端也可以利用预设密钥K和生成的随机数S基于哈希函数生成会话密钥Ks，以使分发端和一个或多个接收端之间利用会话密钥Ks进行通信。

[0050] 作为一种可选的实施方式，分发端和一个或多个接收端之间利用会话密钥Ks进行通信，包括：

[0051] 分发端收到接收方反馈的确认消息，确定被接收方成功接收的随机数S；

[0052] 利用哈希函数对上述被接收方成功接收的随机数S和预设密钥进行哈希运算，生成会话密钥Ks。

[0053] 此时，分发端收到接收端反馈的确认消息，知道接收端都有哪些随机数S被接收，分发端和接收端可以利用哈希函数将预设的密钥K和被成功接收的随机数S进行哈希运算，生成相同的会话密钥Ks，利用会话密钥Ks对分发端要传递的消息进行加密，保证分发端和接收端用户双方通信的安全。

[0054] 作为另一种可选的实施方式，分发端作为分发量子密钥的分发方，可以给多个接收端发送至少一个随机数S。其中，各个接收端都接收到同一个随机数S，或者都接收到相同的多个随机数S，各个接收端分别利用接收的随机数S和预设密钥K基于哈希函数生成会话密钥Ks。因为各接收端接收的随机数S和预设密钥K都相同，所以基于哈希函数生成相同的会话密钥Ks，会话密钥Ks可作为共享会话密钥对多个接收端中任意两个接收端之间传递的消息进行加密，保证通信双方传递消息的安全。

[0055] 综上，本实施例中利用中继网络解决了量子通信距离短的问题，利用中继网络中的多量子通道解决了量子通信易受干扰的问题。

[0056] 为了清楚描述本发明实施例提供的一种量子密钥安全分发系统，以两个量子通道密钥分发系统为例，将该系统限定为包括：一个量子密钥分发端、一个量子密钥接收端、量子中继网络、一个量子通道。如图2所示，系统中量子密钥分发端和量子密钥接收端的交互流程如下：

[0057] 步骤201：分发端生成一个随机数S，此随机数S表示单个随机数值；

[0058] 步骤202：通过量子中继网络中的一个量子通道向接收端传输对应的随机数S；

[0059] 中继网络中有多个中继站，量子通道经过各个中继站的中继转发操作，将分发端发送的随机数S进行中继转发，最终将上述随机数S传输到接收端进行接收。

[0060] 步骤203：接收端接收单个量子通道传输的对应随机数S，利用哈希函数对接收的随机数S和预设密钥K进行哈希运算，生成会话密钥Ks。

[0061] 上述预设密钥K是分发方和接收方事先约定的相同的预设密钥K。

[0062] 步骤204：接收端成功接收到随机数S后，向分发端反馈确认消息。

[0063] 接收端未接收到随机数S后，分发端无法收到接受端发送的反馈确认消息。

[0064] 步骤205：分发端接收到接收端发送的反馈的确认消息，确定被接收方成功接收的随机数S，利用哈希函数对上述被接收方成功接收的随机数S和预设密钥进行哈希运算，生成会话密钥Ks。

[0065] 分发端和接收端使用同样的随机数S和预设密钥利用哈希函数生成相同的会话密钥Ks，利用会话密钥Ks对分发端和接收端之间传递信息进行加密，保证通信双方传输信息的安全。

[0066] 以两个量子通道密钥分发系统为例，将该系统限定为包括：一个量子密钥分发端、一个量子密钥接收端、量子中继网络、两个量子通道。如图3所示，系统中量子密钥分发端和量子密钥接收端的交互流程如下：

[0067] 步骤301：分发端生成两个随机数S_1、S_2，随机数S_1、S_2均表示单个随机数值；

[0068] 步骤302：通过量子中继网络中的两个量子通道A_1、A_2分别向接收端传输对应的随机数S_1、S_2；

[0069] 中继网络中有多个中继站，量子通道A_1、A_2经过各个中继站的中继转发操作，将分发端发送的两个随机数S_1、S_2进行中继转发，最终将上述随机数S_1、S_2传输到接收端进行接收。

