(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 108809632 B
(45)授权公告日 2021.06.15

(21)申请号 201710294804.0
(22)申请日 2017.04.28
(65)同一申请的已公布的文献号
申请公布号 CN 108809632 A
(43)申请公布日 2018.11.13
(73)专利权人 广东国盾量子科技有限公司
地址 510663 广东省广州市大观中路492号岭南科技中心C座5楼
(72)发明人 陈洁容 李凯铭
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王宝筠
(51)Int.Cl.
*H04L 9/08*(2006.01)
*H04L 29/06*(2006.01)

审查员 代悦宁

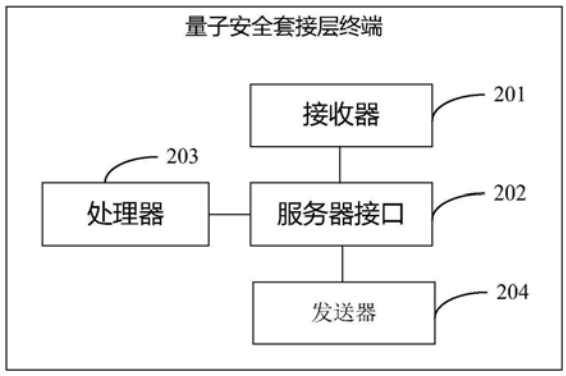
权利要求书2页 说明书11页 附图4页

(54)发明名称

一种量子安全套接层装置及系统

(57)摘要

本发明实施例提供了一种量子安全套接层装置及系统，量子安全套接层终端提供与量子安全服务器进行数据交互的服务器接口，该服务器接口能够实现采用对称的量子密钥，对量子安全套接层终端与量子安全服务器之间交互的数据进行加密解密；量子安全服务器提供与量子安全套接层终端进行数据交互的终端接口，该终端接口能够实现采用对称的量子密钥，对量子安全套接层终端与量子安全服务器之间交互的数据进行加密解密。进而实现了基于量子密钥加密的安全套接层，提供了采用量子密钥加密互联网传输的数据，提高了数据传输的安全性。




CN 108809632 B

1.一种量子安全套接层终端,其特征在于,所述量子安全套接层终端包括:

接收器,用于接收量子安全服务器发送的第一标识和第一密文;

服务器接口,用于根据所述第一标识获得第一量子密钥,利用所述第一量子密钥对所述第一密文进行解密获得第一数据和第二标识;采用所述第二标识获得第二量子密钥,利用所述第二量子密钥给第二数据进行加密获得第二密文,所述第二数据是发送给所述量子安全服务器的数据;

处理器,用于对所述第一数据进行处理;

发送器,用于将所述第二密文发送至所述量子安全服务器。

2.根据权利要求1所述的量子安全套接层终端,其特征在于,所述量子安全套接层终端还包括:

量子密钥存储设备,用于存储多个量子密钥以及每个量子密钥对应的标识。

3.根据权利要求2所述的量子安全套接层终端,其特征在于,

所述量子密钥存储设备,还用于删除作为对交互数据进行加密或解密的密钥使用过一次的量子密钥及该量子密钥对应的标识,所述交互数据是所述量子安全套接层终端与所述量子安全服务器交互的数据。

4.根据权利要求2所述的量子安全套接层终端,其特征在于,

所述量子密钥存储设备,用于接收第一量子设备发送的量子数据,将所述量子数据按照预设的处理逻辑进行处理,获得多个新的量子密钥以及每个新的量子密钥对应的标识,所述第一量子设备与第二量子设备中的量子密钥是对称的量子密钥,所述第二量子设备与所述量子安全服务器相连。

5.根据权利要求1-4任意一项所述的量子安全套接层终端,其特征在于,所述量子安全套接层终端还包括:

告警器,用于满足预设的告警条件时,获得所述预设的告警条件对应的告警信息,所述预设的告警条件包括量子密钥废弃、票据错误或者票据过期;

所述发送器,还用于将所述告警信息发送至所述量子安全服务器。

6.一种量子安全服务器,其特征在于,所述量子安全服务器包括:

终端接口,用于获得第一标识和第二标识,采用所述第一标识对应的第一量子密钥,对第一数据和所述第二标识进行加密获得第一密文,所述第一数据是发送给量子安全套接层终端的数据;采用所述第二标识对应的第二量子密钥,对所述量子安全套接层终端发送的第二密文进行解密获得第二数据;

处理器,用于处理所述第二数据;

第一发送器,用于将所述第一标识和所述第一密文发送至所述量子安全套接层终端;

第一接收器,用于接收所述量子安全套接层终端发送的所述第二密文。

7.根据权利要求6所述的量子安全服务器,其特征在于,所述量子安全服务器还包括:

