(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110380844 B
(45)授权公告日 2021.01.29

(21)申请号 201810332715.5

(22)申请日 2018.04.13

(65)同一申请的已公布的文献号
申请公布号 CN 110380844 A

(43)申请公布日 2019.10.25

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 李政宇 苏长征 胡苏 邹扬

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 冯艳莲

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
CN 105827397 A,2016.08.03
CN 106330434 A,2017.01.11
CN 107508671 A,2017.12.22
WO 2004086666 A3,2005.04.28
US 2013208894 A1,2013.08.15
韩伟等.《基于信任中继的QKD网络路由选择研究》.《军事通信技术》.2013,第34卷(第4期),全文.
赵红涛等.《基于密钥位协商的多路径量子密钥协商技术研》.《中原工学院学报》.2014,第25卷(第6期),全文.

审查员 马晨晨

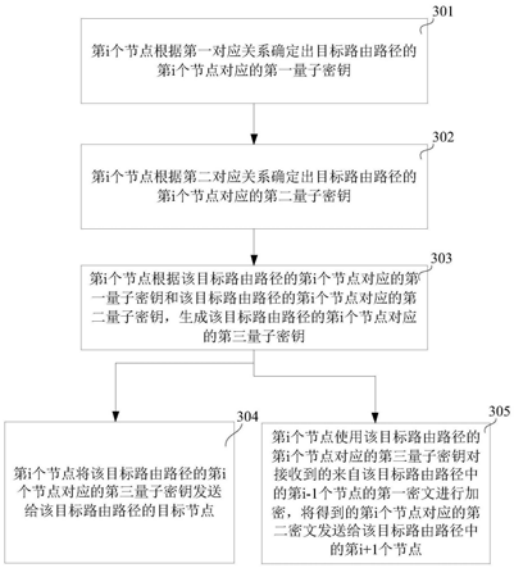
权利要求书5页 说明书21页 附图7页

(54)发明名称

一种量子密钥分发方法、设备及存储介质

(57)摘要

本申请实施例提供一种量子密钥分发方法、设备及存储介质,用于解决现有技术中量子密钥在节点间分发存在的安全性差的问题。本申请实施例中,第i个节点根据确定出的目标路由路径的第i个节点对应的第一量子密钥和目标路由路径的第i个节点对应的第二量子密钥,生成目标路由路径的第i个节点对应的第三量子密钥,并将目标路由路径的第i个节点对应的第三量子密钥发送给目标路由路径的目标节点,或使用目标路由路径的第i个节点对应的第三量子密钥对接收到的第一密文进行加密,将得到的第i个节点对应的第二密文发送给目标路由路径中的第i+1个节点,可见,第i个节点未对接收到的第一密文进行解密,从而可以提高量子密钥分发的安全性。



CN 110380844 B

1.一种量子密钥分发方法,其特征在于,包括:

第i个节点根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥,其中,所述第i个节点为所述目标路由路径中的第i个节点;所述目标路由路径的第i个节点对应的第一量子密钥为所述第i个节点获取的所述第i个节点与所述目标路由路径中第i-1个节点之间共享的量子密钥,所述第一对应关系包括经过所述第i个节点的N条路由路径与所述第i个节点对应的N个第一量子密钥的对应关系,所述N条路由路径和所述第i个节点对应的所述N个第一量子密钥一一对应,所述目标路由路径为所述N条路由路径中的一条路由路径,所述N为正整数,所述i为正整数;

所述第i个节点根据第二对应关系确定出所述目标路由路径的所述第i个节点对应的第二量子密钥,所述目标路由路径的所述第i个节点对应的第二量子密钥为所述第i个节点所获取的所述第i个节点与所述目标路由路径中第i+1个节点之间共享的量子密钥,所述第二对应关系包括经过所述第i个节点的N条路由路径与所述第i个节点对应的N个第二量子密钥的对应关系,所述N条路由路径和所述第i个节点对应的所述N个第二量子密钥一一对应;

所述第i个节点根据所述目标路由路径的所述第i个节点对应的第一量子密钥和所述目标路由路径的所述第i个节点对应的第二量子密钥,生成所述目标路由路径的所述第i个节点对应的第三量子密钥;

所述第i个节点将所述目标路由路径的所述第i个节点对应的第三量子密钥发送给所述目标路由路径的目标节点;或者,所述第i个节点使用所述目标路由路径的所述第i个节点对应的第三量子密钥对接收到的来自所述目标路由路径中的第i-1个节点的第一密文进行加密,将得到的所述第i个节点对应的第二密文发送给所述目标路由路径中的第i+1个节点,其中,所述第i个节点接收到的来自所述目标路由路径中的第i-1个节点的第一密文为所述第i-1个节点发出的所述第i-1个节点对应的第二密文;当所述i为1时,第0个节点为所述目标路由路径的源节点,所述目标路由路径的源节点对应的第二密文为使用所述目标路由路径的源节点对应的第二量子密钥对所述目标路由路径的源节点和所述目标路由路径的目标节点之间待共享量子密钥进行加密得到的;

其中,所述目标路由路径中的第i-1个节点对应的第二量子密钥与所述目标路由路径的第i个节点对应的第一量子密钥相同;且,所述目标路由路径中的第i个节点对应的第二量子密钥与所述目标路由路径的第i+1个节点对应的第一量子密钥相同。

2.如权利要求1所述的方法,其特征在于,若所述N为大于1的整数,则针对经过所述第i个节点的N条路由路径中的第一路由路径和第二路由路径:

所述第一路由路径的第i个节点对应的第一量子密钥与所述第二路由路径的第i个节点对应的第一量子密钥不同;

所述第一路由路径的第i个节点对应的第二量子密钥与所述第二路由路径的第i个节点对应的第二量子密钥不同。

3.如权利要求1或2所述的方法,其特征在于,所述第i个节点根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥之前,还包括:

所述第i个节点接收集中控制器或所述目标路由路径中的第i-1个节点发送的用于指示所述第一对应关系中的所述目标路由路径的所述第i个节点对应所述目标路由路径的第

一量子密钥的指示信息;其中,所述集中控制器用于收集全网的业务请求,优化计算全网的路由路径,统一计算每个节点作为节点时所对应的第一对应关系并下发至相应的节点;

或者;

所述第i个节点根据获取的量子通信系统的网络拓扑信息和第一预设规则确定所述第一对应关系中的所述目标路由路径的所述第i个节点对应所述目标路由路径的第一量子密钥。

4.如权利要求3所述的方法,其特征在于,所述第i个节点根据获取的量子通信系统的网络拓扑信息和第一预设规则确定所述第一对应关系中的所述目标路由路径的所述第i个节点对应所述目标路由路径的第一量子密钥,包括:

所述第i个节点根据经过所述第i个节点的N条路由路径中的N个第i-1个节点的编号之间的排序关系、经过所述第i个节点的N条路由路径中的N个第i+1个节点的编号之间的排序关系,以及经过所述第i个节点的N条路由路径的编号之间的排序关系,确定出经过所述第i个节点的N条路由路径的排序,并依序确定出所述目标路由路径的所述第i个节点对应的第一量子密钥;

或者;

所述第i个节点根据经过所述第i个节点的N条路由路径中的N个第i+1个节点的编号之间的排序关系,以及经过所述第i个节点的N条路由路径的编号之间的排序关系,确定出经过所述第i个节点的N条路由路径的排序,并依序确定出所述目标路由路径的所述第i个节点对应的第一量子密钥;

或者;

所述第i个节点根据经过所述第i个节点的N条路由路径的编号之间的排序关系,确定出经过所述第i个节点的N条路由路径的排序,并依序确定出所述目标路由路径的所述第i个节点对应的第一量子密钥。

5.如权利要求1或2所述的方法,其特征在于,所述第i个节点根据第二对应关系确定出所述目标路由路径的所述第i个节点对应的第二量子密钥之前,还包括:

所述第i个节点接收集中控制器或所述目标路由路径对应的第i+1个节点发送的用于指示所述第二对应关系中的所述目标路由路径的所述第i个节点对应的第二量子密钥的指示信息;

或者;

所述第i个节点根据获取的量子通信系统的网络拓扑信息和第二预设规则确定所述第二对应关系中的所述目标路由路径的所述第i个节点对应的第二量子密钥。

6.如权利要求5所述的方法,其特征在于,所述第i个节点根据获取的量子通信系统的网络拓扑信息和第二预设规则确定所述第二对应关系中的所述目标路由路径的所述第i个节点对应的第二量子密钥,包括:

所述第i个节点根据经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径的编号之间的排序关系,确定出经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径的排序,并依序确定出所述目标路由路径的所述第i个节点对应的第二量子密钥;所述W为不大于所述N的正整数;

或者;

所述第i个节点根据经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径中的W个第i+2个节点的编号之间的排序关系，以及经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径的编号之间的排序关系，确定出经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径的排序，并依序确定出所述目标路由路径的所述第i个节点对应的第二量子密钥。

7.如权利要求1或2所述的方法，其特征在于，所述第i个节点使用所述目标路由路径的所述第i个节点对应的第三量子密钥对接收到的来自所述目标路由路径中的第i-1个节点的第一密文进行加密的第一算法满足以下公式：

$g(f_E(K_{i,i-1}(L_j),K_{i,i+1}(L_j)),f_E(K_{i+1,i}(L_j),K_{i+1,i+2}(L_j)))=f_E(K_{i,i-1}(L_j),K_{i+1,i+2}(L_j))$

其中，所述L_j为所述目标路由路径的标识；

所述$K_{i,i-1}(L_j)$为所述目标路由路径L_j中第i个节点对应的第一量子密钥；

所述$K_{i,i+1}(L_j)$为所述目标路由路径L_j中第i个节点对应的第二量子密钥；

所述$K_{i+1,i}(L_j)$为所述目标路由路径L_j中第i+1个节点对应的第一量子密钥；

所述$K_{i+1,i+2}(L_j)$为所述目标路由路径L_j中第i+1个节点对应的第二量子密钥；

其中，$f_E(\bullet)$为第二算法对应的函数，所述第二算法为根据所述目标路由路径的所述第i个节点对应的第一量子密钥和所述目标路由路径的所述第i个节点对应的第二量子密钥，生成所述目标路由路径的所述第i个节点对应的第三量子密钥时所使用的算法；

$g(\bullet)$为所述第一算法对应的函数。

8.一种量子密钥分发设备，其特征在于，所述量子密钥分发设备为量子通信系统的一条路由路径中的第i个节点，所述量子密钥分发设备包括：

处理器，用于根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥，根据第二对应关系确定出所述目标路由路径的所述第i个节点对应的第二量子密钥，根据所述目标路由路径的所述第i个节点对应的第一量子密钥和所述目标路由路径的所述第i个节点对应的第二量子密钥，生成所述目标路由路径的所述第i个节点对应的第三量子密钥；其中，所述第i个节点为所述目标路由路径中的第i个节点；所述目标路由路径的第i个节点对应的第一量子密钥为所述第i个节点获取的所述第i个节点与所述目标路由路径中第i-1个节点之间共享的量子密钥，所述第一对应关系包括经过所述第i个节点的N条路由路径与所述第i个节点对应的N个第一量子密钥的对应关系，所述N条路由路径和所述第i个节点对应的所述N个第一量子密钥一一对应，所述目标路由路径为所述N条路由路径中的一条路由路径，所述N为正整数，所述i为正整数；所述目标路由路径的所述第i个节点对应的第二量子密钥为所述第i个节点所获取的所述第i个节点与所述目标路由路径中第i+1个节点之间共享的量子密钥，所述第二对应关系包括经过所述第i个节点的N条路由路径与所述第i个节点对应的N个第二量子密钥的对应关系，所述N条路由路径和所述第i个节点对应的所述N个第二量子密钥一一对应；

收发器，用于将所述目标路由路径的所述第i个节点对应的第三量子密钥发送给所述目标路由路径的目标节点；或者，将通过所述处理器使用所述目标路由路径的所述第i个节点对应的第三量子密钥对接收到的来自所述目标路由路径中的第i-1个节点的第一密文进行加密所得到的所述第i个节点对应的第二密文发送给所述目标路由路径中的第i+1个节点；

其中,所述第i个节点接收到的来自所述目标路由路径中的第i-1个节点的第一密文为所述第i-1个节点发出的所述第i-1个节点对应的第二密文;当所述i为1时,第0个节点为所述目标路由路径的源节点,所述目标路由路径的源节点对应的第二密文为使用所述目标路由路径的源节点对应的第二量子密钥对所述目标路由路径的源节点和所述目标路由路径的目标节点之间待共享量子密钥进行加密得到的;

其中,所述目标路由路径中的第i-1个节点对应的第二量子密钥与所述目标路由路径的第i个节点对应的第一量子密钥相同;且,所述目标路由路径中的第i个节点对应的第二量子密钥与所述目标路由路径的第i+1个节点对应的第一量子密钥相同。

9.如权利要求8所述的设备,其特征在于,若所述N为大于1的整数,则针对经过所述第i个节点的N条路由路径中的第一路由路径和第二路由路径:

所述第一路由路径的第i个节点对应的第一量子密钥与所述第二路由路径的第i个节点对应的第一量子密钥不同;

所述第一路由路径的第i个节点对应的第二量子密钥与所述第二路由路径的第i个节点对应的第二量子密钥不同。

10.如权利要求8或9所述的设备,其特征在于,所述收发器,还用于接收集中控制器或所述目标路由路径中的第i-1个节点发送的用于指示所述第一对应关系中的所述目标路由路径的所述第i个节点对应所述目标路由路径的第一量子密钥的指示信息;其中,所述集中控制器用于收集全网的业务请求,优化计算全网的路由路径,统一计算每个节点作为节点时所对应的第一对应关系并下发至相应的节点;