[0070] 步骤303：接收端接收两个量子通道A_1、A_2传输的对应随机数S_1、S_2，利用哈希函数对接收的随机数S_1、S_2和预设密钥K进行哈希运算，生成会话密钥Ks。

[0071] 上述预设密钥K是分发方和接收方事先约定的相同的预设密钥K。

[0072] 步骤304：接收端成功接收到随机数S_1、S_2后，向分发端反馈确认消息。

[0073] 步骤305：分发端接收到接收端发送的反馈的确认消息，确定被接收方成功接收的随机数S_1、S_2，利用哈希函数对上述被接收方成功接收的随机数S_1、S_2和预设密钥进行哈希运算，生成会话密钥Ks。

[0074] 若接收端只接收到随机数S_1，向分发端发送接收到随机数S_1的反馈确认消息，则分发端确认只有随机数S_1被接收端成功接收，分发端和接收端仍可利用哈希函数对预设密钥K和随机数S_1进行哈希运算生成会话密钥Ks。

[0075] 分发端和接收端使用同样的随机数S和预设密钥利用哈希函数生成相同的会话密钥Ks，利用会话密钥Ks对分发端和接收端之间传递信息进行加密，保证通信双方传输信息的安全。

[0076] 以多量子通道密钥分发系统为例，将该系统限定为包括：一个量子密钥分发端、一个量子密钥接收端、量子中继网络、多个量子通道。如图4所示，系统中量子密钥分发端和量子密钥接收端的交互流程如下：

[0077] 步骤401：分发端生成n(n为正整数且大于等于2)个随机数S，此随机数S表示n个随机数值$S_1S_2\cdots S_n$；

[0078] 步骤402：通过量子中继网络中的n(n为正整数且大于等于2)个量子通道A向接收端传输对应的随机数S。

[0079] 其中，每个量子通道传输一个对应的随机数S，即量子通道A_1传输随机数值S_1，通过量子通道A_2传输随机数值S_2，同理，通过量子通道A_n传输随机数Sn；

[0080] 中继网络中有多个中继站，每个量子通道中的各个中继站可以对分发端发送的量

子通道中传输的随机数S进行中继转发，最终将上述随机数S传输到接收端进行接收。

[0081] 步骤403：接收端接收各个量子通道传输的对应随机数S，利用哈希函数对接收的随机数S和预设密钥K进行哈希运算，生成会话密钥Ks。

[0082] 接收端接收各个量子通道传输的随机数S，即接收端接收到的随机数为：$S_1S_2\cdots S_n$，上述预设密钥K是分发方和接收方事先约定的相同的预设密钥K，基于哈希函数利用预设密钥K和随机数$S_1S_2\cdots S_n$进行哈希运算，生成会话密钥Ks。

[0083] 步骤404：接收端成功接收到随机数S后，向分发端反馈确认消息。

[0084] 接收端未接收到随机数S，分发端无法收到接受端发送的反馈确认消息。

[0085] 步骤405：分发端接收到接收端发送的反馈的确认消息，确定被接收方成功接收的随机数S，利用哈希函数对上述被接收方成功接收的随机数S和预设密钥进行哈希运算，生成会话密钥Ks。

[0086] 例如，接收端成功接收到随机数S_1、S_2、S_3、S_4向分发端发送反馈确认消息，未接收到分发端发送的S_4，则向分发端发送反馈确认消息为S_1、S_2、S_3；分发端接收到反馈确认消息后，确定接收端接收到了随机数S_1、S_2、S_3。

[0087] 分发端和接收端使用同样的随机数S_1、S_2、S_3和预设密钥K利用哈希函数生成相同的会话密钥Ks，利用会话密钥Ks对分发端和接收端之间传递信息进行加密，保证通信双方传输信息的安全。

