(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107508671 A
(43)申请公布日 2017.12.22

(21)申请号 201710712132.0

(22)申请日 2017.08.18

(71)申请人 北京邮电大学
地址 100876 北京市海淀区西土城路10号

(72)发明人 赵永利 曹原 高冠军 郁小松 张会彬 张杰

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王莹 吴欢燕

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 12/727(2013.01)

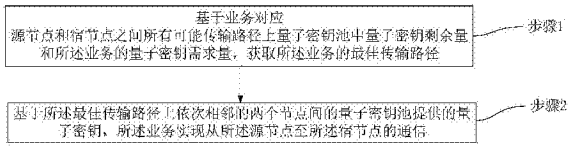
权利要求书2页 说明书7页 附图2页

(54)发明名称

基于量子密钥分发的业务通信方法及装置

(57)摘要

本发明提供一种基于量子密钥分发的业务通信方法及装置。该方法包括:步骤1,基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量,获取所述业务的最佳传输路径;步骤2,基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥,所述业务实现从所述源节点至所述宿节点的通信。本发明使得参与业务传输的每个量子密钥池对应的两个节点相距较近,缩短了量子密钥的增补耗时,从而使得量子密钥池的量子密钥可以及时得到增补,避免了承载业务量较多的量子密钥池或量子密钥需求量较大的业务对应的量子密钥池量子密钥不足导致通信时延和阻塞。



CN 107508671 A

1.一种基于量子密钥分发的业务通信方法,其特征在于,包括:

步骤1,基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量,获取所述业务的最佳传输路径;

步骤2,基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥,所述业务实现从所述源节点至所述宿节点的通信。

2.根据权利要求1所述的方法,其特征在于,所述步骤1具体包括:

步骤11,基于业务对应的源节点、宿节点以及所述源节点与所述宿节点之间的中间节点,获取所述业务的所有可能传输路径;

步骤12,基于所述所有可能传输路径包含中间节点的数目,获取所述业务的较佳可能传输路径;

步骤13,基于所述业务的量子密钥需求量和所述较佳可能传输路径上量子密钥池的量子密钥剩余量,获取所述业务的最佳传输路径。

3.根据权利要求1或2所述的方法,其特征在于,所述步骤2具体包括:

将所述源节点作为当前节点,沿所述业务在所述最佳传输路径上的传输方向,基于所述当前节点和与其相邻的下一节点之间的当前量子密钥池提供的量子密钥,在所述当前节点对所述业务进行加密;将加密后的业务传输至所述下一节点;基于所述当前量子密钥池提供的量子密钥,在所述下一节点对所述业务进行解密;

将所述下一节点作为当前节点,重复上述过程,直至所述下一节点为宿节点。

4.根据权利要求2所述的方法,其特征在于,所述步骤12具体包括:

获取所述所有可能传输路径包含中间节点数目小于预设数目的路径作为所述业务的较佳可能传输路径。

5.根据权利要求2或4所述的方法,其特征在于,所述步骤13具体包括:

步骤131,基于所述业务的量子密钥需求量和所述较佳可能传输路径上量子密钥池中量子密钥剩余量,获取通信顺畅的路径;

步骤132,基于所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差,获取所述业务的最佳传输路径。

6.根据权利要求5所述的方法,其特征在于,所述步骤131具体包括:

获取所述较佳可能传输路径中量子密钥池的量子密钥剩余量均大于等于所述业务量子密钥需求量的路径作为通信顺畅的路径。

7.根据权利要求5所述的方法,其特征在于,所述步骤132具体包括:

若判断获知所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差大于方差阈值,基于所述通信顺畅的路径中各路径上的最小量子密钥剩余量,获取所述业务的最佳传输路径;

若判断获知所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差小于或等于所述方差阈值,基于所述通信顺畅的路径中各路径上量子密钥剩余量的平均值,获取所述业务的最佳传输路径。

8.根据权利要求7所述的方法,其特征在于,所述基于所述通信顺畅的路径中各路径上的最小量子密钥剩余量,获取所述业务的最佳传输路径具体包括:

获取每条所述通信顺畅的路径的最小量子密钥剩余量;