量子密钥存储设备,用于存储多个量子密钥以及每个量子密钥对应的标识。

8.根据权利要求7所述的量子安全服务器,其特征在于,

所述量子密钥存储设备,还用于删除作为对交互数据进行加密或解密的密钥使用过一次的量子密钥及该量子密钥对应的标识,所述交互数据是所述量子安全套接层终端与所述量子安全服务器交互的数据。

9.根据权利要求7所述的量子安全服务器，其特征在于，所述量子安全服务器还包括：

第二接收器，用于接收第二量子设备发送的量子数据，所述第二量子设备与第一量子设备中的量子密钥是对称的量子密钥，所述第一量子设备给所述量子安全套接层终端提供量子数据；

量子设备接口，用于调用与设备标识和通信协议版本都适配的预设的处理逻辑，将所述量子数据利用所述预设的处理逻辑进行处理，获得多个新的量子密钥以及每个新的量子密钥对应的标识，将获得的所述多个新的量子密钥以及每个新的量子密钥对应的标识发送至所述量子密钥存储设备进行更新；

第二发送器，用于向所述第二量子设备发送响应信息。

10.根据权利要求6-9任意一项所述的量子安全服务器，其特征在于，所述量子安全服务器还包括：

告警器，用于满足预设的告警条件时，获得所述预设的告警条件对应的告警信息，所述预设的告警条件包括票据错误或者票据过期；

所述第一发送器，还用于将所述告警信息发送至所述量子安全套接层终端。

11.一种量子安全套接层系统，其特征在于，所述量子安全套接层系统包括：

权利要求1-5任意一项所述的量子安全套接层终端，权利要求6-10任意一项所述的量子安全服务器。

# 一种量子安全套接层装置及系统

## 技术领域

[0001] 本发明涉及通信技术领域,特别是涉及一种量子安全套接层装置及系统。

## 背景技术

[0002] 随着互联网技术和通信技术的发展,能够通过互联网实现数据的网络传输,提高业务响应的时效性。为了避免数据在互联网中传输时,被非法终端设备截获或篡改,需要对所传输的数据进行加密传输。

[0003] 目前,可以采用SSL VPN(Secure Sockets Layer,Virtual Private Network,安全套接层虚拟专用网络)技术构建数据的安全传输网络。但是,SSL VPN技术,是基于非对称加密算法实现对互联网传输的数据进行加密,随着计算机计算能力的提高,该非对称加密算法可被破解,导致互联网中数据传输的安全性低。

## 发明内容

[0004] 本发明解决的技术问题在于提供一种量子安全套接层装置及系统,从而能够采用量子密钥对互联网传输的数据进行加密,实现数据的安全传输。

[0005] 为此,本发明解决技术问题的技术方案是:

[0006] 一种量子安全套接层终端,所述量子安全套接层终端包括:

[0007] 接收器,用于接收量子安全服务器发送的第一标识和第一密文;

[0008] 服务器接口,用于根据所述第一标识获得第一量子密钥,利用所述第一量子密钥对所述第一密文进行解密获得第一数据和第二标识;采用所述第二标识获得第二量子密钥,利用所述第二量子密钥给第二数据进行加密获得第二密文,所述第二数据是发送给所述量子安全服务器的数据;

[0009] 处理器,用于对所述第一数据进行处理;

[0010] 发送器,用于将所述第二密文发送至所述量子安全服务器。

[0011] 在一个例子中,所述量子安全套接层终端还包括:

[0012] 量子密钥存储设备,用于存储多个量子密钥以及每个量子密钥对应的标识。

[0013] 在一个例子中,

[0014] 所述量子密钥存储设备,还用于删除作为对交互数据进行加密或解密的密钥使用过一次的量子密钥及该量子密钥对应的标识,所述交互数据是所述量子安全套接层终端与所述量子安全服务器交互的数据。

[0015] 在一个例子中,

[0016] 所述量子密钥存储设备,用于接收第一量子设备发送的量子数据,将所述量子数据按照预设的处理逻辑进行处理,获得多个新的量子密钥以及每个新的量子密钥对应的标识,所述第一量子设备与第二量子设备中的量子密钥是对称的量子密钥,所述第二量子设备与所述量子安全服务器相连。

[0017] 在一个例子中,所述量子安全套接层终端还包括:

[0018] 告警器，用于满足预设的告警条件时，获得所述预设的告警条件对应的告警信息，所述预设的告警条件包括量子密钥废弃，票据错误，或者票据过期；

[0019] 所述发送器，还用于将所述告警信息发送至所述量子安全服务器。

[0020] 一种量子安全服务器，所述量子安全服务器包括：

[0021] 终端接口，用于获得第一标识和第二标识，采用所述第一标识对应的第一量子密钥，对第一数据和所述第二标识进行加密获得第一密文，所述第一数据是发送给量子安全套接层终端的数据；采用所述第二标识对应的第二量子密钥，对所述量子安全套接层终端发送的第二密文进行解密获得第二数据；