[0088] 综上，根据上述中继网络中量子通道的不同数量，以单量子通道和多量子通道为例，本发明的有益效果总结如下：

[0089] 以单量子通道、分发端发送一个随机数S为例，利用中继网络中的单量子通道将随机数S发送给接收端，接收端利用哈希函数生成会话密钥。

[0090] 基于哈希函数的单向特点，即使上述中继网络中的中继站不可信，攻击者获取了随机数S，但攻击者不知道通信用户间预设的密钥K，因此仍不能获取会话密钥。会话密钥的安全性不依赖与量子网络的中继站是否可信，保证通信用户对会话密钥安全性的要求。

[0091] 以多量子通道、分发端发送n个随机数$S_1S_2\cdots S_n$或n个随机数流$S_1S_2\cdots S_n$，(n为正整数且大于等于2)为例，利用与每个随机数对应的量子通道将随机数或随机数流发送给接收端，接收端利用哈希函数生成会话密钥。

[0092] 基于哈希函数的单向特点及多量子通道传输，即使所有量子通道都不可信，攻击者也无法获取会话密钥，而且采用多量子通道密钥分发，即使一个量子通道受干扰，整个量子通信系统的通信也不受影响。

[0093] 实施例二

[0094] 基于同一发明构思，本发明实施例中提供了一种量子密钥安全分发接收的设备，该设备的具体实施可参见系统实施例部分的描述，重复之处不再赘述。

[0095] 该设备包括处理器、存储器和收发机。

[0096] 处理器负责管理总线架构和通常的处理，存储器可以存储处理器在执行操作时所使用的数据。收发机用于在处理器的控制下接收和发送数据。

[0097] 总线架构可以包括任意数量的互联的总线和桥，具体由处理器代表的一个或多个处理器和存储器代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因

此，本文不再对其进行进一步描述。总线接口提供接口。处理器负责管理总线架构和通常的处理，存储器可以存储处理器在执行操作时所使用的数据。

[0098] 本发明实施例揭示的流程，可以应用于处理器中，或者由处理器实现。在实现过程中，信号处理流程的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。处理器可以是通用处理器、数字信号处理器、专用集成电路、现场可编程门阵列或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件，可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成信号处理流程的步骤。

[0099] 第一设备，一种会话密钥的生成设备。

[0100] 其中，处理器用于读取存储器中的程序并执行下列过程：

[0101] 生成至少一个随机数；

[0102] 通过与所述随机数对应的量子通道传输对应的随机数，以使接收方利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥。

[0103] 作为一种可选的实施方式，生成至少一个随机数，包括：

[0104] 生成一个随机数；

[0105] 通过与所述随机数对应的量子通道传输对应的随机数，包括：

[0106] 通过与一个随机数对应的一个量子通道传输所述随机数。

[0107] 作为一种可选的实施方式，生成至少一个随机数，包括：

[0108] 生成至少两个随机数；

[0109] 通过与所述随机数对应的量子通道传输对应的随机数，包括：

[0110] 通过与每个随机数对应的一个量子通道传输对应的随机数，其中一个随机数对应一个量子通道。

[0111] 作为一种可选的实施方式，处理器还用于：

[0112] 通过量子通信中继网络中与每个随机数对应的量子通道传输对应的随机数。

[0113] 作为一种可选的实施方式，处理器还用于：

[0114] 收到接收方反馈的确认消息，确定被接收方成功接收的随机数；

[0115] 利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥，包括：

[0116] 利用哈希函数对上述被接收方成功接收的随机数和预设密钥进行哈希运算，生成会话密钥。

[0117] 可选的，上述哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

[0118] 第二设备，一种会话密钥的接收设备。

[0119] 其中，处理器用于读取存储器中的程序并执行下列过程：

[0120] 接收量子密钥分发端通过至少两个量子通道传输的对应随机数；

[0121] 利用哈希函数对接收的随机数和预设密钥进行哈希运算，生成会话密钥。

[0122] 作为一种可选的实施方式，处理器还用于：

[0123] 接收量子通信中继网络中至少两个量子通道传输的对应随机数。

[0124] 作为一种可选的实施方式，处理器还用于：

[0125] 成功接收到随机数后，向分发端反馈确认消息。

[0126] 可选的，上述哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

[0127] 实施例三

[0128] 基于同一发明构思，本发明实施例提供了一种量子密钥安全分发接收装置，该装置，该装置的具体实施可参见系统实施例部分的描述，重复之处不再赘述。

[0129] 第一装置，一种会话密钥的生成装置。

[0130] 该装置包括：

[0131] 随机数生成单元，用于生成至少一个随机数；

[0132] 会话密钥单元，用于通过与所述随机数对应的量子通道传输对应的随机数，以使接收方利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥。

