(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 110138552 B
(45)授权公告日 2021.07.20

(21)申请号 201910380711.9

(22)申请日 2019.05.08

(65)同一申请的已公布的文献号
申请公布号 CN 110138552 A

(43)申请公布日 2019.08.16

(73)专利权人 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 王华 郁小松 李亚杰 张杰

(74)专利代理机构 北京风雅颂专利代理有限公司 11403
代理人 陈宙

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

(56)对比文件
CN 108023725 A,2018.05.11
CN 107171792 A,2017.09.15
CN 106961327 A,2017.07.18
US 2009259328 A1,2009.10.15
CN 107508671 A,2017.12.22
Zhang Jie."Multi-dimensional resources allocation based on reconfigurable radio-wavelength selective switch in cloud radio over fiber networks".《Optics express》.2018,
黄伟."基于动态调度优先级的主动配电网多目标优化调度".《电工技术学报》.2018,

审查员 高凯

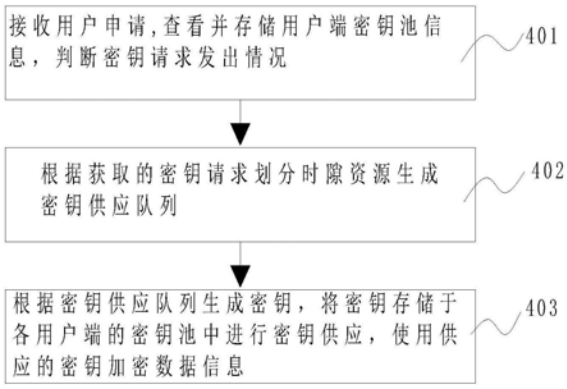
权利要求书1页 说明书9页 附图4页

(54)发明名称

多用户量子密钥供应方法及装置

(57)摘要

本发明公开了一种基于光线路终端的多用户量子密钥供应方法及装置,可以根据接收的密钥请求生成密钥供应队列;根据密钥供应队列生成密钥;并将密钥存储于在各用户端设置的密钥池中进行密钥供应。因此,本发明的方案可以根据收集的密钥请求生成密钥队列,并进行密钥生成,实现集成QKD接入网中设备时隙资源与用户密钥需求之间的高效匹配,从而提升了集成QKD接入网中多用户密钥资源的灵活供应,提高了密钥资源分配效率。



CN 110138552 B

1.一种多用户量子密钥供应方法,其特征在于,包括:

根据接收的密钥请求生成密钥供应队列;

根据密钥供应队列生成密钥;以及

将密钥存储于在各用户端设置的密钥池中进行密钥供应;

所述密钥请求包括请求源节点、请求宿节点、所需密钥量以及用户申请等级;

所述根据接收的密钥请求资源生成密钥供应队列包括:

根据用户申请等级和用户申请是否成对,对各密钥请求划分密钥请求等级;

根据各密钥请求中所需密钥量计算获取需要供应密钥量;以及

根据划分的密钥请求等级排序生成密钥请求队列;

所述根据接收的密钥请求资源生成密钥供应队列进一步包括:

根据需要供应密钥量划分时隙资源,生成密钥请求时段;

根据各密钥请求等级和各密钥请求时段设置密钥供应周期。

2.根据权利要求1所述的方法,其特征在于,所述根据需要供应密钥量划分时隙资源,生成密钥请求时段,包括:查看所有密钥请求中的所需密钥量,将高等级中的双向请求源节点和宿节点所需密钥量相加,查看一个单位时隙内的密钥生成量,并根据该生成量与所需密钥之间的比值来计算所有密钥请求所需时隙数量,这些时隙属于一个密钥请求时段;

所述根据各密钥请求等级和各密钥请求时段设置密钥供应周期包括:排序后的密钥请求顺序为密钥供应周期内的时隙分配顺序,密钥请求时段为密钥供应周期内每个密钥请求对应的时隙长度。

3.根据权利要求1所述的方法,其特征在于,所述方法进一步包括:

当用户之间需要进行安全通信的时候,从两端用户端密钥池中取出密钥加密和解密具有安全需求的数据。

4.根据权利要求1所述的方法,其特征在于,所述方法进一步包括:

查询是否需要更新密钥请求,如需要更新密钥请求,则重新接收密钥请求;如无密钥更新请求,删除下一次密钥供应周期中该请求的时隙分配。

5.根据权利要求1所述的方法,其特征在于,密钥请求由用户端检测到用户端密钥池中密钥量低于密钥补充阈值时发送。

6.一种多用户量子密钥供应装置,其特征在于,包括:

密钥供应队列生成模块,用于接收密钥请求,根据接收的密钥请求生成密钥供应队列;

量子通信模块,用于根据密钥供应队列生成密钥;以及

密钥存储模块,用于将密钥存储于各用户端的密钥池中进行密钥供应;

密钥请求等级划分单元,用于根据用户申请等级划分密钥请求等级;

排序单元,用于对密钥请求等级进行排序生成密钥请求队列;

所述量子通信模块包括:

量子密钥分发设备状态单元,用于读取量子密钥分发设备的开启状态,若开启,则标记该设备为占用状态,若关闭,则等待;

量子密钥分发单元,用于通过量子密钥分发设备根据密钥供应队列生成密钥;以及

时隙资源单元,用于划分时隙资源,生成密钥请求时段,设置密钥供应周期。

多用户量子密钥供应方法及装置

技术领域

[0001] 本发明涉及通信技术领域,特别是指一种多用户量子密钥供应方法及装置。

背景技术

[0002] 接入网通过与城域、骨干网络的连接,直接为用户提供各种各样的数据业务。随着网络技术的发展,用户通信信息变得越来越敏感,业务安全需求不断增加。量子密钥分发(Quantum Key Distribution,QKD)技术可以为用户安全需求提供理论上绝对安全的密钥资源,目前也已形成一些在光接入网中集成QKD的方案。

