(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 113765654 A
(43)申请公布日 2021.12.07

(21)申请号 202010496453.3

(22)申请日 2020.06.03

(71)申请人 科大国盾量子技术股份有限公司
地址 230088 安徽省合肥市高新区望江西路800号合肥创新产业园D3楼
申请人 山东量子科学技术研究院有限公司

(72)发明人 刁一帅 姜胜广

(74)专利代理机构 北京云嘉湃富知识产权代理有限公司 11678
代理人 程凌军

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/08(2006.01)

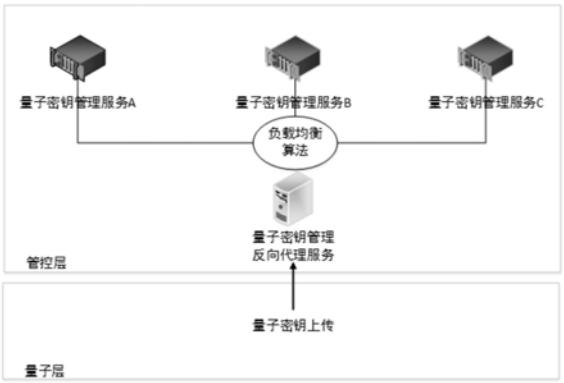
权利要求书2页 说明书8页 附图5页

(54)发明名称

一种负载均衡的量子密钥管理装置

(57)摘要

本发明涉及负载均衡的量子密钥管理装置，其可以包括量子密钥管理反向代理服务器和多个量子密钥管理服务器。量子密钥管理反向代理服务器可以接收量子密钥管理业务的请求；以及响应于请求，基于量子密钥管理服务器的状态，根据负载均衡算法选定用于量子密钥管理业务的量子密钥管理服务器。借助本发明，能够满足高流量业务处理的需求，并保证可靠性。



CN 113765654 A

1.一种负载均衡的量子密钥管理装置,其包括量子密钥管理反向代理服务器和多个量子密钥管理服务器,所述量子密钥管理反向代理服务器与所述量子密钥管理服务器之间建立有数据链路;

其中,所述量子密钥管理反向代理服务器被配置成:

接收量子密钥管理业务的请求;以及,

响应于所述量子密钥管理业务的请求,基于所述量子密钥管理服务器的状态,根据预设的负载均衡算法从所述量子密钥管理服务器中选定用于所述量子密钥管理业务的量子密钥管理服务器。

2.如权利要求1所述的量子密钥管理装置,其中,

所述量子密钥管理业务包括量子密钥接收业务、量子密钥中继业务、量子密钥输出业务中的一种或多种;

以及/或者,所述量子密钥管理服务器的状态包括业务负载、量子密钥量、存储空间中的一种或多种。

3.如权利要求1所述的量子密钥管理装置,其中,

所述量子密钥管理服务器的状态是响应于所述量子密钥管理反向代理服务器向所述量子密钥管理服务器进行的查询来获取的;或者,

所述量子密钥管理服务器的状态是由所述量子密钥管理服务器向所述量子密钥管理反向代理服务器上报的。

4.如权利要求1所述的量子密钥管理装置,其中,所述量子密钥管理反向代理服务器是通过选举的方式从所述量子密钥管理服务器中选出的。

5.如权利要求1所述的量子密钥管理装置,其中,所述量子密钥管理反向代理服务器还被配置成:

接收量子密钥接收业务的请求;并且,

在收到量子密钥时,基于所述量子密钥管理服务器的当前业务负载和存储空间,依据所述负载均衡算法选定用于处理所述量子密钥接收业务的量子密钥管理服务器,并向所述选定的量子密钥管理服务器转发所述量子密钥。

6.如权利要求5所述的量子密钥管理装置,其中,当所述选定的量子密钥管理服务器未成功处理所述量子密钥接收业务时:

所述选定的量子密钥管理服务器将所述量子密钥返回给所述量子密钥管理反向代理服务器;

所述量子密钥管理反向代理服务器重新选定用于处理所述量子密钥接收业务的量子密钥管理服务器。

7.如权利要求1所述的量子密钥管理装置,其中,所述量子密钥管理反向代理服务器还被配置成:

接收量子密钥中继业务的请求;并且,

获取所述量子密钥管理服务器的量子密钥量,计算量子密钥的总量,并将所述量子密钥的总量反馈给路由服务器。

8.如权利要求7所述的量子密钥管理装置,其中,所述量子密钥管理反向代理服务器还被配置成:

当作为中继发起节点时，基于所述量子密钥管理服务器的当前业务负载和量子密钥量，依据所述负载均衡算法选定用于处理所述量子密钥中继业务的量子密钥管理服务器和量子密钥，所述选定的量子密钥为种子密钥。

9.如权利要求8所述的量子密钥管理装置，其中，

所述选定的量子密钥管理服务器将所述种子密钥上传至所述量子密钥管理反向代理服务器；并且，

所述量子密钥管理反向代理服务器基于所述量子密钥管理服务器的当前业务负载以及当前量子密钥量或存储空间，依据所述负载均衡算法选定用于存储所述种子密钥的量子密钥管理服务器。

10.如权利要求7所述的量子密钥管理装置，其中，所述量子密钥管理反向代理服务器还被配置成：

当作为中继目的节点时，根据用于对传输的中继密钥进行加密的量子密钥的唯一标识，将所述传输的中继密钥发送到存储有所述量子密钥的唯一标识的量子密钥管理服务器。

11.如权利要求7所述的量子密钥管理装置，其中，所述量子密钥管理反向代理服务器还被配置成：

当作为中继传输节点时，根据上一跳节点中用于对传输的中继密钥进行加密的量子密钥的唯一标识，将所述传输的中继密钥发送到存储有所述量子密钥的唯一标识的量子密钥管理服务器以进行解密；以及，

基于所述量子密钥管理服务器的当前业务负载和量子密钥量，依据所述负载均衡算法选定用于下一跳节点的量子密钥，并将解密的中继密钥发送到所述选定的用于下一跳节点的量子密钥对应的量子密钥管理服务器。

12.如权利要求1所述的量子密钥管理装置，其中，所述量子密钥管理反向代理服务器还被配置成：

接收量子密钥输出业务的请求；

根据所述量子密钥输出业务的请求所要求的量子密钥量，基于所述量子密钥管理服务器的当前业务负载和量子密钥量，依据所述负载均衡算法选定用于所述量子密钥输出业务的量子密钥管理服务器和量子密钥；