[0133] 作为一种可选的实施方式，生成至少一个随机数，包括：

[0134] 生成一个随机数；

[0135] 通过与所述随机数对应的量子通道传输对应的随机数，包括：

[0136] 通过与一个随机数对应的一个量子通道传输所述随机数。

[0137] 作为一种可选的实施方式，生成至少一个随机数，包括：

[0138] 生成至少两个随机数；

[0139] 通过与所述随机数对应的量子通道传输对应的随机数，包括：

[0140] 通过与每个随机数对应的一个量子通道传输对应的随机数，其中一个随机数对应一个量子通道。

[0141] 作为一种可选的实施方式，会话密钥单元，还用于通过量子通信中继网络中与每个随机数对应的量子通道传输对应的随机数。

[0142] 作为一种可选的实施方式，还用于：

[0143] 收到接收方反馈的确认消息，确定被接收方成功接收的随机数；

[0144] 利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥，用于：

[0145] 利用哈希函数对上述被接收方成功接收的随机数和预设密钥进行哈希运算，生成会话密钥。

[0146] 作为一种可选的实施方式，上述哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

[0147] 第二装置，一种会话密钥的接收装置。

[0148] 该装置包括：

[0149] 接收密钥单元，用于接收量子密钥分发端通过至少两个量子通道传输的对应随机数；

[0150] 会话密钥单元，用于利用哈希函数对接收的随机数和预设密钥进行哈希运算，生成会话密钥。

[0151] 作为一种可选的实施方式，接收密钥单元还用于：

[0152] 接收量子通信中继网络中至少两个量子通道传输的对应随机数。

[0153] 作为一种可选的实施方式，上述装置还用于：

[0154] 成功接收到随机数后，向分发端反馈确认消息。

[0155] 作为一种可选的实施方式，上述哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

[0156] 实施例四

[0157] 方法一、本发明实施例在分发端，提供了一种会话密钥的生成方法，如图5所示，该方法包括：

[0158] 步骤501：生成至少一个随机数。

[0159] 实施中，根据量子通道不同分为以下几种情况：

[0160] 情况一：分发端生成一个随机数，通过一个量子通道将随机数发送给接收端；

[0161] 情况二：分发端生成至少两个随机数，通过与上述随机数对应的至少两个量子通道将随机数发送给接收端。

[0162] 步骤502：通过与所述随机数对应的量子通道传输对应的随机数，以使接收方利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥。