或者;

所述处理器,还用于根据获取的量子通信系统的网络拓扑信息和第一预设规则确定所述第一对应关系中的所述目标路由路径的所述第i个节点对应所述目标路由路径的第一量子密钥。

11.如权利要求10所述的设备,其特征在于,所述处理器,用于:

根据经过所述第i个节点的N条路由路径中的N个第i-1个节点的编号之间的排序关系、经过所述第i个节点的N条路由路径中的N个第i+1个节点的编号之间的排序关系,以及经过所述第i个节点的N条路由路径的编号之间的排序关系,确定出经过所述第i个节点的N条路由路径的排序,并依序确定出所述目标路由路径的所述第i个节点对应的第一量子密钥;

或者;

根据经过所述第i个节点的N条路由路径中的N个第i+1个节点的编号之间的排序关系,以及经过所述第i个节点的N条路由路径的编号之间的排序关系,确定出经过所述第i个节点的N条路由路径的排序,并依序确定出所述目标路由路径的所述第i个节点对应的第一量子密钥;

或者;

根据经过所述第i个节点的N条路由路径的编号之间的排序关系,确定出经过所述第i个节点的N条路由路径的排序,并依序确定出所述目标路由路径的所述第i个节点对应的第一量子密钥。

12.如权利要求8或9所述的设备,其特征在于,所述收发器,还用于接收集中控制器或所述目标路由路径对应的第i+1个节点发送的用于指示所述第二对应关系中的所述目标路

由路径的所述第i个节点对应的第二量子密钥的指示信息；

或者；

所述处理器，还用于根据获取的量子通信系统的网络拓扑信息和第二预设规则确定所述第二对应关系中的所述目标路由路径的所述第i个节点对应的第二量子密钥。

13.如权利要求12所述的设备，其特征在于，所述处理器，用于：

根据经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径的编号之间的排序关系，确定出经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径的排序，并依序确定出所述目标路由路径的所述第i个节点对应的第二量子密钥；所述W为不大于所述N的正整数；

或者；

根据经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径中的W个第i+2个节点的编号之间的排序关系，以及经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径的编号之间的排序关系，确定出经过所述第i个节点和所述目标路由路径中的第i+1个节点的W条路由路径的排序，并依序确定出所述目标路由路径的所述第i个节点对应的第二量子密钥。

14.如权利要求8或9所述的设备，其特征在于，所述处理器使用所述目标路由路径的所述第i个节点对应的第三量子密钥对接收到的来自所述目标路由路径中的第i-1个节点的第一密文进行加密的第一算法满足以下公式：

$g(f_E(K_{i,i-1}(L_j),K_{i,i+1}(L_j)),f_E(K_{i+1,i}(L_j),K_{i+1,i+2}(L_j)))=f_E(K_{i,i-1}(L_j),K_{i+1,i+2}(L_j))$

其中，所述L_j为所述目标路由路径的标识；

所述$K_{i,i-1}(L_j)$为所述目标路由路径L_j中第i个节点对应的第一量子密钥；

所述$K_{i,i+1}(L_j)$为所述目标路由路径L_j中第i个节点对应的第二量子密钥；

所述$K_{i+1,i}(L_j)$为所述目标路由路径L_j中第i+1个节点对应的第一量子密钥；

所述$K_{i+1,i+2}(L_j)$为所述目标路由路径L_j中第i+1个节点对应的第二量子密钥；

其中，$f_E(\bullet)$为第二算法对应的函数，所述第二算法为根据所述目标路由路径的所述第i个节点对应的第一量子密钥和所述目标路由路径的所述第i个节点对应的第二量子密钥，生成所述目标路由路径的所述第i个节点对应的第三量子密钥时所使用的算法；

$g(\bullet)$为所述第一算法对应的函数。

15.一种计算机存储介质，其特征在于，所述计算机存储介质存储有计算机可执行指令，所述计算机可执行指令在被计算机调用时，使所述计算机执行如权利要求1至7任一权利要求所述的方法。

一种量子密钥分发方法、设备及存储介质

技术领域

[0001] 本申请涉及量子通信领域，尤其涉及一种量子密钥分发方法、设备及存储介质。

背景技术

[0002] 随着科学技术的进步，信息化程度的加快，通信的频率更加频繁，人们对通信的安全性的要求越来越高。量子保密通信是量子特性与传统密码结合的产物，它利用量子力学的基本原理和特性来确保通信的安全性。经过三十多年的发展，量子保密通信目前正在走向市场实用化。

[0003] 现阶段最接近实用的量子保密通信技术是量子密钥分发(QKD)技术，其功能是在已共享部分安全密钥的前提下，实现对称密钥的无条件安全分发。图1示出了现有技术中量子密钥分发方法的示意图，如图1所示，路由路径中包括源节点A_1、中继节点A_2、中继节点A_3和目的节点A_4。K_1为源节点A_1和目的节点A_4之间的待共享量子密钥，需要从源节点A_1传输至目的节点A_4。现有技术中，源节点A_1使用K_{A1A2}对K_1加密，得到K_2，并将得到的K_2传输至中继节点A_2，其中，K_{A1A2}为源节点A_1和中继节点A_2共享的一个私钥。中继节点A_2使用K_{A1A2}对K_2解密，之后使用K_{A2A3}对K_1加密，得到K_3，并将得到的K_3传输至中继节点A_3，其中，K_{A2A3}为中继节点A_2和中继节点A_3共享的一个私钥。中继节点A_3使用K_{A2A3}对K_3解密，之后使用K_{A3A4}对K_1加密，得到K_4，并将得到的K_4传输至目的节点A_4，其中，K_{A3A4}为中继节点A_3和目的节点A_4共享的一个私钥。目的节点A_4使用K_{A3A4}对K_4解密，得到K_1。

[0004] 图1所示的方案中，源节点A_1和目的节点A_4之间的待共享量子密钥K_1在各个中间节点均会被解密，安全性较差。

发明内容

[0005] 本申请实施例提供一种量子密钥分发方法、设备及存储介质，可以解决现有技术中量子密钥在节点间分发存在的安全性差的问题。

[0006] 第一方面，本申请实施例提供一种量子密钥分发方法，该方法包括：

[0007] 第i个节点根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥，其中，第i个节点为目标路由路径中的第i个节点；目标路由路径的第i个节点对应的第一量子密钥为第i个节点获取的第i个节点与目标路由路径中第i-1个节点之间共享的量子密钥，第一对应关系包括经过第i个节点的N条路由路径与第i个节点对应的N个第一量子密钥的对应关系，N条路由路径和第i个节点对应的N个第一量子密钥一一对应，目标路由路径为N个条路由路径中的一条路由路径，N为正整数，i为正整数；

[0008] 第i个节点根据第二对应关系确定出目标路由路径的第i个节点对应的第二量子密钥，目标路由路径的第i个节点对应的第二量子密钥为第i个节点所获取的第i个节点与目标路由路径中第i+1个节点之间共享的量子密钥，第二对应关系包括经过第i个节点的N条路由路径与第i个节点对应的N个第二量子密钥的对应关系，N条路由路径和第i个节点对应的N个第二量子密钥一一对应；

[0009] 第i个节点根据目标路由路径的第i个节点对应的第一量子密钥和目标路由路径的第i个节点对应的第二量子密钥,生成目标路由路径的第i个节点对应的第三量子密钥;

[0010] 第i个节点将目标路由路径的第i个节点对应的第三量子密钥发送给目标路由路径的目标节点;或者;第i个节点使用目标路由路径的第i个节点对应的第三量子密钥对接收到的来自目标路由路径中的第i-1个节点的第一密文进行加密,将得到的第i个节点对应的第二密文发送给目标路由路径中的第i+1个节点,其中,第i个节点接收到的来自目标路由路径中的第i-1个节点的第一密文为第i-1个节点发出的第i-1个节点对应的第二密文;当i为1时,第0个节点为目标路由路径的源节点,目标路由路径的源节点对应的第二密文为使用目标路由路径的源节点对应的第二量子密钥对目标路由路径的源节点和目标路由路径的目标节点之间待共享量子密钥进行加密得到的;

[0011] 其中,目标路由路径中的第i-1个节点对应的第二量子密钥与目标路由路径的第i个节点对应的第一量子密钥相同;且,目标路由路径中的第i个节点对应的第二量子密钥与目标路由路径的第i+1个节点对应的第一量子密钥相同。

[0012] 本申请实施例中,目标路由路径的源节点对应的第二密文为使用目标路由路径的源节点对应的第二量子密钥对目标路由路径的源节点和目标路由路径的目标节点之间待共享量子密钥进行加密得到的,且第i-1个节点发出的第i-1个节点对应的第二密文为第i个节点接收到的来自目标路由路径中的第i-1个节点的第一密文。第i个节点将目标路由路径的第i个节点对应的第三量子密钥发送给目标路由路径的目标节点;或者;第i个节点使用目标路由路径的第i个节点第三量子密钥对接收到的来自目标路由路径中的第i-1个节点的第一密文进行加密,将得到的第i个节点对应的第二密文发送给目标路由路径中的第i+1个节点,可见,第i个节点并未对接收到的第一密文进行解密,即源节点和目标路由路径的目标节点之间待共享量子密钥不会在节点落地,因此提高了量子密钥分发的安全性。

[0013] 在一种可能地实现方式中,若N为大于1的整数,则针对经过第i个节点的N条路由路径中的第一路由路径和第二路由路径:第一路由路径的第i个节点对应的第一量子密钥与第二路由路径的第i个节点对应的第一量子密钥不同;第一路由路径的第i个节点对应的第二量子密钥与第二路由路径的第i个节点对应的第二量子密钥不同。如此,针对每条路由路径,节点为该路由路径分配对应的量子密钥,从而实现一次一密,可以进一步提高量子密钥分配的安全性。

[0014] 在一种可能地实现方式中,第i个节点根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥之前,还包括:第i个节点接收集中控制器或目标路由路径中的第i-1个节点发送的用于指示第一对应关系中的目标路由路径的第i个节点对应目标路由路径的第一量子密钥的指示信息;或者;第i个节点根据获取的量子通信系统的网络拓扑信息和第一预设规则确定第一对应关系中的目标路由路径的第i个节点对应目标路由路径的第一量子密钥。可见可以通过多种方案确定出路由路径的节点对应的第一量子密钥,提高了方案的灵活性。

[0015] 在一种可能地实现方式中,第i个节点根据获取的量子通信系统的网络拓扑信息和第一预设规则确定第一对应关系中的目标路由路径的第i个节点对应目标路由路径的第一量子密钥,包括:第i个节点根据经过第i个节点的N条路由路径中的N个第i-1个节点的编号之间的排序关系、经过第i个节点的N条路由路径中的N个第i+1个节点的编号之间的排序

关系,以及经过第i个节点的N条路由路径的编号之间的排序关系,确定出经过第i个节点的N条路由路径的排序,并依序确定出目标路由路径的第i个节点对应的第一量子密钥;或者;第i个节点根据经过第i个节点的N条路由路径中的N个第i+1个节点的编号之间的排序关系,以及经过第i个节点的N条路由路径的编号之间的排序关系,确定出经过第i个节点的N条路由路径的排序,并依序确定出目标路由路径的第i个节点对应的第一量子密钥;或者;第i个节点根据经过第i个节点的N条路由路径的编号之间的排序关系,确定出经过第i个节点的N条路由路径的排序,并依序确定出目标路由路径的第i个节点对应的第一量子密钥。可见,可以通过多种方式为经过第i个节点的多条路由路径进行排序,进而根据对路由路径的排序依序确定出该目标路由路径的第i个节点对应的第一量子密钥,从而可以提高确定出路由路径的第i个节点对应的第一量子密钥的便捷性和灵活性。

[0016] 在一种可能地实现方式中,第i个节点根据第二对应关系确定出目标路由路径的第i个节点对应的第二量子密钥之前,还包括:第i个节点接收集中控制器或目标路由路径对应的第i+1个节点发送的用于指示第二对应关系中的目标路由路径的第i个节点对应的第二量子密钥的指示信息;或者;第i个节点根据获取的量子通信系统的网络拓扑信息和第二预设规则确定第二对应关系中的目标路由路径的第i个节点对应的第二量子密钥。可见可以通过多种方案确定出路由路径的节点对应的第二量子密钥,提高了方案的灵活性。

[0017] 在一种可能地实现方式中,第i个节点根据经过第i个节点和目标路由路径中的第i+1个节点的W条路由路径的编号之间的排序关系,确定出经过第i个节点和目标路由路径中的第i+1个节点的W条路由路径的排序,并依序确定出目标路由路径的第i个节点对应的第二量子密钥;W为不大于N的正整数;或者;第i个节点根据经过第i个节点和目标路由路径中的第i+1个节点的W条路由路径中的W个第i+2个节点的编号之间的排序关系,以及经过第i个节点和目标路由路径中的第i+1个节点的W条路由路径的编号之间的排序关系,确定出经过第i个节点和目标路由路径中的第i+1个节点的W条路由路径的排序,并依序确定出目标路由路径的第i个节点对应的第二量子密钥。可见,可以通过多种方式为经过第i个节点的多条路由路径进行排序,进而根据对路由路径的排序依序确定出该目标路由路径的第i个节点对应的第二量子密钥,从而可以提高确定出路由路径的第i个节点对应的第二量子密钥的便捷性和灵活性。

[0018] 在一种可能地实现方式中,第i个节点使用该目标路由路径的第i个节点对应的第三量子密钥对接收到的来自该目标路由路径中的第i-1个节点的第一密文进行加密的第一算法满足后续具体实施例中的公式(1),如此,可以使目的节点对接收到的第一密文进行解密操作后,得到待共享量子密钥,具体详细的分析过程可以参见后续具体实施例中的叙述,在此不再赘述。