将由所述选定的量子密钥管理服务器上传的所述选定的量子密钥进行整合。

13.如权利要求1所述的量子密钥管理装置，其中，

当在所述量子密钥管理反向代理服务器或与其建立有所述数据链路的量子密钥管理服务器中出现未能根据量子密钥的唯一标识发现所述量子密钥的故障时，在出现所述故障的所述量子密钥管理反向代理服务器和对端的量子密钥管理反向代理服务器之间同步放弃所述故障对应的量子密钥。

一种负载均衡的量子密钥管理装置

技术领域

[0001] 本发明涉及量子保密通信领域，具体涉及一种负载均衡的量子密钥管理装置，其用于量子密钥生命周期管理中的量子密钥输出。

背景技术

[0002] 现有的量子密钥管理体系结构按照逻辑进行分层，其架构可以包括量子层、管控层和应用层，如图1所示。

[0003] 在图1所示的架构中，量子层的作用是通过量子密钥分发过程生成量子密钥，并将量子密钥上传到管控层；管控层的作用是接收量子层传输的量子密钥，完成量子密钥的存储、量子密钥的中继与量子密钥的输出；应用层的作用是对接最终用户，向管控层申请量子密钥，并使用量子密钥对用户传输的数据进行加解密等操作，例如，加密操作在通信发起方用户发生，解密操作在通信接收方用户发生。

[0004] 现有技术中，对于管控层的量子密钥管理功能，主要是采用双机热备技术来对量子密钥进行管理，即，将经典通信链路与量子密钥通过使用成熟的解决方案进行备份。但是，使用这种方式进行互相备份的管控层设备，同一时刻只能有一个进行正常工作，因此只能实现可靠性指标的提升，无法应对高流量下业务处理出现瓶颈的问题。

发明内容

[0005] 针对现有技术中的不足之处，本发明人首次基于反向代理负载均衡技术提出一种负载均衡的量子密钥管理装置，能够满足高流量业务处理的需求，实现对高流量业务的负载均衡，同时还可以保证原有的可靠性。

[0006] 本发明的负载均衡的量子密钥管理装置可以包括量子密钥管理反向代理服务器和多个量子密钥管理服务器，所述量子密钥管理反向代理服务器与所述量子密钥管理服务器之间建立有数据链路；

[0007] 其中，所述量子密钥管理反向代理服务器被配置成：

[0008] 接收量子密钥管理业务的请求；以及，

[0009] 响应于所述量子密钥管理业务的请求，基于所述量子密钥管理服务器的状态，根据预设的负载均衡算法从所述量子密钥管理服务器中选定用于所述量子密钥管理业务的量子密钥管理服务器。

[0010] 进一步地，所述量子密钥管理业务包括量子密钥接收业务、量子密钥中继业务、量子密钥输出业务中的一种或多种；以及/或者，所述量子密钥管理服务器的状态包括业务负载、量子密钥量、存储空间中的一种或多种。

[0011] 进一步地，所述量子密钥管理服务器的状态是响应于所述量子密钥管理反向代理服务器向所述量子密钥管理服务器进行的查询来获取的；或者，所述量子密钥管理服务器的状态是由所述量子密钥管理服务器向所述量子密钥管理反向代理服务器上报的。

[0012] 进一步地，所述量子密钥管理反向代理服务器是通过选举的方式从所述量子密钥

管理服务器中选出的。

[0013] 进一步地，所述量子密钥管理反向代理服务器还被配置成：接收量子密钥接收业务的请求；并且，在收到量子密钥时，基于所述量子密钥管理服务器的当前业务负载和存储空间，依据所述负载均衡算法选定用于处理所述量子密钥接收业务的量子密钥管理服务器，并向所述选定的量子密钥管理服务器转发所述量子密钥。

[0014] 更进一步地，当所述选定的量子密钥管理服务器未成功处理所述量子密钥接收业务时：所述选定的量子密钥管理服务器将所述量子密钥返回给所述量子密钥管理反向代理服务器；所述量子密钥管理反向代理服务器重新选定用于处理所述量子密钥接收业务的量子密钥管理服务器。

[0015] 进一步地，所述量子密钥管理反向代理服务器还被配置成：接收量子密钥中继业务的请求；并且，获取所述量子密钥管理服务器的量子密钥量，计算量子密钥的总量，并将所述量子密钥的总量反馈给路由服务器。

[0016] 更进一步地，所述量子密钥管理反向代理服务器还被配置成：当作为中继发起节点时，基于所述量子密钥管理服务器的当前业务负载和量子密钥量，依据所述负载均衡算法选定用于处理所述量子密钥中继业务的量子密钥管理服务器和量子密钥，所述选定的量子密钥为种子密钥。其中，所述选定的量子密钥管理服务器将所述种子密钥上传至所述量子密钥管理反向代理服务器；并且，所述量子密钥管理反向代理服务器基于所述量子密钥管理服务器的当前业务负载以及当前量子密钥量或存储空间，依据所述负载均衡算法选定用于存储所述种子密钥的量子密钥管理服务器。

[0017] 更进一步地，所述量子密钥管理反向代理服务器还被配置成：当作为中继目的节点时，根据用于对传输的中继密钥进行加密的量子密钥的唯一标识，将所述传输的中继密钥发送到存储有所述量子密钥的唯一标识的量子密钥管理服务器。

[0018] 更进一步地，所述量子密钥管理反向代理服务器还被配置成：当作为中继传输节点时，根据上一跳节点中用于对传输的中继密钥进行加密的量子密钥的唯一标识，将所述传输的中继密钥发送到存储有所述量子密钥的唯一标识的量子密钥管理服务器以进行解密；以及，基于所述量子密钥管理服务器的当前业务负载和量子密钥量，依据所述负载均衡算法选定用于下一跳节点的量子密钥，并将解密的中继密钥发送到所述选定的用于下一跳节点的量子密钥对应的量子密钥管理服务器。