[0163] 作为一种可选的实施方式，通过与每个随机数对应的量子通道传输对应的随机数，包括：

[0164] 通过量子通信中继网络中与每个随机数对应的量子通道传输对应的随机数。

[0165] 作为一种可选的实施方式，还包括：

[0166] 收到接收方反馈的确认消息，确定被接收方成功接收的随机数；

[0167] 利用哈希函数对接收的随机数与预设密钥进行哈希运算生成会话密钥，包括：

[0168] 利用哈希函数对上述被接收方成功接收的随机数和预设密钥进行哈希运算，生成会话密钥。

[0169] 作为一种可选的实施方式，上述哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

[0170] 方法二、本发明实施例在接收端，提供了一种会话密钥的接收方法，如图6所示，该方法包括：

[0171] 步骤601：接收量子密钥分发端通过至少两个量子通道传输的对应随机数；

[0172] 实施中，发送方发送至少两个随机数，接收方接收至少一个随机数，因为如果发送方发送两个随机数，一旦有一条量子链路受到干扰，接受方只能接收到一个随机数。

[0173] 步骤602：利用哈希函数对接收的随机数和预设密钥进行哈希运算，生成会话密钥。

[0174] 作为一种可选的实施方式，接收量子密钥分发端通过至少两个量子通道传输的对应随机数，包括：

[0175] 接收量子通信中继网络中至少两个量子通道传输的对应随机数。

[0176] 作为一种可选的实施方式，还包括：

[0177] 成功接收到随机数后，向分发端反馈确认消息。

[0178] 作为一种可选的实施方式，哈希函数为安全散列算法SHA-256或者安全散列算法SHA-512或者安全散列算法SHA-3。

[0179] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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和光学存储器等)上实施的计算机程序产品的形式。

[0180] 本发明是参照根据本发明实施例的方法、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设备。

[0181] 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设备的制造品，该指令设备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。

