(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 105827397 A
(43)申请公布日 2016.08.03

(21)申请号 201510009615.5

(22)申请日 2015.01.08

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 付颖芳 刘栓林 高亚滨 陈秀忠

(74)专利代理机构 北京市清华源律师事务所 11441
代理人 沈泳 李赞坚

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

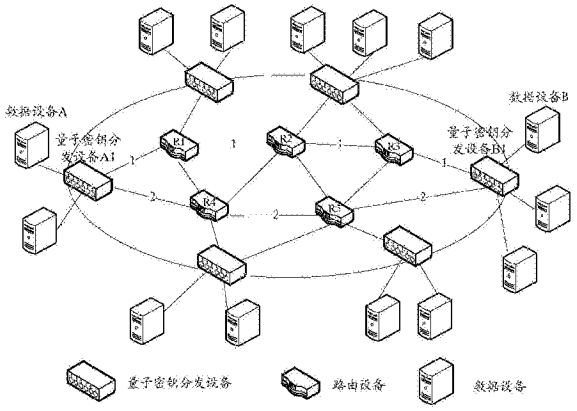
权利要求书5页 说明书17页 附图5页

(54)发明名称

基于可信中继的量子密钥分发系统、方法及装置

(57)摘要

本申请公开了一种基于可信中继的量子密钥分发系统，一种基于可信中继的量子密钥分发方法及装置。其中，所述系统包括：量子密钥分发设备、用于中继密钥和转发加密数据的路由设备、以及数据设备；所述每个量子密钥分发设备与至少一个所述路由设备相连，所述每个量子密钥分发设备与至少一个所述数据设备相连，所述路由设备彼此连接形成网状拓扑；其中，所述量子密钥分发设备用于采用两条或者两条以上的不同路径与对端量子密钥分发设备进行密钥协商、并采用预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。采用上述系统，不仅可以有效提高量子密钥的成码量，而且可以提高量子密钥分发网络的安全性。



CN 105827397 A

1. 一种基于可信中继的量子密钥分发系统，其特征在于，包括：量子密钥分发设备、用于中继密钥和转发加密数据的路由设备、以及用作数据传输的源端或目的端的数据设备；所述每个量子密钥分发设备与至少一个所述路由设备相连，所述每个量子密钥分发设备与至少一个所述数据设备相连，所述路由设备彼此连接形成网状拓扑；

其中，所述量子密钥分发设备用于采用两条或者两条以上的不同路径与对端量子密钥分发设备进行密钥协商、并采用预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

2. 根据权利要求 1 所述的基于可信中继的量子密钥分发系统，其特征在于，所述量子密钥分发设备还用于在发起量子密钥协商之前，将本次量子密钥协商的路径信息发送给所述路径包含的路由设备以及接收方量子密钥分发设备；

相应的，所述路由设备和所述接收方量子密钥分发设备还用于根据接收到的路径信息，对与其进行密钥协商的路由设备或量子密钥分发设备的身份进行验证。

3. 根据权利要求 1 所述的基于可信中继的量子密钥分发系统，其特征在于，所述每个量子密钥分发设备与至少两个所述路由设备相连。

4. 根据权利要求 3 所述的基于可信中继的量子密钥分发系统，其特征在于，所述两条或者两条以上的不同路径是指，其中任意两条路径都不包含相同的路由设备。

5. 根据权利要求 1-4 任一所述的基于可信中继的量子密钥分发系统，其特征在于，所述量子密钥分发设备所采用的两条或者两条以上的不同路径，是根据负载均衡策略选择的。

6. 根据权利要求 1-4 任一所述的基于可信中继的量子密钥分发系统，其特征在于，所述量子密钥分发设备还用于对在所述数据设备之间传输的数据进行加解密。

7. 根据权利要求 1-4 任一所述的基于可信中继的量子密钥分发系统，其特征在于，所述系统还包括：量子网关设备，所述量子密钥分发设备通过所述量子网关设备与所述数据设备相连，所述量子网关设备用于采用与其相连的量子密钥分发设备提供的量子密钥，对在所述数据设备之间传输的数据进行加解密。

8. 根据权利要求 1-4 任一所述的基于可信中继的量子密钥分发系统，其特征在于，所述量子密钥分发设备采用两条或者两条以上的不同路径与对端量子密钥分发设备进行密钥协商包括，在所述任一路径中采用波分复用技术和 / 或时分复用技术，实现多量子信道的密钥协商。

9. 根据权利要求 1 所述的基于可信中继的量子密钥分发系统，其特征在于，所述路由设备采用光分叉复用技术、光交叉互联技术、和 / 或光分组交换技术，对采用量子密钥加密后的数据进行转发。

10. 根据权利要求 1 所述的基于可信中继的量子密钥分发系统，其特征在于，所述量子密钥分发系统部署于云计算数据中心；

所述数据设备是指，云计算数据中心的服务器。

11. 根据权利要求 10 所述的基于可信中继的量子密钥分发系统，其特征在于，所述系统还包括：光交换机，所述路由设备通过所述光交换机与量子密钥分发设备相连。

12. 根据权利要求 10 所述的量子密钥分发系统，其特征在于，所述每个量子密钥分发设备与复数个功能相同的服务器相连；或者，所述每个量子密钥设备与复数个功能不同的

服务器相连。

13. 根据权利要求 10-12 任一所述的基于可信中继的量子密钥分发系统，其特征在于，所述系统还包括：具有量子密钥分发设备的云使用商网络；所述云使用商网络的量子密钥分发设备与所述云计算数据中心的两个或者两个以上量子密钥分发设备相连；

所述云使用商网络的量子密钥分发设备用于采用两条或者两条以上的不同路径与所述云计算数据中心的对端量子密钥分发设备进行密钥协商、并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

14. 根据权利要求 13 所述的基于可信中继的量子密钥分发系统，其特征在于，所述云使用商网络的量子密钥分发设备采用两条或者两条以上的不同路径与所述云计算数据中心的对端量子密钥分发设备进行密钥协商包括，在所述任一路径中采用波分复用技术和 / 或时分复用技术实现多量子信道的密钥协商。

15. 根据权利要求 13 所述的基于可信中继的量子密钥分发系统，其特征在于，所述云使用商网络的量子密钥分发设备的数量为两个或者两个以上，其中每个量子密钥分发设备都与所述云计算数据中心的两个或者两个以上量子密钥分发设备相连。

16. 根据权利要求 1 所述的基于可信中继的量子密钥分发系统，其特征在于，所述量子密钥分发系统分别部署于分布式云计算网络的多个数据中心，所述数据设备是指各数据中心的服务器，所述多个数据中心之间通过量子密钥分发设备相连形成网状拓扑；

其中，所述量子密钥分发设备还用于采用两条或者两条以上的不同路径与位于不同数据中心的对端量子密钥分发设备进行密钥协商，并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

17. 根据权利要求 16 所述的基于可信中继的量子密钥分发系统，其特征在于，还包括：具有量子密钥分发设备的云使用商网络，所述云使用商网络通过其量子密钥分发设备与两个或者两个以上数据中心的量子密钥分发设备相连；

所述云使用商网络的量子密钥分发设备用于采用两条或者两条以上的不同路径与所述数据中心的对端量子密钥分发设备进行密钥协商、并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

18. 根据权利要求 17 所述的基于可信中继的量子密钥分发系统，其特征在于，所述云使用商网络的量子密钥分发设备采用两条或者两条以上的不同路径与所述数据中心的对端量子密钥分发设备进行密钥协商包括：在所述任一路径中采用波分复用技术和 / 或时分复用技术实现多量子信道的密钥协商。

19. 一种基于可信中继的量子密钥分发方法，其特征在于，所述方法在如权利要求 1 所述的量子密钥分发系统中实施，包括：

发送方量子密钥分发设备通过路由设备的中继、采用两条或者两条以上的不同路径，与接收方量子密钥分发设备进行密钥协商；

所述发送方或接收方量子密钥分发设备根据预先设定的策略，判断是否需要对通过所述密钥协商过程获取的共享密钥进行合并操作；

若是，所述发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作，生成新的共享密钥。

20. 根据权利要求 19 所述的基于可信中继的量子密钥分发方法，其特征在于，在进行

所述密钥协商之前，执行下述操作：

所述发送方量子密钥分发设备根据量子密钥分发系统的拓扑信息，选择与接收方量子密钥分发设备进行密钥协商的两条或者两条以上的不同路径。

21. 根据权利要求 20 所述的基于可信中继的量子密钥分发方法，其特征在于，所述发送方量子密钥分发设备在选择所述两条或者两条以上的不同路径后，执行下述操作：

通过经典信道，将每条路径信息发送给所述路径包含的路由设备以及接收方量子密钥分发设备；

相应的，在所述密钥协商过程中，所述路径包含的路由设备以及接收方量子密钥分发设备执行如下操作：

根据接收到的所述路径信息，对与其进行密钥协商的对端设备的身份进行验证；

若通过验证，与所述对端设备进行密钥协商并完成本节点的密钥中继操作；

否则，通知所述发送方量子密钥分发设备放弃相应路径的密钥协商过程。

22. 根据权利要求 19 所述的基于可信中继的量子密钥分发方法，其特征在于，所述采用两条或者两条以上的不同路径进行密钥协商，采用如下方式实现：

通过所述路由设备的动态选路功能，实现经由两条或者两条以上的不同路径进行所述密钥协商。

23. 根据权利要求 22 所述的基于可信中继的量子密钥分发方法，其特征在于，在完成所述密钥协商之后，执行下述操作：

所述发送方或接收方量子密钥分发设备通过获取本次密钥协商的路径信息，对参与每一条路径密钥协商过程的各个设备的身份合法性进行验证；

若检测到非法设备，则所述发送方和接收方量子密钥分发设备放弃经由相应路径协商获取的共享密钥。

24. 根据权利要求 19 所述的基于可信中继的量子密钥分发方法，其特征在于，所述两条或者两条以上的不同路径是指，其中任意两条路径都不包含相同的路由设备。

25. 根据权利要求 19-24 任一所述的基于可信中继的量子密钥分发方法，其特征在于，所述两条或者两条以上的不同路径，是根据负载均衡策略选择的。

26. 根据权利要求 19 所述的基于可信中继的量子密钥分发方法，其特征在于，在进行所述密钥协商之前，执行下述操作：

所述发送方和接收方量子密钥分发设备通过经典信道，对对方设备进行身份验证；若所述对方设备未通过所述身份验证，则结束本方法的执行。

27. 根据权利要求 19 所述的基于可信中继的量子密钥分发方法，其特征在于，所述发送方或接收方量子密钥分发设备根据预先设定的策略，判断是否需要对通过所述密钥协商过程获取的共享密钥进行合并操作，包括：