[0019] 进一步地，所述量子密钥管理反向代理服务器还被配置成：接收量子密钥输出业务的请求；根据所述量子密钥输出业务的请求所要求的量子密钥量，基于所述量子密钥管理服务器的当前业务负载和量子密钥量，依据所述负载均衡算法选定用于所述量子密钥输出业务的量子密钥管理服务器和量子密钥；将由所述选定的量子密钥管理服务器上传的所述选定的量子密钥进行整合。

[0020] 进一步地，当在所述量子密钥管理反向代理服务器或与其建立有所述数据链路的量子密钥管理服务器中出现未能根据量子密钥的唯一标识发现所述量子密钥的故障时，在出现所述故障的所述量子密钥管理反向代理服务器和对端的量子密钥管理反向代理服务器之间同步放弃所述故障对应的量子密钥。

附图说明

[0021] 下面结合附图对本发明的具体实施方式作进一步详细的说明。

[0022] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需使用的附图作简单地介绍，显而易见，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图来获得其他的附图。

[0023] 图1示出了现有量子密钥管理体系结构的逻辑架构；

[0024] 图2示出了反向代理负载均衡技术的一种示例；

[0025] 图3示出了本发明的负载均衡的量子密钥管理装置在处理量子密钥接收业务请求时的工作流程；

[0026] 图4示出了本发明的负载均衡的量子密钥管理装置在处理量子密钥中继业务请求时的工作流程；

[0027] 图5A示出了在中继密钥传输过程中，作为中继发起节点的量子密钥管理装置的工作流程；

[0028] 图5B示出了在中继密钥传输过程中，作为中继目的节点的量子密钥管理装置的工作流程；

[0029] 图5C示出了在中继密钥传输过程中，作为中继传输节点的量子密钥管理装置的工作流程；

[0030] 图6示出了本发明的负载均衡的量子密钥管理装置在处理量子密钥输出业务请求时的工作流程；

[0031] 图7示出了本发明的负载均衡的量子密钥管理装置在出现某种故障时的一种示例性的解决方案。

具体实施方式

[0032] 在下文中，本发明的示例性实施例将参照附图来详细描述。下面的实施例以举例的方式提供，以便充分传达本发明的精神给本发明所属领域的技术人员。因此，本发明不限于本文公开的实施例。

[0033] 基于现有量子密钥管理体系存在的不足，本发明通过研究提出了基于负载均衡技术的量子密钥管理思路，使得既可以保证可靠性，又能够适应高流量的业务处理需求。具体而言，本发明在深入剖析经典通信中HTTP重定向负载均衡技术、DNS域名解析负载均衡技术和反向代理负载均衡技术等的基础上，首次创新性地提出了将反向代理负载均衡技术应用于量子密钥的管理，并具体公开了一种基于负载均衡的量子密钥管理装置。

[0034] 在反向代理负载均衡技术中，负载均衡的实现依赖于反向代理服务器，通过反向代理服务器隐藏后续服务的实现细节，通过反向代理服务器的负载均衡算法对到达的业务进行均衡，以分配到具体处理业务的服务器中，即仅依赖于代理服务器与业务服务器之间的交互细节。图2示出了反向代理负载均衡技术的一种示例，如图所示，外部的业务处理请求首先到达反向代理服务器，反向代理服务器根据负载均衡算法选择对应的业务处理服务器处理业务请求，并将业务处理的结果反馈给请求者。

[0035] 图3-6分别以示例的方式描述了根据本发明的负载均衡的量子密钥管理装置。

[0036] 如图所示,本发明的量子密钥管理装置设置在管控层,其可以包括量子密钥管理反向代理服务器和多个量子密钥管理服务器(例如服务器A、B和C),并且,量子密钥管理反向代理服务器与多个量子密钥管理服务器之间建立了数据链路并实现了认证。

[0037] 在本发明的量子密钥管理装置中,将由量子密钥管理反向代理服务器接收量子密钥管理业务请求。响应于量子密钥管理业务请求,量子密钥管理反向代理服务器可以根据预设的负载均衡算法从多个量子密钥管理服务器中选择量子密钥管理服务器来处理该量子密钥管理业务。量子密钥管理业务可以包括但不限于量子密钥接收业务,量子密钥中继业务,以及量子密钥输出业务。

[0038] 在本发明中,量子密钥管理反向代理服务器可以获取各个量子密钥管理服务器的当前状态。作为示例,量子密钥管理服务器的状态可以包括业务负载,量子密钥量,以及存储空间等。作为示例,可以由量子密钥管理反向代理服务器主动向量子密钥管理服务器发送查询信息来获取其当前状态;或者,可以由量子密钥管理服务器主动向量子密钥管理反向代理服务器上报其当前状态。

[0039] 因此,量子密钥管理反向代理服务器能够响应于量子密钥管理业务请求,基于各个量子密钥管理服务器的当前状态,依据预设的负载均衡算法来选择适合用于处理该量子密钥管理业务请求的量子密钥管理服务器。

[0040] 下面将结合图3-6,以举例的方式结合具体的量子密钥管理业务请求,详细说明本发明的量子密钥管理装置的工作原理。

[0041] 图3示出了本发明的负载均衡的量子密钥管理装置在处理量子密钥接收业务请求时的工作流程。

[0042] 如图3所示,量子密钥管理装置可以包括量子密钥管理反向代理服务器和多个量子密钥管理服务器(例如,量子密钥管理服务器A、B和C),量子密钥管理反向代理服务器与多个量子密钥管理服务器之间建立有数据链路,且实现了认证。

[0043] 量子密钥管理反向代理服务器获取各个量子密钥管理服务器(例如服务器A、服务器B和服务器C)当前的业务负载和存储空间。

[0044] 量子层将量子密钥上传至量子密钥管理反向代理服务器,提出量子密钥接收业务请求。

[0045] 在收到由量子层上传的量子密钥后,量子密钥管理反向代理服务器基于各个量子密钥管理服务器当前的业务负载和存储空间,依据预设的负载均衡算法进行负载均衡计算,从中挑选出合适的量子密钥管理服务器,并将量子密钥转发给选定的量子密钥管理服务器。

[0046] 在选定的量子密钥管理服务器处,对接收到的量子密钥进行处理。若处理成功,则可以向量子密钥管理反向代理服务器发送消息,告知量子密钥处理完成;否则,可以将量子密钥再返回给量子密钥管理反向代理服务器,并通知其重新挑选量子密钥管理服务器。