[0182] 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。

[0183] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

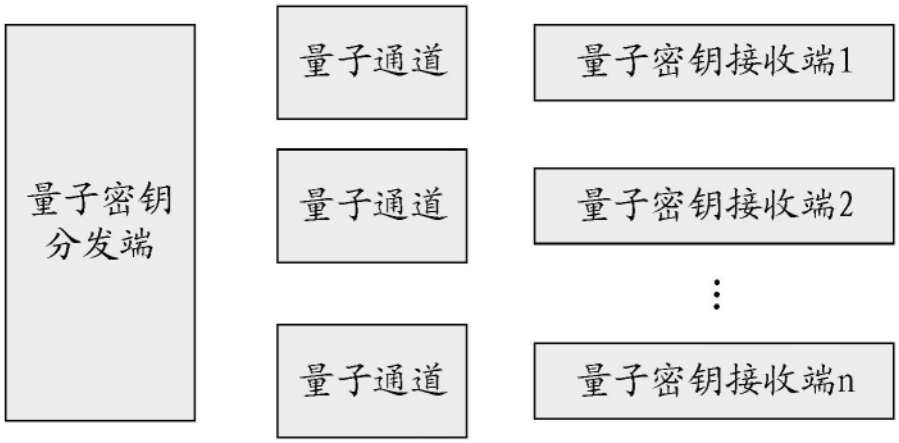

量子密钥
分发端
量子通道
量子通道
量子通道
量子密钥接收端1
量子密钥接收端2
量子密钥接收端n

图1

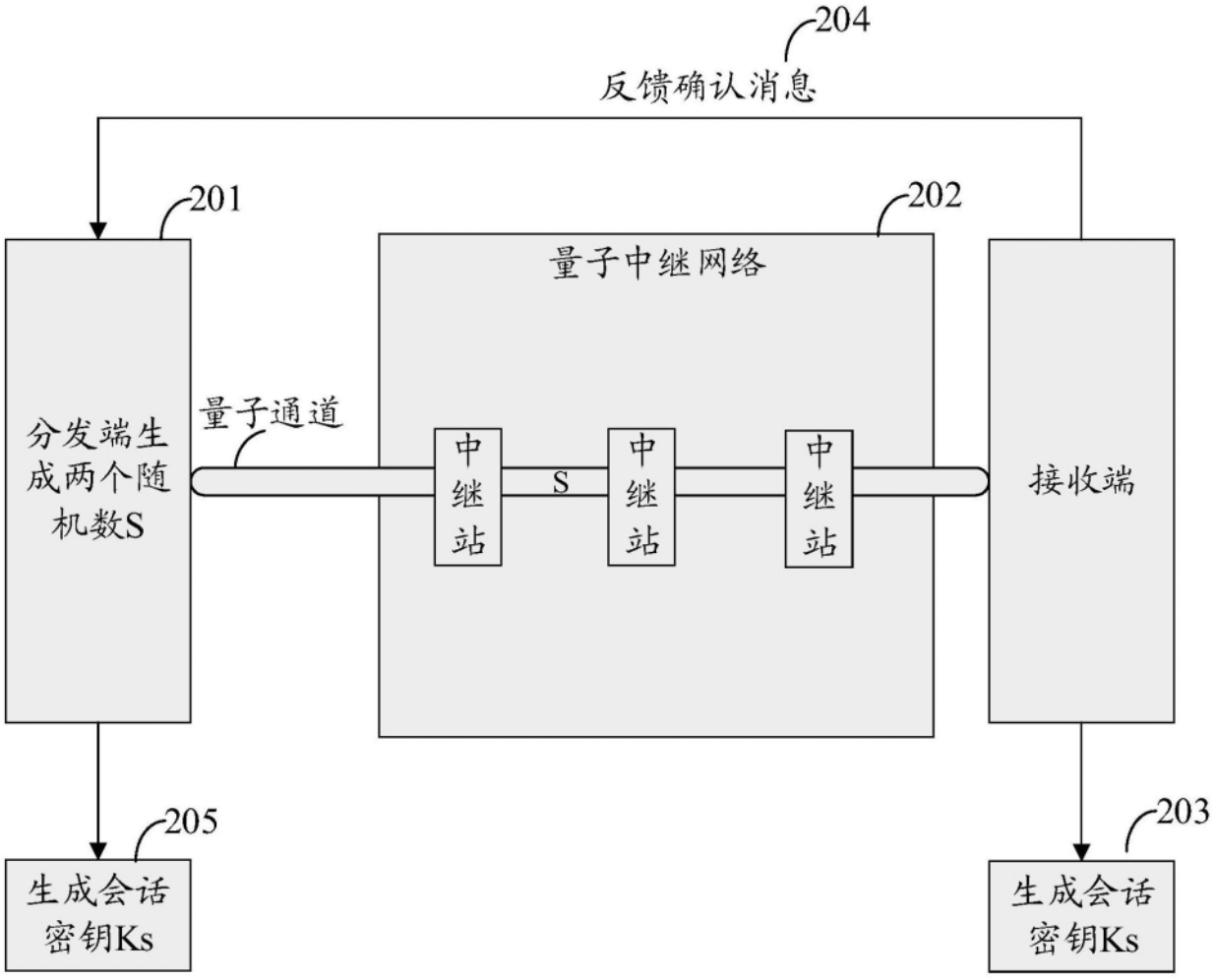

204
反馈确认消息
201
202
量子中继网络
分发端生
成两个随
机数S
量子通道
中
继
站
S
中
继
站
中
继
站
接收端
205
203
生成会话
密钥Ks
生成会话
密钥Ks