[0003] 目前,接入网通过光线路终端(Optical Line Terminal,OLT)对用户所需业务进行管控,但是其特有的用户请求汇聚与数据信息广播过程面临着严重的安全威胁。QKD可以通过设备部署为OLT与用户之间的数据信息提供安全的密钥,但是已有的接入网集成QKD方案只能够实现密钥的实时生成,不仅不能按需满足用户的密钥请求,而且无法高效灵活的实现多用户间的密钥请求。从而造成现有QKD接入网中密钥供应不灵活、密钥资源分配效率不高的问题。

发明内容

[0004] 有鉴于此,本发明的目的在于提出一种多用户量子密钥供应方法及装置,解决了现有QKD接入网中密钥供应不灵活、密钥资源分配效率不高的问题。

[0005] 根据本发明的一个方面,提供一种多用户量子密钥供应方法,包括:

[0006] 根据接收的密钥请求生成密钥供应队列;

[0007] 根据密钥供应队列生成密钥;以及

[0008] 将密钥存储于在各用户端设置的密钥池中进行密钥供应。

[0009] 可选的,所述密钥请求包括请求源节点、请求宿节点、所需密钥量以及用户申请等级。

[0010] 可选的,所述根据接收的密钥请求资源生成密钥供应队列包括:

[0011] 根据用户申请等级和用户申请是否成对,对各密钥请求划分密钥请求等级;

[0012] 根据各密钥请求中所需密钥量计算获取需要供应密钥量;以及

[0013] 根据划分的密钥请求等级排序生成密钥请求队列。

[0014] 可选的,所述根据接收的密钥请求资源生成密钥供应队列进一步包括:

[0015] 根据需要供应密钥量划分时隙资源,生成密钥请求时段;

[0016] 根据各密钥请求等级和各密钥请求时段设置密钥供应周期。

[0017] 可选的,所述根据需要供应密钥量划分时隙资源,生成密钥请求时段,包括:查看所有密钥请求中的所需密钥量,将高等级中的双向请求源节点和宿节点所需密钥量相加,查看一个单位时隙内的密钥生成量,并根据该生成量与所需密钥之间的比值来计算所有密钥请求所需时隙数量,这些时隙属于一个密钥请求时段;

[0018] 所述根据各密钥请求等级和各密钥请求时段设置密钥供应周期包括:排序后的密

钥请求顺序为密钥供应周期内的时隙分配顺序，密钥请求时段为密钥供应周期内每个密钥请求对应的时隙长度。

[0019] 可选的，所述多用户量子密钥供应方法进一步包括：

[0020] 当用户之间需要进行安全通信的时候，从两端用户端密钥池中取出密钥加密和解密具有安全需求的数据。

[0021] 可选的，所述多用户量子密钥供应方法进一步包括：

[0022] 查询是否需要更新密钥请求，如需要更新密钥请求，则重新接收密钥请求；如无密钥更新请求，删除下一次密钥供应周期中该请求的时隙分配。

[0023] 可选的，密钥请求由用户端检测到用户端密钥池中密钥量低于密钥补充阈值时发送。

[0024] 一种多用户量子密钥供应装置，包括：

[0025] 密钥供应队列生成模块，用于接收密钥请求，根据接收的密钥请求生成密钥供应队列；

[0026] 量子通信模块，用于根据密钥供应队列生成密钥；以及

[0027] 密钥存储模块，用于将密钥存储于各用户端的密钥池中进行密钥供应。

[0028] 可选的，所述密钥供应队列生成模块包括：

[0029] 密钥请求等级划分单元，用于根据用户申请等级划分密钥请求等级；

[0030] 排序单元，用于对密钥请求等级进行排序生成密钥请求队列；

[0031] 所述量子通信模块包括：

[0032] 量子密钥分发设备状态单元，用于读取量子密钥分发设备的开启状态，若开启，则标记该设备为占用状态，若关闭，则等待；

[0033] 量子密钥分发单元，用于通过量子密钥分发设备根据密钥供应队列生成密钥；以及

[0034] 时隙资源单元，用于划分时隙资源，生成密钥请求时段，设置密钥供应周期。

[0035] 从上面所述的技术方案可以看出，本发明提供的多用户量子密钥供应方法及装置，在接收到多个用户申请后，查看并存储用户端密钥池信息，判断密钥请求发出情况；根据获取的密钥请求划分时隙资源生成密钥供应队列；根据密钥供应队列生成密钥，将密钥存储于各用户端的密钥池中进行密钥供应，使用供应的密钥加密数据信息。因此本发明方案可以根据密钥请求生成密钥供应队列，同时划分时隙资源，进行密钥生成，不仅实现密钥的实时生成，还能按需满足用户的密钥请求，实现集成QKD接入网中设备时隙资源与用户密钥需求之间的高效匹配，从而提升了集成QKD接入网中多用户密钥资源的灵活供应，提高了密钥资源分配效率。

[0036] 更进一步，在本发明的方案中，光线路终端在密钥供应队列的生成过程中，可以先根据用户申请的等级对密钥请求进行等级划分，得到不同的密钥请求等级后，对密钥请求进行排序，从而得到密钥供应队列，因此，按照该密钥供应队列生成密钥可以保证优先级高的密钥请求优先获得密钥，从而可以进一步提高密钥资源的分配效率。

附图说明

[0037] 图1为光接入网中光线路终端和光网络单元的连接示意图；

[0038] 图2为本发明实施例一种多用户量子密钥供应方法的QKD设备部署方案示意图：QKD接收机←QKD发射机；

[0039] 图3为本发明实施例所述的多用户量子密钥供应方法的流程示意图；

[0040] 图4为本发明实施例所述的多用户量子密钥供应方法的流程示意图中步骤401的一示意性流程图；

[0041] 图5为本发明实施例所述的多用户量子密钥供应方法的流程示意图中步骤402的一示意性流程图；

[0042] 图6为本发明实施例所述的多用户量子密钥供应方法的流程示意图中步骤403的一示意性流程图；

[0043] 图7为本发明另一实施例所述的多用户量子密钥供应方法的流程示意图；

[0044] 图8为本发明实施例具体一次量子密钥分发接入网多用户密钥按需供应方法的密钥供应周期示意图；

[0045] 图9为本发明实施例所述的多用户量子密钥供应装置示意图。

具体实施方式

[0046] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本发明进一步详细说明。

[0047] 如图1所示，光线路终端(Optical Line Terminal,OLT)是经典光接入网中的核心组件，具有业务汇聚、业务安全管理、网络配置管理等功能。随着用户所需业务种类的增多，它需要对用户端光网络单元(Optical Network Unit,ONU)进行控制、管理等操作。OLT通过汇聚来自ONU的用户请求信息，转发这些请求于上级网络并向所有ONU广播所得数据信息，从而实现OLT与用户之间的数据管控。