[0047] 在本发明的量子密钥管理装置中,重复根据上述规则对从量子层接收到的量子密钥进行处理。若最终处理成功,则可以向量子层发送消息,告知量子密钥接收成功;否则,可以向量子层发送消息,告知量子密钥接收失败。

[0048] 图4示出了本发明的负载均衡的量子密钥管理装置在处理量子密钥中继业务请求时的工作流程。

[0049] 需要说明的是,出于简洁目的,与上文重复的内容可能不再赘述。

[0050] 如图4所示,量子密钥管理装置可以包括量子密钥管理反向代理服务器和多个量子密钥管理服务器(例如,量子密钥管理服务器A、B和C),量子密钥管理反向代理服务器与多个量子密钥管理服务器之间建立有数据链路,且实现了认证。

[0051] 对于量子密钥中继业务,将由管控层内部发起量子密钥中继流程。当管控层检测到需要进行量子密钥中继时,由路由服务器进行中继发起节点到中继目的节点的路由计算。在路由计算中,量子密钥管理反向代理服务器将表现为一个可路由节点。

[0052] 因此,在路由计算中,当量子密钥管理反向代理服务器接收到量子密钥中继业务请求时,量子密钥管理反向代理服务器获取各个量子密钥管理服务器(例如服务器A、服务器B和服务器C)当前的业务负载和量子密钥量,计算各个量子密钥管理服务器的量子密钥的总量,并将量子密钥的总量反馈给路由服务器。即,对于路由服务器而言,由量子密钥管理反向代理服务器实现的路由节点中的量子密钥量等于与其连接的多个量子密钥管理服务器的量子密钥的总量。

[0053] 路由服务器根据量子密钥管理反向代理服务器反馈的量子密钥的总量,进行中继路径的计算。

[0054] 当计算出中继发起节点到中继目的节点的量子密钥中继路径可达时,管控层开始进行量子密钥中继过程,开始向各个量子密钥管理反向代理服务器发送中继密钥传输指令。

[0055] 图5A示出了在中继密钥传输过程中,作为中继发起节点的量子密钥管理装置的工作流程。

[0056] 如图5A所示,当量子密钥管理反向代理服务器发现自己为中继发起节点时,可以基于各个量子密钥管理服务器当前的业务负载和量子密钥量,依据预设的负载均衡算法,在各个量子密钥管理服务器中进行量子密钥的挑选。选中的量子密钥管理服务器中的量子密钥将被作为中继的种子密钥进行存储。所述种子密钥可以作为中继密钥使用,也可以与密钥生成算法(例如AES)结合生成中继密钥,或者与其他密钥或随机数(例如量子随机数)结合生成中继密钥。所述种子密钥还可以作为加密中继密钥的密钥使用。

[0057] 作为种子密钥存储方案的一种示例,种子密钥可以存储在当前的量子密钥管理服务器中。

[0058] 作为种子密钥存储方案的另一种示例,可以由量子密钥管理服务器将种子密钥上传至量子密钥管理反向代理服务器,再由量子密钥管理反向代理服务器基于各个量子密钥管理服务器的业务负载和量子密钥量(或存储空间),依据预设的负载均衡算法重新挑选量子密钥管理服务器,以用于对其进行存储。

[0059] 在本发明,可以由量子密钥管理反向代理服务器确定选用何种种子密钥存储方案。

[0060] 图5B示出了在中继密钥传输过程中,作为中继目的节点的量子密钥管理装置的工作流程。

[0061] 根据量子密钥中继原理,当传输的中继密钥到达目的节点时,用于对传输的中继密钥进行加密的量子密钥已在上一跳节点被选定,因此,目的节点在进行传输的中继密钥的解密时,可以根据上一跳节点发送的用于对传输的中继密钥加密的量子密钥的唯一标

识,将传输的中继密钥发送到存储该量子密钥的唯一标识的量子密钥管理服务器。

[0062] 因此,如图5B所示,当量子密钥管理反向代理服务器发现自己为中继目的节点时,可以根据中继传输过程中携带的信息(用于对传输的中继密钥加密的量子密钥的唯一标识),直接将对应的传输的中继密钥发送到存储有该量子密钥的唯一标识的量子密钥管理服务器中,以利用相应的量子密钥对传输的中继密钥进行解密,最终获得传输的中继密钥。

[0063] 图5C示出了在中继密钥传输过程中,作为中继传输节点的量子密钥管理装置的工作流程。

[0064] 如图5C所示,当量子密钥管理反向代理服务器发现自己既非中继发起节点,也不是中继目的节点时,则该量子密钥管理反向代理服务器还需要处理中继密钥传输服务。

[0065] 首先,量子密钥管理反向代理服务器需要根据中继传输过程中携带的信息(即,上一跳节点中用于对传输的中继密钥进行加密的量子密钥的唯一标识),直接将对应的传输的中继密钥发送到存储有该量子密钥的唯一标识的量子密钥管理服务器中,以利用相应的量子密钥对传输的中继密钥进行解密。

[0066] 然后,量子密钥管理反向代理服务器可以基于各个量子密钥管理服务器当前的业务负载和量子密钥量,依据预设的负载均衡算法,在各个量子密钥管理服务器中挑选用于下一跳节点的量子密钥,并将解密的中继密钥发送到对应的量子密钥管理服务器,利用选定的量子密钥进行加密。

[0067] 通过上述过程,量子密钥管理反向代理服务器按照路由服务器计算的路径逐跳进行量子密钥的中继过程。若中继过程成功,则会在中继发起节点与中继目的节点生成相应的中继密钥;否则,本次中继过程失败。无论成功还是失败,中继过程中使用的量子密钥均会被销毁。

[0068] 图6示出了本发明的负载均衡的量子密钥管理装置在处理量子密钥输出业务请求时的工作流程。同样出于简洁目的,与上文重复的内容可能不再赘述。

[0069] 如图6所示,量子密钥管理装置可以包括量子密钥管理反向代理服务器和多个量子密钥管理服务器(例如,量子密钥管理服务器A、B和C),量子密钥管理反向代理服务器与多个量子密钥管理服务器之间建立有数据链路,且实现了认证。