获取所述最小量子密钥剩余量中的最大量子密钥剩余量对应的路径作为最佳传输路径。

9.根据权利要求7所述的方法，其特征在于，所述基于所述通信顺畅的路径中各路径上量子密钥剩余量的平均值，获取所述业务的最佳传输路径具体包括：

获取所述通信顺畅的路径中具有最大量子密钥剩余量平均值的路径作为最佳传输路径。

10.一种基于量子密钥分发的业务通信装置，其特征在于，包括：最佳传输路径获取模块和通信模块；

所述最佳传输路径获取模块，用于基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量，获取所述业务的最佳传输路径；

所述通信模块，用于基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥，所述业务实现从所述源节点至所述宿节点的通信。

基于量子密钥分发的业务通信方法及装置

技术领域

[0001] 本发明涉及信息安全技术领域，更具体地，涉及一种基于量子密钥分发的业务通信方法及装置。

背景技术

[0002] 基于量子力学原理的量子密钥分发(Quantum Key Distribution,QKD)技术是一种利用通信双方部署的QKD终端和QKD链路，构建为通信双方分配量子密钥资源的量子密钥池(Quantum Key Pool,QKP)以用于敏感数据的安全通信的技术。图1为现有技术中利用一对数据通信节点间的QKD终端和QKD链路构建一个量子密钥池的示意图。其中，QKD链路包括量子信道和经典信道；量子密钥池用于存储QKD终端之间协商产生的量子密钥，并为网络节点双方对应的数据通信终端分配量子密钥，实现网络业务的安全保密通信。

[0003] 图2为现有技术基于量子密钥分发的安全通信网络体系架构。该架构自下而上包括QKD层和数据层。QKD层包括放置于每个节点处的QKD终端及连接QKD终端的QKD链路，每对QKD终端之间协商产生的量子密钥存储于一个量子密钥池中；数据层包括放置于每个节点处的数据通信终端及连接数据通信终端的数据通信链路，每对数据通信终端之间的业务安全通信由对应业务源宿节点的量子密钥池为其分配量子密钥，继而完成数据加密和数据传输。可知，业务通信过程会不断消耗量子密钥池中的量子密钥。通常，当某个量子密钥池中的量子密钥量小于预设的量子密钥量最小值时，量子密钥池对应的两个QKD终端会对量子密钥池进行量子密钥增补。具体地，利用QKD链路连通该量子密钥池对应的QKD终端并增补量子密钥，直至量子密钥量达到预设的量子密钥量最大值。

[0004] 但一方面，现阶段QKD技术水平和设备条件有限，量子密钥资源的增补速率较低，当量子密钥池对应的两个节点相距较远时，量子密钥资源的增补用时更长。另一方面，由于传输不同数据量的业务加密所需的量子密钥量不同以及网络中不同节点和链路承载的业务数量各不相同，网络中多个量子密钥池的量子密钥剩余量分布不均衡。基于上述原因，承载业务量较多的量子密钥池或量子密钥需求量较大的业务对应的量子密钥池容易出现量子密钥不足。而量子密钥池中量子密钥不足会导致业务安全通信的时延和阻塞率大大增加，并严重影响网络的性能。

发明内容

[0005] 本发明提供一种基于量子密钥分发的业务通信方法及装置，以克服现有技术中，承载业务量较多的量子密钥池或量子密钥需求量较大的业务对应的量子密钥池容易出现量子密钥不足而导致业务安全通信的时延和阻塞率大大增加、严重影响网络性能的问题。

[0006] 根据本发明的第一方面，提供一种基于量子密钥分发的业务通信方法，该方法包括：步骤1，基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量，获取所述业务的最佳传输路径；步骤2，基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥，所述业务实现从所述

源节点至所述宿节点的通信。

[0007] 结合本发明第一方面的第一种可能实现方式，在第二种可能实现方式中，所述步骤1具体包括：步骤11，基于业务对应的源节点、宿节点以及所述源节点与所述宿节点之间的中间节点，获取所述业务的所有可能传输路径；步骤12，基于所述所有可能传输路径包含中间节点的数目，获取所述业务的较佳可能传输路径；步骤13，基于所述业务的量子密钥需求量和所述较佳可能传输路径上量子密钥池的量子密钥剩余量，获取所述业务的最佳传输路径。