所述量子密钥分发设备获取经由每一条路径进行密钥协商的安全评估结果；

根据预先设定的策略及所述安全评估结果，判断是否需要执行所述合并操作；

若是，执行下述操作：

选取执行密钥合并操作的具体处理方式；

通过经典信道，与对端量子密钥分发设备协商并确认所述密钥合并的具体处理方式；

转到所述发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作的步骤执

行。

28. 根据权利要求 19-27 任一所述的基于可信中继的量子密钥分发方法，其特征在于，还包括：

所述发送方量子密钥分发设备使用最终获取的共享密钥对待传输数据进行加密，并经由路由设备转发给所述接收方量子密钥分发设备；

所述接收方量子密钥分发设备采用与所述发送方相同的共享密钥对接收到的数据进行解密。

29. 根据权利要求 19 所述的基于可信中继的量子密钥分发方法，其特征在于，所述方法应用于云计算数据中心；所述发送方和接收方量子密钥分发设备是指，与进行保密数据传输的源端和目的端服务器分别相连的量子密钥分发设备。

30. 根据权利要求 19 所述的基于可信中继的量子密钥分发方法，其特征在于，所述方法应用于由云计算数据中心和云使用商网络组成的系统中；

所述发送方和接收方量子密钥分发设备是指，云使用商网络的量子密钥分发设备、以及与云使用商网络进行保密数据传输的服务器相连的量子密钥分发设备，所述服务器位于所述云计算数据中心内。

31. 根据权利要求 19 所述的基于可信中继的量子密钥分发方法，其特征在于，所述方法应用于由分布式云计算数据中心和云使用商网络组成的系统中；

所述发送方和接收方量子密钥分发设备是指，与进行保密数据传输的源端和目的端服务器相连的量子密钥分发设备，所述源端和目的端服务器位于不同的云计算数据中心；或者，

云使用商网络的量子密钥分发设备、以及与云使用商进行保密数据传输的服务器相连的量子密钥分发设备，所述服务器位于所述分布式云计算数据中心内。

32. 一种基于可信中继的量子密钥分发装置，其特征在于，包括：

多路径协商单元，用于发送方量子密钥分发设备通过路由设备的中继、采用两条或者两条以上的不同路径，与接收方量子密钥分发设备进行密钥协商；

合并判断单元，用于所述发送方或接收方量子密钥分发设备根据预先设定的策略，判断是否需要对通过所述密钥协商过程获取的共享密钥进行合并操作；

合并执行单元，用于当所述合并判断单元的输出为“是”时，所述发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作，生成新的共享密钥。

33. 根据权利要求 32 所述的基于可信中继的量子密钥分发装置，其特征在于，所述装置还包括：

路径获取单元，用于在触发所述多路径协商单元工作之前，所述发送方量子密钥分发设备根据量子密钥分发系统的拓扑信息，选择与接收方量子密钥分发设备进行密钥协商的两条或者两条以上的不同路径。

34. 根据权利要求 33 所述的基于可信中继的量子密钥分发装置，其特征在于，所述装置还包括：

路径分发单元，用于在触发所述多路径协商单元工作之前，发送方量子密钥分发设备通过经典信道，将每条路径信息发送给所述路径包含的路由设备以及接收方量子密钥分发设备；

相应的，所述多路径协商单元除了包括实现其功能的本体子单元外，还包括路径验证子单元，所述路径验证子单元用于实现下述功能：所述路径包含的路由设备以及接收方量子密钥分发设备，根据接收到的所述路径信息，对与其进行密钥协商的对端设备的身份进行验证；若通过验证，与所述对端设备进行密钥协商并完成本节点的密钥中继操作；否则，通知所述发送方量子密钥分发设备放弃相应路径的密钥协商过程。

35. 根据权利要求 32 所述的基于可信中继的量子密钥分发装置，其特征在于，所述多路径协商单元具体用于，通过所述路由设备的动态选路功能，实现经由两条或者两条以上的不同路径进行所述密钥协商。

36. 根据权利要求 35 所述的基于可信中继的量子密钥分发装置，其特征在于，所述装置包括：

路径验证单元，用于在所述多路径协商单元执行完毕后，所述发送方或接收方量子密钥分发设备通过获取本次密钥协商的路径信息，对参与每一条路径密钥协商过程的各个设备的身份合法性进行验证；若检测到非法设备，则所述发送方和接收方量子密钥分发设备放弃经由相应路径协商获取的共享密钥。

37. 根据权利要求 32 所述的基于可信中继的量子密钥分发装置，其特征在于，所述装置还包括：

身份验证单元，用于在触发所述多路径协商单元工作之前，所述发送方和接收方量子密钥分发设备通过经典信道，对对方设备进行身份验证；若所述对方设备未通过所述身份验证，则结束本方法的执行。

38. 根据权利要求 32 所述的基于可信中继的量子密钥分发装置，其特征在于，所述合并判断单元包括：

安全评估结果获取子单元，用于所述量子密钥分发设备获取经由每一条路径进行密钥协商的安全评估结果；

策略判断子单元，用于所述量子密钥分发设备根据预先设定的策略及所述安全评估结果，判断是否需要执行所述合并操作；

选择协商子单元，用于所述量子密钥分发设备选取执行密钥合并操作的具体处理方式，以及通过经典信道，与对端量子密钥分发设备协商并确认所述密钥合并的具体处理方式，并触发所述合并执行单元工作。

39. 根据权利要求 32-38 任一所述的基于可信中继的量子密钥分发装置，其特征在于，所述装置还包括：

数据加密传输单元，用于所述发送方量子密钥分发设备使用最终获取的共享密钥对待传输数据进行加密，并经由路由设备转发给所述接收方量子密钥分发设备；

数据解密单元，用于所述接收方量子密钥分发设备采用与所述发送方相同的共享密钥对接收到的数据进行解密。

基于可信中继的量子密钥分发系统、方法及装置

技术领域

[0001] 本申请涉及量子密钥分发领域，具体涉及一种基于可信中继的量子密钥分发系统。本申请同时提供一种基于可信中继的量子密钥分发方法，以及一种基于可信中继的量子密钥分发装置。

背景技术

[0002] 量子密码作为量子力学和密码学的交叉产物，其安全性由量子力学基于原理保证，任何企图截获或测量量子密钥的操作都会改变量子状态，接收端可以通过量子态的改变判断通信过程中是否存在窃听者，从而可以确定是否舍弃此次密钥，由此给通信带来无条件安全的保障。目前采用 BB84 等量子密钥协商协议可以实现端到端的量子密钥分发 (Quantum Key Distribution-QKD)。

[0003] 随着端到端量子密钥分发技术的日益完善，人们开始关注 QKD 网络，一些公司和研究机构已经开始尝试以不同方式建立 QKD 网络，包括 :基于光学器件的 QKD 网络、基于可信中继的 QKD 网络、以及基于量子中继的纯量子网络。其中基于信任中继的 QKD 网络，可以同时保证多用户和长距离传输的要求，理论上甚至可以实现全球性的密钥分配网络，而且在现有技术条件下，这种网络易于实现，因此可信中继成为了实现大规模 QKD 网络架构的有效手段。例如 :欧洲建立的 SECOQC 量子保密通信网络、日本建立的东京高速量子网络、以及我国建立的量子政务网都采用了可信中继的手段。

[0004] 请参见附图 1，其为可信中继量子密钥传输模型的示意图，Alice 与 Bob 之间要进行保密通信，两者之间的密钥协商路径共包括了 3 个可信中继节点。首先发送方 Alice 先和可信中继节点 1 之间建立密钥分发链路，进行量子密钥协商，产生一个密钥 K1 ;随后，可信中继节点 1 和可信中继节点 2 之间建立密钥分发链路，进行量子密钥协商，产生一个共享密钥 K2，且把密钥 K1 用 K2 加密后传送给可信中继节点 2 ;..... 依此类推，最终 Bob 接收到用密钥 K4 加密的 K1，Bob 利用 K4 对其解密后获得 K1，Alice 与 Bob 之间就可以使用密钥 K1 进行保密通信了。

[0005] 通过上述对密钥中继过程的描述可以看出，基于可信中继的 QKD 网络要求中继节点必须是安全的，如果任何一个中继节点被攻破，整个路径都变得不安全了，数据通信的安全性和稳定性将受到很大影响 ;而且采用上述密钥中继方式，密钥成码量 (即 :密钥分发量) 也比较低，无法满足使用密钥量较大的应用场景的需求，例如 :云计算。

发明内容

[0006] 本申请提供一种基于可信中继的量子密钥分发系统，以解决现有的基于可信中继的量子密钥分发网络安全性低、密钥分发量低的问题。本申请另外提供一种基于可信中继的量子密钥分发方法，以及一种基于可信中继的量子密钥分发装置。

[0007] 本申请提供一种基于可信中继的量子密钥分发系统，包括 :

[0008] 量子密钥分发设备、用于中继密钥和转发加密数据的路由设备、以及用作数据传

输的源端或目的端的数据设备；所述每个量子密钥分发设备与至少一个所述路由设备相连，所述每个量子密钥分发设备与至少一个所述数据设备相连，所述路由设备彼此连接形成网状拓扑；

[0009] 其中，所述量子密钥分发设备用于采用两条或者两条以上的不同路径与对端量子密钥分发设备进行密钥协商、并采用预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

[0010] 可选的，所述量子密钥分发设备还用于在发起量子密钥协商之前，将本次量子密钥协商的路径信息发送给所述路径包含的路由设备以及接收方量子密钥分发设备；

[0011] 相应的，所述路由设备和所述接收方量子密钥分发设备还用于根据接收到的路径信息，对与其进行密钥协商的路由设备或量子密钥分发设备的身份进行验证。

[0012] 可选的，所述每个量子密钥分发设备与至少两个所述路由设备相连。

[0013] 可选的，所述两条或者两条以上的不同路径是指，其中任意两条路径都不包含相同的路由设备。

[0014] 可选的，所述量子密钥分发设备所采用的两条或者两条以上的不同路径，是根据负载均衡策略选择的。

[0015] 可选的，所述量子密钥分发设备还用于对在所述数据设备之间传输的数据进行加解密。

[0016] 可选的，所述系统还包括：量子网关设备，所述量子密钥分发设备通过所述量子网关设备与所述数据设备相连，所述量子网关设备用于采用与其相连的量子密钥分发设备提供的量子密钥，对在所述数据设备之间传输的数据进行加解密。

[0017] 可选的，所述量子密钥分发设备采用两条或者两条以上的不同路径与对端量子密钥分发设备进行密钥协商包括，在所述任一路径中采用波分复用技术和/或时分复用技术，实现多量子信道的密钥协商。

[0018] 可选的，所述路由设备采用光分叉复用技术、光交叉互联技术、和/或光分组交换技术，对采用量子密钥加密后的数据进行转发。

[0019] 可选的，所述量子密钥分发系统部署于云计算数据中心；

[0020] 所述数据设备是指，云计算数据中心的服务器。

[0021] 可选的，所述系统还包括：光交换机，所述路由设备通过所述光交换机与量子密钥分发设备相连。

[0022] 可选的，所述每个量子密钥分发设备与复数个功能相同的服务器相连；或者，所述每个量子密钥设备与复数个功能不同的服务器相连。

[0023] 可选的，所述系统还包括：具有量子密钥分发设备的云使用商网络；所述云使用商网络的量子密钥分发设备与所述云计算数据中心的两个或者两个以上量子密钥分发设备相连；