[0070] 量子密钥管理反向代理服务器获取各个量子密钥管理服务器(例如服务器A、服务器B和服务器C)当前的业务负载和量子密钥量。

[0071] 应用层向量子密钥管理反向代理服务器提出量子密钥输出业务请求(即量子密钥申请请求)。

[0072] 量子密钥管理反向代理服务器根据量子密钥输出业务请求中请求的量子密钥量,基于各个量子密钥管理服务器当前的业务负载和量子密钥量,依据预设的负载均衡算法进行负载均衡计算,从而选定用于输出给应用层的量子密钥,亦即量子密钥所对应的量子密钥管理服务器。随后,量子密钥管理反向代理服务器将量子密钥输出业务请求发送至选定的一个或多个量子密钥管理服务器。

[0073] 量子密钥管理服务器响应于量子密钥输出业务请求,将选定的量子密钥发送到量子密钥管理反向代理服务器。量子密钥管理反向代理服务器将量子密钥进行整合后,发送给应用层(即,量子密钥输出业务请求方)。

[0074] 下面将进一步以应用层为进行加解密业务提出的量子密钥输出业务请求为例,进

一步说明本发明的量子密钥管理装置的工作流程。

[0075] 应用层的加密端向量子密钥管理反向代理服务器发送量子密钥输出业务请求。

[0076] 量子密钥管理反向代理服务器根据量子密钥输出业务请求，基于各个量子密钥管理服务器当前的业务负载和量子密钥量，依据预设的负载均衡算法进行负载均衡计算，选定需要输出的量子密钥及其对应的量子密钥管理服务器。

[0077] 量子密钥管理反向代理服务器向选定的量子密钥管理服务器发送量子密钥输出业务请求，并等待量子密钥管理服务器的响应。

[0078] 量子密钥管理服务器做出响应，将选定的量子密钥发送给量子密钥管理反向代理服务器。

[0079] 量子密钥管理反向代理服务器将选定的量子密钥进行整合，并发送到应用层的加密端。

[0080] 应用层的加密端接收到量子密钥后，将通知应用层的解密端向对应的量子密钥管理反向代理服务器提出量子密钥输出业务请求，请求用于解密的量子密钥。此时，量子密钥输出业务请求中可以包含用于解密的量子密钥的唯一标识。

[0081] 量子密钥管理反向代理服务器直接根据应用层的解密端提供的量子密钥的唯一标识，向相应的量子密钥管理服务器中申请相应的量子密钥，然后将申请到的量子密钥进行整合，并将其发送到应用层的解密端。

[0082] 通过上文可以理解，在本发明的负载均衡的量子密钥管理装置中，由于量子密钥分布式地存储在各个量子密钥管理服务器中，因此当一台量子密钥管理服务器因为故障停止工作时，量子密钥管理反向代理服务器依然能够借助剩余的量子密钥管理服务器进行业务的处理，从而保证其可靠性。

[0083] 根据本发明，为了进一步提高可靠性指标，还可以不单独部署量子密钥管理反向代理服务器，而是在多个量子密钥管理服务器中，通过节点选举的方式选举一个量子密钥管理服务器兼任量子密钥管理反向代理服务器。因此，当正在使用中的量子密钥管理反向代理服务器出现故障不能继续工作时，剩余的量子密钥管理服务器可以通过选举算法重新选择一个量子密钥管理反向代理服务器，保证业务不中断。

[0084] 此外，在本发明的负载均衡的量子密钥管理装置，有可能出现以下故障，即：存储量子密钥的量子密钥管理服务器在对应位置上出现故障，导致量子密钥管理反向代理服务器无法根据量子密钥的唯一标识找到对应的量子密钥，例如图7所示。

[0085] 因此，在本发明的量子密钥管理装置中，当检测到量子密钥管理服务器或量子密钥管理反向代理服务器出现故障时，可以在两个(本端和对端)量子密钥管理反向代理服务器之间进行量子密钥的同步，例如在两个服务器处同步放弃故障所对应的量子密钥。

[0086] 综上可见，在本发明的量子密钥管理装置中，采用负载均衡的方式替换了现有技术中主机热备的方式，且在负载均衡中采用选举机制，可以在保证主备的前提下，实现了业务的负载均衡。

[0087] 由于本发明的量子密钥管理装置建立于成熟稳定的反向代理负载均衡技术上，并针对量子密钥管理特点进行了独特的设计，其非常适合在产业上大规模的推广应用。

[0088] 另外，在本发明中，借助负载均衡算法还可以根据实际环境动态增加/减少设备数量，并自动进行业务动态调整，从而减少人工配置的复杂度。并且，本发明中还提出利用量

子密钥信息同步的方式处理因量子密钥管理服务器出现故障引起的量子密钥不同步的异常，从而为量子密钥管理装置的应用提出了全面的解决方案。

[0089] 尽管前面结合附图通过具体实施例对本发明进行了说明，但是，本领域技术人员容易认识到，上述实施例仅仅是示例性的，用于说明本发明的原理，其并不会对本发明的范围造成限制，本领域技术人员可以对上述实施例进行各种组合、修改和等同替换，而不脱离本发明的精神和范围。