[0008] 结合本发明第一方面的第一或第二种可能实现方式，在第三种可能实现方式中，所述步骤2具体包括：将所述源节点作为当前节点，沿所述业务在所述最佳传输路径上的传输方向，基于所述当前节点和与其相邻的下一节点之间的当前量子密钥池提供的量子密钥，在所述当前节点对所述业务进行加密；将加密后的业务传输至所述下一节点；基于所述当前量子密钥池提供的量子密钥，在所述下一节点对所述业务进行解密；将所述下一节点作为当前节点，重复上述过程，直至所述下一节点为宿节点。

[0009] 结合本发明第一方面的第二种可能实现方式，在第四种可能实现方式中，所述步骤12具体包括：获取所述所有可能传输路径包含中间节点数目小于预设数目的路径作为所述业务的较佳可能传输路径。

[0010] 结合本发明第一方面的第二或第四种可能实现方式，在第五种可能实现方式中，所述步骤13具体包括：步骤131，基于所述业务的量子密钥需求量和所述较佳可能传输路径上量子密钥池中量子密钥剩余量，获取通信顺畅的路径；步骤132，基于所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差，获取所述业务的最佳传输路径。

[0011] 结合本发明第一方面的第五种可能实现方式，在第六种可能实现方式中，所述步骤131具体包括：获取所述较佳可能传输路径中量子密钥池的量子密钥剩余量均大于等于所述业务量子密钥需求量的路径作为通信顺畅的路径。

[0012] 结合本发明第一方面的第五种可能实现方式，在第七种可能实现方式中，所述步骤132具体包括：若判断获知所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差大于方差阈值，基于所述通信顺畅的路径中各路径上的最小量子密钥剩余量，获取所述业务的最佳传输路径；若判断获知所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差小于或等于所述方差阈值，基于所述通信顺畅的路径中各路径上量子密钥剩余量的平均值，获取所述业务的最佳传输路径。

[0013] 结合本发明第一方面的第七种可能实现方式，在第八种可能实现方式中，所述基于所述通信顺畅的路径中各路径上的最小量子密钥剩余量，获取所述业务的最佳传输路径具体包括：获取每条所述通信顺畅的路径的最小量子密钥剩余量；获取所述最小量子密钥剩余量中的最大量子密钥剩余量对应的路径作为最佳传输路径。

[0014] 结合本发明第一方面的第七种可能实现方式，在第九种可能实现方式中，所述基于所述通信顺畅的路径中各路径上量子密钥剩余量的平均值，获取所述业务的最佳传输路径具体包括：获取所述通信顺畅的路径中具有最大量子密钥剩余量平均值的路径作为最佳传输路径。

[0015] 根据本发明的第二方面，提供一种基于量子密钥分发的业务通信方法装置，该装置包括：最佳传输路径获取模块和通信模块；所述最佳传输路径获取模块，用于基于业务对

应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量，获取所述业务的最佳传输路径；所述通信模块，用于基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥，所述业务实现从所述源节点至所述宿节点的通信。

[0016] 本发明提出的基于量子密钥分发的业务通信方法及装置，通过基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量，获取所述业务的最佳传输路径，基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥，所述业务实现从所述源节点至所述宿节点的通信。本发明提出的方法使得参与业务传输的每个量子密钥池对应的两个节点相距较近，缩短了量子密钥的增补耗时，从而使得量子密钥池的量子密钥可以及时得到增补，避免了承载业务量较多的量子密钥池或量子密钥需求量较大的业务对应的量子密钥池量子密钥不足导致通信时延和阻塞。此外，本发明提出的方法使得整个网络各量子密钥池中量子密钥消耗量相当，保证了整个网络各量子密钥池中量子密钥剩余量的均衡分布，使得网络性能更加稳定。

附图说明

[0017] 图1为现有技术中利用一对数据通信节点间的QKD终端和QKD链路构建一个量子密钥池的示意图；

[0018] 图2为现有技术基于量子密钥分发的安全通信网络体系架构；

[0019] 图3为根据本发明实施例的基于量子密钥分发的业务通信方法流程图；

[0020] 图4为根据本发明实施例的具有4个节点的网络示意图；

[0021] 图5为根据本发明实施例的基于量子密钥分发的业务通信装置示意图。

具体实施方式

[0022] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0023] 如图3所示，根据本发明的第一方面，提供一种基于量子密钥分发的业务通信方法，该方法包括：步骤1，基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量，获取所述业务的最佳传输路径；步骤2，基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥，所述业务实现从所述源节点至所述宿节点的通信。