[0048] 图2为本发明实施例所述的多用户量子密钥供应方法的QKD设备部署方案示意图，QKD接收机←QKD发射机，为保障OLT与ONU之间的信息安全，需要在OLT处放置QKD接收机，QKD发射机可以放置在ONU侧。为快速向用户提供密钥，在每个QKD发射机和接收机处均需要放置密钥池，它在QKD发射机和接收机两侧用于存储生成的密钥。同时，为方便用户间密钥的生成和节约成本，可信/量子中继与OLT处的QKD设备放置在一起。如在图2中，与ONU1相连的QKD发射机与接收机通过WDM和TDM技术在光纤中进行QKD过程以产生ONU与OLT之间的安全密钥，再通过OLT侧中继生成的ONU与ONU之间的密钥，将密钥分别存储在该QKD发射机和接收机两侧的密钥池中。

[0049] 需要说明的是，图2仅仅显示了一种QKD设备部署方案，在实际的应用中，还可以将QKD发射机放置在OLT处，而将QKD接收机放置在ONU侧；亦或者还可以在OLT处同时放置QKD发射机和QKD接收机，同时在ONU侧也同时放置QKD发射机和QKD接收机。这些QKD设备的部署方案在OLT和ONU之间都可以实现密钥的生成，且均不影响本发明提出的多用户量子密钥供应方法及装置。另外，ONU和OLT之间的光纤可以通过波分复用技术(Wavelength division multiplexing,WDM)和时分复用(Time Division Multiplexing,TDM)技术完成QKD过程。

[0050] 图3为本发明实施例所述的多用户量子密钥供应方法的流程示意图，该方法可以由ONU和OLT共同执行完成。为了实现多用户量子密钥的按需供应，上述ONU处设置有密钥池，用于缓存生成的密钥。其中，在本发明的实施例中，ONU也称为用户端；ONU对应的密钥池

也称为用户端密钥池。

[0051] 如图3所示，所述方法包括：

[0052] 步骤401、用户端接收用户申请，查看并记录用户端部署的密钥池信息，判断密钥请求发出情况。

[0053] 其中，接收用户申请包括记录用户申请等级，分为高级与低级。

[0054] 所述密钥请求包括请求源节点、请求宿节点、所需密钥量以及用户申请等级。

[0055] 所述查看并存储用户端密钥池信息，包括查看并存储密钥池容量、现有密钥量和密钥补充阈值。

[0056] 所述判断密钥请求发出情况，包括：

[0057] 当用户端密钥池现有密钥量低于密钥补充阈值，判定需要发出密钥请求，并向用户端发送判定信息；

[0058] 否则，判定不需要发出密钥请求，并继续接受用户申请；

[0059] 用户端根据判定信息，发出密钥请求。

[0060] 该步骤还可包括：

[0061] 读取量子密钥分发设备的开启状态，若开启，则标记该设备为占用状态，若关闭，则等待。

[0062] 步骤402、OLT根据从用户端获取的密钥请求生成密钥供应队列。

[0063] 在本发明的实施例中，上述步骤402可包括：

[0064] 读取密钥请求的请求源节点、请求宿节点、所需密钥量以及用户申请等级；

[0065] 根据用户申请等级和用户申请是否成对，对各密钥请求划分密钥请求等级；

[0066] 根据各密钥请求中所需密钥量计算获取需要供应密钥量；以及

[0067] 根据划分的密钥请求等级排序生成密钥请求队列。

[0068] 在本发明的实施例中，上述步骤402还可进一步包括：

[0069] 根据需要供应密钥量划分时隙资源，生成密钥请求时段；以及

[0070] 根据各密钥请求等级和密钥请求时段设置密钥供应周期。

[0071] 步骤403、OLT根据密钥供应队列生成密钥，将密钥存储于各用户端的密钥池中进行密钥供应。

[0072] 需要说明的是，在上述步骤403中，OLT将触发QKD设备操作根据密钥供应队列生成密钥。

[0073] 在执行完上述步骤403之后，就完成了密钥的供应。此后，当用户之间需要进行安全通信的时候，即可从两端用户端密钥池中取出密钥加密和解密具有安全需求的数据。

[0074] 更进一步，OLT还可以进一步查询是否需要更新密钥请求，如需要更新密钥请求，则重新接收用户请求；如无密钥更新请求，删除下一次密钥供应周期中该请求的时隙分配。

[0075] 图4根据本发明实施例的多用户量子密钥供应方法的步骤401的一示意性流程图。

[0076] 图4中包括：

[0077] 步骤501、查看并记录密钥池容量、现有密钥量和密钥补充阈值，记录用户申请等级。

[0078] 其中，密钥补充阈值用于密钥补充预警，用户申请等级分为高级和低级两个类型。

[0079] 步骤502、判断现有密钥量是否低于密钥补充阈值，若是，进入步骤503，若否，重复

步骤502。

[0080] 步骤503、发出密钥请求，包括密钥请求的请求源节点、请求宿节点、所需密钥量及用户申请等级。

[0081] 步骤504、读取量子密钥分发设备是否空闲，若是，则进入步骤505，若否，则通知用户端光网络单元等待，并重复步骤504。

[0082] 步骤505、标记该设备为占用状态。

[0083] 图5根据本发明实施例一种基于光线路终端的多用户量子密钥供应方法的步骤402的一示意性流程图。

[0084] 图5中包括：

[0085] 步骤601、根据用户申请等级和用户是否成对，对各密钥请求划分密钥请求等级。

[0086] 其中，在本发明的实施例中，用户申请等级由用户给出的密钥请求信息提出，用户是否成对表示双向或单向用户需要建立密钥。综合考虑用户申请等级和实际用户共享密钥是否成对，密钥请求等级从高往低可以分为以下四个类型：