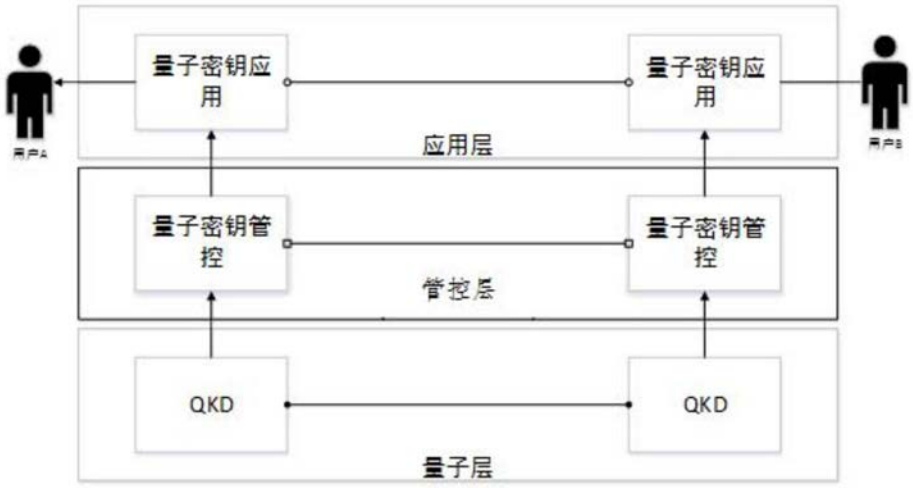

量子密钥应用
量子密钥应用
应用层
量子密钥管控
量子密钥管控
管控层
QKD
QKD
量子层

图1

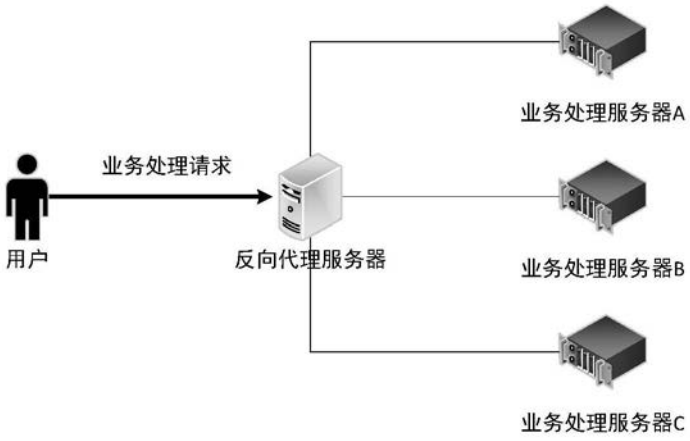

业务处理请求
用户
反向代理服务器
业务处理服务器A
业务处理服务器B
业务处理服务器C

图2

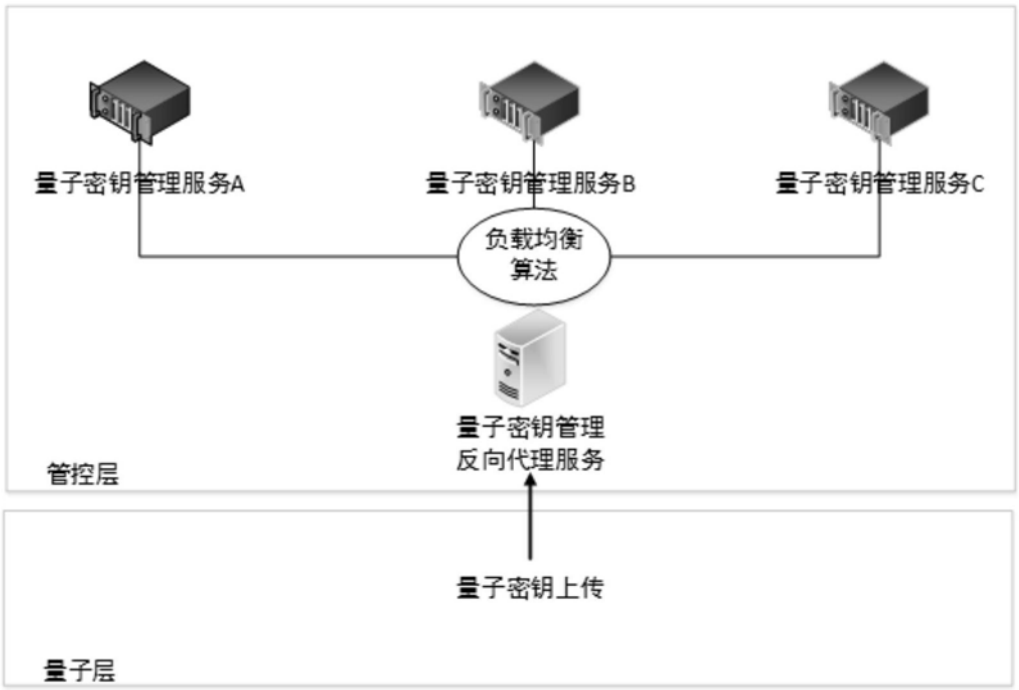

量子密钥管理服务A
量子密钥管理服务B
量子密钥管理服务C
负载均衡
算法
量子密钥管理
反向代理服务
管控层
量子密钥上传
量子层

图3

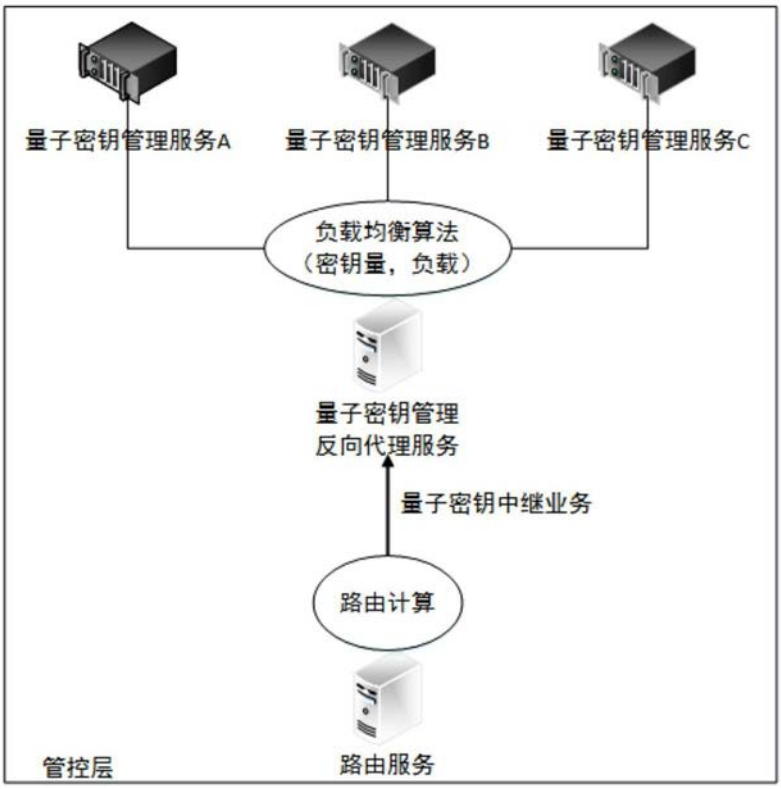

量子密钥管理服务A
量子密钥管理服务B
量子密钥管理服务C
负载均衡算法
（密钥量，负载）
量子密钥管理
反向代理服务
量子密钥中继业务
路由计算
管控层
路由服务