[0024] 在本实施例中，由于通信网络中在源节点和宿节点之间存在诸多中间节点，因此，当需要将业务从源节点安全发送至宿节点时，业务具有多条传输路径。量子密钥池因承载的业务量不同、业务的量子密钥需求量不同，量子密钥池的量子密钥剩余量也各不相同。为了避免量子密钥剩余量较少量子密钥池中量子密钥的过度消耗，造成通信延时或阻塞，在本实施例中选择量子密钥池的量子密钥剩余量整体最充足的路径即最佳传输路径进行业务通信。

[0025] 在本实施例中，当获取最佳传输路径后，便可通过最佳传输路径进行业务通信。通过最佳传输路径进行业务通信过程中，业务在最佳传输路径沿途中的每个中间节点均先解密再加密。其中，解密时，利用该中间节点与其在最佳传输路径传输上相邻的上一节点之间

的量子密钥池提供的量子密钥;加密时,利用该中间节点与其在最佳传输路径传输上相邻的下一节点之间的量子密钥池提供的量子密钥。

[0026] 本发明提出的基于量子密钥分发的业务通信方法及装置,通过基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量,获取所述业务的最佳传输路径,基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥,所述业务实现从所述源节点至所述宿节点的通信。本发明提出的方法使得参与业务传输的每个量子密钥池对应的两个节点相距较近,缩短了量子密钥的增补耗时,从而使得量子密钥池的量子密钥可以及时得到增补,避免了承载业务量较多的量子密钥池或量子密钥需求量较大的业务对应的量子密钥池量子密钥不足导致通信时延和阻塞。此外,本发明提出的方法使得整个网络各量子密钥池中量子密钥消耗量相当,保证了整个网络各量子密钥池中量子密钥剩余量的均衡分布,使得网络性能更加稳定。

[0027] 作为一种可选实施例,所述步骤1具体包括:步骤11,基于业务对应的源节点、宿节点以及所述源节点与所述宿节点之间的中间节点,获取所述业务的所有可能传输路径;步骤12,基于所述所有可能传输路径包含中间节点的数目,获取所述业务的较佳可能传输路径;步骤13,基于所述业务的量子密钥需求量和所述较佳可能传输路径上量子密钥池的量子密钥剩余量,获取所述业务的最佳传输路径。

[0028] 图4为根据本发明实施例的具有4个节点的网络示意图。由图4可知,将业务从源节点2安全发送至宿节点4的所有路径包括:源节点2至宿节点4,源节点2至中间节点1至宿节点4,源节点2至中间节点3至宿节点4的各路径。

[0029] 由于业务在经过中间节点时需加解密,因此,当中间节点数目越大时,业务在通信过程中需经过的节点就越多,业务通信所需的时间就越长。为避免业务通信耗时过度增长,需去除中间节点过多的路径,获取较佳可能传输路径。

[0030] 较佳可能传输路径的各路径中量子密钥池过去因承载的业务量不同、业务的量子密钥需求量不同,当前,量子密钥池的量子密钥剩余量也各不相同。为了避免量子密钥剩余量较少量子密钥池中量子密钥的过度消耗,造成通信延时或阻塞,在本实施例中选择量子密钥池的量子密钥剩余量整体最充足的路径即最佳传输路径进行业务通信。

[0031] 作为一种可选实施例,所述步骤2具体包括:将所述源节点作为当前节点,沿所述业务在所述最佳传输路径上的传输方向,基于所述当前节点和与其相邻的下一节点之间的当前量子密钥池提供的量子密钥,在所述当前节点对所述业务进行加密;将加密后的业务传输至所述下一节点;基于所述当前量子密钥池提供的量子密钥,在所述下一节点对所述业务进行解密;将所述下一节点作为当前节点,重复上述过程,直至所述下一节点为宿节点。

[0032] 在本实施例中,业务沿最佳传输路径从源节点传输至宿节点的方向上依次经过源节点、第一中间节点、第二中间节点、……、宿节点。并在源节点完成加密,在中间各节点完成加解密以及在宿节点完成解密。