[0087] 等级1，用户请求等级为高级，用户端之间为双向密钥需求；

[0088] 等级2，用户请求等级为高级，用户端之间为单向密钥需求；

[0089] 等级3，用户请求等级为低级，用户端之间为双向密钥需求；

[0090] 等级4，用户请求等级为低级，用户端之间为单向密钥需求。

[0091] 步骤602、根据各密钥请求中所需密钥量计算获取需要供应密钥量。

[0092] 其中，由于QKD接入网中具有安全需求的业务大部分是随机产生的，不同类型密钥池中的密钥同样被随机消耗。所有ONU连接的密钥池根据密钥补充阈值触发密钥请求。OLT向具有密钥请求的ONU广播以获取密钥池现存密钥量，OLT根据密钥池容量和现存密钥量之差计算获取需要供应密钥量。

[0093] 步骤603、根据划分的密钥请求等级排序生成密钥请求队列。

[0094] 其中，OLT新建一个密钥请求队列用于存储ONU密钥请求和所需供应密钥量。队列需要根据密钥请求等级从前往后排列密钥请求。如果ONU密钥请求发生变化后，需要对队列排序进行更新。

[0095] 在本发明的实施例中，上述图5还可以进一步包括：

[0096] 步骤604、查看空闲的时隙资源，根据需要供应密钥量划分时隙资源，生成密钥请求时段。

[0097] 其中，OLT查看所有ONU密钥请求中的所需密钥量，将高等级中的双向请求源节点和宿节点所需密钥量相加。OLT查看一个单位时隙内的密钥生成量，并根据该生成量与所需密钥之间的比值来计算所有请求所需时隙数量。这些时隙属于一个密钥请求时段。

[0098] 步骤605、根据各密钥请求等级和密钥请求时段设置密钥供应周期。

[0099] 其中，OLT排序后的多用户请求顺序为密钥供应周期内的时隙分配顺序，密钥请求时段为密钥供应周期内每个请求对应的时隙长度。OLT将时隙设置情况分别发送给所有ONU。

[0100] 图6根据本发明实施例的多用户量子密钥供应方法的步骤403的一示意性流程图。

[0101] 图6中包括：

[0102] 步骤701、在密钥请求时段内，进行多个密钥请求的密钥生成，将密钥存储于各用

户端的密钥池中进行密钥供应。

[0103] 其中，在密钥请求时段内，OLT根据每对节点之间所需密钥数量先进行OLT与两个ONU之间的密钥生成，再在OLT处通过可信/量子中继对OLT与两个ONU之间生成的密钥进行异或操作来生成两个ONU之间的密钥，并将生成后的密钥存储至两端的密钥池内。其中，密钥生成需要占用它们之间光纤内的量子信道和经典光信道。

[0104] 在执行完步骤701之后OLT就完成了密钥的供应，此后还可以进一步执行如下操作：

[0105] 步骤702、用户端进行安全通信时，从两端密钥池中取出密钥加密和解密具有安全需求的数据。

[0106] 步骤703、OLT查询是否需要更新密钥请求信息，若是，执行步骤704，若否，执行步骤705。

[0107] 步骤704、更新密钥请求，重新发送更新后的密钥请求，返回步骤401。

[0108] 步骤705、删除下一次量子密钥供应周期中该请求的时隙分配。

[0109] 作为本发明的另一种实施例，一种基于光线路终端的多用户量子密钥供应方法，如图7所示，

[0110] 步骤1：基于OLT的密钥请求获取，包括：

[0111] 1.1记录部署的密钥池设备信息。密钥池用于密钥存储及管理，QKD接入网中不同用户具有不同大小的安全需求。为合理使用密钥，每个用户需要根据安全需求大小配置一个匹配的密钥池。具体地，密钥池类型分为大型、中型和小型密钥池。密钥池包含参数有密钥容量和密钥补充阈值，密钥补充阈值用于密钥补充预警。

[0112] 1.2 OLT密钥请求收集。OLT在一定时间间隔向ONU广播消息来查询是否具有密钥请求。当用户密钥池中密钥量低于密钥补充阈值，ONU需要发送密钥请求于OLT来补充密钥量。密钥请求具体包括请求源节点、请求宿节点、所需密钥量以及用户申请等级。其中，用户申请等级分为高级和低级两个类型。

[0113] 1.3 QKD设备状态查询。OLT查看与它相连的QKD设备(QKD发射机或接收机)是否处于空闲状态。如果该QKD设备处于空闲状态，则标记该设备为占用状态；如不处于空闲状态，则通知所有ONU等待。

[0114] 步骤2：基于OLT的多用户密钥供应设置，包括：

[0115] 2.1密钥请求等级生成。OLT对多个ONU的密钥请求进行等级划分。OLT可以获取两个相关信息，即用户申请等级和用户是否成对。用户申请等级由用户给出的密钥请求信息提出，用户是否成对表示双向或单向用户需要建立密钥。综合考虑用户申请等级和实际用户共享密钥是否成对，密钥请求等级从高往低可以分为以下四个类型：等级1(用户请求等级高，双向)，等级2(用户请求等级高，单向)，等级3(用户请求等级低，双向)和等级4(用户请求等级低，单向)。

[0116] 2.2密钥量供应计算。由于QKD接入网中具有安全需求的业务大部分是随机产生的，不同类型密钥池中的密钥同样被随机消耗。所有ONU连接的密钥池根据密钥补充阈值触发密钥请求。OLT向具有密钥请求的ONU广播以获取密钥池现存密钥量，OLT根据密钥池容量和现存密钥量之差计算获取需要供应密钥量。