图4

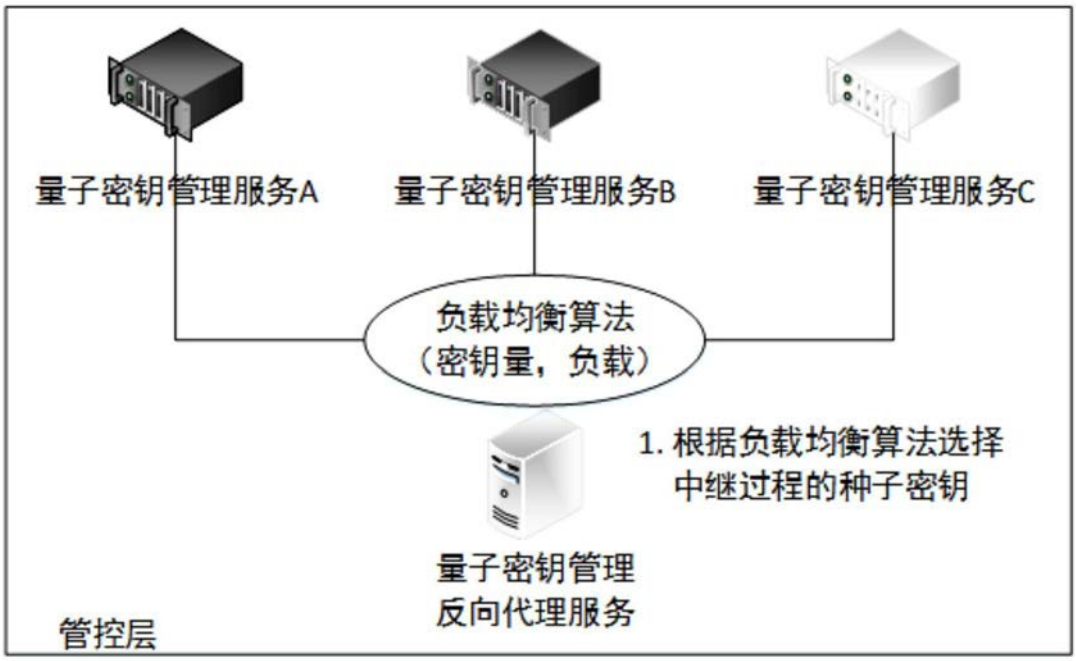

量子密钥管理服务A
量子密钥管理服务B
量子密钥管理服务C
负载均衡算法
（密钥量，负载）
1. 根据负载均衡算法选择
中继过程的种子密钥
量子密钥管理
反向代理服务
管控层
中继发起节点

图5A

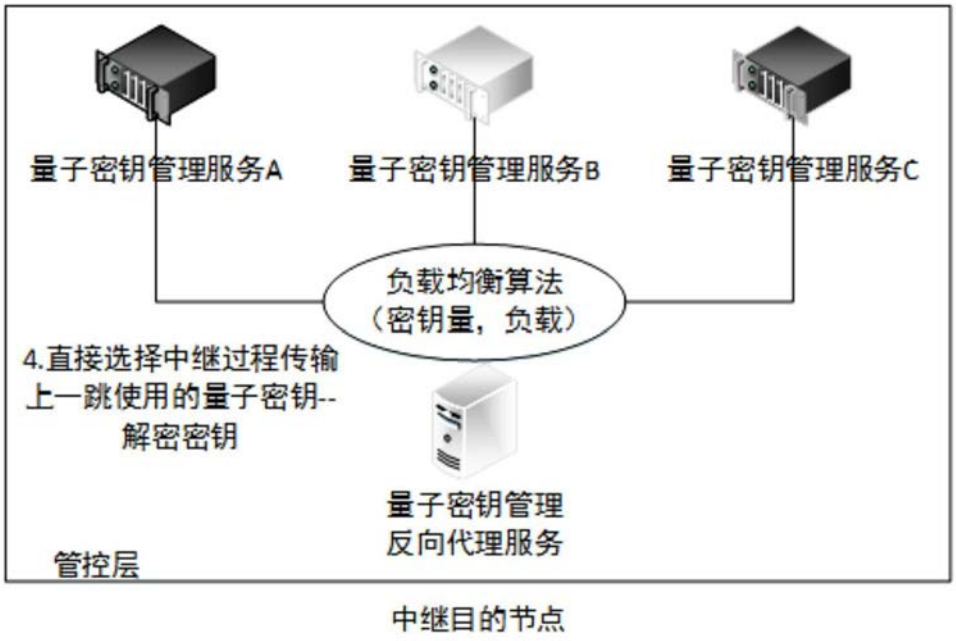

量子密钥管理服务A
量子密钥管理服务B
量子密钥管理服务C
负载均衡算法
（密钥量，负载）
4.直接选择中继过程传输
上一跳使用的量子密钥--
解密密钥
量子密钥管理
反向代理服务
管控层
中继目的节点

图5B

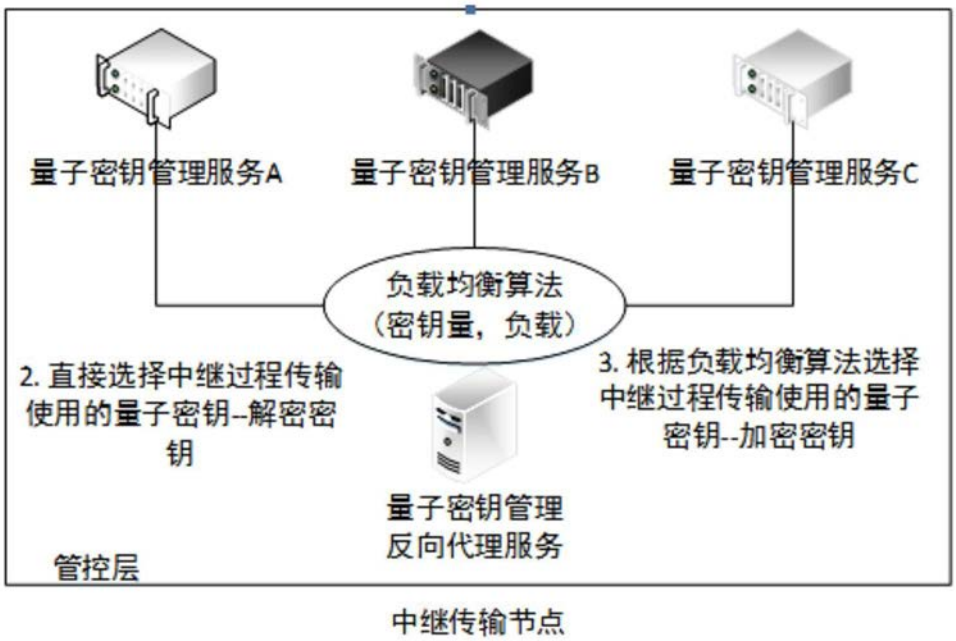

量子密钥管理服务A
量子密钥管理服务B
量子密钥管理服务C
负载均衡算法
（密钥量，负载）
2. 直接选择中继过程传输使用的量子密钥--解密密钥
3. 根据负载均衡算法选择中继过程传输使用的量子密钥--加密密钥
量子密钥管理
反向代理服务
管控层
中继传输节点