[0024] 所述云使用商网络的量子密钥分发设备用于采用两条或者两条以上的不同路径与所述云计算数据中心的对端量子密钥分发设备进行密钥协商、并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

[0025] 可选的，所述云使用商网络的量子密钥分发设备采用两条或者两条以上的不同路径与所述云计算数据中心的对端量子密钥分发设备进行密钥协商包括，在所述任一路径中

采用波分复用技术和/或时分复用技术实现多量子信道的密钥协商。

[0026] 可选的，所述云使用商网络的量子密钥分发设备的数量为两个或者两个以上，其中每个量子密钥分发设备都与所述云计算数据中心的两个或者两个以上量子密钥分发设备相连。

[0027] 可选的，所述量子密钥分发系统分别部署于分布式云计算网络的多个数据中心，所述数据设备是指各数据中心的服务器，所述多个数据中心之间通过量子密钥分发设备相连形成网状拓扑；

[0028] 其中，所述量子密钥分发设备还用于采用两条或者两条以上的不同路径与位于不同数据中心的对端量子密钥分发设备进行密钥协商，并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

[0029] 可选的，所述系统还包括：具有量子密钥分发设备的云使用商网络，所述云使用商网络通过其量子密钥分发设备与两个或者两个以上数据中心的量子密钥分发设备相连；

[0030] 所述云使用商网络的量子密钥分发设备用于采用两条或者两条以上的不同路径与所述数据中心的对端量子密钥分发设备进行密钥协商、并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

[0031] 可选的，所述云使用商网络的量子密钥分发设备采用两条或者两条以上的不同路径与所述数据中心的对端量子密钥分发设备进行密钥协商包括：在所述任一路径中采用波分复用技术和/或时分复用技术实现多量子信道的密钥协商。

[0032] 此外，本申请还提供一种基于可信中继的量子密钥分发方法，所述方法在上述量子密钥分发系统中实施，包括：

[0033] 发送方量子密钥分发设备通过路由设备的中继、采用两条或者两条以上的不同路径，与接收方量子密钥分发设备进行密钥协商；

[0034] 所述发送方或接收方量子密钥分发设备根据预先设定的策略，判断是否需要对通过所述密钥协商过程获取的共享密钥进行合并操作；

[0035] 若是，所述发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作，生成新的共享密钥。

[0036] 可选的，在进行所述密钥协商之前，执行下述操作：

[0037] 所述发送方量子密钥分发设备根据量子密钥分发系统的拓扑信息，选择与接收方量子密钥分发设备进行密钥协商的两条或者两条以上的不同路径。

[0038] 可选的，所述发送方量子密钥分发设备在选择所述两条或者两条以上的不同路径后，执行下述操作：

[0039] 通过经典信道，将每条路径信息发送给所述路径包含的路由设备以及接收方量子密钥分发设备；

[0040] 相应的，在所述密钥协商过程中，所述路径包含的路由设备以及接收方量子密钥分发设备执行如下操作：

[0041] 根据接收到的所述路径信息，对与其进行密钥协商的对端设备的身份进行验证；

[0042] 若通过验证，与所述对端设备进行密钥协商并完成本节点的密钥中继操作；

[0043] 否则，通知所述发送方量子密钥分发设备放弃相应路径的密钥协商过程。

[0044] 可选的，所述采用两条或者两条以上的不同路径进行密钥协商，采用如下方式实

现：

[0045] 通过所述路由设备的动态选路功能，实现经由两条或者两条以上的不同路径进行所述密钥协商。

[0046] 可选的，在完成所述密钥协商之后，执行下述操作：

[0047] 所述发送方或接收方量子密钥分发设备通过获取本次密钥协商的路径信息，对参与每一条路径密钥协商过程的各个设备的身份合法性进行验证；

[0048] 若检测到非法设备，则所述发送方和接收方量子密钥分发设备放弃经由相应路径协商获取的共享密钥。

[0049] 可选的，所述两条或者两条以上的不同路径是指，其中任意两条路径都不包含相同的路由设备。

[0050] 可选的，所述两条或者两条以上的不同路径，是根据负载均衡策略选择的。

[0051] 可选的，在进行所述密钥协商之前，执行下述操作：

[0052] 所述发送方和接收方量子密钥分发设备通过经典信道，对对方设备进行身份验证；若所述对方设备未通过所述身份验证，则结束本方法的执行。

[0053] 可选的，所述发送方或接收方量子密钥分发设备根据预先设定的策略，判断是否需要对通过所述密钥协商过程获取的共享密钥进行合并操作，包括：

[0054] 所述量子密钥分发设备获取经由每一条路径进行密钥协商的安全评估结果；

[0055] 根据预先设定的策略及所述安全评估结果，判断是否需要执行所述合并操作；

[0056] 若是，执行下述操作：

[0057] 选取执行密钥合并操作的具体处理方式；

[0058] 通过经典信道，与对端量子密钥分发设备协商并确认所述密钥合并的具体处理方式；

[0059] 转到所述发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作的步骤执行。

[0060] 可选的，所述方法还包括：

[0061] 所述发送方量子密钥分发设备使用最终获取的共享密钥对待传输数据进行加密，并经由路由设备转发给所述接收方量子密钥设备；

[0062] 所述接收方量子密钥分发设备采用与所述发送方相同的共享密钥对接收到的数据进行解密。

[0063] 可选的，所述方法应用于云计算数据中心；所述发送方和接收方量子密钥分发设备是指，与进行保密数据传输的源端和目的端服务器分别相连的量子密钥分发设备。

[0064] 可选的，所述方法应用于由云计算数据中心和云使用商网络组成的系统中；

[0065] 所述发送方和接收方量子密钥分发设备是指，云使用商网络的量子密钥分发设备、以及与云使用商网络进行保密数据传输的服务器相连的量子密钥分发设备，所述服务器位于所述云计算数据中心内。

[0066] 可选的，所述方法应用于由分布式云计算数据中心和云使用商网络组成的系统中；

[0067] 所述发送方和接收方量子密钥分发设备是指，与进行保密数据传输的源端和目的端服务器相连的量子密钥分发设备，所述源端和目的端服务器位于不同的云计算数据中

心；或者，

[0068] 云使用商网络的量子密钥分发设备、以及与云使用商进行保密数据传输的服务器相连的量子密钥分发设备，所述服务器位于所述分布式云计算数据中心内。

[0069] 相应的，本申请还提供一种基于可信中继的量子密钥分发装置，包括：

[0070] 多路径协商单元，用于发送方量子密钥分发设备通过路由设备的中继、采用两条或者两条以上的不同路径，与接收方量子密钥分发设备进行密钥协商；

[0071] 合并判断单元，用于所述发送方或接收方量子密钥分发设备根据预先设定的策略，判断是否需要对通过所述密钥协商过程获取的共享密钥进行合并操作；

[0072] 合并执行单元，用于当所述合并判断单元的输出为“是”时，所述发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作，生成新的共享密钥。

[0073] 可选的，所述装置还包括：

[0074] 路径获取单元，用于在触发所述多路径协商单元工作之前，所述发送方量子密钥分发设备根据量子密钥分发系统的拓扑信息，选择与接收方量子密钥分发设备进行密钥协商的两条或者两条以上的不同路径。

[0075] 可选的，所述装置还包括：

[0076] 路径分发单元，用于在触发所述多路径协商单元工作之前，发送方量子密钥分发设备通过经典信道，将每条路径信息发送给所述路径包含的路由设备以及接收方量子密钥分发设备；

[0077] 相应的，所述多路径协商单元除了包括实现其功能的本体子单元外，还包括路径验证子单元，所述路径验证子单元用于实现下述功能：所述路径包含的路由设备以及接收方量子密钥分发设备，根据接收到的所述路径信息，对与其进行密钥协商的对端设备的身份进行验证；若通过验证，与所述对端设备进行密钥协商并完成本节点的密钥中继操作；否则，通知所述发送方量子密钥分发设备放弃相应路径的密钥协商过程。

[0078] 可选的，所述多路径协商单元具体用于，通过所述路由设备的动态选路功能，实现经由两条或者两条以上的不同路径进行所述密钥协商。

[0079] 可选的，所述装置包括：

[0080] 路径验证单元，用于在所述多路径协商单元执行完毕后，所述发送方或接收方量子密钥分发设备通过获取本次密钥协商的路径信息，对参与每一条路径密钥协商过程的各个设备的身份合法性进行验证；若检测到非法设备，则所述发送方和接收方量子密钥分发设备放弃经由相应路径协商获取的共享密钥。

[0081] 可选的，所述装置还包括：

[0082] 身份验证单元，用于在触发所述多路径协商单元工作之前，所述发送方和接收方量子密钥分发设备通过经典信道，对对方设备进行身份验证；若所述对方设备未通过所述身份验证，则结束本方法的执行。

[0083] 可选的，所述合并判断单元包括：

[0084] 安全评估结果获取子单元，用于所述量子密钥分发设备获取经由每一条路径进行密钥协商的安全评估结果；

[0085] 策略判断子单元，用于所述量子密钥分发设备根据预先设定的策略及所述安全评估结果，判断是否需要执行所述合并操作；

[0086] 选择协商子单元，用于所述量子密钥分发设备选取执行密钥合并操作的具体处理方式，以及通过经典信道，与对端量子密钥分发设备协商并确认所述密钥合并的具体处理方式，并触发所述合并执行单元工作。

[0087] 可选的，所述装置还包括：

[0088] 数据加密传输单元，用于所述发送方量子密钥分发设备使用最终获取的共享密钥对待传输数据进行加密，并经由路由设备转发给所述接收方量子密钥设备；

[0089] 数据解密单元，用于所述接收方量子密钥分发设备采用与所述发送方相同的共享密钥对接收到的数据进行解密。

[0090] 与现有技术相比，本申请具有以下优点：

[0091] 本申请提供的基于可信中继的量子密钥分发系统及方法，在路由设备彼此连接形成网状拓扑的基础上，在发送方量子密钥分发设备与接收方量子密钥分发设备之间多路径地进行密钥协商、并采用预先设定的策略确定是否需要对所述多路径协商得到的共享密钥进行合并、并执行相应的合并操作。采用上述技术方案，在网络安全性比较高的应用场景下，由于同时使用多条路径进行密钥协商，可以有效提高量子密钥的分发量；在网络安全性比较低的应用场景下，则可以对经由不同路径协商的密钥进行合并生成新的共享密钥，从而有效抵御对可信中继节点的攻击等安全隐患，提高整个量子密钥分发网络的安全性。