[0117] 2.3密钥请求队列生成。OLT对多个用户ONU密钥请求进行排序。OLT新建一个密钥

请求队列用于存储ONU密钥请求和所需供应密钥量。队列需要根据密钥请求等级从前往后排列密钥请求。如果ONU密钥请求发生变化后，需要对队列排序进行更新。

[0118] 2.4多用户密钥供应分配。OLT根据用户请求来划分时隙资源生成密钥。OLT查看所有ONU密钥请求中的所需密钥量，将高等级中的双向请求源节点和宿节点所需密钥量相加。OLT查看一个单位时隙内的密钥生成量，并根据该生成量与所需密钥之间的比值来计算所有请求所需时隙数量。这些时隙属于一个密钥请求时段。

[0119] 2.5密钥供应周期生成。OLT根据密钥请求等级和多用户时隙划分设置密钥供给周期。OLT排序后的多用户请求顺序为密钥供应周期内的时隙分配顺序，密钥请求时段为密钥供应周期内每个请求对应的时隙长度。OLT将时隙设置情况分别发送给所有ONU。

[0120] 步骤3：基于OLT的量子密钥供应，包括：

[0121] 3.1多用户安全密钥生成。在密钥请求时段内，OLT根据每对节点之间所需密钥数量先进行OLT与两个ONU之间的密钥生成，再在OLT处通过可信/量子中继对OLT与两个ONU之间生成的密钥进行异或操作来生成两个ONU之间的密钥，并将生成后的密钥存储至两端的密钥池内。其中，密钥生成需要占用它们之间光纤内的量子信道和经典光信道。

[0122] 3.2多用户安全密钥使用。当ONU之间需要进行安全通信的时候，从两端密钥池中取出密钥加密和解密具有安全需求的数据。

[0123] 3.3多用户密钥请求更新。OLT广播ONU，查询ONU是否需要更新密钥请求信息。如ONU需要更新密钥请求，则重复步骤1和2；如ONU无密钥更新请求，删除下一次量子密钥供应周期中该请求的时隙分配。

[0124] 基于上述多用户量子密钥按需供应方法，下面将完成具体一次量子密钥分发接入网多用户密钥按需供应方法实施例。如图2所示，接入网与OLT之间配置QKD接收机和密钥池，各个ONU侧配置QKD发射机和密钥池。

[0125] 步骤1：记录用户于ONU处选择的不同大小类型进行部署的密钥池。

[0126] 步骤2：OLT广播3个ONU是否具有密钥请求。由于3个密钥池中的密钥量均低于密钥补充阈值，3个ONU将密钥请求发送至OLT。

[0127] 步骤3：OLT查看它附近的QKD接收设备是否处于空闲状态。假设QKD接收设备处于空闲状态，ONU1，ONU2和ONU3可以通过共享该QKD接收设备来产生OLT和ONU之间的密钥。

[0128] 步骤4：OLT收到3个密钥请求，即ONU1→ONU2(用户申请等级高)，ONU2→ONU1(用户申请等级高)，ONU3→ONU1(用户申请等级低)。由于只有ONU1和ONU2之间是双向密钥需求，则判断ONU1→ONU2和ONU2→ONU1为等级1，ONU3→ONU1为等级4。

[0129] 步骤5：OLT广播ONU来收集3个密钥池所需供应密钥量。即ONU1→ONU2(3比特)，ONU2→ONU1(1比特)，ONU3→ONU1(4比特)。

[0130] 步骤6：OLT新建一个密钥请求队列来存储3个ONU密钥请求及其所需密钥量。根据密钥请求等级排列队列中的请求顺序为ONU1→ONU2，ONU2→ONU1和ONU3→ONU1。

[0131] 步骤7：OLT将ONU1和ONU2的密钥请求相加为4bit，根据一个时隙内QKD的密钥生成速率(如2比特/时隙)进行时隙划分来产生密钥，ONU1→ONU2和ONU2→ONU1一共需要占用2个时隙，ONU3→ONU1需要占用2个时隙。这4个时隙分别是两个密钥请求时段。

[0132] 步骤8：OLT将密钥请求队列中的排序作为密钥供应的排序，即ONU1→ONU2，ONU2→ONU1和ONU3→ONU1。OLT将密钥请求时段作为密钥供应周期中每个请求的时隙长度，即ONU1

→ONU2和ONU2→ONU1占用2个时隙，ONU3→ONU1占用2个时隙，如图8所示。

[0133] 步骤9：在2个时隙内，OLT附近的QKD接收机分别与ONU1，ONU2和ONU3处的QKD发射机进行QKD过程。例如对于ONU1和ONU2之间的密钥请求，先产生OLT和ONU1之间的4比特密钥，再OLT和ONU2之间的4比特密钥。最后可信/量子中继将两个4比特密钥进行异或以形成ONU1和ONU2之间的4比特密钥，将这4比特密钥分别存储至ONU1和ONU2处的密钥池中。

[0134] 步骤10：当ONU1，ONU2和ONU3之间进行安全通信的时候，从源节点对应的密钥池中取出密钥对信息加密，在宿节点对应密钥池中取出密钥进行解密。

[0135] 步骤11：OLT查询3个ONU是否需要更新密钥请求。如需更新密钥请求，则重复步骤1-9；如不需更新密钥请求，删除下一次量子密钥供应周期中该请求的时隙分配。

[0136] 下面根据上述多用户量子密钥供应方法，介绍一种多用户量子密钥供应装置，如图9所示，包括：

[0137] 密钥供应队列生成模块91，用于接收密钥请求，根据接收的密钥请求生成密钥供应队列；以及

[0138] 量子通信模块92，用于根据密钥供应队列生成密钥；

[0139] 密钥存储模块93，用于将密钥存储于各用户端的密钥池中进行密钥供应。

[0140] 其中，所述密钥供应队列生成模块91包括：

[0141] 密钥请求等级划分单元911，用于根据用户申请等级划分密钥请求等级；

[0142] 排序单元912，用于对密钥请求等级进行排序生成密钥请求队列。

[0143] 上述量子通信模块92包括：

[0144] 量子密钥分发设备状态单元921，用于读取量子密钥分发设备的开启状态，若开启，则标记该设备为占用状态，若关闭，则等待；

[0145] 量子密钥分发单元922，用于通过量子密钥分发设备根据密钥供应队列生成密钥。

[0146] 上述量子通信模块92还可以进一步包括：

[0147] 时隙资源单元923，用于划分时隙资源，生成密钥请求时段，设置密钥供应周期。

[0148] 需要说明的是，上述密钥存储模块93将密钥存储于各用户端的密钥池中进行密钥供应，实现密钥量的查询、密钥的存储、密钥的更新、密钥量的预警以及密钥使用后的删除操作。