[0022] 处理器，用于处理所述第二数据；

[0023] 第一发送器，用于将所述第一标识和所述第一密文发送至所述量子安全套接层终端；

[0024] 第一接收器，用于接收所述量子安全套接层终端发送的所述第二密文。

[0025] 在一个例子中，所述量子安全服务器还包括：

[0026] 量子密钥存储设备，用于存储多个量子密钥以及每个量子密钥对应的标识。

[0027] 在一个例子中，

[0028] 所述量子密钥存储设备，还用于删除作为对交互数据进行加密或解密的密钥使用过一次的量子密钥及该量子密钥对应的标识，所述交互数据是所述量子安全套接层终端与所述量子安全服务器交互的数据。

[0029] 在一个例子中，所述量子安全服务器还包括：

[0030] 第二接收器，用于接收第二量子设备发送的量子数据，所述第二量子设备与第一量子设备中的量子密钥是对称的量子密钥，所述第一量子设备给所述量子安全套接层终端提供量子数据；

[0031] 量子设备接口，用于调用与设备标识和通信协议版本都适配的预设的处理逻辑，将所述量子数据利用所述预设的处理逻辑进行处理，获得多个新的量子密钥以及每个新的量子密钥对应的标识，将获得的所述多个新的量子密钥以及每个新的量子密钥对应的标识发送至所述量子密钥存储设备进行更新；

[0032] 第二发送器，用于向所述第二量子设备发送响应信息。

[0033] 在一个例子中，所述量子安全服务器还包括：

[0034] 告警器，用于满足预设的告警条件时，获得所述预设的告警条件对应的告警信息，所述预设的告警条件包括票据错误，或者票据过期；

[0035] 所述第一发送器，还用于将所述告警信息发送至所述量子安全套接层终端。

[0036] 一种量子安全套接层系统，所述量子安全套接层系统包括：

[0037] 上述内容所述的量子安全套接层终端，上述内容所述的量子安全服务器。

[0038] 通过上述技术方案可知，本发明有如下有益效果：

[0039] 本发明实施例提供了一种量子安全套接层装置及系统，量子安全套接层终端提供与量子安全服务器进行数据交互的服务器接口，该服务器接口能够实现采用对称的量子密钥，对量子安全套接层终端与量子安全服务器之间交互的数据进行加密解密；量子安全服务器提供与量子安全套接层终端进行数据交互的终端接口，该终端接口能够实现采用对称的量子密钥，对量子安全套接层终端与量子安全服务器之间交互的数据进行加密解密。进

而实现了基于量子密钥加密的安全套接层，提供了采用量子密钥加密互联网传输的数据，提高了数据传输的安全性。

## 附图说明

[0040] 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要使用的附图作简单地介绍，显而易见地，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获得其他的附图。

[0041] 图1为本发明提供的量子安全套接层装置及系统的应用场景结构示意图；

[0042] 图2为本发明实施例提供的量子安全套接层终端一实例结构示意图；

[0043] 图3为本发明实施例提供的量子安全套接层终端另一实例结构示意图；

[0044] 图4为本发明实施例提供的量子安全套接层终端又一实例结构示意图；

[0045] 图5为本发明实施例提供的量子安全套接层终端再一实例结构示意图；

[0046] 图6为本发明实施例提供的量子安全服务器一实例结构示意图；

[0047] 图7为本发明实施例提供的量子安全服务器另一实例结构示意图；

[0048] 图8为本发明实施例提供的量子安全服务器又一实例结构示意图；

[0049] 图9为本发明实施例提供的量子安全套接层系统结构示意图。

## 具体实施方式

[0050] 为了给出在互联网中数据安全传输的实现方案，本发明实施例提供了一种量子安全套接层装置及系统，以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。并且在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0051] 现有技术中，基于SSL VPN技术实现互联网中的数据加密传输时，采用非对称加密算法。非对称加密算法需要两个密钥，公钥和私钥。第一设备生成公钥和私钥，将公钥告知第二设备。第二设备向第一设备发送数据时，采用公钥对该数据进行加密获得密文。第一设备接收到密文后，利用私钥对该密文进行解密，从而获得第二设备发送的数据。第一设备生成公钥和私钥时，是采用大数分解算法，或者椭圆密码算法等技术生成的。随着计算机计算能力的提高，该公钥和私钥是能够被破解的，导致数据传输的安全性低。

[0052] 本发明实施例提供的量子安全套接层装置及系统，能够实现采用量子密钥对互联网传输的数据进行加密。量子密钥以量子力学为基础，安全性是建立在测不准原理、量子的不可克隆以及量子相干性等物理特性之上的，被证明是无条件安全的。因此，采用量子密钥对数据进行加密后，在互联网中传输，提高了数据传输的安全性。