图2

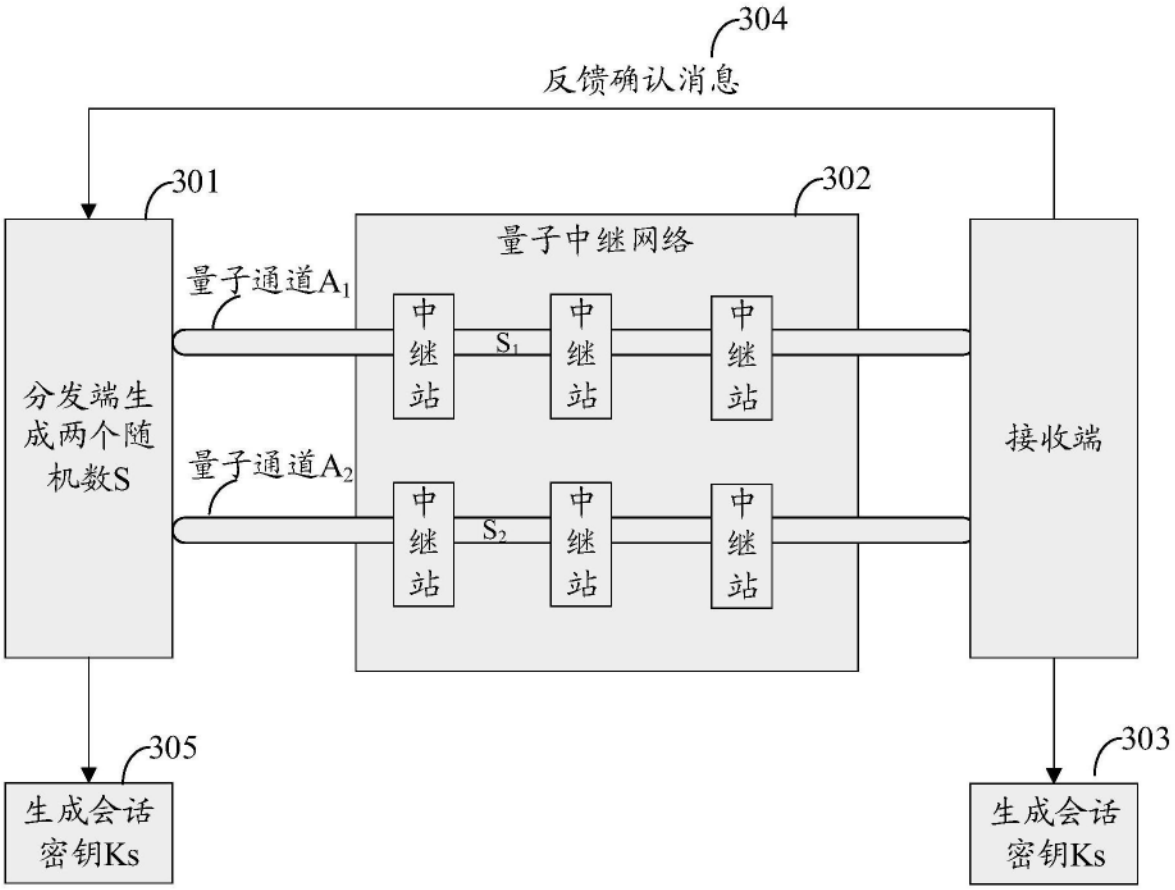

304
反馈确认消息
301
302
量子中继网络
量子通道A1
中继站
S1
中继站
中继站
分发端生成两个随机数S
接收端
量子通道A2
中继站
S2
中继站
中继站
305
303
生成会话密钥Ks
生成会话密钥Ks