[0033] 作为一种可选实施例,所述步骤12具体包括:获取所述所有可能传输路径包含中间节点数目小于预设数目的路径作为所述业务的较佳可能传输路径。

[0034] 在本实施例中,预设数目可根据具体情况设置,本实施例对此不作限定。从上述将业务从源节点2安全发送至宿节点4的所有可能传输路径中筛选出小于预设数目(预设数目

等于2)的路径作为较佳可能传输路径。较佳可能传输路径包括:源节点2至宿节点4,源节点2至中间节点1至宿节点4,源节点2至中间节点3至宿节点4的各路径。

[0035] 作为一种可选实施例,所述步骤13具体包括:步骤131,基于所述业务的量子密钥需求量和所述较佳可能传输路径上量子密钥池中量子密钥剩余量,获取通信顺畅的路径;步骤132,基于所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差,获取所述业务的最佳传输路径。

[0036] 在本实施例中,业务在传输中涉及的量子密钥池均需提供量子密钥资源以供业务加解密。如,源节点和与之相邻的第一中间节点对应的量子密钥池需提供量子密钥资源以供业务在源节点加密并在第一中间节点解密。当量子密钥池中的量子密钥资源不能满足加解密的需求时,该路径会出现延时或阻塞,因此,需从较佳可能传输路径中获取各量子密钥池中的量子密钥资源均能满足业务加解密需求的路径,即通信顺畅的路径,进行业务通信。例如,从上述将业务从源节点2安全发送至宿节点4的较佳可能传输路径中,分别查找较佳可能传输路径上的量子密钥池(QKP2-4、QKP1-2和QKP1-4、QKP2-3和QKP3-4),并查询各个量子密钥池的量子密钥剩余量,筛选出量子密钥池中的量子密钥均充足的路径作为通信顺畅的路径。

[0037] 在本实施例中,通信顺畅的路径的各路径中量子密钥池过去因承载的业务量不同、业务的量子密钥需求量不同,当前,量子密钥池的量子密钥剩余量也各不相同。而路径上量子密钥池中量子密钥剩余量的方差反应了该路径中各量子密钥池中量子密钥剩余量的差异大小,基于该差异可在差异较大或较小时,基于一定的方法选择量子密钥池的量子密钥剩余量整体最充足的路径作为最佳传输路径,以避免量子密钥剩余量较少量子密钥池中量子密钥的过度消耗,造成通信延时或阻塞。

[0038] 作为一种可选实施例,所述步骤131具体包括:获取所述较佳可能传输路径中量子密钥池的量子密钥剩余量均大于等于所述业务量子密钥需求量的路径作为通信顺畅的路径。

[0039] 在本实施例中,通过将量子密钥池的量子密钥剩余量均大于等于所述业务量子密钥需求量的路径作为通信顺畅的路径,以保证业务传输过程中通信顺畅。

[0040] 作为一种可选实施例,所述步骤132具体包括:若判断获知所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差大于方差阈值,基于所述通信顺畅的路径中各路径上的最小量子密钥剩余量,获取所述业务的最佳传输路径;若判断获知所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差小于或等于所述方差阈值,基于所述通信顺畅的路径中各路径上量子密钥剩余量的平均值,获取所述业务的最佳传输路径。

[0041] 当路径上量子密钥池中量子密钥剩余量的方差较大,说明该路径上各量子密钥池中量子密钥剩余量的差距较大,可能存在一些量子密钥剩余量很大,另一些量子密钥剩余量很小的情况。此时,可基于最小密钥剩余量,获取最佳传输路径。

[0042] 当路径上量子密钥池中量子密钥剩余量的方差较小,说明该路径上各量子密钥池中量子密钥剩余量的相当。此时,可基于密钥剩余量平均值,获取最佳传输路径。

[0043] 作为一种可选实施例,所述基于所述通信顺畅的路径中各路径上的最小量子密钥剩余量,获取所述业务的最佳传输路径具体包括:获取每条所述通信顺畅的路径的最小量子密钥剩余量;获取所述最小量子密钥剩余量中的最大量子密钥剩余量对应的路径作为最