[0149] 上述多用户量子密钥供应装置还可以进一步包括时钟单元，用于提供准确的时间同步信息。通过获取、校准时间信息为QKD单元和密钥管理单元提供准确的时间同步信息。

[0150] 综上所述，本发明所述的多用户量子密钥供应方法及装置，在接收到多个用户申请后，查看并存储用户端密钥池信息，判断密钥请求发出情况；根据获取的密钥请求划分时隙资源生成密钥供应队列；根据密钥供应队列生成密钥，将密钥存储于各用户端的密钥池中进行密钥供应，使用供应的密钥加密数据信息。因此本发明方案可以收集密钥请求并生成密钥供应队列，并按照该密钥供应队列进行密钥的生成，实现集成QKD接入网中设备时隙资源与用户密钥需求之间的高效匹配，从而提升了集成QKD接入网中多用户密钥资源的灵活供应，提高了密钥资源分配效率。

[0151] 所属领域的普通技术人员应当理解：以上任何实施例的讨论仅为示例性的，并非旨在暗示本公开的范围(包括权利要求)被限于这些例子；在本发明的思路下，以上实施例或者不同实施例中的技术特征之间也可以进行组合，步骤可以以任意顺序实现，并存在如

上所述的本发明的不同方面的许多其它变化，为了简明它们没有在细节中提供。

[0152] 本发明的实施例旨在涵盖落入所附权利要求的宽泛范围之内的所有这样的替换、修改和变型。因此，凡在本发明的精神和原则之内，所做的任何省略、修改、等同替换、改进等，均应包含在本发明的保护范围之内。

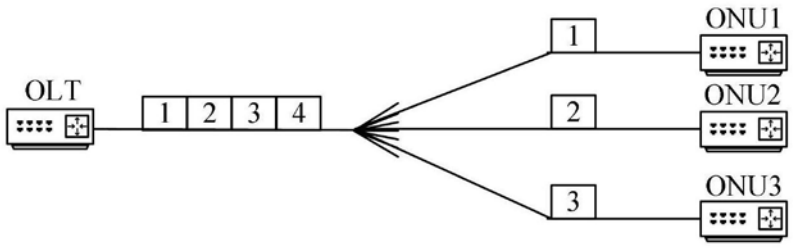

OLT
1
2
3
4
1
2
3
ONU1
ONU2
ONU3

图1

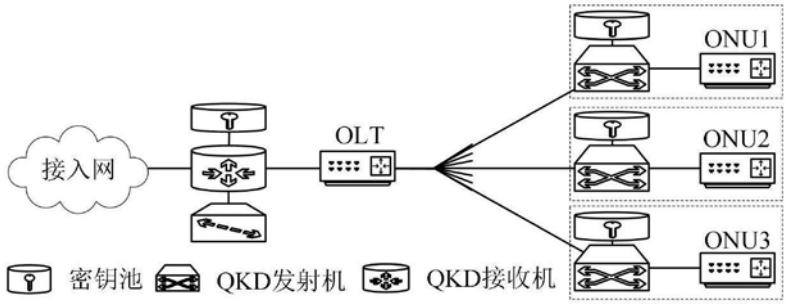

接入网
OLT
ONU1
ONU2
ONU3
密钥池
QKD发射机
QKD接收机

图2

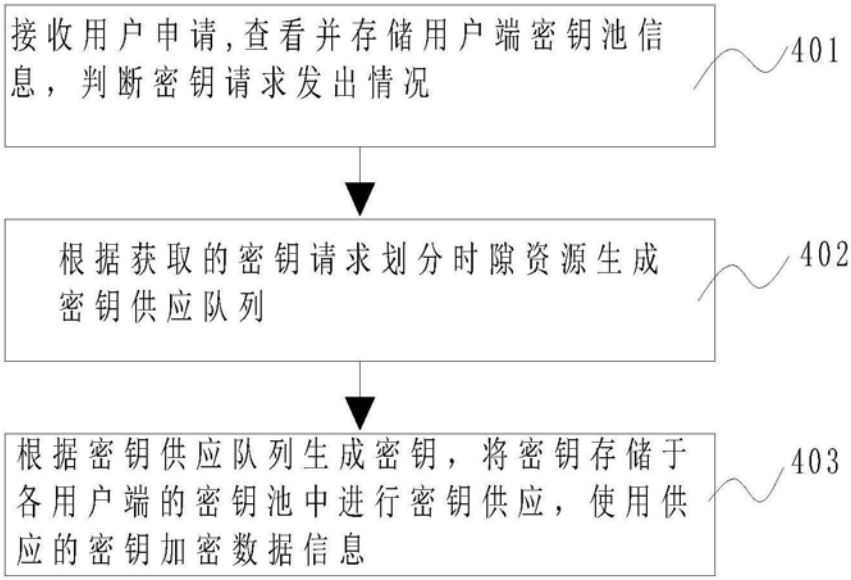

接收用户申请,查看并存储用户端密钥池信息，判断密钥请求发出情况
401
根据获取的密钥请求划分时隙资源生成密钥供应队列
402
根据密钥供应队列生成密钥，将密钥存储于各用户端的密钥池中进行密钥供应，使用供应的密钥加密数据信息
403