附图说明

[0092] 图 1 是基于可信中继的量子密钥传输模型的示意图；

[0093] 图 2 是本申请的一种基于可信中继的量子密钥分发系统的示意图；

[0094] 图 3 是本实施例提供的云使用商访问数据中心的系统架构的示意图；

[0095] 图 4 是本实施例提供的分布式数据中心及云使用商访问分布式数据中心的系统架构示意图；

[0096] 图 5 是本申请的一种基于可信中继的量子密钥分发方法的实施例的流程图；

[0097] 图 6 是本实施例提供的采用多路径进行密钥协商的处理流程图；

[0098] 图 7 是本申请的一种基于可信中继的量子密钥分发装置的实施例的示意图。

具体实施方式

[0099] 在下面的描述中阐述了很多具体细节以便于充分理解本申请。但是本申请能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本申请内涵的情况下做类似推广，因此本申请不受下面公开的具体实施的限制。

[0100] 在本申请中，提供了一种基于可信中继的量子密钥分发系统，一种基于可信中继的量子密钥分发方法，以及一种相应的装置。在下面的实施例中逐一进行详细说明。

[0101] 请参考图 2，其为本申请的一种基于可信中继的量子密钥分发系统的示意图，所述量子密钥分发系统包括：量子密钥分发设备、用于中继密钥和转发加密数据的路由设备、以及用作数据传输的源端或目的端的数据设备；所述每个量子密钥分发设备与至少一个所述路由设备相连，所述每个量子密钥分发设备与至少一个所述数据设备相连，所述路由设备彼此连接形成网状拓扑；其中，所述量子密钥分发设备用于采用两条或者两条以上的不同路径与对端量子密钥分发设备进行密钥协商、并采用预先设定的策略确定是否需要对所述

协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

[0102] 现有的基于信任中继的量子密钥分发网络，一方面只要有任意一个中继节点被攻破，就无法保证密钥的安全性，另一方面密钥分发量也比较低。针对上述问题，本申请的技术方案提供了一种新的密钥协商方式，在路由设备彼此连接形成网状拓扑的基础上，量子密钥分发设备采用两条或者两条以上的不同路径与对端量子密钥分发进行密钥协商。本申请实施例所述的两条或者两条以上的不同路径是指，其中任意两条路径所包含的路由设备都不完全相同。

[0103] 在具体实施时，可以采用静态路由（也称指定路由）方式选择进行量子密钥协商的不同路径。具体说，量子密钥分发设备可以通过网络泛洪等机制维护整个网络拓扑信息，从而可以在发起量子密钥协商过程之前，采用负载均衡策略，综合考虑网络拓扑中路由设备的负载状况和链路的占用状况，选择相对空闲的路由设备以及链路，组成两条或者多条不同的路径，每条路径所涉及的各路由设备按照所述路径进行密钥协商与中继。此外，也可以采用动态路由方式，即，量子密钥分发设备与路由设备采用逐跳动态选路的方式，根据本地存储的路由表信息，基于负载均衡等策略选择到达对端量子密钥分发设备的下一跳路由。

[0104] 在路由设备彼此连接形成网状拓扑的基础上，本实施例还提供一种优选实施方式，每个量子密钥分发设备与至少两个路由设备相连，由于路由设备彼此之间采用网状拓扑相连，因此量子密钥分发设备进行密钥协商时可以采用完全不相关的多条路径，即：其中任意两条路径都不包含相同的路由设备，也就是说任意两条路径都没有共用的路由设备。

[0105] 请参见图2，其中数据设备A与数据设备B之间要进行保密数据传输，量子密钥分发设备A1采用路径1和路径2与对端量子密钥分发设备B1进行密钥协商，其中路径1包含路由设备R1、R2、R3，路径2包含路由设备R4、R5，由于路径1与路径2不包含相同的路由设备，因此是两条完全不相关路径。

[0106] 量子密钥分发设备采用两条或者两条以上的不同路径与对端量子密钥分发设备进行密钥协商。在每一条路径中，每两个相邻设备利用彼此之间的QKD链路通过密钥传输、数据筛选、数据协调以及隐私放大等阶段获取两者之间的共享密钥，并逐段利用所述共享密钥对发送方量子密钥分发设备获取的共享密钥进行“加密－解密－加密……解密”的中继转发操作，最终接收方量子密钥分发设备与发送方量子密钥分发设备获取相同的共享密钥。由于采用多路径协商，因此收发双方可以获取多个共享密钥。例如，在图2所示的例子中，通过两条路径的密钥协商过程，量子密钥分发设备A1和量子密钥分发设备B1获取了两个共享密钥key1和key2。

[0107] 对于获取的两个或者两个以上的共享密钥，收发双方的量子密钥协商设备可以采用预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。

[0108] 所述预先设定的策略，包括从安全性角度出发，依据密钥协商过程中的误码率和/或风险概率来确定是否需要执行密钥合并操作。在通过中继方式进行密钥协商的过程中，每两个相邻设备在协商过程中，都会对本次密钥协商的误码率进行估算，还可以进一步计算可能存在的各种攻击（例如，强光致盲攻击、光束分离攻击、死时间攻击等）的风险概率，并可以将每一条路径的每一段中继链路的误码率估计值和/或风险概率汇总起来，如果某

一条路径的上述数据超出了预先设定的安全范围，则可以认为该路径的密钥协商过程存在被攻击的风险，中继节点（即：本实施例所述的路由设备）也存在被攻破的安全隐患，因此在这种情况下，可以对协商得到的共享密钥进行合并的方式，从而抵御中继节点被攻破带来的风险，提高量子密钥分发的安全性。

[0109] 所述对协商得到的共享密钥进行合并是指，采用预先设定的算法，对通过多路径协商得到的多个共享密钥进行处理、生成新密钥的过程。例如：可以对所述多个共享密钥执行异或操作，或者先移位再执行异或操作等。具体采用何种合并算法，本实施例不做具体限定。

[0110] 例如，在图 2 所示的例子中，量子密钥分发设备 A1 和 B1 通过路径 1 协商得到共享密钥 key1，通过路径 2 协商得到共享密钥 key2，通过将路径 1 中的每一段中继链路的误码率估计值和风险概率进行汇总后，计算出了表征密钥协商过程安全性的指标值，该指标值超出了预先设定的安全范围，说明经由路径 1 的密钥协商过程可能受到攻击，各中继节点的安全性也存在隐患，而路径 2 的相应指标值没有超出所述安全范围，因此量子密钥分发设备 A1 和 B1 采用预先设定的异或算法对 key1 和 key2 执行合并操作，生成新的密钥 key3，即：key3 = key1xor key2，并采用 key3 对数据设备 A 与数据设备 B 之间传输的数据进行加解密。

[0111] 在上述例子中，如果针对路径 1 和路径 2 汇总得到的安全指标值，都没有超出预先设定的安全范围，也就是说基于路径 1 和路径 2 的密钥协商过程都是安全的，各中继节点也是安全的，则可以不执行密钥合并操作，那么通过本次协商，量子密钥分发设备 A1 和 B1 得到了两个共享密钥，并可以将这两个密钥用于数据设备 A 和 B 之间的保密通信。

[0112] 通过上述分析可以看出，本实施例提供的量子密钥分发系统，在网络安全性比较高的应用场景下，由于使用多条路径进行密钥协商，从而通过提高路由设备以及链路利用率，达到提高密钥分发量的目的；在网络安全性比较低的应用场景下，即使其中有某一条或者几条路径的中继节点被攻破，协商得到的相应密钥不再安全，但只要其中有一条路径是安全的（各中继节点均没有被攻击），仍然可以通过对不同路径密钥的合并操作生成新的、安全的共享密钥，从而可以抵御部分中继节点被攻击的安全隐患，提高整个量子密钥分发网络的安全性。

[0113] 需要说明的是，上述给出的是一个具体的例子，在其他实施方式中，可以进行相应的变更或者调整。例如，可以不采用汇总路径中每条中继链路的误码率以及风险概率，而是从中抽取某几条链路进行汇总；也可以不采用误码率和 / 或风险概率作为安全性的评估参数，而是采用其他指标，例如，通过监控中继节点的安全性而获取的指标等；如何根据评估参数或者指标确定是否需要进行合并的策略也可以根据实际应用需要进行调整；具体的合并算法也可以与本例不同。上述这些都是具体实施方式的变更，都不偏离本申请的核心，都在本申请的保护范围之内。

[0114] 进一步地，针对量子密钥协商过程中可能存在的中间人攻击（中间人采用截获、重发的方式进行攻击），本实施例还提供了一种采用路径验证技术的优选实施方式。具体说，收发双方的量子密钥分发设备在协商密钥之前，由发起量子密钥协商的量子密钥分发设备通过经典信道把本次进行密钥协商的路径信息发给该路径包含的各个路由节点以及接收方量子密钥分发设备。由于每条路径都是由一段一段的中继链路组成的，所述路径信

息包括路径中每段链路的节点信息，因此也称为路径链信息。

[0115] 路由设备和接收方量子密钥分发设备存储接收到的路径链信息，并在随后的量子密钥协商过程中，根据所述路径链信息，对与其进行密钥协商的路由设备或量子密钥分发设备的身份合法性进行验证，如果发现与所述路径链信息不一致，则说明可能存在中间人攻击，那么可以放弃本次量子密钥协商过程，重新选择其他路径进行量子密钥协商。

[0116] 上面描述的实施方式通常与静态路由方式配合使用，即，量子密钥协商过程的发起方在启动量子密钥协商过程之前，就可以获知本次协商的完整路径信息，因此可以预先将路径信息发送给该路径包含的设备。

[0117] 在具体实施过程中，如果采用动态路由方式，也可以通过在网络内部设置监视节点实现与上述类似的路径链验证功能。具体说，监视节点通过对密钥协商过程的监控，可以获取本协商过程所经路径中的各个中继节点的信息，并通过对该信息的分析，辨别是否存在异常的中间节点，从而判断是否存在中间人攻击，如果存在，则放弃本次密钥协商过程获取的共享密钥。

[0118] 采用路径链验证技术，可以对量子密钥协商过程中各个节点身份的合法性进行验证，避免中间人攻击，进一步保证量子密钥协商过程的安全性。

[0119] 本实施例提供的技术方案，在前面描述的多路径进行密钥协商的基础上，还进一步采用了波分复用技术(Wavelength Division Multiplex,WDM)实现多量子信道的密钥协商。所述WDM技术，是一种为了充分利用单模光纤低损耗区巨大的带宽资源，根据每一个信道光波频率（或波长）的不同而将光纤的低损耗窗口划分成若干个信道的技术，用不同的波长传送各自的信息，即使在同一根光纤上也不会相互干扰，以达到提高光纤的通信容量。

[0120] 具体到本实施例，在进行多路径密钥协商的任一路径中，量子密钥分发设备与作为中继节点的路由设备之间，以及所述路由设备之间在进行量子密钥协商时，可以同时使用不同的光波长协商密钥，从而提高密钥的分发量。