佳传输路径。

[0044] 在本实施例中，当所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差大于方差阈值时，选择最小量子密钥剩余量最大的路径作为最佳传输路径，以避免选取最小量子密钥剩余量较小的路径进一步消耗资源。

[0045] 作为一种可选实施例，所述基于所述通信顺畅的路径中各路径上量子密钥剩余量的平均值，获取所述业务的最佳传输路径具体包括：获取所述通信顺畅的路径中具有最大量子密钥剩余量平均值的路径作为最佳传输路径。

[0046] 在本实施例中，当所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差小于等于方差阈值时，选择量子密钥剩余量平均值最大的路径作为最佳传输路径，以避免选取量子密钥剩余量平均值较小的路径进一步消耗资源。

[0047] 如图5所示，根据本发明的第二方面，提供一种基于量子密钥分发的业务通信方法装置，该装置包括：最佳传输路径获取模块和通信模块；所述最佳传输路径获取模块，用于基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量，获取所述业务的最佳传输路径；所述通信模块，用于基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥，所述业务实现从所述源节点至所述宿节点的通信。

[0048] 本发明提出的基于量子密钥分发的业务通信装置，通过最佳传输路径获取模块，基于业务对应源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量和所述业务的量子密钥需求量，获取所述业务的最佳传输路径，通过通信模块，基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量子密钥，所述业务实现从所述源节点至所述宿节点的通信。本发明提出的装置使得参与业务传输的每个量子密钥池对应的两个节点相距较近，缩短了量子密钥的增补耗时，从而使得量子密钥池的量子密钥可以及时得到增补，避免了承载业务量较多的量子密钥池或量子密钥需求量较大的业务对应的量子密钥池量子密钥不足导致通信时延和阻塞。此外，本发明提出的装置使得整个网络各量子密钥池中量子密钥消耗量相当，保证了整个网络各量子密钥池中量子密钥剩余量的均衡分布，使得网络性能更加稳定。

[0049] 作为一种可选实施例，所述最佳传输路径获取模块包括：所有可能传输路径获取单元，由于基于业务对应的源节点、宿节点以及所述源节点与所述宿节点之间的中间节点，获取所述业务的所有可能传输路径；较佳可能传输路径获取单元，基于所述所有可能传输路径包含中间节点的数目，获取所述业务的较佳可能传输路径；最佳传输路径获取单元，用于基于所述业务的量子密钥需求量和所述较佳可能传输路径上量子密钥池的量子密钥剩余量，获取所述业务的最佳传输路径。

[0050] 作为一种可选实施例，所述通信模块具体用于将所述源节点作为当前节点，沿所述业务在所述最佳传输路径上的传输方向，基于所述当前节点和与其相邻的下一节点之间的当前量子密钥池提供的量子密钥，在所述当前节点对所述业务进行加密；将加密后的业务传输至所述下一节点；基于所述当前量子密钥池提供的量子密钥，在所述下一节点对所述业务进行解密；将所述下一节点作为当前节点，重复上述过程，直至所述下一节点为宿节点。

[0051] 作为一种可选实施例，所述较佳可能传输路径获取单元具体用于获取所述所有可

能传输路径包含中间节点数目小于预设数目的路径作为所述业务的较佳可能传输路径。

[0052] 作为一种可选实施例，所述最佳传输路径获取模块包括：通信顺畅路径获取单元，用于基于所述业务的量子密钥需求量和所述较佳可能传输路径上量子密钥池中量子密钥剩余量，获取通信顺畅的路径；最佳传输路径获取单元，用于基于所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差，获取所述业务的最佳传输路径。

[0053] 作为一种可选实施例，所述通信顺畅路径获取单元具体用于获取所述较佳可能传输路径中量子密钥池的量子密钥剩余量均大于等于所述业务量子密钥需求量的路径作为通信顺畅的路径。

[0054] 作为一种可选实施例，所述最佳传输路径获取单元具体用于若判断获知所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差大于方差阈值，基于所述通信顺畅的路径中各路径上的最小量子密钥剩余量，获取所述业务的最佳传输路径；若判断获知所述通信顺畅的路径上量子密钥池中量子密钥剩余量的方差小于或等于所述方差阈值，基于所述通信顺畅的路径中各路径上量子密钥剩余量的平均值，获取所述业务的最佳传输路径。