[0019] 第二方面,本申请实施例提供一种量子密钥分发设备,量子密钥分发设备包括存储器、收发器和处理器,其中:存储器用于存储指令;处理器用于根据执行存储器存储的指令,并控制收发器进行信号接收和信号发送,当处理器执行存储器存储的指令时,量子密钥分发设备用于执行上述第一方面或第一方面中任一种方法。

[0020] 第三方面,本申请实施例提供一种量子密钥分发设备,用于实现上述第一方面或第一方面中的任意一种方法,包括相应的功能模块,分别用于实现以上方法中的步骤。功能可以通过硬件实现,也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与

上述功能相对应的模块。

[0021] 在一个可能的设计中，量子密钥分发设备的结构中包括处理单元和收发单元，这些单元可以执行上述方法示例中相应功能，具体参见方法示例中的详细描述，此处不做赘述。

[0022] 第四方面，本申请实施例提供一种计算机存储介质，计算机存储介质中存储有指令，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法。

[0023] 第五方面，本申请实施例提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法。

附图说明

[0024] 图1示出了现有技术中量子密钥分发方法的示意图；

[0025] 图2为本申请实施例提供的一种量子通信系统架构示意图；

[0026] 图3为本申请实施例提供的一种量子密钥分配方法的流程示意图；

[0027] 图4为本申请实施例提供的一种针对图2的路由路径L_2进行量子密钥分配方法的示意图；

[0028] 图5为本申请实施例提供的另一种针对图2的路由路径L_2进行量子密钥分配方法的示意图；

[0029] 图6为本申请实施例中图2中的节点D应用实施方式a3-1生成节点D对应的第一对应关系的示意图；

[0030] 图7为本申请实施例中图2中的节点D应用实施方式a3-2生成路由路径L_2的节点D对应的第一量子密钥的示意图；

[0031] 图8为本申请实施例中图2中的节点D应用实施方式a3-3生成路由路径L_2的节点D对应的第一量子密钥的示意图；

[0032] 图9为本申请实施例中图2中的节点D应用实施方式b3-1生成节点D对应的第二对应关系的示意图；

[0033] 图10为本申请实施例中图2中的节点E应用实施方式a3-1生成节点E对应的第一对应关系的示意图；

[0034] 图11为本申请实施例中图2中的节点D应用实施方式b3-2生成路由路径L_2的节点D对应的第二量子密钥的示意图；

[0035] 图12为本申请实施例提供的一种量子通信中局域网划分的结构示意图；

[0036] 图13为本申请实施例提供的一种量子密钥分配设备的结构示意图；

[0037] 图14为本申请实施例提供的另一种量子密钥分配设备的结构示意图。

具体实施方式

[0038] 图2示例性示出了本申请实施例提供的一种量子通信系统架构示意图，如图2所示，该量子通信系统中包括多个节点，比如节点B、节点C、节点D、节点E、节点F、节点G、节点H、节点P、节点Q和节点R。多个节点之间可以组成多条路由路径，一条路由路径中的除源节点和目的节点之外的节点可以称为中继节点。一个节点可能在一条路由路径中作为源节

点，在另一条路由路径中作为中继节点或目的节点。图2中示例性示出了几条路由路径，分别为：

[0039] 路由路径L_1“源节点B-中继节点D-中继节点E-中继节点G-目的节点P”；

[0040] 路由路径L_2“源节点B-中继节点D-中继节点E-中继节点G-目的节点Q”；

[0041] 路由路径L_3“源节点B-中继节点D-中继节点E-目的节点H”；

[0042] 路由路径L_4“源节点C-中继节点D-目的节点F”；

[0043] 路由路径L_5“源节点B-中继节点D-目的节点F”；

[0044] 路由路径L_6“源节点R-中继节点E-目的节点H”。

[0045] 基于图2所示的量子通信架构示意图，本申请实施例提供一种量子密钥分配方法，图3示例性示出了本申请实施例提供的一种量子密钥分配方法的流程示意图，如图3所示，本申请实施例提供的方法包括：

[0046] 步骤301，第i个节点根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥。一种可选地实施方式中，第i个节点为目标路由路径的第i个中继节点。

[0047] 其中，第i个节点为目标路由路径中的第i个节点；目标路由路径的第i个节点对应的第一量子密钥为第i个节点获取的第i个节点与目标路由路径中第i-1个节点之间共享的量子密钥，第一对应关系包括经过第i个节点的N条路由路径与第i个节点对应的N个第一量子密钥的对应关系，N条路由路径和第i个节点对应的N个第一量子密钥一一对应，N为正整数，i为正整数。目标路由路径为N个条路由路径中的任一条路由路径，本申请实施例中的目标路由路径仅仅是为了描述方便而命名，并不具有其它限定意义。

[0048] 步骤302，第i个节点根据第二对应关系确定出目标路由路径的第i个节点对应的第二量子密钥。

[0049] 目标路由路径的第i个节点对应的第二量子密钥为第i个节点所获取的第i个节点与目标路由路径中第i+1个节点之间共享的量子密钥，第二对应关系包括经过第i个节点的N条路由路径与第i个节点对应的N个第二量子密钥的对应关系，N条路由路径和第i个节点对应的N个第二量子密钥一一对应。

[0050] 步骤303，第i个节点根据该目标路由路径的第i个节点对应的第一量子密钥和该目标路由路径的第i个节点对应的第二量子密钥，生成该目标路由路径的第i个节点对应的第三量子密钥。在步骤303之后本申请实施例提供两种可选地实施方案，一种可选地实施方案中，在步骤303之后执行步骤304，另一种在步骤303之后执行步骤305。在步骤303之后执行步骤304还是步骤305可以由技术人员根据实际应用场景灵活自由选择。

[0051] 步骤304，第i个节点将该目标路由路径的第i个节点对应的第三量子密钥发送给该目标路由路径的目标节点。

[0052] 步骤305，第i个节点使用该目标路由路径的第i个节点对应的第三量子密钥对接收到的来自该目标路由路径中的第i-1个节点的第一密文进行加密，将得到的第i个节点对应的第二密文发送给该目标路由路径中的第i+1个节点。

[0053] 其中，第i个节点接收到的来自该目标路由路径中的第i-1个节点的第一密文为第i-1个节点发出的第i-1个节点对应的第二密文；当i为1时，第0个节点为该目标路由路径的源节点，该目标路由路径的源节点对应的第二密文为使用该目标路由路径的源节点对应的第二量子密钥对该目标路由路径的源节点和该目标路由路径的目标节点之间待共享量子

密钥进行加密得到的。

[0054] 其中，该目标路由路径中的第i-1个节点对应的第二量子密钥与该目标路由路径的第i个节点对应的第一量子密钥相同；且，该目标路由路径中的第i个节点对应的第二量子密钥与该目标路由路径的第i+1个节点对应的第一量子密钥相同。

[0055] 本申请实施例中，第i个节点使用目标路由路径的第i个节点对应的第三量子密钥对接收到的来自目标路由路径中的第i-1个节点的第一密文进行加密的算法可以称为第一算法。本申请实施例中，根据目标路由路径的第i个节点对应的第一量子密钥和目标路由路径的第i个节点对应的第二量子密钥，生成目标路由路径的第i个节点对应的第三量子密钥时所使用的算法可以称为第二算法。

[0056] 下面以目标路由路径为图2中的路由路径L_2对上述图3所示的量子密钥分配方法进行详细描述。图4示例性示出了一种针对图2的路由路径L_2进行量子密钥分配方法的示意图，图4所示的方案执行上述步骤305对应的方案，如图4所示，源节点B与目的节点Q之间的待共享量子密钥为$K_{BQ}(L_2)$，源节点B需将待共享量子密钥$K_{BQ}(L_2)$传输至目的节点Q。具体流程如下：

[0057] 如图4所示，对于源节点来说，源节点B获取待共享量子密钥$K_{BQ}(L_2)$。源节点B对应的第二量子密钥为源节点B确定出的路由路径L_2中的源节点B对应的源节点B与中继节点D之间共享的量子密钥，图4中以$K_{BD}(L_2)$表示路由路径L_2中源节点B对应的第二量子密钥。

[0058] 源节点B使用源节点B对应的第二量子密钥$K_{BD}(L_2)$对该目标路由路径的源节点和该目标路由路径的目标节点之间待共享量子密钥$K_{BQ}(L_2)$进行加密，得到源节点B对应的第二密文$K_B(L_2)$，源节点B向中继节点D发送源节点对应的第二密文$K_B(L_2)$。其中，使用$K_{BD}(L_2)$对$K_{BQ}(L_2)$进行加密的算法可以称为第三算法，第三算法可以与上述第一算法相同，也可以采用其它算法。

[0059] 相对应地，中继节点D接收来自源节点B的第一密文$K_B(L_2)$。也就是说源节点B发出的源节点B对应的第二密文与中继节点D接收到的第一密文为同一个密文。本申请实施例中中继节点接收到的第一密文也可以称为该中继节点对应的第一密文，比如中继节点D接收到的第一密文$K_B(L_2)$也可以称为中继节点D对应的第一密文$K_B(L_2)$。若目标路由路径为路由路径L_2，D节点为该目标路由路径中的第i个节点，则B节点为该目标路由路径的第i-1个节点，E节点为该目标路由路径的第i+1个节点，G节点为该目标路由路径的第i+2个节点后续类似，不再赘述。中继节点D根据路目标由路径的中继节点D对应的第一量子密钥$K_{DB}(L_2)$，以及目标路由路径的中继节点D对应的第二量子密钥$K_{DE}(L_2)$生成目标路由路径的中继节点D对应的第三量子密钥$K_{BE}(L_2)$。

[0060] 进一步，中继节点D使用第三量子密钥$K_{BE}(L_2)$对接收到的中继节点D对应的第一密文$K_B(L_2)$进行加密，得到中继节点D对应的第二密文$K_D(L_2)$，中继节点D向中继节点E发送中继节点D对应的第二密文$K_D(L_2)$。使用第三量子密钥$K_{BE}(L_2)$对第一密文$K_B(L_2)$进行加密生成第二密文的$K_D(L_2)$的算法可以为第一算法。

[0061] 相对应地，中继节点E接收来自中继节点D的第一密文$K_D(L_2)$。也就是说中继节点D发出的中继节点D对应的第二密文与中继节点E接收到的第一密文为同一个密文。中继节点E根据路由路径L_2的中继节点E对应的第一量子密钥$K_{ED}(L_2)$，以及路由路径L_2的中继节点E对应的第二量子密钥$K_{EG}(L_2)$生成路由路径L_2的中继节点E对应的第三量子密钥$K_{DG}(L_2)$。进一

步，中继节点E使用第三量子密钥$K_{DG}(L_2)$对第一密文$K_D(L_2)$进行加密，得到中继节点E对应的第二密文$K_E(L_2)$，中继节点E向中继节点G发送中继节点E对应的第二密文$K_E(L_2)$。

[0062] 相对应地，中继节点G接收来自中继节点E的第一密文$K_E(L_2)$。也就是说中继节点E发出的中继节点E对应的第二密文与中继节点G接收到的第一密文为同一个密文。中继节点G根据路由路径L_2的中继节点G对应的第一量子密钥$K_{GE}(L_2)$，以及路由路径L_2的中继节点G对应的第二量子密钥$K_{GQ}(L_2)$生成路由路径L_2的中继节点G对应的第三量子密钥$K_{EQ}(L_2)$。进一步，中继节点G使用第三量子密钥$K_{EQ}(L_2)$对第一密文$K_E(L_2)$进行加密，得到中继节点G对应的第二密文$K_G(L_2)$，中继节点G向中继节点Q发送中继节点G对应的第二密文$K_G(L_2)$。

[0063] 进一步，目的节点Q接收来自中继节点G的第一密文$K_G(L_2)$，$K_G(L_2)$可以称为目的节点Q对应的第一密文。目的节点Q使用路由路径L_2的目的节点Q对应的第一量子密钥$K_{QG}(L_2)$对第一密文$K_G(L_2)$进行解密处理，得到待共享量子密钥为$K_{BQ}(L_2)$。其中，解密处理所使用的算法可以称为第四算法，第四算法可以与上述第一算法相同，也可以是其它算法。

[0064] 目的节点使用目标路由路径的目的节点对应的第一量子密钥对目的节点对应的第一密文进行解密处理，从而得到待共享量子密钥的过程可以参见下述内容中公式(1)的相关描述。

[0065] 图5示例性示出了另一种针对图2的路由路径L_2L_2进行量子密钥分配方法的示意图，图4所示的方案执行上述步骤304对应的方案，如图5所示，源节点将生成的$K_B(L_2)$发送至目的节点Q，可以通过经典信号，也可以通过量子信道发送。各个中继节点也将各个中继节点对应生成的第三量子密钥发送至目的节点Q。比如图5中，中继节点D将生成的路由路径L_2的中继节点D对应的第三量子密钥$K_{BE}(L_2)$发送至目的节点Q，中继节点E将生成的路由路径L_2的中继节点E对应的第三量子密钥$K_{DG}(L_2)$发送至目的节点Q，中继节点G将生成的路由路径L_2的中继节点G对应的第三量子密钥$K_{EQ}(L_2)$发送至目的节点Q，目的节点Q使用$K_{BE}(L_2)$对$K_B(L_2)$进行加密处理，对得到的结果使用$K_{DG}(L_2)$进行加密处理，之后再对得到的结果使用$K_{EQ}(L_2)$进行加密处理，之后对得到的结果使用$K_{QG}(L_2)$进行解密处理，从而得到待共享量子密钥$K_{BQ}(L_2)$。可以看出该方案中，各个中继节点计算出第三量子密钥之后即发送至目的节点，从而可以节省各个中继节点操作时长，可以进一步提高量子密钥分配效率。