图3

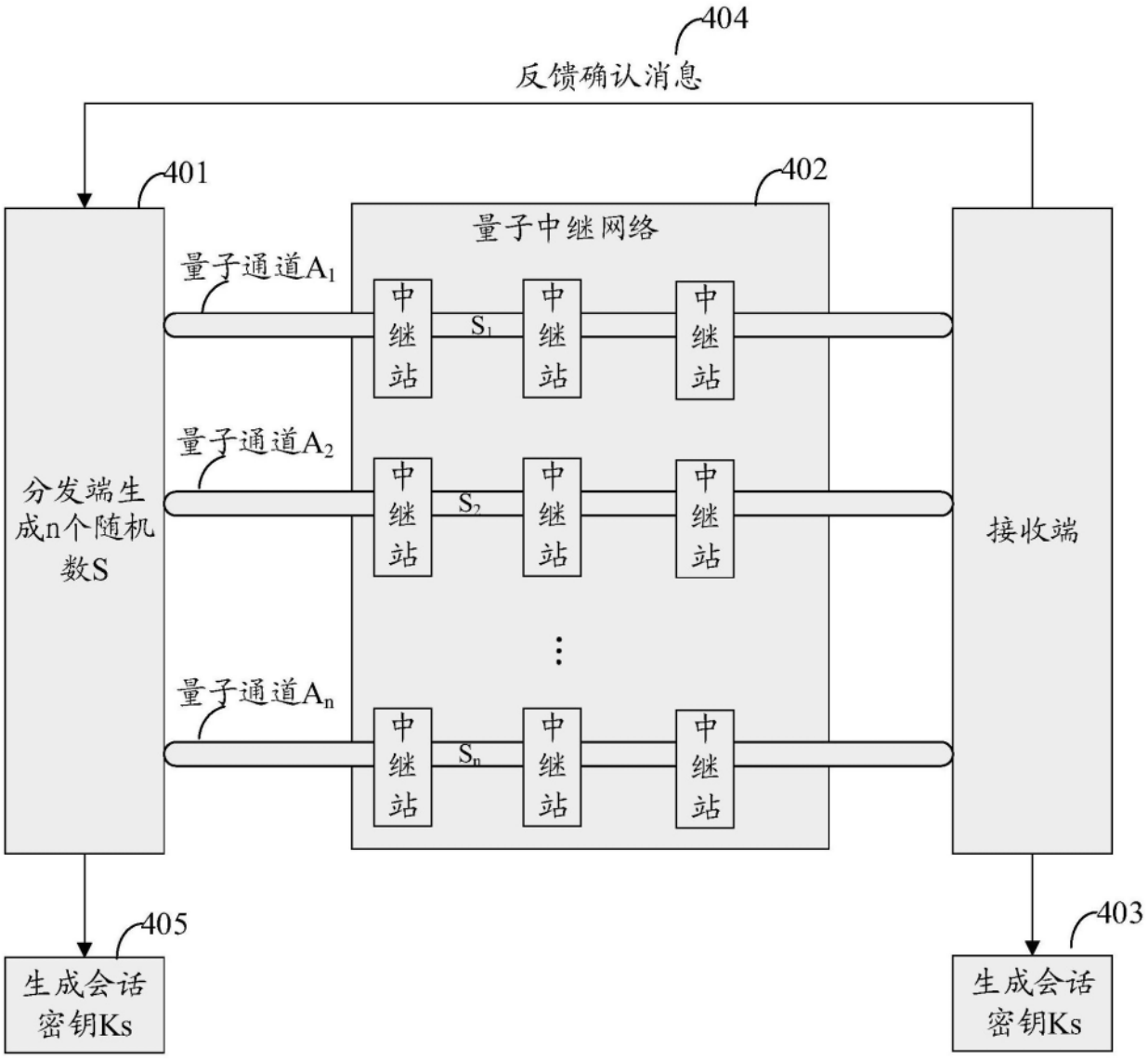

404
反馈确认消息
401
402
量子中继网络
量子通道A1
量子通道A2
量子通道An
中继站
S1
S2
Sn
分发端生成n个随机数S
接收端
405
生成会话密钥Ks
403
生成会话密钥Ks

图4

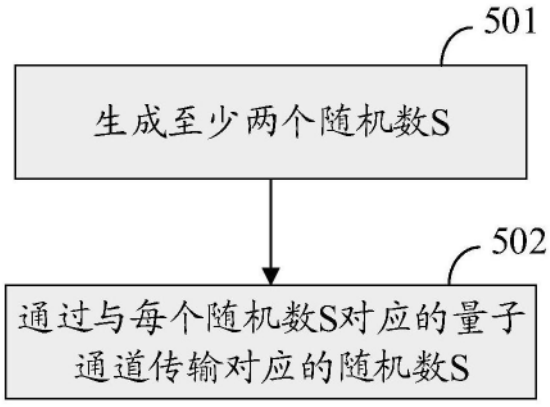

501
生成至少两个随机数S
502
通过与每个随机数S对应的量子通道传输对应的随机数S

图5

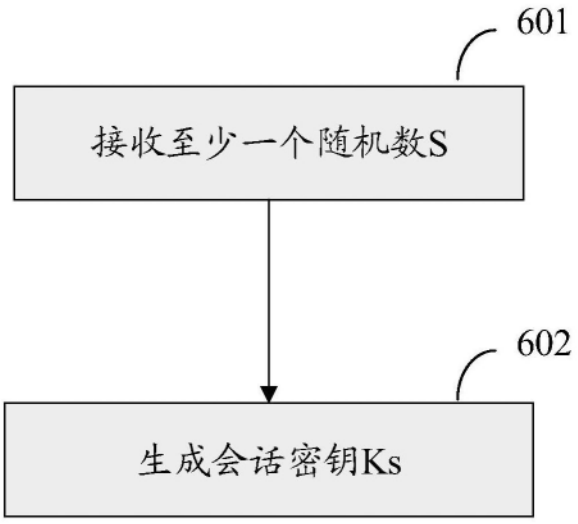


图6