图5C

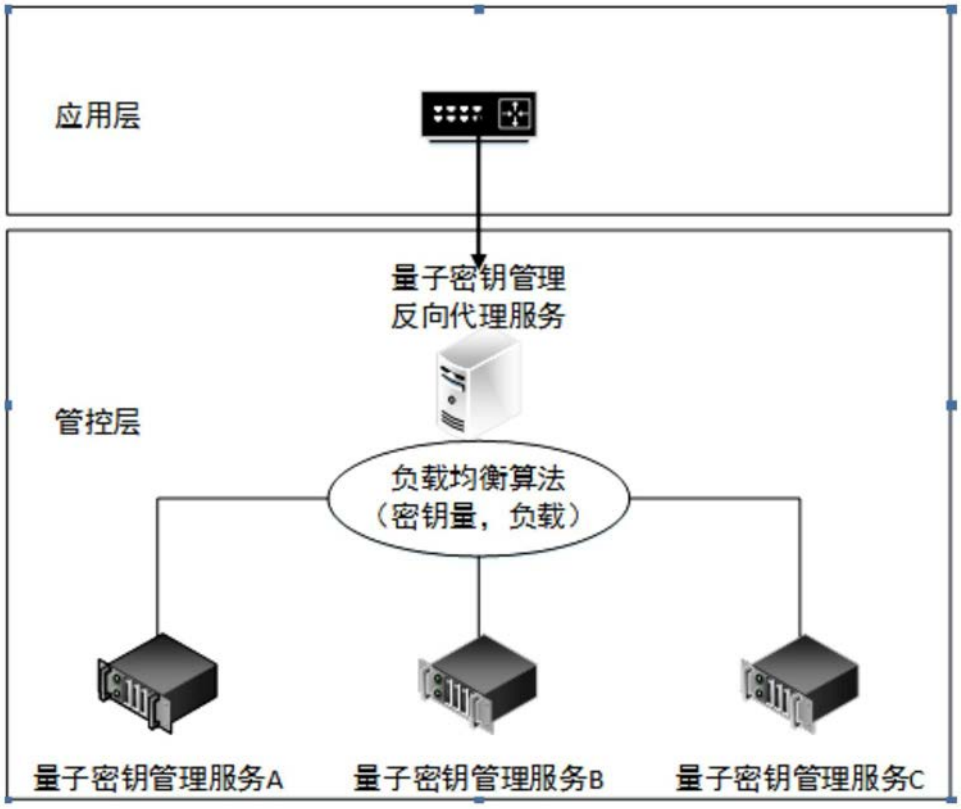

应用层
量子密钥管理
反向代理服务
管控层
负载均衡算法
（密钥量，负载）
量子密钥管理服务A
量子密钥管理服务B
量子密钥管理服务C

图6

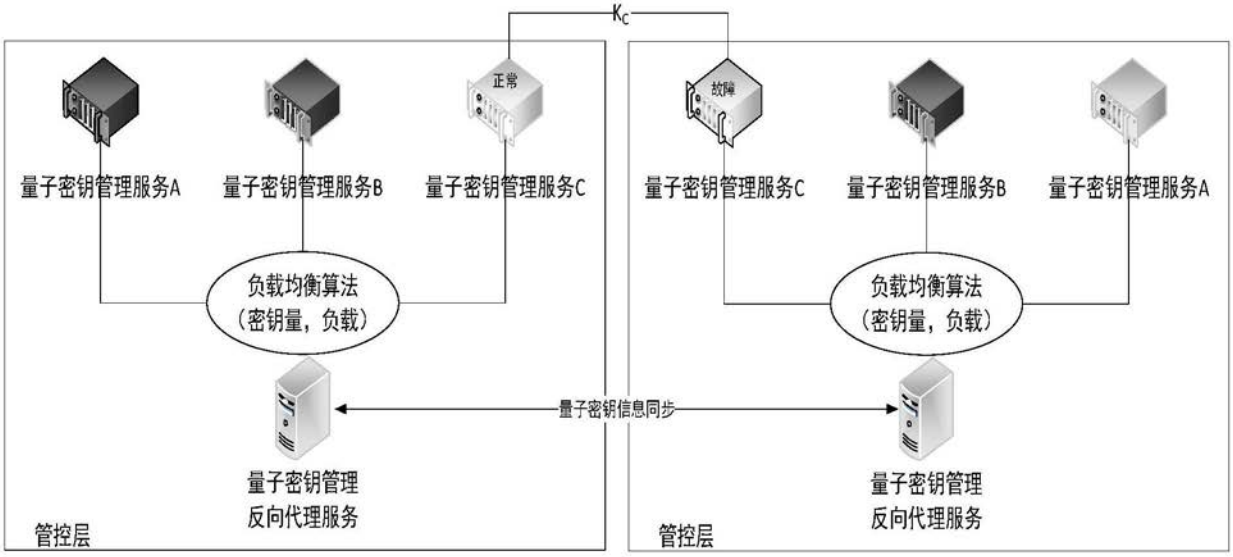

Kc
正常
故障
量子密钥管理服务A
量子密钥管理服务B
量子密钥管理服务C
量子密钥管理服务C
量子密钥管理服务B
量子密钥管理服务A
负载均衡算法
（密钥量，负载）
负载均衡算法
（密钥量，负载）
量子密钥信息同步
量子密钥管理
反向代理服务
量子密钥管理
反向代理服务
管控层
管控层

图7