[0066] 通过上述图4和图5所示的示例可以看出，首先，本申请实施例中，中继节点不再对该中继节点的前一个节点发送的信息进行再次的解密，从而可以使得源节点和目的节点之间的待共享量子密钥在中继节点不再落地，即中继节点不会解密出源节点和目的节点之间的待共享量子密钥，可以提高源节点和目的节点之间的待共享量子密钥的安全性。

[0067] 其次，中继节点不再对该中继节点的前一个节点发送的信息进行再次的加密和解密，可以节省待共享量子密钥在路由路径上的光电转换所占用时间和资源。

[0068] 第三，本申请实施例中，中继节点可以在生成第三量子密钥之后删除该中继节点对应的第一量子密钥和第二量子密钥，可以看出，中继节点可以不留下被攻击的窗口期，降低窃听者解密待共享量子密钥的能力，从而可以进一步提高量子密钥分配过程中信息传输的安全性。

[0069] 第四，中继节点的第三量子密钥的相关信息是可以公布的，从而可以降低对信息的安全存储要求。这为进一步地实现全部和中继节点属性相关的所有信息都公布奠定基础，一个节点可以公布当该节点作为一条路由路径上的中继节点时所对应的操作和访问情

况的日志,以及芯片本身的资源利用情况。在该过程中,计算出中继节点的第三量子密钥的中间步骤以及中间所使用到的相关信息结果是不可公开的。本申请实施例中中继节点可以将其相关的信息,比如作为中继节点的操作和访问情况的日志公开,从而也可以有助于分析网络运行状况,进而可以提升对客户的透明度。

[0070] 在本申请实施例中,该目标路由路径中的第i-1个节点对应的第二量子密钥与该目标路由路径的第i个节点对应的第一量子密钥相同,且,该目标路由路径中的第i个节点对应的第二量子密钥与该目标路由路径的第i+1个节点对应的第一量子密钥相同。比如图4中,$K_{BD}(L_2)$与$K_{DB}(L_2)$相同,$K_{DE}(L_2)$与$K_{ED}(L_2)$相同,$K_{EG}(L_2)$与$K_{GE}(L_2)$相同,$K_{GQ}(L_2)$与$K_{QG}(L_2)$相同,从而可以使目的节点解析出待共享量子密钥。

[0071] 上述图4和图5中以第一算法和第二算法均为异或算法为例进行介绍,本领域技术人员可知,第一算法和第二算法也可以为其它算法。在上述步骤303中根据该目标路由路径的第i个节点对应的第一量子密钥和该目标路由路径的第i个节点对应的第二量子密钥,生成该目标路由路径的第i个节点对应的第三量子密钥时所使用的算法为第二算法,第i个节点使用该目标路由路径的第i个节点对应的第三量子密钥对接收到的来自该目标路由路径中的第i-1个节点的第一密文进行加密的算法为第一算法。

[0072] 一种可选地实施方式中,第一算法满足公式(1):

[0073] $g(f_E(K_{i,i-1}(L_j),K_{i,i+1}(L_j)),f_E(K_{i+1,i}(L_j),K_{i+1,i+2}(L_j)))=f_E(K_{i,i-1}(L_j),K_{i+1,i+2}(L_j))$……公式(1)

[0074] 在公式(1)中,L_j为该目标路由路径的标识;

[0075] $K_{i,i-1}(L_j)$为该目标路由路径L_j中第i个节点对应的第一量子密钥;

[0076] $K_{i,i+1}(L_j)$为该目标路由路径L_j中第i个节点对应的第二量子密钥;

[0077] $K_{i+1,i}(L_j)$为该目标路由路径L_j中第i+1个节点对应的第一量子密钥;

[0078] $K_{i+1,i+2}(L_j)$为该目标路由路径L_j中第i+1个节点对应的第二量子密钥;

[0079] 其中,$f_E(\bullet)$为第二算法对应的函数,第二算法为根据该目标路由路径的第i个节点对应的第一量子密钥和该目标路由路径的第i个节点对应的第二量子密钥,生成该目标路由路径的第i个节点对应的第三量子密钥时所使用的算法;

[0080] $g(\bullet)$为第一算法对应的函数。

[0081] 结合图4举个例子,比如当第i个节点为中继节点E时,上述公式(1)可以对应写为:

[0082] $g(f_E(K_{DB}(L_2),K_{DE}(L_2)),f_E(K_{ED}(L_2),K_{EG}(L_2)))=f_E(K_{DB}(L_2),K_{EG}(L_2))$

[0083] 其中,$f_E(K_{DB}(L_2),K_{DE}(L_2))$是对路由路径$L_2$的中继节点D对应的第一量子密钥$K_{DB}(L_2)$和路由路径$L_2$的中继节点D对应的第二量子密钥$K_{DE}(L_2)$进行第二算法对应的运算,$f_E(K_{DB}(L_2),K_{DE}(L_2))$的计算结果即为图4中所示的路由路径$L_2$的中继节点D对应的第三量子密钥$K_{BE}(L_2)$;

[0084] $f_E(K_{ED}(L_2),K_{EG}(L_2))$是对路由路径$L_2$的中继节点E对应的第一量子密钥$K_{ED}(L_2)$和路由路径$L_2$的中继节点E对应的第二量子密钥$K_{EG}(L_2)$进行第二算法对应的运算,$f_E(K_{ED}(L_2),K_{EG}(L_2))$的计算结果即为图4中所示的路由路径$L_2$的中继节点E对应的第三量子密钥$K_{DG}(L_2)$;

[0085] $g(f_E(K_{DB}(L_2),K_{DE}(L_2)),f_E(K_{ED}(L_2),K_{EG}(L_2)))$是对路由路径$L_2$的中继节点D对应的第三量子密钥$K_{BE}(L_2)$和路由路径$L_2$的中继节点E对应的第三量子密钥$K_{DG}(L_2)$进行第一算法

对应的运算，当$K_{DE}(L_2)$与$K_{ED}(L_2)$相同时，其结果等于$f_E(K_{DB}(L_2),K_{EG}(L_2))$。

[0086] 当应用上述公式(1)时，且结合图4中各个节点对应的第三量子密钥的计算方式，以及各个节点对应的第二密文的计算方式，结合图4进行示例性说明，目的节点Q所进行的运算可以视为如下公式(2)所示：

[0087] $K_G(L_2)\oplus K_{QG}(L_2)$

[0088] $=[K_E(L_2)\oplus K_{EQ}(L_2)]\oplus K_{QG}(L_2)$

[0089] $=[K_D(L_2)\oplus K_{DG}(L_2)]\oplus K_{EQ}(L_2)\oplus K_{QG}(L_2)$

[0090] $=[K_B(L_2)\oplus K_{BE}(L_2)]\oplus K_{DG}(L_2)\oplus K_{EQ}(L_2)\oplus K_{QG}(L_2)$

[0091] $=[K_{BQ}(L_2)\oplus K_{BD}(L_2)]\oplus K_{BE}(L_2)\oplus K_{DG}(L_2)\oplus K_{EQ}(L_2)\oplus K_{QG}(L_2)$

[0092] $=[K_{BQ}(L_2)\oplus K_{BD}(L_2)]\oplus[K_{DB}(L_2)\oplus K_{DE}(L_2)]\oplus[K_{ED}(L_2)\oplus K_{EG}(L_2)]\oplus[K_{GE}(L_2)\oplus K_{GQ}(L_2)]\oplus K_{QG}(L_2)$

[0093] $=K_{BQ}(L_2)$

[0094] ……公式(2)

[0095] 在公式(2)中，可以看出，目的节点对接收到的第一密文进行操作后，可以得到待共享量子密钥。本领域技术人员可知，在目的节点的实际操作中，可以并不执行如上述公式(2)所示的详细计算结果，仅仅目的节点对接收到的$K_G(L_2)$使用$K_{QG}(L_2)$进行第一算法对应的运算即可。

[0096] 上述图4和图5中仅仅以第一算法、第二算法、第三算法和第四算法均为异或算法为例进行说明，在具体实施过程中，第一算法、第二算法、第三算法和第四算法有多种实现方式，比如两个节点对应使用的两套第一算法为两套不同的算法，或者两个节点对应使用的两套第二算法为两套不同的算法。

[0097] 比如，$f_E(\bullet)$可以是一个函数集合，其中可以包括一系列加密函数$\{f_{E0},f_{E1}...\}$，还可以设置一个解密函数f_D，其中，f_{E0}为上述第三算法，用于对源节点和目的节点之间的待共享量子密钥进行加密处理，$f_{E1},f_{E2}...$则分别是各个中继节点用于计算第三量子密钥，以及对接收到的第一密文进行加密操作所使用的函数，即为第一算法对应的函数和第二算法对应的函数相同(比如f_{E1}为路由路径中第1个中继节点用于计算第1个中继节点对应的第三量子密钥，以及对接收到的第一密文进行加密操作所使用的函数)，f_D为第四算法，即目的节点对接收到的第一密文进行解密处理，从而得到待共享量子密钥。其中，$\{f_{E0},f_{E1}...\}$和f_D中的任两个函数可以相同，也可以不同，本申请实施例中不做限制。

[0098] 通过上述示例可以看出，本申请实施例中，在不知道在量子密钥分配进程中所使用到的相邻两个节点之间共享的量子密钥(包括不知道目的节点和目的节点的前一个节点之间共享的量子密钥)的前提下，任何人获取部分或全部节点的第三量子密钥以及源节点发出的第二密文，都无法计算出待共享量子密钥，从而可以提高量子密钥分配过程的安全性。

[0099] 本申请实施例再列举一种第一算法和第二算法的可选实施方式：比如可以定义第二算法为每两位做模4的减法运算，具体来说：

[0100] 比如针对$f_E(\bullet)$函数集合$\{f_{E0},f_{E1}...\}$中的任一个函数，输入为两个长度为2n的二进制序列，比如$X=x_1x_2...x_{2k-1}x_{2k}...x_{2n-1}x_{2n}$，$Y=y_1y_2...y_{2k-1}y_{2k}...y_{2n-1}y_{2n}$，其输出仍为一个长度为2n的二进制序列，比如$Z=z_1z_2...z_{2k-1}z_{2k}...z_{2n-1}z_{2n}=f_E(X,Y)$，则$z_{2k-1}z_{2k}$的得出可

以遵循如下计算方法：

[0101] 计算$a_k=2x_{2k-1}+x_{2k}$，$b_k=2y_{2k-1}+y_{2k}$；且：

[0102] 如果$a_k \geq b_k$，则$z_{2k-1}z_{2k}$就是a_k-b_k的二进制表示；如果$a_k<b_k$，则$z_{2k-1}z_{2k}$就是a_k-b_k+4的二进制表示。

[0103] 而解密函数f_D可以为每两位做模4的加法运算，则不难验证，该示例中的函数也可以满足上述实施方案。另注释，上述公式(1)并不是满足本申请实施例所提供的方案的充要条件，仅是一个充分条件，也可以存在其它满足上述实施例的数学特征的函数形式，本申请实施例不做限制。

[0104] 本申请实施例适用的通信系统可以包括多个路由路径，若N为大于1的整数，则针对经过第i个节点的N条路由路径中的第一路由路径和第二路由路径：第一路由路径的第i个节点对应的第一量子密钥与第二路由路径的第i个节点对应的第一量子密钥不同；第一路由路径的第i个节点对应的第二量子密钥与第二路由路径的第i个节点对应的第二量子密钥不同。第一路由路径和第二路由路径为N条路由路径中的两条不同的路由路径。如上述图2所示，经过中继节点D有五条路由路径，针对其中任两条路由路径，比如路由路径L_1和路由路径L_5，其中，中继节点D在路由路径L_1中对应的第一量子密钥与中继节点D在路由路径L_5中对应的第一量子密钥不同，中继节点D在路由路径L_1中对应的第二量子密钥与中继节点D在路由路径L_5中对应的第二量子密钥不同。也就是说，针对每条路由路径，节点为该路由路径分配对应的量子密钥，从而实现一次一密，可以进一步提高量子密钥分配的安全性。且本申请实施例可以适用多路径的情况，适用的网络可以更为复杂。

[0105] 量子通信系统在实际应用中，会不断的产生量子密钥，以推送给密钥管理层，因此可以为每个量子密钥分配一个编号，量子密钥对应的编号也可以称为该量子密钥对应的标识。以图2为例，节点D和节点E之间持续的生成量子密钥K_{DE}，可以以256比特为一个量子密钥长度，每个量子密钥的编号都对应一个256比特的量子密钥。经过节点D和节点E的路由路径有多条，比如图2中所展示的路由路径L_1、路由路径L_2和路由路径L_3。则节点D和节点E分别需要把节点D和节点E之间产生的量子密钥分配给路由路径L_1、路由路径L_2和路由路径L_3。本申请实施例中要求节点D为一条路由路径分配的第二量子密钥与节点E为该目标路由路径分配的第一量子密钥是同一个量子密钥，比如，要求节点D为路由路径L_1分配的第二量子密钥与节点E为路由路径L_1分配的第一量子密钥是同一个量子密钥。为了满足该要求，可以在上述步骤301之前，获取第一对应关系，在上述步骤302之前，获取第二对应关系。第一对应关系和第二对应关系可以有多种表现形式，比如用表格的形式，或者文本的形式等等，本申请实施例不做限制，下述内容以表格形式进行示例性介绍。

[0106] 上述步骤301中的第一对应关系和上述步骤302中的第二对应关系的获取可以有多种方式，下面通过可选地实施方式a1、实施方式a2和实施方式a3介绍几种获取第一对应关系中路由路径的第i个节点对应的第一量子密钥的方式。