[0121] 类似的，还可以在上述密钥协商过程中，采用时分复用技术，达到多信道传输的目的，提高密钥的分发量。所述时分复用技术是指，采用同一物理连接的不同时段来传输不同的信号。波分复用和时分复用都属于比较成熟的现有技术，此处不再赘述。

[0122] 在本实施例提供的量子密钥分发系统中，所述量子密钥分发设备除了具备多路径密钥协商功能，还可以用于对在数据设备之间传输的数据进行加解密。在图2所示的例子中，量子密钥分发设备A1使用与B1协商得到的共享密钥，对数据设备A发送的数据进行加密；加密后的数据通过各路由设备转发给量子密钥分发设备B1，B1同样采用与A1协商的共享密钥对接收到的数据进行解密，然后将解密后的数据发送给数据设备B，从而完成了数据设备A与数据设备B之间的保密通信。

[0123] 在其他实施方式中，也可以将对数据进行加解密的功能从量子密钥分发设备中剥离出来，交由量子网关完成。也就是说，在上述量子密钥分发系统中，还可以包括量子网关设备，量子密钥分发设备通过量子网关设备与数据设备相连。所述量子密钥分发设备负责多路径地进行密钥协商，并将协商获取的量子密钥提供给与其相连的量子网关设备，量子网关设备则采用所述量子密钥，对在所述数据设备之间传输的数据进行加解密。

[0124] 在具体实施中，可以根据实际需要从上述两种加解密方式中选择其中一种。加密后的数据经由路由设备的转发，最终到达对端的量子密钥分发设备，并经解密后发送给本

次数据传输的目的端数据设备。在路由设备对加密数据进行转发的过程中，可以采用现有的光分插复用技术、光交叉互联技术、光分组交换技术中的一种或者几种，由于采用多路径密钥协商方式，提高了密钥的分发量，因此加密数据的交互吞吐量也可以得到有效的提高。上述光传输技术属于比较成熟的现有技术，下面对仅对其作简要说明。

[0125] 1）光分插复用（Optical Add/Drop Multiplex，OADM）技术，一种用滤光器或分用器从波分复用传输链路插入或分出光信号的技术。在WDM系统中有选择地上／下所需速率、格式和协议类型的光波长信号，即：在节点上只分接／插入所需的波长信号，其它波长信号则光学透明地通过这个节点；

[0126] 2）光分叉互联技术，用于光纤网络节点的设备，通过对光信号进行交叉连接，能够有效灵活地管理光纤传输网络，是实现可靠的网络保护／恢复以及自动配线和监控的重要手段；

[0127] 3）光分组交换技术，全光分组交换可分成两大类：时隙和非时隙。在时隙网络中，分组长度是固定的，并在时隙中传输。时隙的长度应大于分组的时限，以便在分组的前后设置保护间隔。在非时隙网络中，分组的大小是可变的，而且在交换之前，不需要排列，异步的，自由地交换每一个分组。

[0128] 在具体实施中，所述量子密钥分发系统，在进行密钥协商或数据加解密交互的过程中，可以综合运用波分复用、时分复用以及上述光传输技术，以达到多路径密钥协商、提高密钥分发量及数据交互吞吐量的目的。

[0129] 至此，描述了本实施例提供的基于可信中继的量子密钥分发系统，所述系统由于采用了多路径密钥协商机制，因此可以取得提高密钥分发量以及提高密钥分发安全性的有益效果。

[0130] 考虑到现有的云计算环境中，云骨干网的各服务器之间重要数据的交互、云网络中各个数据中心之间数据的远程备份及交互、云使用商访问云资源等都对密钥安全提出了较高的要求。经典网络中的加密方法无法提供可靠的安全性保障，而现有的各种小型量子密钥分发网络也无法满足云密钥安全分发的需求，包括，量子密钥分发网络的吞吐量、成码量；密钥的传输距离；多用户需求；保证任意用户可以与云骨干网进行通信以及和现有公共网络融合等。

[0131] 基于上述考虑，可以将本实施例提供的基于可信中继的量子密钥分发系统应用到云网络架构中，从而解决上述问题。下面从云骨干网（数据中心）、云使用商访问数据中心，以及分布式数据中心三个方面作进一步说明。

[0132] （一）云骨干网系统架构。

[0133] 在云运营商的云骨干网中（即：本实施例所述的数据中心），通常包含各种服务器集群，比如文件服务器集群、Web服务器集群、应用服务器集群、管理服务器集群、目录服务器集群，每个集群都包含若干台服务器，这些服务器之间交互的数据量通常比较大，对密钥的分发量、整个网络的数据吞吐量的要求都比较高。

[0134] 将本实施例提供的基于可信中继的量子密钥分发系统部署于上述的云计算数据中心，所述用作数据传输的源端或者目的端的数据设备，就是上述的各种服务器。与每个量子密钥分发设备相连的复数个服务器可以是功能相同的服务器（例如都是文件服务器），也可以是功能彼此不同的服务器（例如，web服务器和管理服务器等）。本实施例所述的复

数个是指两个或者两个以上。

[0135] 由于现有的云计算数据中心通常是采用三层架构，而本实施例提供的量子密钥分发系统采用的是基于路由设备的扁平架构，为了实现现有三层架构与扁平架构之间的平滑过渡，同时也为了扩展量子密钥分发设备的有限端口数量，实现更多服务器的接入，可以在部署了本实施例提供的量子密钥分发系统的数据中心网络架构中引入光交换机，一个路由设备可以与一个或者一个以上光交换机相连，一个光交换机与一个或者一个以上的量子密钥分发设备相连。

[0136] 由于将本实施例提供的量子密钥分发系统部署于云计算数据中心，为了实现数据中心服务器之间的保密通信，与所述服务器相连的量子密钥分发设备采用两条或者两条以上的路径进行密钥协商，并采用预先设定的策略执行所需的密钥合并操作。此外，在本实施例前面描述的路径链验证、波分复用、时分复用以及其他光传输技术等也都可以应用于所述数据中心，以达到提高密钥分发量、数据交互吞吐量，以及提高密钥分发过程安全性的目的，从而满足云计算数据中心的需求，对于上述内容请参见上文的相关文字，此处不再赘述。

[0137] （二）云使用商访问数据中心的系统架构。

[0138] 在（一）中将本实施例提供的量子密钥分发系统部署于云计算数据中心的基础上，为了满足云使用商访问数据中心的需求，本系统还可以包括：具有量子密钥分发设备的云使用商网络；所述云使用商网络的量子密钥分发设备与所述云计算数据中心的两个或者两个以上量子密钥分发设备相连。

[0139] 请参见图3，其为本实施例提供的云使用商访问数据中心的系统架构示意图，在该例子中，包括一个云计算数据中心、两个云使用商网络（甲网络和乙网络），云使用商甲网络使用其量子密钥分发设备、通过接入光纤与云计算数据中心的三个量子密钥分发设备相连，云使用商乙网络使用其量子密钥分发设备、通过接入光纤与云计算数据中心的两个量子密钥分发设备相连。云使用商网络中通常还包括内部网关以及用于访问云计算数据中心的多种终端设备，此示意图中没有示出。

[0140] 所述云使用商网络的量子密钥分发设备用于采用两条或者两条以上的不同路径与所述云计算数据中心的对端量子密钥分发设备进行密钥协商、并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。通过多路径协商机制，提高量子密钥分发过程的安全性以及量子密钥的分发量。

[0141] 所述云使用商网络的量子密钥分发设备在任一路径的密钥协商过程中，也可以采用波分复用技术和/或时分复用技术实现多量子信道的密钥协商，以进一步提高密钥分发量。

[0142] 此外，在本实施例前面描述的路径链验证、以及光分插复用技术、光交叉互联技术、光分组交换技术等也都可以应用在云使用商访问数据中心的系统架构中，以达到提高密钥分发量及数据交互吞吐量的目的。

[0143] 需要说明的是，在具体实施中，根据实际业务的需要，云使用商网络也可以设置两个或者两个以上的量子密钥分发设备，其中每个量子密钥分发设备都与所述云计算数据中心的两个或者两个以上量子密钥分发设备相连。

[0144] （三）分布式数据中心的系统架构。

[0145] 云供应商通过数据中心向云使用商提供业务服务的同时，通常还使用备份数据中心进行数据备份，或者云供应商采用双活数据中心为云使用商提供业务服务，另外，随着云计算技术的发展，云供应商仅提供单一的数据中心已经无法满足云使用商的需求，因此通常在不同的地域设置多个数据中心。在上述基于多数据中心的分布式架构下，也可以通过部署本实施例提供的量子密钥分发网络，满足分布式云计算对密钥分发量以及密钥安全性的要求。

[0146] 具体说，所述量子密钥分发系统分别部署于分布式云计算网络的多个数据中心，所述数据设备是指各数据中心的服务器，所述多个数据中心之间通过量子密钥分发设备相连形成网状拓扑。

[0147] 请参见图 4，其为本实施例提供的分布式数据中心及云使用商访问数据中心的系统架构示意图，在该例子中，包括云供应商的 4 个双活数据中心，这 4 个数据中心之间通过量子密钥分发设备相连形成网状拓扑。这 4 个数据中心彼此进行数据备份或者数据传输时，作为源端的数据中心的量子密钥分发设备可以采用两条或者两条以上的不同路径与位于不同数据中心的对端量子密钥分发设备进行密钥协商，并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。通过多路径协商机制，提高量子密钥分发过程的安全性以及量子密钥的分发量。

[0148] 进一步地，上述系统还可以包括具有量子密钥分发设备的云使用商网络，所述云使用商网络通过其量子密钥分发设备与两个或者两个以上数据中心的量子密钥分发设备相连。

[0149] 在图 4 所示的例子中，包括 2 个云使用商网络（甲网络、乙网络），甲、乙网络使用各自的量子密钥分发设备、通过接入光纤分别与两个数据中心的量子密钥分发设备相连。云使用商网络中通常还包括内部网关以及用于访问云计算数据中心的多种终端设备，此示意图中没有示出。

[0150] 所述云使用商网络的量子密钥分发设备用于采用两条或者两条以上的不同路径与所述数据中心的对端量子密钥分发设备进行密钥协商、并采用所述预先设定的策略确定是否需要对所述协商得到的共享密钥进行合并、并在需要时执行相应的合并操作。通过多路径协商机制，提高量子密钥分发过程的安全性以及量子密钥的分发量。

[0151] 所述云使用商网络的量子密钥分发设备在任一路径的密钥协商过程中，也可以采用波分复用技术和 / 或时分复用技术实现多量子信道的密钥协商，以进一步提高密钥分发量。

[0152] 此外，在本实施例前面描述的路径链验证、以及光分插复用技术、光交叉互联技术、光分组交换技术等也都可以应用在分布式云计算数据中心及云使用商访问数据中心的系统架构中，以达到提高密钥分发量及数据交互吞吐量的目的。