[0055] 作为一种可选实施例，所述最佳传输路径获取单元具体用于获取每条所述通信顺畅的路径的最小量子密钥剩余量；获取所述最小量子密钥剩余量中的最大量子密钥剩余量对应的路径作为最佳传输路径。

[0056] 作为一种可选实施例，所述最佳传输路径获取单元具体用于获取所述通信顺畅的路径中具有最大量子密钥剩余量平均值的路径作为最佳传输路径。

[0057] 最后，本发明的方法仅为较佳的实施方案，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

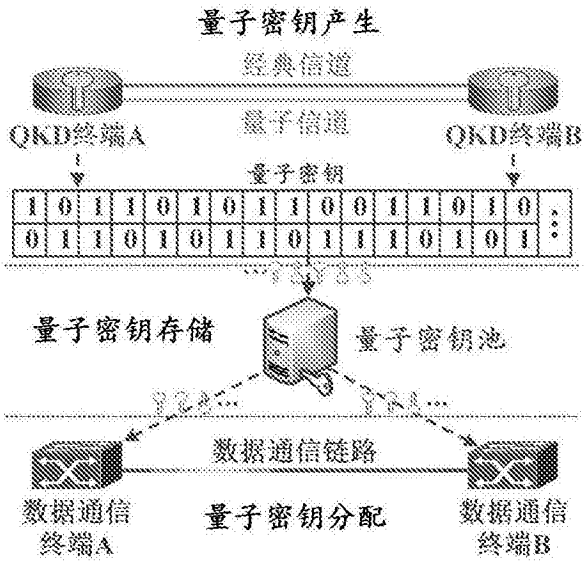

量子密钥产生
经典信道
量子信道
QKD终端A
QKD终端B
量子密钥
量子密钥存储
量子密钥池
数据通信链路
数据通信终端A
量子密钥分配
数据通信终端B

图1

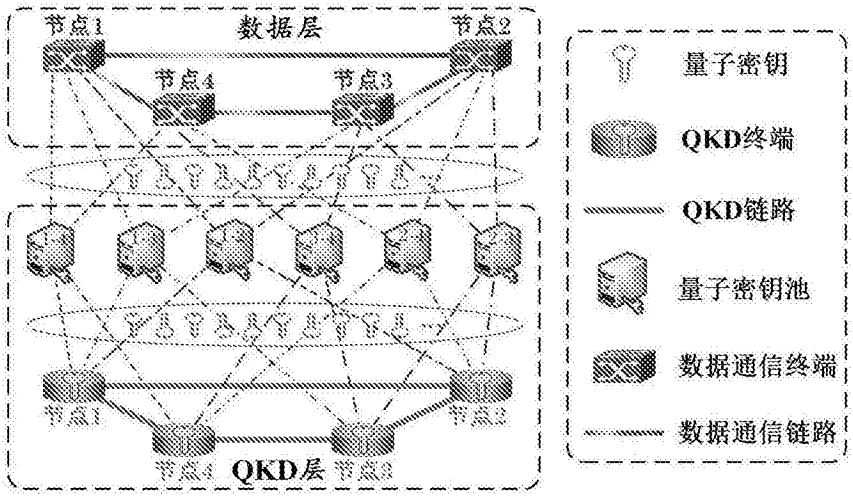

节点1
数据层
节点2