[0107] 实施方式a1，通过集中控制器下发用于指示第一对应关系中目标路由路径的第i个节点对应的第一量子密钥指示信息。

[0108] 第i个节点接收集中控制器发送的用于指示该目标路由路径的第i个节点对应的第一量子密钥的指示信息。本申请实施例中，用于指示该目标路由路径的第i个节点对应的第一量子密钥的指示信息可以直接是目标路由路径的第i个节点对应的第一量子密钥，也

可以其它能指示出这种对应关系的信息。可选地，第i个节点接收集中控制器发送的用于指示该目标路由路径的第i个节点对应的第二量子密钥的指示信息。集中控制器可以收集全网的业务请求，并可以优化计算全网的路由路径，之后可以统一计算每个节点作为节点时所对应的第一对应关系，然后下发至相应的节点。

[0109] 实施方式a2，通过该目标路由路径对应的第i-1个节点发送用于指示第一对应关系中目标路由路径的第i个节点对应的第一量子密钥的指示信息。

[0110] 该实施方式中，路由路径对应的第i-1个节点可以计算出该目标路由路径对应的第i-1个节点对应的第二量子密钥，之后发送至第i个节点，由于该目标路由路径对应的第i-1个节点对应的第二量子密钥与该目标路由路径对应的第i个节点对应的第一量子密钥相同，因此，第i个节点可以获知第一对应关系中的该目标路由路径的第i个节点对应的第一量子密钥。

[0111] 基于该实施方式，一种可选地实施方式中，目标路由路径中的每个节点(除目标节点之外)均计算每个节点在目标路由路径上对应的第二量子密钥，之后每个节点均将自己在目标路由路径上对应的第二量子密钥发送给自己在目标路由路径上的下一个节点，由于每个节点在目标路由路径上对应的第二量子密钥与每个节点的在目标路由路径上的下一个节点在目标路由路径上对应的第一量子密钥相同，如此，目标路由路径中的节点可以通过实施方式a2的方式获取第一对应关系中路由路径的第i个节点对应的第一量子密钥。

[0112] 实施方式a3，第i个节点根据获取的量子通信系统的网络拓扑信息和第一预设规则确定该目标路由路径的第i个节点对应的第一量子密钥。

[0113] 针对上述实施方式a3，第i个节点根据获取的量子通信系统的网络拓扑信息和第一预设规则确定该目标路由路径的第i个节点对应的第一量子密钥，可以有多种实施方式，下面通过可选地实施方式a3-1、实施方式a3-2和实施方式a3-3进行介绍。

[0114] 实施方式a3-1

[0115] 第i个节点根据经过第i个节点的N条路由路径中的多个第i-1个节点的编号之间的排序关系、经过第i个节点的多条路由路径中的N个第i+1个节点的编号之间的排序关系，以及经过第i个节点的N条路由路径的编号之间的排序关系，确定出经过第i个节点的多条路由路径的排序，并依序确定出该目标路由路径的第i个节点对应的第一量子密钥。

[0116] 图6示例性示出了图2中的节点D应用实施方式a3-1生成节点D对应的第一对应关系的示意图，如图6所示，在图2所示的6条路由路径中，每个节点会有一个全局编号，可选地，每个节点的全局编号之间可以有排序关系，比如可以用阿拉伯数字、或者字母或者一些有预设排序关系的字符来表示，图2中假设各个节点对应的字母之间的排序关系遵循字母表的排序，则如图6所示，节点D作为中继节点的所有路由路径为L_1至L_5，先将该5条路由路径中的节点D的上一跳节点排序，如图6所示，节点D的上一跳节点有两个，分别为节点B和节点C，排序如图6中第二列所示。

[0117] 进一步，将节点D的上一跳节点为B节点的4条路由路径中的节点D的下一跳节点排序，如图6所示，节点D的上一跳节点为B节点时，节点D的下一跳节点为节点E和节点F，排序如图6中第三列中的第2行至第5行所示。将节点D的上一跳节点为C节点的1条路由路径中的节点C的下一跳节点排序，如图6所示，节点D的上一跳节点为C节点时，节点D的下一跳节点为节点F，排序如图6中第三列中的第6行所示。

[0118] 进一步，当经过同一个节点D的上一跳节点以及经过同一个节点D的下一跳节点的路由路径有多条时，可以根据路由路径的全局编号来排序。可选地，每条路由路径在全局可以有一个编号，路由路径的编号之间可以有排序关系。假设图2中的6条路由路径的编号在全局的排序关系依次为L_1至L_6。如图6所示，经过节点B、节点D和节点E的路由路径有3条，分别为L_1、L_2和L_3。第四列中的第2行至第4行即为根据L_1、L_2和L_3的编号在全局的排序关系所呈现。而经过节点B、节点D和节点F的路由路径仅有一条，经过节点C、节点D和节点F的路由路径也仅有一条，相应排在图6的第3列的第5行和第6行即可。

[0119] 从图6中可以看出，节点D已经对经过节点D的所有路由路径均作了排序，之后可以依据该排序关系依次为各个路由路径分配量子密钥，如图6的第4列所示，以图6第4列的第2行和第3行为例进行说明，节点D为路由路径L_1分配的第一量子密钥为$K_{DB}(L_1)$，节点D为路由路径L_2分配的第一量子密钥为$K_{DB}(L_2)$。

[0120] 可选地，可能某条路由路径上的量子密钥消耗量比较大，因此可以根据每条路由路径上的量子密钥消耗量和/或者业务的属性信息为每条路由路径设置权重，从而决定为每条路由路径在每个量子密钥分配周期内所分配的量子密钥的数量。也就是说，$K_{DB}(L_1)$仅仅是节点D为路由路径L_1分配的第一量子密钥对应的标识，当在一个量子密钥分配周期仅仅为路由路径L1分配一个量子密钥时，假设一个量子密钥长度为256比特，则$K_{DB}(L_1)$在每个量子密钥分配周期内可以是一个256比特的量子密钥对应的标识；若在一个量子密钥分配周期为路由路径L1分配多个(比如3个)量子密钥时，假设一个量子密钥长度为256比特，则$K_{DB}(L_1)$在每个量子密钥分配周期内可以是3个256比特的量子密钥对应的标识。

[0121] 具体实施中，路由路径的排序方案灵活多变，图6仅仅示出了一种可能地实施方式，也可以有其它的实施方式，比如先根据经过第i个节点的多条路由路径中的多个第i+1个节点的编号之间的排序关系对多个第i+1个节点排序，再根据经过第i个节点的多条路由路径中的多个第i-1个节点的编号之间的排序关系对多个第i-1个节点排序，最后再根据经过第i个节点的多条路由路径的编号之间的排序关系对多条路由路径排序等等，在此不再赘述。

[0122] 实施方式a3-2

[0123] 第i个节点根据经过第i个节点的N条路由路径中的多个第i+1个节点的编号之间的排序关系，以及经过第i个节点的N条路由路径的编号之间的排序关系，确定出经过第i个节点的多条路由路径的排序，并依序确定出该目标路由路径的第i个节点对应的第一量子密钥。

[0124] 图7示例性示出了图2中的节点D应用实施方式a3-2生成路由路径L_2的节点D对应的第一量子密钥的示意图，如图7所示，该示例中，可以先确定经过节点D的多条路由路径分别为L_1、L_2、L_3、L_4和L_5。之后，可以针对路由路径L_1、L_2、L_3、L_4和L_5中节点D的下一跳排序，如图7的第二列的第2行至第6行所示，经过节点D的多条路由路径对应的下一跳包括节点E和节点F，之后，再针对路由路径L_1、L_2、L_3、L_4和L_5的路由路径的编号进行排序，排序结果如图7的第三列的第2行至第6行所示，之后依据路由路径L_1、L_2、L_3、L_4和L_5的排序依序为每个路由路径分配节点D在各个路由路径对应的第一量子密钥。

[0125] 实施方式a3-3

[0126] 第i个节点根据经过第i个节点的N条路由路径的编号之间的排序关系，确定出经

过第i个节点的N条路由路径的排序，并依序确定出该目标路由路径的第i个节点对应的第一量子密钥。

[0127] 图8示例性示出了图2中的节点D应用实施方式a3-3生成路由路径L_2的节点D对应的第一量子密钥的示意图，如图8所示，可以先确定经过节点D的多条路由路径分别为L_1、L_2、L_3、L_4和L_5。之后，可以针对路由路径L_1、L_2、L_3、L_4和L_5的路由路径的编号进行排序，排序结果如图8的第二列的第2行至第6行所示，之后依据路由路径L_1、L_2、L_3、L_4和L_5的排序依序为每个路由路径分配对应的第一量子密钥。

[0128] 本申请实施例中通过可选地实施方式b1、实施方式b2和实施方式b3介绍几种获取第二对应关系中路由路径的第i个节点对应的第二量子密钥的方式。

[0129] 实施方式b1，通过集中控制器下发用于指示第二对应关系中路由路径的第i个节点对应的第二量子密钥的指示信息。

[0130] 本申请实施例中，用于指示第二对应关系中路由路径的第i个节点对应的第二量子密钥的指示信息可以直接是目标路由路径的第i个节点对应的第而量子密钥，也可以其它能指示出这种对应关系的信息。可选地，第i个节点接收集中控制器发送的用于指示该目标路由路径的第i个节点对应的第一量子密钥的指示信息。集中控制器可以收集全网的业务请求，并可以优化计算全网的路由路径，之后可以统一计算每个节点作为节点时所对应的第二对应关系，然后下发至相应的节点。

[0131] 实施方式b2，通过该目标路由路径对应的第i+1个节点发送用于指示第二对应关系中路由路径的第i个节点对应的第二量子密钥的指示信息。

[0132] 该实施方式中，路由路径对应的第i+1个节点可以计算出该目标路由路径对应的第i+1个节点对应的第一量子密钥，之后发送至第i个节点，由于该目标路由路径对应的第i+1个节点对应的第一量子密钥与该目标路由路径对应的第i个节点对应的第二量子密钥相同，因此，第i个节点可以获知第二对应关系中的该目标路由路径的第i个节点对应的第二量子密钥。

[0133] 基于该实施方式，一种可选地实施方式中，目标路由路径中的每个节点(除源节点之外)均计算每个节点在目标路由路径上对应的第一量子密钥，之后每个节点均将自己在目标路由路径上对应的第一量子密钥发送给自己在目标路由路径上的上一个节点，由于每个节点在目标路由路径上对应的第一量子密钥与每个节点的在目标路由路径上的上一个节点在目标路由路径上对应的第二量子密钥相同，如此，目标路由路径中的节点可以通过实施方式b2的方式获取第二对应关系中路由路径的第i个节点对应的第二量子密钥。

[0134] 实施方式b3，第i个节点根据获取的量子通信系统的网络拓扑信息和第二预设规则确定该目标路由路径的第i个节点对应的第二量子密钥。

[0135] 针对上述实施方式b3，第i个节点根据获取的量子通信系统的网络拓扑信息和第二预设规则确定该目标路由路径的第i个节点对应的第二量子密钥，可以有多种实施方式，下面通过可选地实施方式b3-1和实施方式b3-2进行介绍。

[0136] 实施方式b3-1

[0137] 第i个节点根据经过第i个节点和该目标路由路径中的第i+1个节点的多条路由路径中的多个第i+2个节点的编号之间的排序关系，以及经过第i个节点和该目标路由路径中的第i+1个节点的多条路由路径的编号之间的排序关系，确定出经过第i个节点和该目标路

由路径中的第i+1个节点的多条路由路径的排序，并依序确定出该目标路由路径的第i个节点对应的第二量子密钥。

[0138] 图9示例性示出了图2中的节点D应用实施方式b3-1生成节点D对应的第二对应关系的示意图，如图9所示，假设需要确定节点D和节点E之间共享的量子密钥，则需要先确定出经过节点D和节点E的所有路由路径，如图2所示，经过节点D和节点E的所有路由路径为L_1、L_2和L_3。之后，可以针对路由路径L_1、L_2和L_3中节点E的下一跳排序，排序结果如图6的第二列的第2行至第4行所示，路由路径L_1、L_2和L_3中节点E的下一跳有两个，分别为节点G和节点H，之后针对节点E的下一跳为节点G的多条路由路径，根据该多条路由路径的编号进行排序，如图9第三列的第2行至第3行所示，经过节点E的下一跳为节点H的路由路径仅一条，则排在图9第3列的第4行即可。之后依据路由路径L_1、L_2和L_3的排序依序为每个路由路径分配节点D在各个路由路径对应的第二量子密钥。

[0139] 可见，该实施方式b3-1，是先筛选出经过第i个节点和该目标路由路径中的第i+1个节点的多条路由路径，之后针对这些路由路径进行排序。

[0140] 图10示例性示出了图2中的节点E应用实施方式a3-1生成节点E对应的第一对应关系的示意图，如图10所示，节点E作为节点的所有路由路径为L_1、L_2、L_3和L_6，先将该4条路由路径中的节点E的上一跳节点排序，如图10所示，节点E的上一跳节点有两个，分别为节点D和节点R，排序如图10中第二列所示。

[0141] 进一步，将节点E的上一跳节点为D节点的3条路由路径中的节点E的下一跳节点排序，如图10所示，节点E的上一跳节点为D节点时，节点E的下一跳节点为节点G和节点H，排序如图10中第三列中的第2行至第4行所示。将节点E的上一跳节点为R节点的1条路由路径中的节点R的下一跳节点排序，如图10所示，节点E的上一跳节点为R节点时，节点E的下一跳节点为节点H，排序如图10中第三列中的第5行所示。

[0142] 进一步，如图10所示，经过节点D、节点E和节点G的路由路径有2条，分别为L_1和L_2。第四列中的第2行至第3行即为根据L_1和L_2的编号在全局的排序关系所呈现。而经过节点D、节点E和节点H的路由路径仅有一条，经过节点R、节点E和节点H的路由路径也仅有一条，相应排在图10的第3列的第4行和第5行即可。