[0153] 在上述实施例中提供了一种基于可信中继的量子密钥分发系统，在此基础上，本申请还提供一种基于可信中继的量子密钥分发方法，所述方法在上述量子密钥分发系统中实施。请参考图 5，其为本申请提供的一种基于可信中继的量子密钥分发方法的实施例的流程图，本实施例与第一实施例内容相同的部分不再赘述，下面重点描述不同之处。本申请提供的基于可信中继的量子密钥分发方法包括：

[0154] 步骤 501：发送方量子密钥分发设备通过路由设备的中继、采用两条或者两条以

上的不同路径，与接收方量子密钥分发设备进行密钥协商。

[0155] 本技术方案的核心在于，多路径地进行量子密钥协商，一方面可以提高量子密钥的成码量，另一方面可以抵御对中继节点（即：路由设备）的攻击。为了进一步提高量子密钥协商过程的安全性，在本步骤中还提供了收发双方进行身份验证、以及对密钥协商路径进行验证的优选实施方式，下面结合附图 6 对本步骤作进一步说明。

[0156] 步骤 501-1：所述发送方和接收方量子密钥分发设备通过经典信道，对对方设备进行身份验证。

[0157] 具体说，发送方量子密钥分发设备（简称 A 设备）首先通过经典信道，向接收方量子密钥分发设备（简称 B 设备）发送密钥协商请求，请求中至少包含 A 设备的身份信息（例如，账户信息）。该请求经过若干个路由器设备的转发到达 B 设备，B 设备验证所述请求中携带的 A 设备身份的合法性，如果合法则向 A 设备发送应答，同时可以在应答中携带 B 设备的身份信息，同理，A 设备收到所述应答后对 B 设备的身份进行验证。如果经过上述验证过程，A 设备和 B 设备都认为对方设备是合法的，则可以继续后续的处理，否则本方法结束。

[0158] 上面给出了收发双方量子密钥分发设备通过经典信道进行身份验证的一种方式，在具体实施过程中，也可以采用其他身份验证方式，例如，采用数字证书等方式，只要能够确认即将与其进行量子密钥协商的对端量子密钥分发设备的身份是否合法即可。

[0159] 步骤 501-2：所述发送方量子密钥分发设备根据量子密钥分发系统的拓扑信息，选择与接收方量子密钥分发设备进行密钥协商的两条或者两条以上的不同路径。

[0160] 发送方量子密钥分发设备根据预先获取的网络拓扑信息，选择两条或者两条以上的不同路径，其中任意两条路径所包含的路由设备都不完全相同，也就说，允许不同的路径之间共用相同的路由设备。所述发送方量子密钥分发设备在进行路径选择时，可以采用负载均衡策略。

[0161] 步骤 501-3：发送方量子密钥分发设备通过经典信道，将每条路径信息发送给所述路径包含的路由设备以及接收方量子密钥分发设备。

[0162] 所述路径信息中包含了路径中每个节点的相关信息，所述发送方量子密钥分发设备选择完路径后，可以通过经典信道将每条路径的路径信息发送给该路径包含的路由设备及接收方量子密钥分发设备，供这些设备在中继量子密钥的过程中对对方身份进行验证（参见步骤 501-4 中的说明）。

[0163] 步骤 501-4：收发双方的量子密钥协商设备及路由设备通过所述两条或者两条以上的不同路径进行密钥协商，并在该过程中进行路径验证。

[0164] 为了满足远距离传输的需求，本技术方案采用了信任中继的方式，因此在每一条路径中，每两个相邻设备可以通过量子信道的密钥协商过程获取共享密钥，并逐段实现密钥的中继转发，最终使得收发双方的量子密钥分发设备获取相同的共享密钥。在具体实施中，每两个相邻设备之间的共享密钥，可以采用上述动态协商的方式获取，也可以采用出厂预置的初始密钥或双方预先协商好的共享密钥，同样可以实现上述中继功能。

[0165] 由于并发进行密钥协商的多条路径，通常是采用负载均衡机制选取的，可能共用相同的路由设备，因此路由设备在实现上述中继功能时，可能只是执行转发操作，也可能需要通过各种复用手段执行合并操作，或者通过相应的解复用手段执行相应的分拆操作，最终多路径地完成端到端的量子密钥协商过程。

[0166] 进一步地，为了防止中间人攻击，本技术方案还采用了路径验证技术，每个路由设备以及接收方量子密钥分发设备，在与相邻设备进行密钥协商及执行相应的中继操作之前，先根据接收到的路径信息，对所述相邻设备的身份进行验证；若通过验证，与所述相邻设备进行密钥协商并完成本节点的密钥中继操作；否则，通知发送方量子密钥分发设备放弃相应路径的密钥协商过程。

[0167] 需要说明的是，上面给出的是采用静态选路方式实现多路径密钥协商的实施过程。在具体实施中，也可以通过路由设备基于负载均衡策略进行动态选路，实现经由两条或者两条以上的不同路径进行所述密钥协商。如果采用动态选路方式，可以在量子密钥协商过程完成后，进行路径验证，即：发送方或接收方量子密钥分发设备或者监视节点，通过收集本次密钥协商的路径信息，对参与每一条路径密钥协商过程的各个设备身份的合法性进行验证；若检测到非法设备（说明可能存在中间人攻击），则通知发送方和接收方量子密钥分发设备放弃经由相应路径协商获取的共享密钥。

[0168] 此外，为了最大限度地抵御对中继节点的攻击，本实施例还提供一种优选实施方式，即：本步骤进行端到端量子密钥协商采用的路径是完全不相关的多条路径，也就说，对任意一个中继节点的攻击只可能对一条路径的安全性产生影响，而不会影响到其他路径。

[0169] 步骤 502：所述发送方或接收方量子密钥分发设备根据预先设定的策略，判断是否需要对通过所述密钥协商过程获取的共享密钥进行合并操作；若是，执行步骤 503。

[0170] 通过步骤 501 的多路径协商过程，收发双方的量子密钥分发设备通常可以获取多个共享密钥（与路径数目一致），在本步骤中通过预先设定的策略判断是否需要执行合并操作。

[0171] 发送方或者接收方量子密钥分发设备获取经由每一条路径进行密钥协商的安全评估结果（例如包括误码率、丢包率等）；如果任一路径的所述安全评估结果超出了所述策略中设定的安全范围，则说明该路径或中继节点存在安全隐患，需要针对多路径获取的共享密钥执行相应的合并操作，以保证密钥的安全性。

[0172] 在具体实施中，可以采用多种密钥合并方式，因此作出上述判断的量子密钥分发设备可以选取执行密钥合并操作的具体处理方式，并通过经典信道，与对端量子密钥分发设备协商并确认所述密钥合并的具体处理方式，从而使得收发双方的量子密钥分发设备能够在步骤 503 中对共享密钥进行相同的合并处理，从而双方最终得到新的共享密钥。

[0173] 步骤 503：所述发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作，生成新的共享密钥。

[0174] 本实施例并不对合并操作所采用的算法，进行具体的限定。关于本步骤的说明，请参见“基于可信中继的量子密钥分发系统”实施例中的相关文字，此处不再赘述。

[0175] 通过上述步骤 501-503 描述的多路径密钥协商过程可以看出，在网络安全性比较高的应用场景下，收发双方的量子密钥分发设备可以同时协商获取多个共享密钥，提高密钥分发量；在网络安全性比较低的应用场景下，即使其中有某一条或者几条路径的中继节点被攻破，但只要其中有一条路径是安全的，仍然可以通过对不同路径密钥的合并操作生成新的、安全的共享密钥，从而提高整个量子密钥分发网络的安全性。

[0176] 相应的，发送方量子密钥分发设备可以使用最终获取的共享密钥对待传输数据进行加密，并经由路由设备转发给所述接收方量子密钥分发设备，接收方量子密钥分发设备

采用与所述发送方相同的共享密钥对接收到的数据进行解密。由于密钥分发量的提高，数据交互吞吐量也能得到相应提高。

[0177] 进一步地，可以将上述实施例描述的量子密钥分发方法，应用在云计算网络中，以满足云计算网络对云密钥的安全性、成码量、传输距离、以及数据吞吐量等各方面的要求。

[0178] （一）将所述方法应用在云骨干网络（数据中心）。

[0179] 为了实现云计算数据中心的任意两台服务器之间的保密数据传输，与所述服务器分别相连的量子密钥分发设备可以多路径地进行密钥协商，并用最终获取的共享密钥对数据进行加解密，从而实现数据的保密传输。

[0180] （二）将所述方法应用在云骨干网络（数据中心）和云使用商网络组成的系统中。

[0181] 为了实现云使用商网络与云计算数据中心的任一服务器之间的保密数据传输，云使用商网络的量子密钥分发设备和与所述服务器相连的量子密钥分发设备，可以多路径地进行密钥协商，并用最终获取的共享密钥对数据进行加解密，从而实现数据的保密传输。

[0182] （三）将所述方法应用在由分布式云计算数据中心和云使用商网络组成的系统中。

[0183] 为了实现位于不同云计算数据中心的任意两台服务器之间的保密数据传输（数据备份或者是数据访问），与所述服务器分别相连的量子密钥分发设备可以多路径地进行密钥协商，并用最终获取的共享密钥对数据进行加解密，从而实现数据的保密传输。

[0184] 为了实现云使用商网络与分布式云计算数据中心的任一服务器之间的保密数据传输，云使用商网络的量子密钥分发设备和与所述服务器相连的量子密钥分发设备，可以多路径地进行密钥协商，并用最终获取的共享密钥对数据进行加解密，从而实现数据的保密传输。

[0185] 在上述的实施例中，提供了一种基于可信中继的量子密钥分发方法，与之相对应的，本申请还提供一种基于可信中继的量子密钥分发装置。请参看图 7，其为本申请的一种基于可信中继的量子密钥分发装置的实施例的示意图。由于装置实施例基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。下述描述的装置实施例仅仅是示意性的。

[0186] 本实施例的一种基于可信中继的量子密钥分发装置，包括：多路径协商单元 701，用于发送方量子密钥分发设备通过路由设备的中继、采用两条或者两条以上的不同路径，与接收方量子密钥分发设备进行密钥协商；合并判断单元 702，用于所述发送方或接收方量子密钥分发设备根据预先设定的策略，判断是否需要对通过所述密钥协商过程获取的共享密钥进行合并操作；合并执行单元 703，用于当所述合并判断单元的输出为“是”时，所述发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作，生成新的共享密钥。

[0187] 可选的，所述装置还包括：

[0188] 路径获取单元，用于在触发所述多路径协商单元工作之前，所述发送方量子密钥分发设备根据量子密钥分发系统的拓扑信息，选择与接收方量子密钥分发设备进行密钥协商的两条或者两条以上的不同路径。