图3

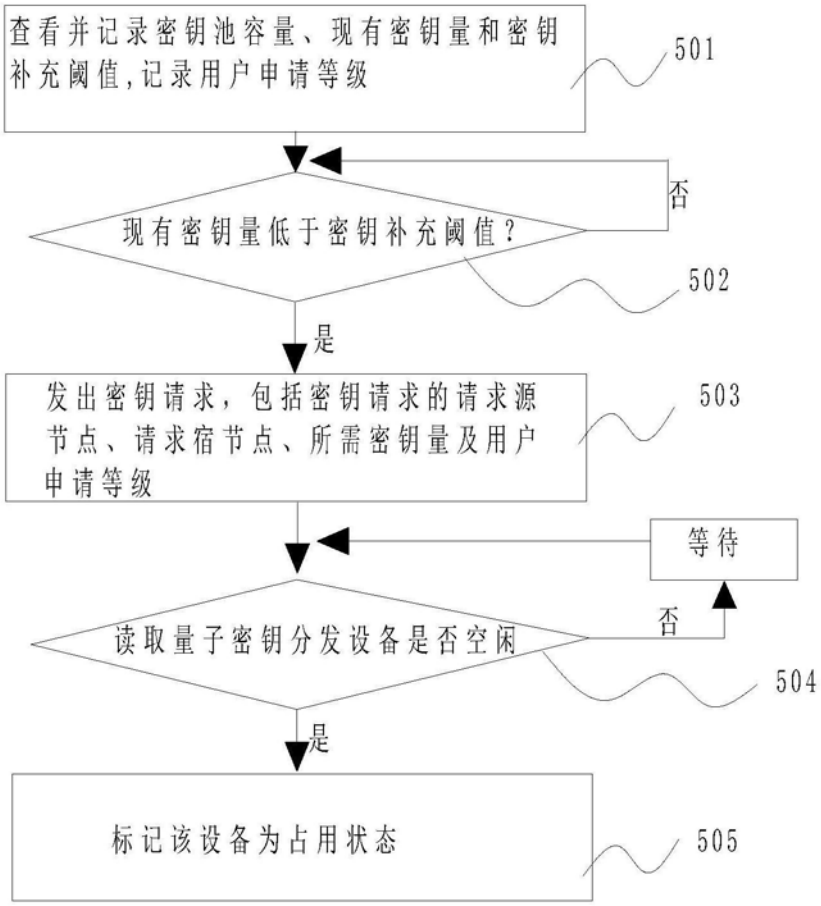

查看并记录密钥池容量、现有密钥量和密钥补充阈值,记录用户申请等级
501
现有密钥量低于密钥补充阈值？
否
502
是
发出密钥请求，包括密钥请求的请求源节点、请求宿节点、所需密钥量及用户申请等级
503
等待
读取量子密钥分发设备是否空闲
否
504
是
标记该设备为占用状态
505

图4

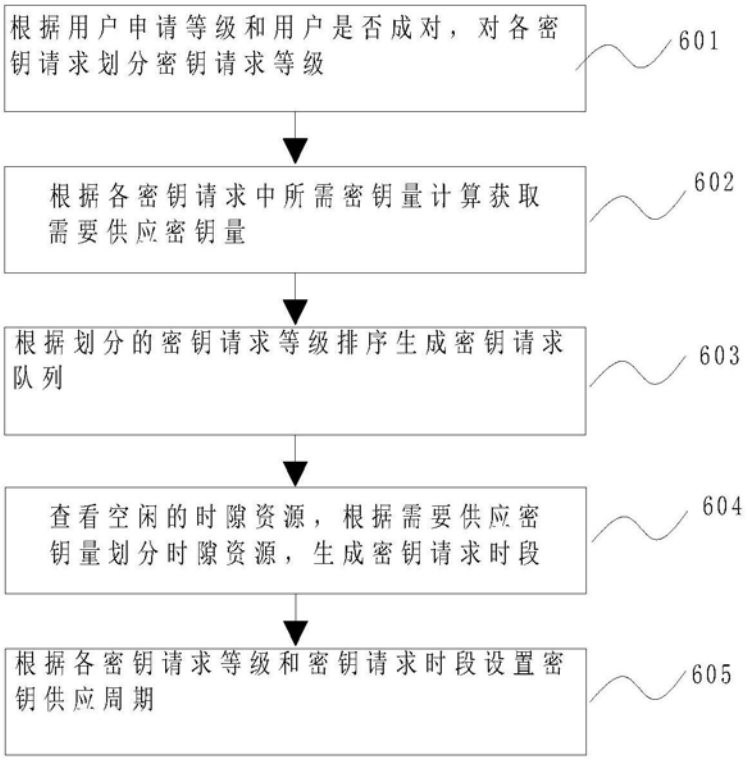

根据用户申请等级和用户是否成对，对各密钥请求划分密钥请求等级
601
根据各密钥请求中所需密钥量计算获取需要供应密钥量
602
根据划分的密钥请求等级排序生成密钥请求队列
603
查看空闲的时隙资源，根据需要供应密钥量划分时隙资源，生成密钥请求时段
604
根据各密钥请求等级和密钥请求时段设置密钥供应周期
605