[0143] 从图10中可以看出，节点E已经对经过节点E的所有路由路径均作了排序，之后可以依据该排序关系依次为各个路由路径分配节点E对应的各个路由路径对应的第一量子密钥。

[0144] 结合图9和图10可以发现，图9的第二列至第三列与图10的第三列至第四列中的第2行至第4行的内容一致，也就是说，节点D确定节点D对应的节点D和节点E之间的第二量子密钥的规则与节点E确定节点E和节点D之间的第一量子密钥的规则相同，因此，可以保证路由路径中第i个节点对应的第二量子密钥与该目标路由路径中的第i+1个节点对应的第一量子密钥相同。

[0145] 实施方式b3-2

[0146] 第i个节点根据经过第i个节点和该目标路由路径中的第i+1个节点的多条路由路径的编号之间的排序关系，确定出经过第i个节点和该目标路由路径中的第i+1个节点的多条路由路径的排序，并依序确定出该目标路由路径的第i个节点对应的第二量子密钥。

[0147] 图11示例性示出了图2中的节点D应用实施方式b3-2生成路由路径L_2的节点D对应

的第二量子密钥的示意图，如图11所示，假设需要确定的是路由路径L_2的节点D对应的第二量子密钥，则可以先确定经过节点D和节点E的多条路由路径分别为L_1、L_2和L_3。之后，可以针对路由路径L_1、L_2和L_3的路由路径的编号进行排序，排序结果如图11的第2行至第4行所示，之后依据路由路径L_1、L_2、L_3和L_4的排序依序为每个路由路径分配对应的第一量子密钥。

[0148] 可见，该实施方式b3-2相比与实施方式b3-1来讲，是先筛选出经过第i个节点和该目标路由路径中的第i+1个节点的多条路由路径，之后直接根据经过第i个节点和该目标路由路径中的第i+1个节点的多条路由路径的编号进行排序，而上述实施方式b3-1中则会先根据该多条路由路径中的节点E的下一跳节点排序，之后再根据该多条路由路径的编号进行排序。

[0149] 上述实施方式中，图6至图11仅仅示例性示出了一种可能性的实施方式，具体实际应用中，可以有多种，比如一种可选地实施方式中第i个节点根据经过第i个节点的多条路由路径中的多个第i+1个节点的编号之间的排序关系、经过第i个节点的多条路由路径中的多个第i-1个节点的编号之间的排序关系，以及经过第i个节点的多条路由路径的编号之间的排序关系，确定出经过第i个节点的多条路由路径的排序，并依序确定出该目标路由路径的第i个节点对应的第二量子密钥。可选地，第i个节点根据经过第i个节点和该目标路由路径中的第i-1个节点的多条路由路径中的多个第i-2个节点的编号之间的排序关系，以及经过第i个节点和该目标路由路径中的第i-1个节点的多条路由路径的编号之间的排序关系，确定出经过第i个节点和该目标路由路径中的第i-1个节点的多条路由路径的排序，并依序确定出该目标路由路径的第i个节点对应的第一量子密钥。

[0150] 在上述实施方式a2、实施方式a3、实施方式b2和实施方式b3中，可以由各个节点自行计算第一对应关系和/或第二对应关系，该种实施方式可以基于分布式信息的方法，即全网的业务请求可以不做集中收集，而是利用经典路由的方法得出每个业务请求的路由路径，之后将每个路由路径对应存储在该目标路由路径所经过的每个节点中，每个节点根据自己内部存储的经过自己的所有路由路径的拓扑信息，可以自行计算第一对应关系和/或第二对应关系。

[0151] 上述实施方式a1、实施方式a2和实施方式a3中的任一种实施方式可以与实施方式b1、实施方式b2和实施方式b3中的任一种实施方式结合使用，举个例子，比如可以采用上述实施方式a1由集中控制器下发第一对应关系中的路由路径的第i个节点对应的第一量子密钥，而第二对应关系中路由路径的第i个节点对应的第二量子密钥可以由上述实施方式b3中所示的由第i个节点自行计算。

[0152] 再比如，第一对应关系中的路由路径的第i个节点对应的第一量子密钥可以由上述实施方式a2中所示的由第i-1个节点发出，而第二对应关系中路由路径的第i个节点对应的第二量子密钥可以由上述实施方式b3中所示的由第i个节点自行计算。

[0153] 再比如，第一对应关系中的路由路径的第i个节点对应的第一量子密钥可以由上述实施方式a3中所示的由第i个节点自行计算，而第二对应关系中路由路径的第i个节点对应的第二量子密钥可以由上述实施方式b2中所示的由第i+1个节点发出。

[0154] 再比如，第一对应关系中的路由路径的第i个节点对应的第一量子密钥可以由上述实施方式a3中所示的由第i个节点自行计算，而第二对应关系中路由路径的第i个节点对应的第二量子密钥可以由上述实施方式b3中所示的由第i个节点自行计算。而该种示例中，

第i个节点也可以采用实施方式a3-1至a3-3中的任一种实施方式确定路由路径的第i个节点对应的第一量子密钥，也可以采用b3-1至b3-2中的任一种实施方式确定路由路径的第i个节点对应的第二量子密钥，选择方式灵活，比如可以将实施方式a3-1和b3-1组合使用，也可以将实施方式a3-2和实施方式b3-2组合使用，也可以将实施方式a3-3和实施方式b3-2组合使用。

[0155] 可选地，本申请实施例中图6中所示的表格可以循环使用，以图6为例，经过节点B和节点D的路由路径有L_1、L_2、L_3和L_4，排序依次为L_1、L_2、L_3、L_4。从节点B和节点D相连的QKD系统推送上来的第一个量子密钥可以分配给路由路径L_1，第一个量子密钥的标识在图6中可以$K_{DB}(L_1)$表示，第二个密钥分配给路由路径L_2，第三个密钥分配给路由路径L_3，第四个密钥分配给路由路径L_4，当地五个密钥上来时，就又重新分配给了路由路径L_1，依次类推，进行循环。当为L1至L4全部分配一次量子密钥时，可以称为一个量子密钥分配周期，在一个周期中，可以为每个路由路径分配一个量子密钥，也可以为根据权重或预设规则为不同的路由路径设置不同的量子密钥分配数量，比如可以在一个量子密钥分配周期中为一条路由路径分配3个量子密钥。

[0156] 本申请实施例中的量子通信系统可以划分多个局域网，图12示例性示出了本申请实施例提供的一种量子通信中局域网划分的结构示意图，如图12所示，可以将量子通信网络划分多个局域网，如图12所示的局域网1201和局域网1202，在每个局域网中可以设置网关节点，每个局域网中可以设置一个或多个网关节点，图12中仅示例性示出了一个局域网中设置一个网关节点的示例。如图12所示，局域网1201中的节点(比如节点M_1)需要与局域网1202中的节点(比如节点M_6)通信时，节点M_1可以先将数据发送至该局域网1201中的网关节点S_1，之后局域网1201中的网关节点S_1将数据对应发送至局域网1202中的网关节点S_2，由网关节点S_2转发至局域网1202内的节点M_6。也就是说，不同的局域网内的节点进行通信时，源节点可以将数据发送至该源节点所属的局域网内的网关节点，之后传输至目的节点所在的局域网中的网关节点，从而通过目的节点所在的局域网中的网关节点传输至目的节点。这种情况下，每个局域网内部的业务请求对应的路由路径可以由该局域网内部的网关节点来辅助计算，从而可以减轻集中控制器的压力。

[0157] 基于上述内容，本申请实施例提供一种量子通信方法，具体操作流程如下

[0158] 在0至T1时刻，一个或多个节点发起加密业务请求，该加密业务请求可以包括新增的业务对应的加密业务请求，也可以包括取消现有业务所对应的加密业务请求。

[0159] 可选地实施方式中，节点发起的加密业务请求可以向集中控制器发送，也可以向节点所在的局域网中的网关节点发送。或者设置一个集中控制端，节点发起的加密业务请求可以向该集中控制端发送。

[0160] 当节点向集中控制器发送加密业务请求时，集中控制器可以规划各个加密业务请求对应的路由路径。由集中控制器规划路由路径可以从全局出发优化路由路径。本申请实施例中集中控制器也可以替代为集中控制端，或者其它具有本申请实施例中集中控制器所具有的功能的设备。

[0161] 当节点向节点所在的局域网中的网关节点发送加密业务请求时，网关节点可以规划该网关节点所在的局域网内部的路由路径，当加密业务请求需要跨越至少两个局域网时，可以由集中控制器规划不同的局域网之间的网关节点和网关节点之间的路由路径，这

种实施方式可以减轻集中控制器的压力。

[0162] 路由路径下发之后可以下发至该目标路由路径所包括的所有节点中的每个节点上。

[0163] 可选地，还可以记录每个加密业务需要的密钥更新速率是多少。对于密钥更新速率较高的节点对儿，可以采用多条并行路由路径以增加最终总的密钥获取率，或者在某一条路由路径上增加其权重。在计算路由路径时，可以根据每条实际QKD链路的最大密钥生成速率，优化调整路由路径，以防止经过同一段链路的路由路径太多，从而限制了这些路径的密钥生成速率。

[0164] 在T1至T2时刻，各个节点根据新下发的路由路径的信息确定各自对应的第一对应关系和第二对应关系，具体方式可以采用上述实施方式a1至实施方式b2中的方式，在此不再赘述。

[0165] 若各个节点此时还存着历史的第一对应关系和第二对应关系，则可以使用新获取的第一对应关系和第二对应关系更改历史的第一对应关系和第二对应关系。

[0166] 可选地，在这个时间段，目的节点可以合理的处理这个时间段收到的各类信息。

[0167] 在T2至T3时刻，针对各个节点中的每个节点，该节点根据更新后的第一对应关系和第二对应关系，计算经过该节点的每条路由路径的该节点对应的第三量子密钥，在计算出结果之后的预设时长内删除过该节点的每条路由路径的该节点所对应的第一量子密钥和第二量子密钥。预设时长可以设置为较小的值，比如可以是1分钟或30秒内，如此可以提高量子密钥分配的安全性。

[0168] 可选地，该节点可以公开经过该节点的每条路由路径的该节点对应的第三量子密钥，以及经过该节点的每条路由路径的相关信息。节点公开信息的方式有多种，比如可以仅向集中控制节点报告；可以内部公开，即量子网络内部某个群体间公开；可以对第三方公开，比如公开给第三方监督机构；甚至可以进行全网公开，因为这部分信息不影响安全性。但总体考虑可以对不同域公开不同的信息。考虑到这部分公开信息如果合理利用会有助于分析网络情况，因此信息公开时需要增加认证，以确保此信息是本节点发出的。此外，还可以将公开的信息上载到区块链中，以进一步防止被篡改。

[0169] 可选地，针对一条路由路径中的源节点，该源节点可以在收到该路由路径的全部节点中的每个节点所公开的：该节点可以公开经过该节点的每条路由路径的该节点对应的第三量子密钥，以及经过该节点的每条路由路径的相关信息之后，再发出源节点对应的第二密文。

[0170] 可选地，针对一条路由路径中的目的节点，该目的节点可以在收到该路由路径的全部节点中的每个节点所公开的：该节点可以公开经过该节点的每条路由路径的该节点对应的第三量子密钥，以及经过该节点的每条路由路径的相关信息之后，可以从源节点对应的第二密文中解析出源节点和目的节点之间的待共享量子密钥。可选地，可以将待共享量子密钥存入业务密钥池中，业务密钥池属于保密存储空间。

[0171] 基于相同构思，本申请提供一种量子密钥分配设备1301，用于执行上述方法中的接收侧的任一个方案。图13示例性示出了本申请提供的一种量子密钥分配设备的结构示意图，如图13所示，量子密钥分配设备1301包括处理器1303、收发器1302、存储器1305和通信接口1304；其中，处理器1303、收发器1302、存储器1305和通信接口1304通过总线相互连接。

该示例中的量子密钥分配设备1301可以是上述内容中的一个路由路径中的第i个节点，本领域技术人员可知，该量子密钥分配设备1301在其它路由路径中也可以是源节点、目的节点或节点，本申请实施例中限定当量子密钥分配设备1301作为节点时所执行的方案。

[0172] 存储器1305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)；存储器也可以包括非易失性存储器(non-volatile memory)，例如快闪存储器(flash memory)，硬盘(hard disk drive，HDD)或固态硬盘(solid-state drive，SSD)；存储器1305还可以包括上述种类的存储器的组合。

[0173] 通信接口1304可以为有线通信接入口，无线通信接口或其组合，其中，有线通信接口例如可以为以太网接口。以太网接口可以是光接口，电接口或其组合。无线通信接口可以为WLAN接口。

[0174] 处理器1303可以是中央处理器(central processing unit，CPU)，网络处理器(network processor，NP)或者CPU和NP的组合。处理器1303还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路(application-specific integrated circuit，ASIC)，可编程逻辑器件(programmable logic device，PLD)或其组合。上述PLD可以是复杂可编程逻辑器件(complex programmable logic device，CPLD)，现场可编程逻辑门阵列(field-programmable gate array，FPGA)，通用阵列逻辑(generic array logic，GAL)或其任意组合。