[0189] 可选的，所述装置还包括：

[0190] 路径分发单元，用于在触发所述多路径协商单元工作之前，发送方量子密钥分发设备通过经典信道，将每条路径信息发送给所述路径包含的路由设备以及接收方量子密钥

分发设备；

[0191] 相应的，所述多路径协商单元除了包括实现其功能的本体子单元外，还包括路径验证子单元，所述路径验证子单元用于实现下述功能：所述路径包含的路由设备以及接收方量子密钥分发设备，根据接收到的所述路径信息，对与其进行密钥协商的对端设备的身份进行验证；若通过验证，与所述对端设备进行密钥协商并完成本节点的密钥中继操作；否则，通知所述发送方量子密钥分发设备放弃相应路径的密钥协商过程。

[0192] 可选的，所述多路径协商单元具体用于，通过所述路由设备的动态选路功能，实现经由两条或者两条以上的不同路径进行所述密钥协商。

[0193] 可选的，所述装置包括：

[0194] 路径验证单元，用于在所述多路径协商单元执行完毕后，所述发送方或接收方量子密钥分发设备通过获取本次密钥协商的路径信息，对参与每一条路径密钥协商过程的各个设备的身份合法性进行验证；若检测到非法设备，则所述发送方和接收方量子密钥分发设备放弃经由相应路径协商获取的共享密钥。

[0195] 可选的，所述装置还包括：

[0196] 身份验证单元，用于在触发所述多路径协商单元工作之前，所述发送方和接收方量子密钥分发设备通过经典信道，对对方设备进行身份验证；若所述对方设备未通过所述身份验证，则结束本方法的执行。

[0197] 可选的，所述合并判断单元包括：

[0198] 安全评估结果获取子单元，用于所述量子密钥分发设备获取经由每一条路径进行密钥协商的安全评估结果；

[0199] 策略判断子单元，用于所述量子密钥分发设备根据预先设定的策略及所述安全评估结果，判断是否需要执行所述合并操作；

[0200] 选择协商子单元，用于所述量子密钥分发设备选取执行密钥合并操作的具体处理方式，以及通过经典信道，与对端量子密钥分发设备协商并确认所述密钥合并的具体处理方式，并触发所述合并执行单元工作。

[0201] 可选的，所述装置还包括：

[0202] 数据加密传输单元，用于所述发送方量子密钥分发设备使用最终获取的共享密钥对待传输数据进行加密，并经由路由设备转发给所述接收方量子密钥分发设备；

[0203] 数据解密单元，用于所述接收方量子密钥分发设备采用与所述发送方相同的共享密钥对接收到的数据进行解密。

[0204] 本申请虽然以较佳实施例公开如上，但其并不是用来限定本申请，任何本领域技术人员在不脱离本发明的精神和范围内，都可以做出可能的变动和修改，因此本申请的保护范围应当以本申请权利要求所界定的范围为准。

[0205] 在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入 / 输出接口、网络接口和内存。

[0206] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和 / 或非易失性内存等形式，如只读存储器 (ROM) 或闪存 (flash RAM)。内存是计算机可读介质的示例。

[0207] 1、计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何

方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[0208] 2、本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请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。