图5

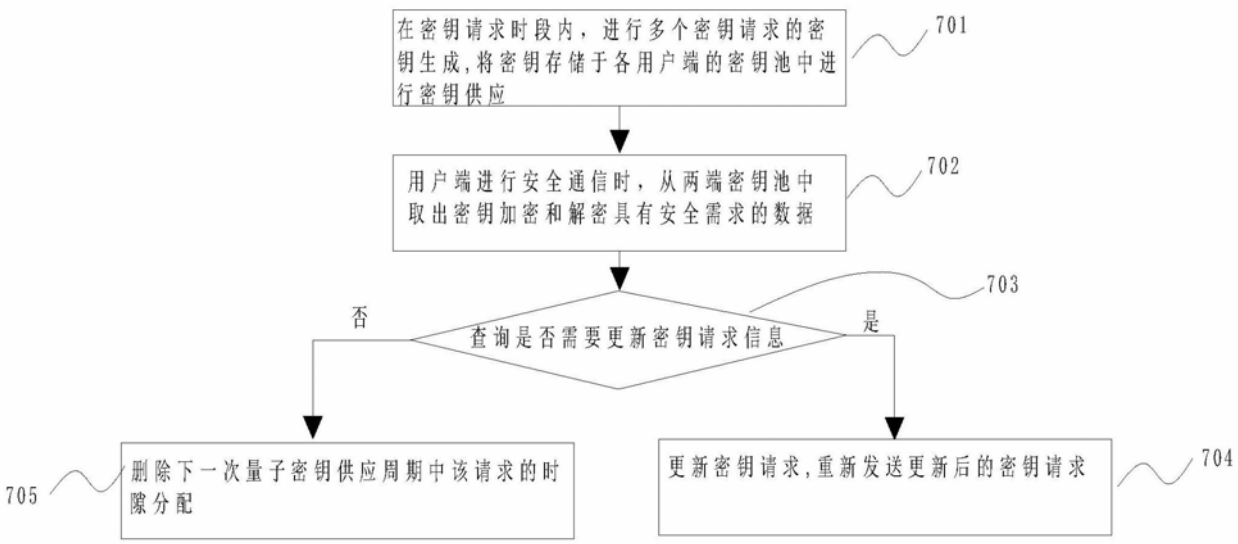

在密钥请求时段内，进行多个密钥请求的密钥生成,将密钥存储于各用户端的密钥池中进行密钥供应
701
用户端进行安全通信时，从两端密钥池中取出密钥加密和解密具有安全需求的数据
702
703
否
查询是否需要更新密钥请求信息
是
删除下一次量子密钥供应周期中该请求的时隙分配
705
更新密钥请求,重新发送更新后的密钥请求
704

图6

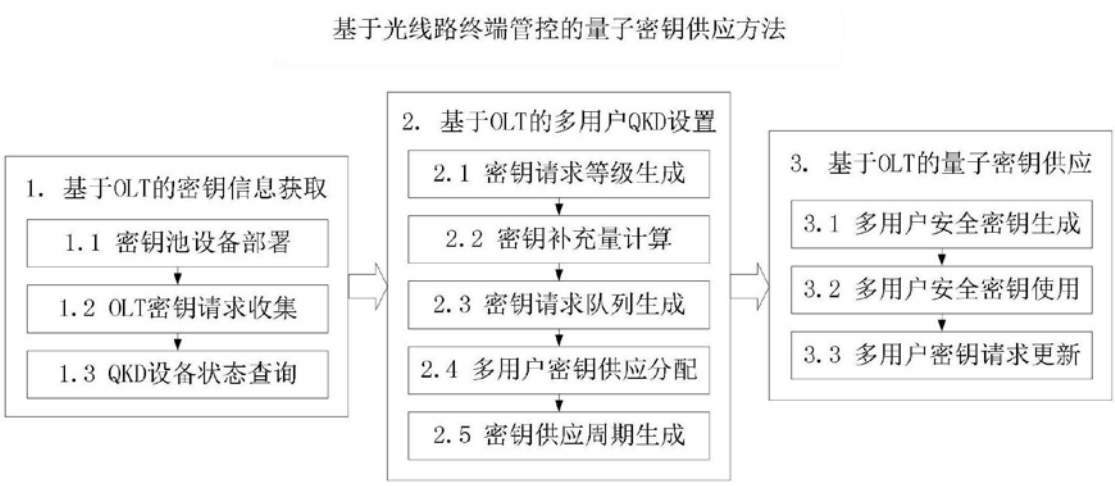

基于光线路终端管控的量子密钥供应方法
1. 基于OLT的密钥信息获取
1.1 密钥池设备部署
1.2 OLT密钥请求收集
1.3 QKD设备状态查询
2. 基于OLT的多用户QKD设置
2.1 密钥请求等级生成
2.2 密钥补充量计算
2.3 密钥请求队列生成
2.4 多用户密钥供应分配
2.5 密钥供应周期生成
3. 基于OLT的量子密钥供应
3.1 多用户安全密钥生成
3.2 多用户安全密钥使用
3.3 多用户密钥请求更新

图7


ONU1<->ONU2
ONU1<->ONU3
时隙1
时隙2
时隙3
时隙4
密钥供应周期

图8

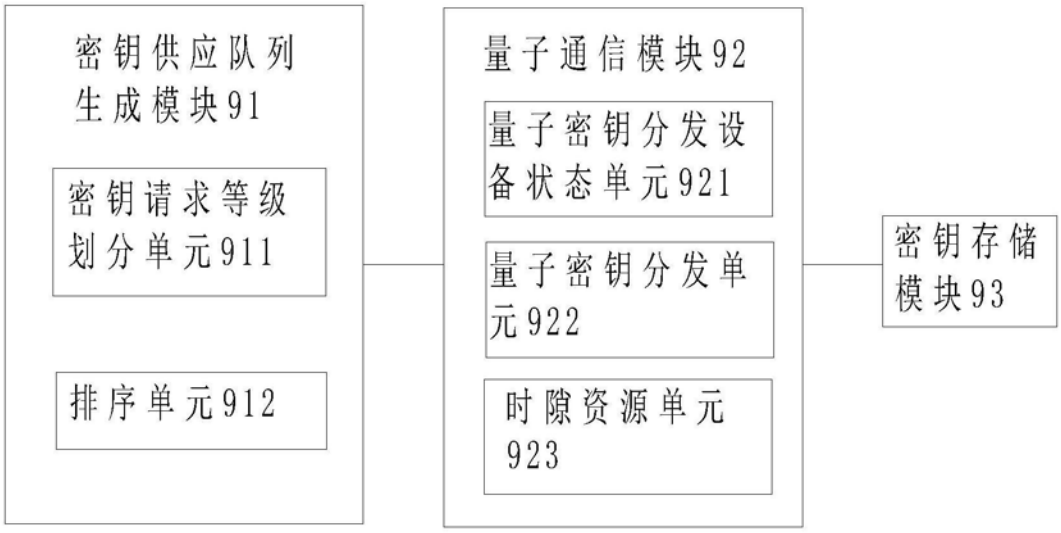

密钥供应队列生成模块91
密钥请求等级划分单元911
排序单元912
量子通信模块92
量子密钥分发设备状态单元921
量子密钥分发单元922
时隙资源单元923
密钥存储模块93

图9