[0175] 可选地，存储器1305还可以用于存储程序指令，处理器1303调用该存储器1305中存储的程序指令，可以执行上述方案中所示实施例中的一个或多个步骤，或其中可选的实施方式，使得量子密钥分配设备1301实现上述方法中第i个节点的功能。量子密钥分发设备为量子通信系统的一条路由路径中的第i个节点。量子密钥分发设备中的处理器1303，用于根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥，根据第二对应关系确定出目标路由路径的第i个节点对应的第二量子密钥，根据目标路由路径的第i个节点对应的第一量子密钥和目标路由路径的第i个节点对应的第二量子密钥，生成目标路由路径的第i个节点对应的第三量子密钥；其中，第i个节点为目标路由路径中的第i个节点；目标路由路径的第i个节点对应的第一量子密钥为第i个节点获取的第i个节点与目标路由路径中第i-1个节点之间共享的量子密钥，第一对应关系包括经过第i个节点的N条路由路径与第i个节点对应的N个第一量子密钥的对应关系，N条路由路径和第i个节点对应的N个第一量子密钥一一对应，目标路由路径为N个条路由路径中的一条路由路径，N为正整数，i为正整数；目标路由路径的第i个节点对应的第二量子密钥为第i个节点所获取的第i个节点与目标路由路径中第i+1个节点之间共享的量子密钥，第二对应关系包括经过第i个节点的N条路由路径与第i个节点对应的N个第二量子密钥的对应关系，N条路由路径和第i个节点对应的N个第二量子密钥一一对应；收发器1302，用于将目标路由路径的第i个节点对应的第三量子密钥发送给目标路由路径的目标节点；或者；将通过处理器使用目标路由路径的第i个节点对应的第三量子密钥对接收到的来自目标路由路径中的第i-1个节点的第一密文进行加密所得到的第i个节点对应的第二密文发送给目标路由路径中的第i+1个节点。

[0176] 其中，第i个节点接收到的来自目标路由路径中的第i-1个节点的第一密文为第i-1个节点发出的第i-1个节点对应的第二密文；当i为1时，第0个节点为目标路由路径的源节点，目标路由路径的源节点对应的第二密文为使用目标路由路径的源节点对应的第二量子

密钥对目标路由路径的源节点和目标路由路径的目标节点之间待共享量子密钥进行加密得到的。

[0177] 其中，目标路由路径中的第i-1个节点对应的第二量子密钥与目标路由路径的第i个节点对应的第一量子密钥相同；且，目标路由路径中的第i个节点对应的第二量子密钥与目标路由路径的第i+1个节点对应的第一量子密钥相同。

[0178] 在一种可能地实现方式中，若N为大于1的整数，则针对经过第i个节点的N条路由路径中的第一路由路径和第二路由路径：第一路由路径的第i个节点对应的第一量子密钥与第二路由路径的第i个节点对应的第一量子密钥不同；第一路由路径的第i个节点对应的第二量子密钥与第二路由路径的第i个节点对应的第二量子密钥不同。

[0179] 在一种可能地实现方式中，收发器1302，还用于接收集中控制器或目标路由路径中的第i-1个节点发送的用于指示第一对应关系中的目标路由路径的第i个节点对应目标路由路径的第一量子密钥的指示信息；或者；处理器1303，还用于根据获取的量子通信系统的网络拓扑信息和第一预设规则确定第一对应关系中的目标路由路径的第i个节点对应目标路由路径的第一量子密钥。

[0180] 确定该目标路由路径的第i个节点对应的第一量子密钥的方式有多种，具体可以参见上述内容中的实施方式a3-1、实施方式a3-2和实施方式a3-3的描述，在此不再赘述。

[0181] 在一种可能地实现方式中，收发器1302，用于：接收集中控制器或目标路由路径对应的第i+1个节点发送的用于指示第二对应关系中的目标路由路径的第i个节点对应的第二量子密钥的指示信息；或者；处理器1303，用于根据获取的量子通信系统的网络拓扑信息和第二预设规则确定第二对应关系中的目标路由路径的第i个节点对应的第二量子密钥。

[0182] 确定该目标路由路径的第i个节点对应的第二量子密钥的方式有多种，具体可以参见上述内容中的实施方式b3-1和实施方式b3-2的描述，在此不再赘述。

[0183] 基于相同构思，本申请实施例提供一种量子密钥分配设备，用于执行上述方法流程中的第i个节点侧的任一个方案。图14示例性示出了本申请实施例提供的一种量子密钥分配设备的结构示意图，如图14所示，量子密钥分配设备1401包括收发单元1402和处理单元1403。该示例中的量子密钥分配设备1401可以是上述内容中的一个路由路径中的第i个节点，本领域技术人员可知，该量子密钥分配设备1401在其它路由路径中也可以是源节点、目的节点或节点，本申请实施例中限定当量子密钥分配设备1401作为节点时所执行的方案。

[0184] 处理单元1403，用于根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥，根据第二对应关系确定出目标路由路径的第i个节点对应的第二量子密钥，根据目标路由路径的第i个节点对应的第一量子密钥和目标路由路径的第i个节点对应的第二量子密钥，生成目标路由路径的第i个节点对应的第三量子密钥；其中，第i个节点为目标路由路径中的第i个节点；目标路由路径的第i个节点对应的第一量子密钥为第i个节点获取的第i个节点与目标路由路径中第i-1个节点之间共享的量子密钥，第一对应关系包括经过第i个节点的N条路由路径与第i个节点对应的N个第一量子密钥的对应关系，N条路由路径和第i个节点对应的N个第一量子密钥一一对应，目标路由路径为N个条路由路径中的一条路由路径，N为正整数，i为正整数；目标路由路径的第i个节点对应的第二量子密钥为第i个节点所获取的第i个节点与目标路由路径中第i+1个节点之间共享的量子密钥，第二

对应关系包括经过第i个节点的N条路由路径与第i个节点对应的N个第二量子密钥的对应关系,N条路由路径和第i个节点对应的N个第二量子密钥一一对应;收发器1402,用于将目标路由路径的第i个节点对应的第三量子密钥发送给目标路由路径的目标节点;或者;将通过处理器使用目标路由路径的第i个节点对应的第三量子密钥对接收到的来自目标路由路径中的第i-1个节点的第一密文进行加密所得到的第i个节点对应的第二密文发送给目标路由路径中的第i+1个节点。

[0185] 其中,第i个节点接收到的来自目标路由路径中的第i-1个节点的第一密文为第i-1个节点发出的第i-1个节点对应的第二密文;当i为1时,第0个节点为目标路由路径的源节点,目标路由路径的源节点对应的第二密文为使用目标路由路径的源节点对应的第二量子密钥对目标路由路径的源节点和目标路由路径的目标节点之间待共享量子密钥进行加密得到的。其中,目标路由路径中的第i-1个节点对应的第二量子密钥与目标路由路径的第i个节点对应的第一量子密钥相同;且,目标路由路径中的第i个节点对应的第二量子密钥与目标路由路径的第i+1个节点对应的第一量子密钥相同。

[0186] 应理解,以上各个量子密钥分配设备的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。本申请实施例中,收发单元1402可以由上述图13的收发器1302实现,处理单元1403可以由上述图13的处理器1303实现。也就是说,本申请实施例中收发单元1402可以执行上述图13的收发器1302所执行的方案,本申请实施例中处理单元1403可以执行上述图13的处理器1303所执行的方案,其余内容可以参见上述内容,在此不再赘述。如上述图13所示,量子密钥分配设备1301包括的存储器1305中可以用于存储该量子密钥分配设备1301包括的处理器1303执行方案时的代码,该代码可为量子密钥分配设备1301出厂时预装的程序/代码。

[0187] 在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现、当使用软件程序实现时,可以全部或部分地以计算机程序产品的形式实现。计算机程序产品包括一个或多个指令。在计算机上加载和执行计算机程序指令时,全部或部分地产生按照本申请实施例的流程或功能。计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。指令可以存储在计算机存储介质中,或者从一个计算机存储介质向另一个计算机存储介质传输,例如,指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。计算机存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质,(例如,软盘、硬盘、磁带、磁光盘(MO)等)、光介质(例如,CD、DVD、BD、HVD等)、或者半导体介质(例如ROM、EPROM、EEPROM、非易失性存储器(NAND FLASH)、固态硬盘(Solid State Disk,SSD))等。

[0188] 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。

[0189] 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。

[0190] 这些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。

[0191] 这些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。

[0192] 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。

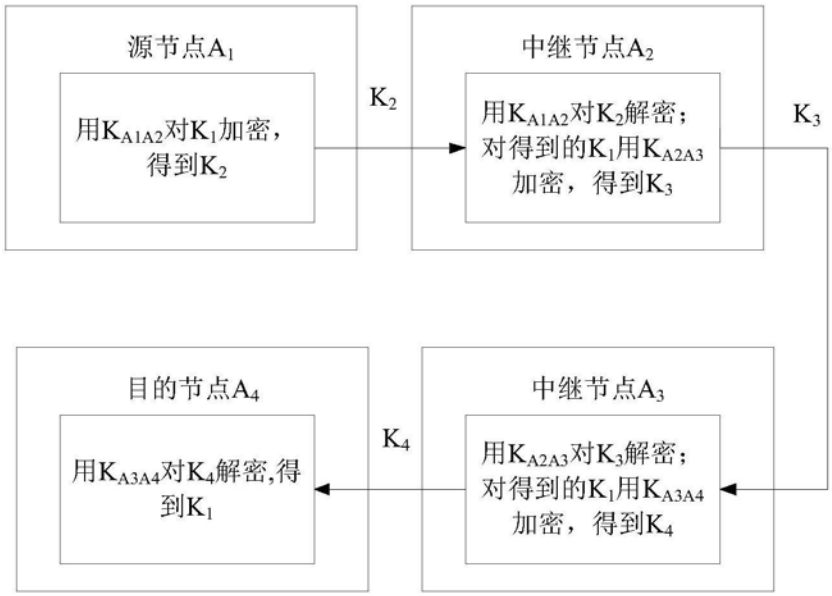
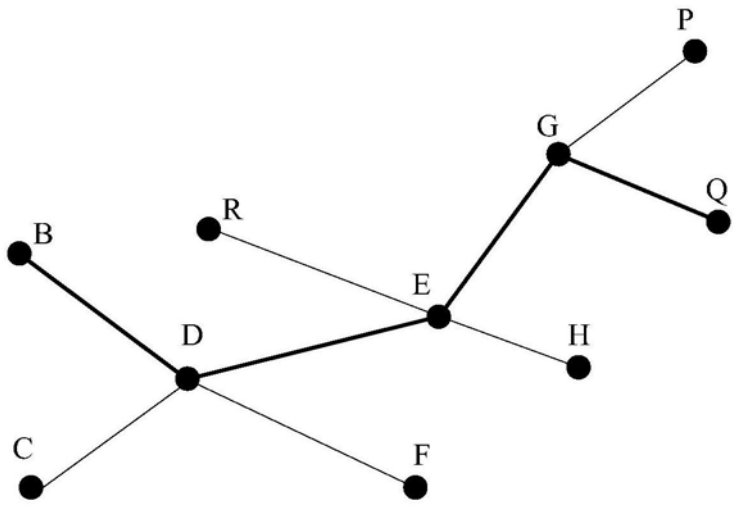


图1



图例： 路由路径L_1: B-D-E-G-P

路由路径L_2: B-D-E-G-Q

路由路径L_3: B-D-E-H

路由路径L_4: C-D-F

路由路径L_5: B-D-F

路由路径L_6: R-E-H

图2

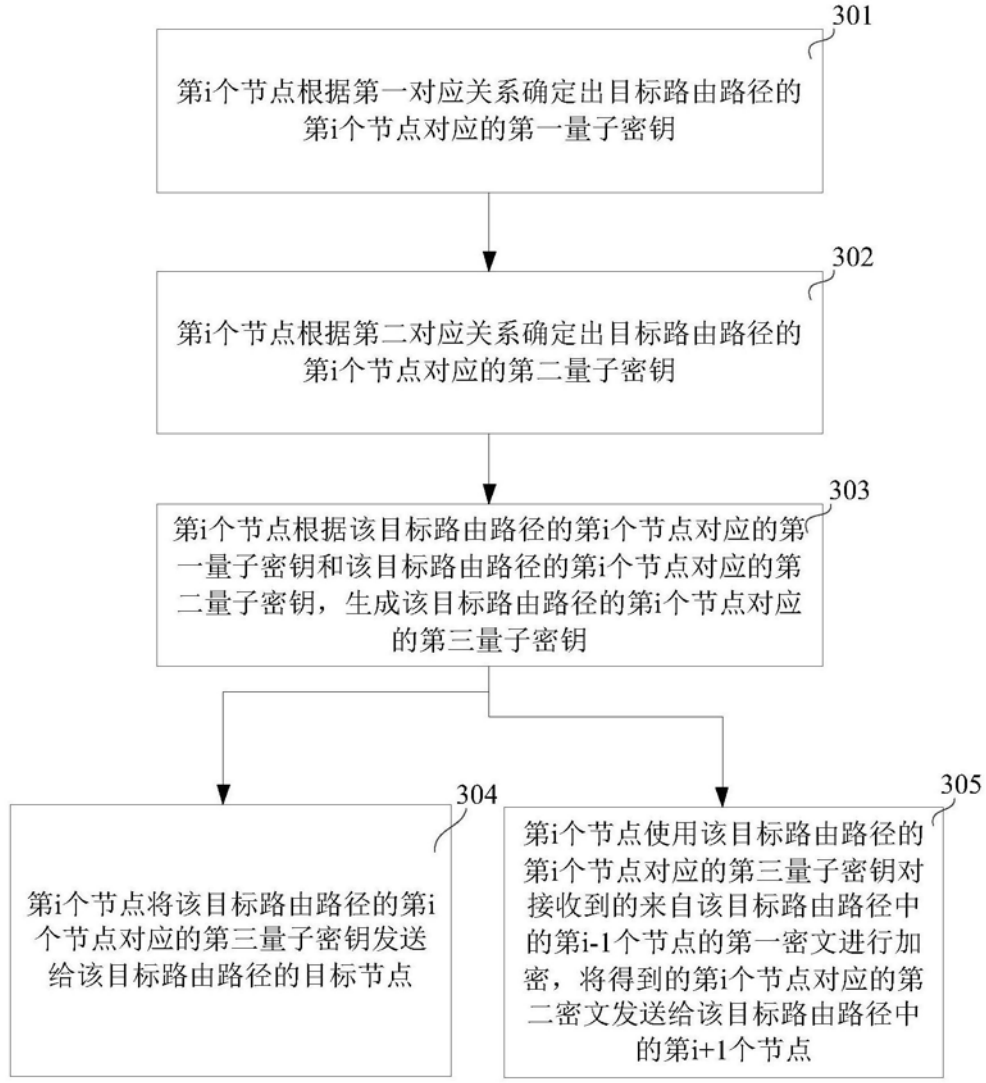

301
第i个节点根据第一对应关系确定出目标路由路径的第i个节点对应的第一量子密钥
302
第i个节点根据第二对应关系确定出目标路由路径的第i个节点对应的第二量子密钥
303
第i个节点根据该目标路由路径的第i个节点对应的第一量子密钥和该目标路由路径的第i个节点对应的第二量子密钥，生成该目标路由路径的第i个节点对应的第三量子密钥
304
第i个节点将该目标路由路径的第i个节点对应的第三量子密钥发送给该目标路由路径的目标节点
305
第i个节点使用该目标路由路径的第i个节点对应的第三量子密钥对接收到的来自该目标路由路径中的第i-1个节点的第一密文进行加密，将得到的第i个节点对应的第二密文发送给该目标路由路径中的第i+1个节点