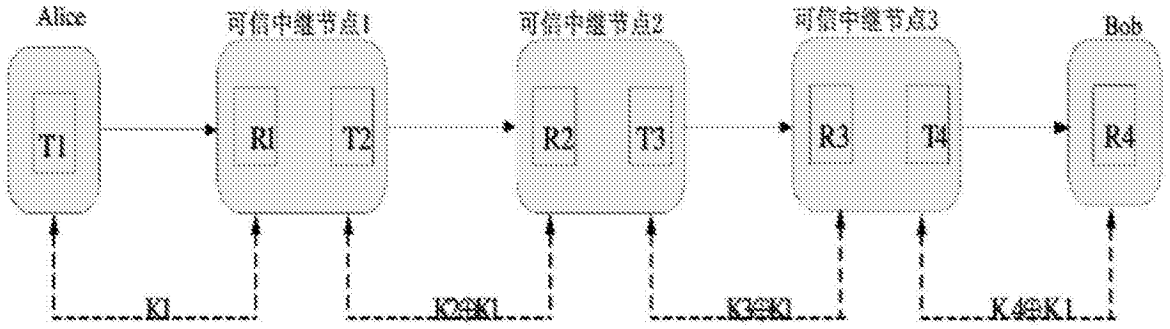

Alice
可信中继节点1
可信中继节点2
可信中继节点3
Bob
T1
R1
T2
R2
T3
R3
T4
R4
K1
K2⊕K1
K3⊕K2
K4⊕K3

图 1

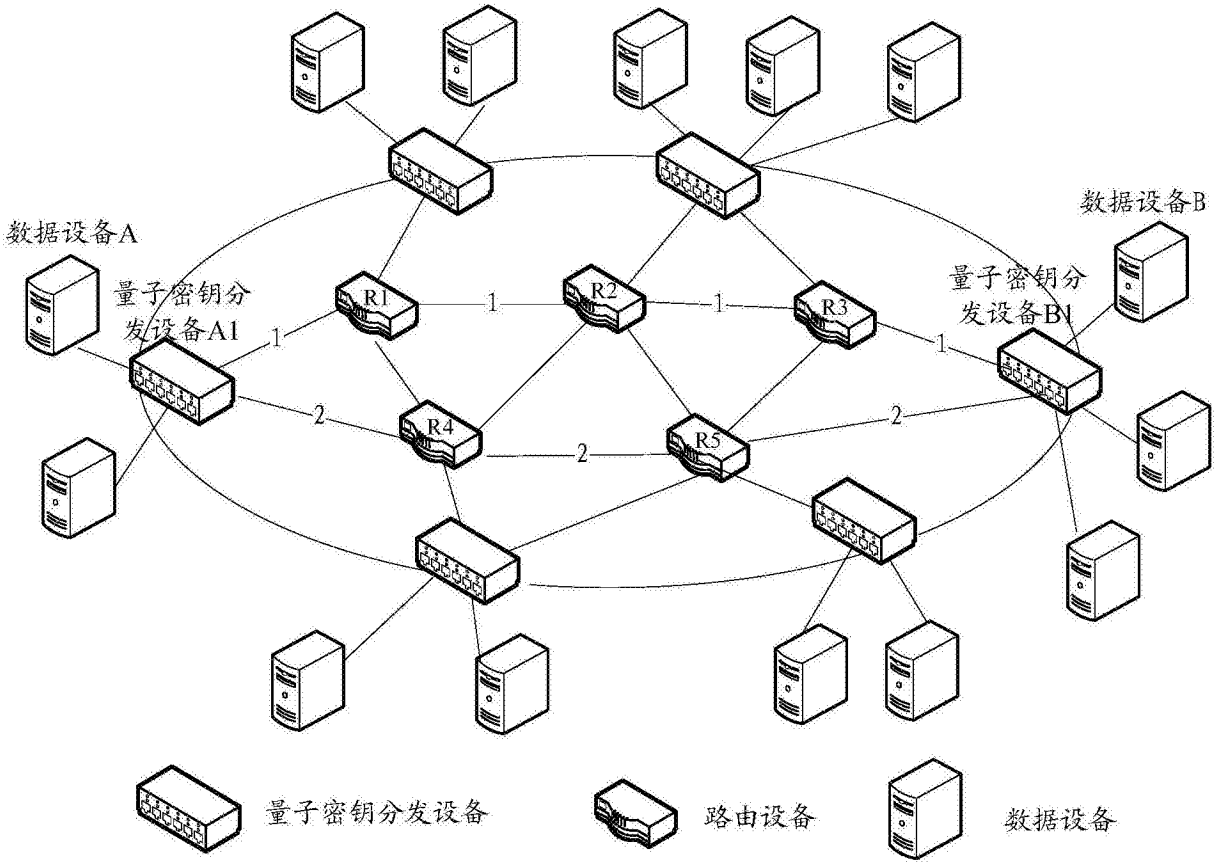

数据设备A
量子密钥分发设备A1
数据设备B
量子密钥分发设备B1
R1
R2
R3
R4
R5
1
2
量子密钥分发设备
路由设备
数据设备

图 2

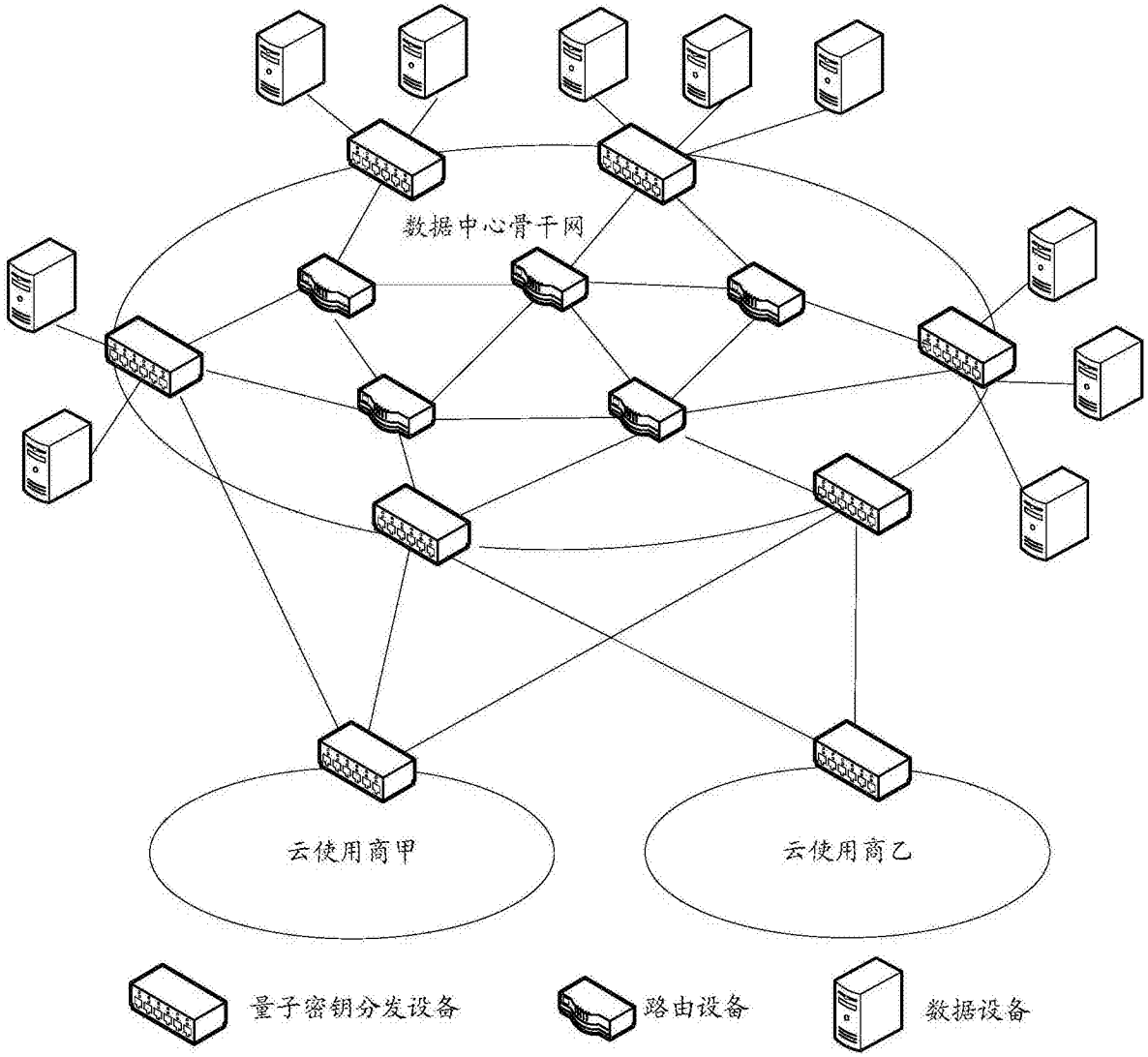


图 3

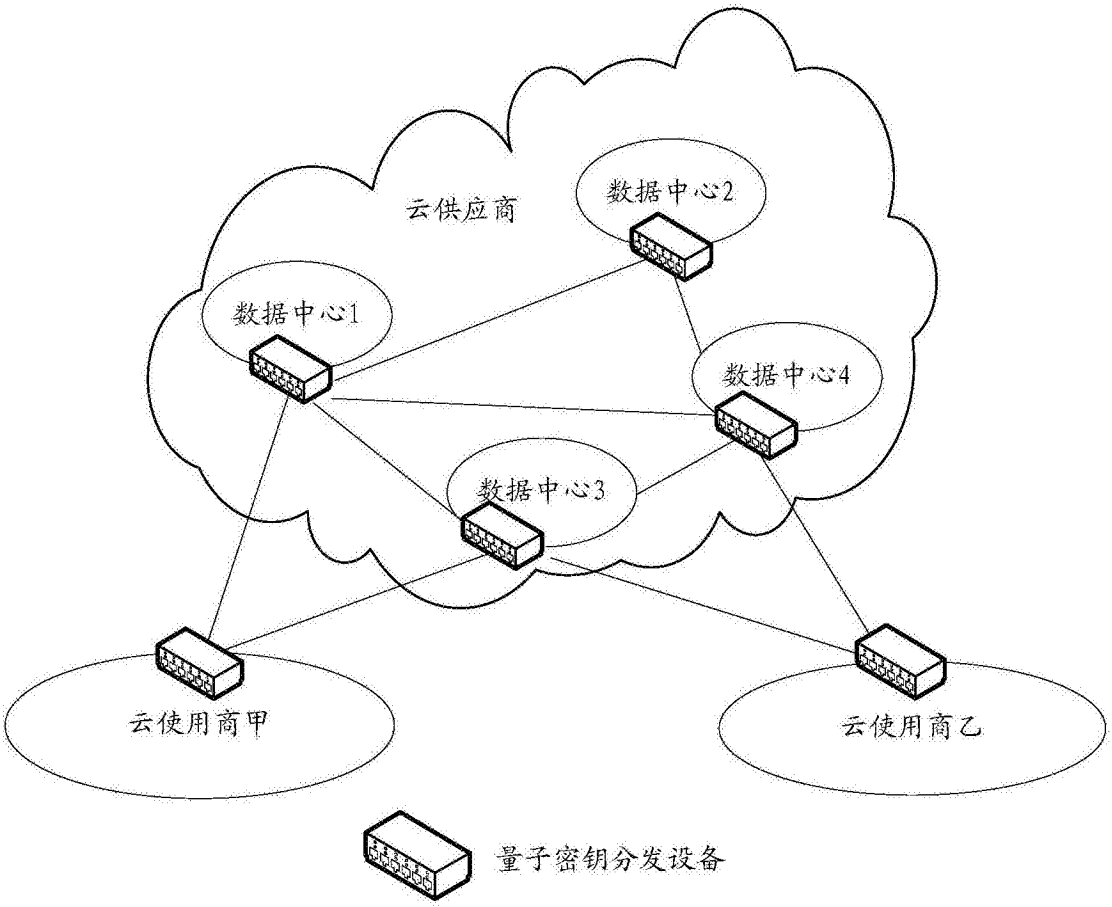


图 4

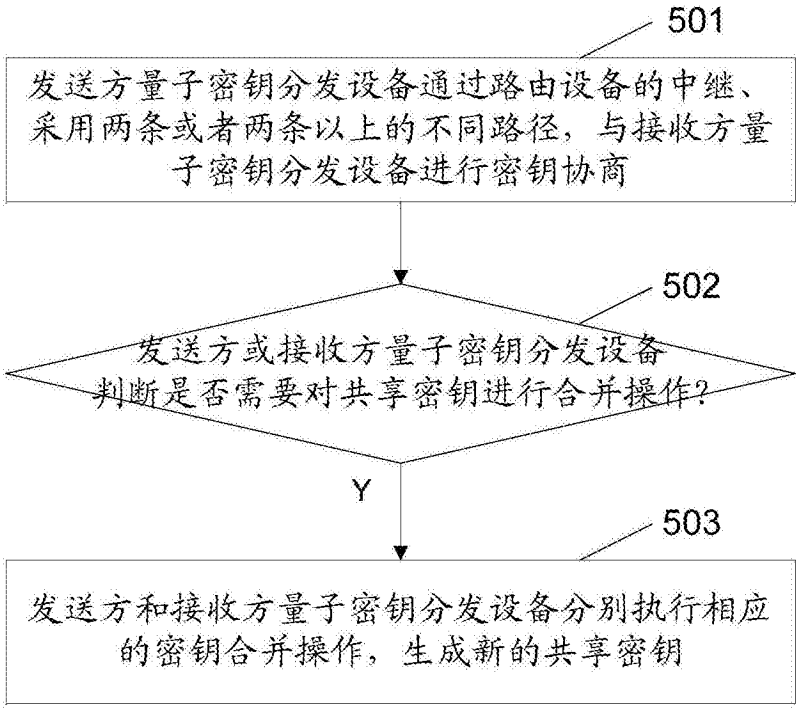

501
发送方量子密钥分发设备通过路由设备的中继、采用两条或者两条以上的不同路径，与接收方量子密钥分发设备进行密钥协商
502
发送方或接收方量子密钥分发设备判断是否需要对共享密钥进行合并操作?
Y
503
发送方和接收方量子密钥分发设备分别执行相应的密钥合并操作，生成新的共享密钥

图 5

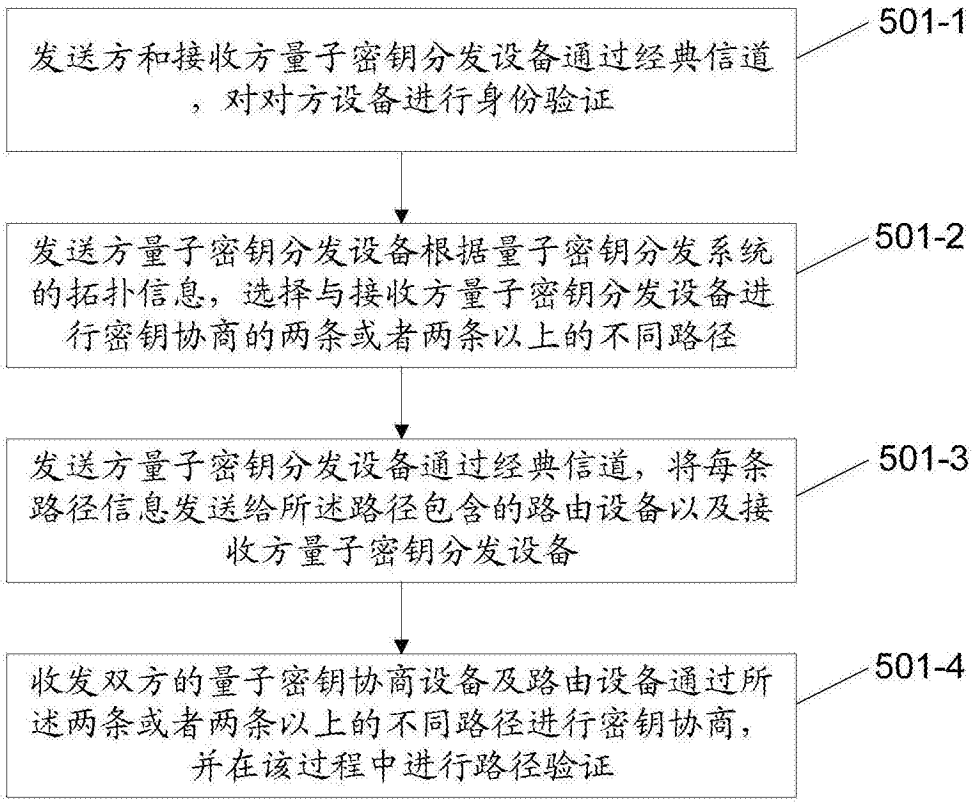

发送方和接收方量子密钥分发设备通过经典信道，对对方设备进行身份验证
501-1
发送方量子密钥分发设备根据量子密钥分发系统的拓扑信息，选择与接收方量子密钥分发设备进行密钥协商的两条或者两条以上的不同路径
501-2
发送方量子密钥分发设备通过经典信道，将每条路径信息发送给所述路径包含的路由设备以及接收方量子密钥分发设备
501-3
收发双方的量子密钥协商设备及路由设备通过所述两条或者两条以上的不同路径进行密钥协商，并在该过程中进行路径验证
501-4

图 6

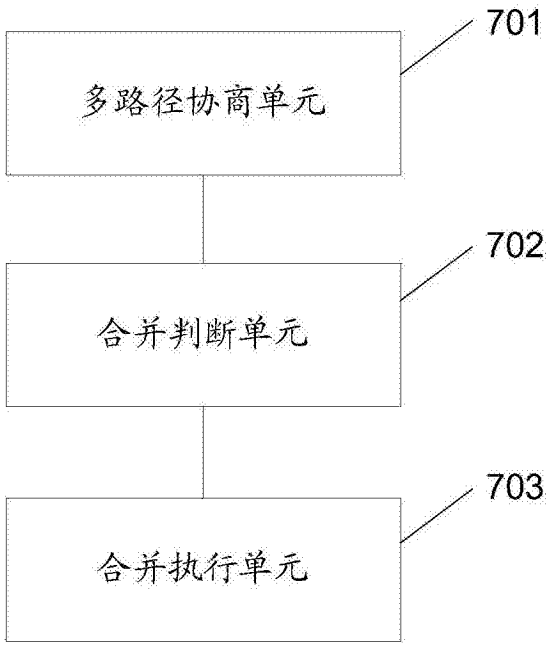


图 7