节点4
节点3
节点1
节点2
节点4
QKD层
节点3
量子密钥
QKD终端
QKD链路
量子密钥池
数据通信终端
数据通信链路

图2

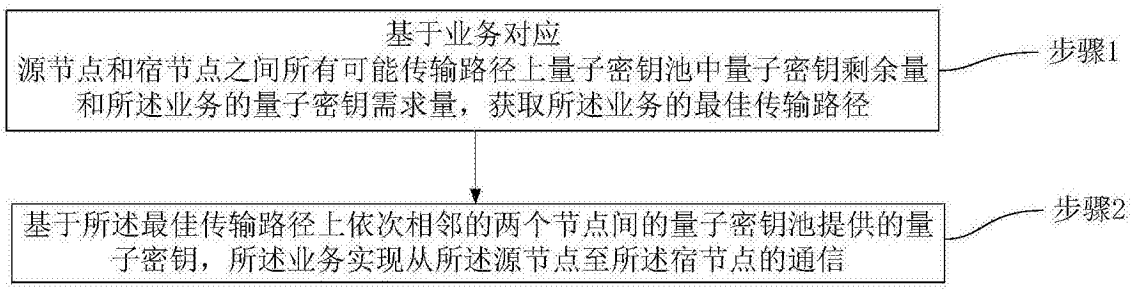

基于业务对应
源节点和宿节点之间所有可能传输路径上量子密钥池中量子密钥剩余量
和所述业务的量子密钥需求量，获取所述业务的最佳传输路径
步骤1
基于所述最佳传输路径上依次相邻的两个节点间的量子密钥池提供的量
子密钥，所述业务实现从所述源节点至所述宿节点的通信
步骤2

图3

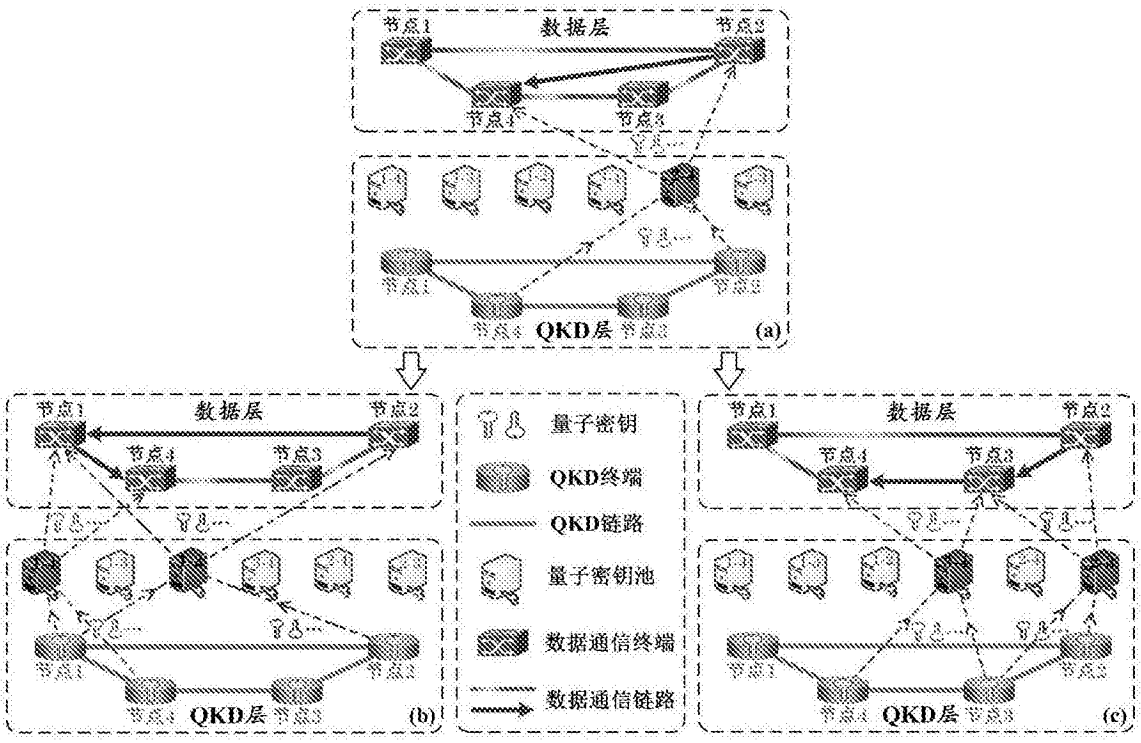

数据层
节点1
节点2
节点3
节点4
QKD层
(a)
(b)
(c)
量子密钥
QKD终端
QKD链路
量子密钥池
数据通信终端
数据通信链路

图4

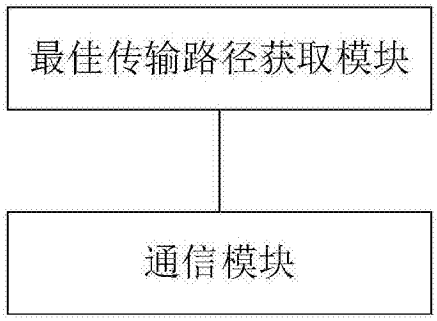

最佳传输路径获取模块
通信模块

图5