图3

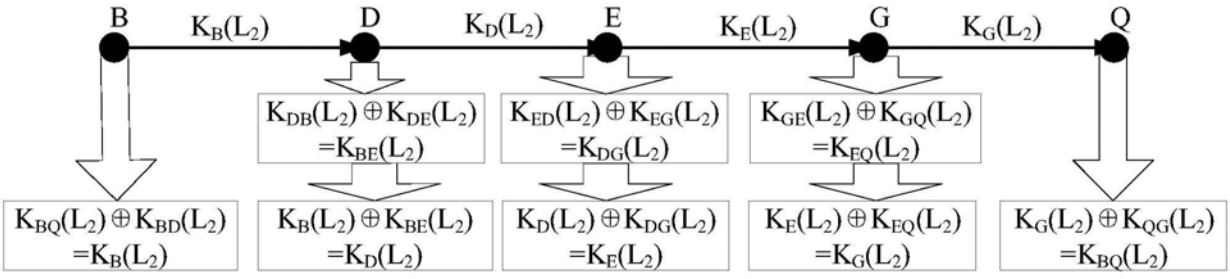

B
$K_B(L_2)$
D
$K_D(L_2)$
E
$K_E(L_2)$
G
$K_G(L_2)$
Q
$K_{DB}(L_2) \oplus K_{DE}(L_2) = K_{BE}(L_2)$
$K_{ED}(L_2) \oplus K_{EG}(L_2) = K_{DG}(L_2)$
$K_{GE}(L_2) \oplus K_{GQ}(L_2) = K_{EQ}(L_2)$
$K_{BQ}(L_2) \oplus K_{BD}(L_2) = K_B(L_2)$
$K_B(L_2) \oplus K_{BE}(L_2) = K_D(L_2)$
$K_D(L_2) \oplus K_{DG}(L_2) = K_E(L_2)$
$K_E(L_2) \oplus K_{EQ}(L_2) = K_G(L_2)$
$K_G(L_2) \oplus K_{QG}(L_2) = K_{BQ}(L_2)$

图4

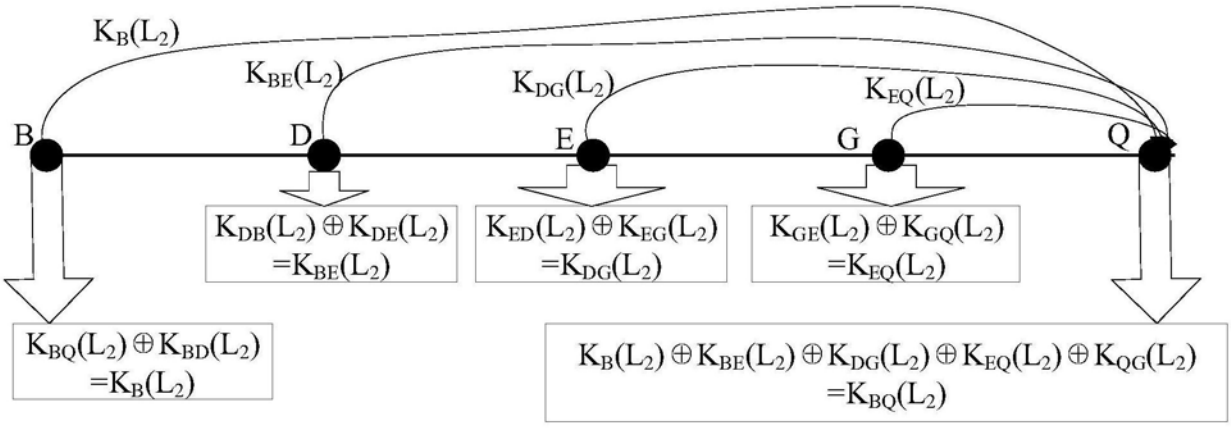


图5

行号	经过节点 D 的所有路由路径中的节点 D 的上一跳节点的排序	经过节点 D 的所有路由路径中的节点 D 的下一跳节点的排序	经过节点 D 的所有路由路径的排序	经过节点 D 的所有路由路径的节点 D 对应的第一量子密钥
第 2 行	B	E	路由路径 L_1	路由路径 L_1 的节点 D 对应的第一量子密钥：$K_{DB}(L_1)$
第 3 行			路由路径 L_2	路由路径 L_2 的节点 D 对应的第一量子密钥：$K_{DB}(L_2)$
第 4 行			路由路径 L_3	路由路径 L_3 的节点 D 对应的第一量子密钥：$K_{DB}(L_3)$
第 5 行		F	路由路径 L_5	路由路径 L_4 的节点 D 对应的第一量子密钥：$K_{DB}(L_5)$
第 6 行	C	F	路由路径 L_4	路由路径 L_5 的节点 D 对应的第一量子密钥：$K_{DC}(L_4)$

图6

行号	经过节点D的所有路由路径中的节点D的下一跳节点的排序	经过节点D的所有路由路径的排序	经过节点D的所有路由路径的节点D对应的第一量子密钥
第2行	E	路由路径L_1	路由路径L_1的节点D对应的第一量子密钥：$K_{DB}(L_1)$
第3行		路由路径L_2	路由路径L_2的节点D对应的第一量子密钥：$K_{DB}(L_2)$
第4行		路由路径L_3	路由路径L_3的节点D对应的第一量子密钥：$K_{DB}(L_3)$
第5行	F	路由路径L_4	路由路径L_4的节点D对应的第一量子密钥：$K_{DC}(L_4)$
第6行		路由路径L_5	路由路径L_5的节点D对应的第一量子密钥：$K_{DB}(L_5)$

图7

行号	经过节点D的所有路由路径的排序	经过节点D的所有路由路径的节点D对应的第一量子密钥
第2行	路由路径 L_1	路由路径 L_1 的节点D对应的第一量子密钥：$K_{DB}(L_1)$
第3行	路由路径 L_2	路由路径 L_2 的节点D对应的第一量子密钥：$K_{DB}(L_2)$
第4行	路由路径 L_3	路由路径 L_3 的节点D对应的第一量子密钥：$K_{DB}(L_3)$
第5行	路由路径 L_4	路由路径 L_4 的节点D对应的第一量子密钥：$K_{DC}(L_4)$
第6行	路由路径 L_5	路由路径 L_5 的节点D对应的第一量子密钥：$K_{DB}(L_5)$

图8

行号	经过节点D和节点E的所有路由路径中的节点E的下一跳节点的排序	经过节点D和节点E的所有路由路径的排序	路由路径的节点D对应的第二量子密钥
第2行	G	路由路径 L_1	路由路径 L_1 的节点D对应的第二量子密钥：$K_{DE}(L_1)$
第3行		路由路径 L_2	路由路径 L_2 的节点D对应的第二量子密钥：$K_{DE}(L_2)$
第4行	H	路由路径 L_3	路由路径 L_3 的节点D对应的第二量子密钥：$K_{DE}(L_3)$

图9

行号	经过节点E的所有路由路径中的节点E的上一跳节点的排序	经过节点E的所有路由路径中的节点E的下一跳节点的排序	经过节点E的所有路由路径的排序	经过节点E的所有路由路径的节点E对应的第一量子密钥
第2行	D	G	路由路径L_1	路由路径L_1的节点E对应的第一量子密钥：$K_{ED}(L_1)$
第3行			路由路径L_2	路由路径L_2的节点E对应的第一量子密钥：$K_{ED}(L_2)$
第4行		H	路由路径L_3	路由路径L_3的节点E对应的第一量子密钥：$K_{ED}(L_3)$
第5行	R	H	路由路径L_6	路由路径L_6的节点E对应的第一量子密钥：$K_{EB}(L_6)$

图10

行号	经过节点D和节点E的所有路由路径的排序	路由路径的节点D对应的第二量子密钥
第2行	路由路径L_1	路由路径L_1的节点D对应的第二量子密钥：$K_{DE}(L_1)$
第3行	路由路径L_2	路由路径L_2的节点D对应的第二量子密钥：$K_{DE}(L_2)$
第4行	路由路径L_3	路由路径L_3的节点D对应的第二量子密钥：$K_{DE}(L_3)$

图11

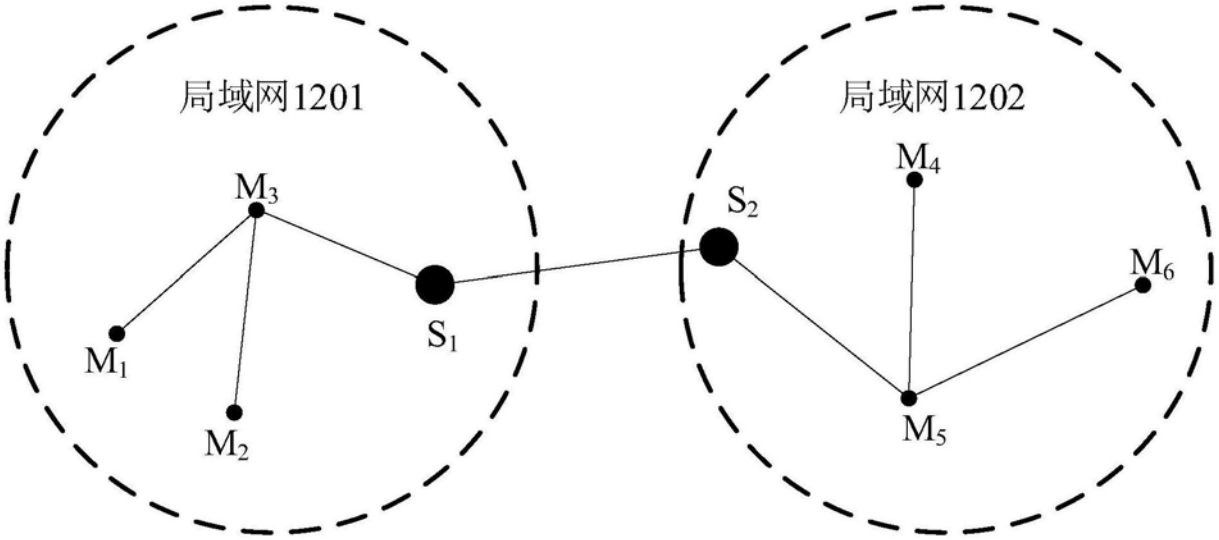

局域网1201
局域网1202
M3
M4
S2
M6
S1
M1
M2
M5

图12

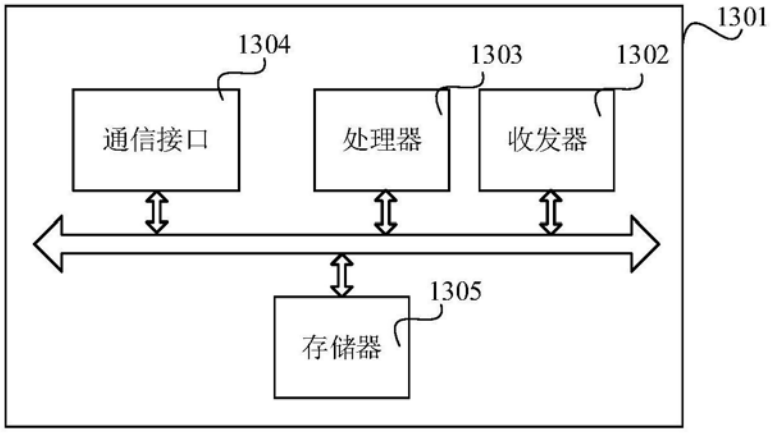

1301
1304
1303
1302
通信接口
处理器
收发器
1305
存储器

图13

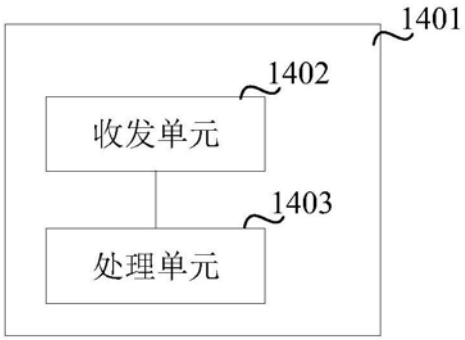

1401
1402
收发单元
1403
处理单元

图14