[0053] 下面结合附图先对本发明提供的量子安全套接层装置及系统的应用场景进行概述。

[0054] 如图1所示，量子安全套接层终端与用户终端建立通信，量子安全套接层终端与用户终端可以集成为同一个物理实体，也可以是不同的物理实体。量子安全套接层终端与用户终端是不同的物理实体时，量子安全套接层终端与用户终端处于同一个私网内，量子安全套接层终端与用户终端之间进行数据交互无需加密。

[0055] 量子安全套接层终端能够给不同的用户终端，提供与量子安全服务器交互的接口，该接口能够实现对量子安全套接层终端与量子安全服务器之间的数据，采用量子密钥进行加密和解密。例如：该用户终端可以是电子商务用户终端，可以是网络银行用户终端，还可以是电子邮件用户终端等等。也就是说，量子安全套接层终端接收用户终端发送的数据，将该数据采用量子密钥进行加密后，再发送至量子安全服务器。

[0056] 量子安全服务器，一方面，量子安全服务器提供与量子安全套接层终端交互的接口，该接口能够实现对量子安全套接层终端与量子安全服务器之间的数据，采用量子密钥进行加密和解密；另一方面，量子安全服务器还能够提供与量子设备交互的接口，该接口能够根据量子设备的标识与通信协议版本的不同，调用能够处理该量子设备发送的数据的处理器。

[0057] 因此，量子安全套接层终端和量子安全服务器所组成的量子安全套接层系统，能够支持不同种类的用户终端，也能够支持不同种类(生产厂家不同，或者通信协议的版本不同等)的量子设备，实现对互联网中传输的数据采用量子密钥加密传输，提高互联网中数据传输的安全性。

[0058] 其中，量子设备可以是量子密钥管理设备，也可以是量子密钥分发设备。

[0059] 下面结合附图对本发明实施例提供的安全套接层的装置及系统进行逐一详细说明。

[0060] 图2为本发明实施例提供的量子安全套接层终端结构示意图，包括：

[0061] 接收器201，用于接收量子安全服务器发送的第一标识和第一密文。

[0062] 服务器接口202，用于根据第一标识获得第一量子密钥，利用第一量子密钥对第一密文进行解密获得第一数据和第二标识；采用第二标识获得第二量子密钥，利用第二量子密钥给第二数据进行加密获得第二密文，第二数据是发送给量子安全服务器的数据。

[0063] 处理器203，用于对第一数据进行处理。

[0064] 发送器204，用于将第二密文发送至量子安全服务器。

[0065] 量子安全套接层终端与一个用户终端相连，量子安全套接层终端与用户终端可以集成为一个物理实体，量子安全套接层终端与用户终端分别为不同的物理实体时，量子安全套接层终端与用户终端位于同一私网内，用户终端给量子安全套接层终端发送数据时，无需加密，量子安全套接层终端与用户终端传输的数据不会被泄露。

[0066] 在实际应用时，用户终端可以是多种类型的用户终端，可以是互联网中任意一种需要传输加密数据的用户终端，即该量子安全套接层终端可以支持多种不同类型的用户终端。例如：用户终端可以是电子商务应用中的用户终端，可以是网络银行应用中的用户终端，还可以是电子邮件应用中的用户终端，等等。当然，用户终端还可以是其他类型的用户终端，这里不再一一赘述。

[0067] 量子安全套接层终端可以支持多种网络通信协议，例如：TCP/IP协议(Transmission Control Protocol/Internet Protocol，传输控制协议/因特网互联协议)，FTP协议(File Transfer Protocol，文件传输协议)，以及HTTP协议(Hypertext Transfer Protocol，超文本传输协议)等。因此，量子安全套接层终端可以接收采用不同的网络通信协议的用户终端发送的数据。

[0068] 量子安全套接层终端的接收器201，用于接收量子安全服务器发送的第一标识和

第一密文。第一标识用于唯一标识第一量子密钥，第一密文是采用第一量子密钥对第一数据加密获得的。

[0069] 量子安全套接层终端的服务器接口202，能够根据第一标识获得该第一标识对应的第一量子密钥，利用第一量子密钥对第一密文进行解密，获得第一数据和第二标识。其中，第一数据是量子安全服务器发送给量子安全套接层终端的数据。

[0070] 可以理解的是，量子安全套接层终端存储有标识和量子密钥的对应关系，量子安全服务器也存储有标识和量子密钥的对应关系。量子安全套接层终端与量子安全服务器中，同一个标识对应的量子密钥是对称的量子密钥，采用一个标识对应的量子密钥加密获得的密文，可以利用该标识对应的量子密钥对密文进行解密。

[0071] 第二标识用于标识量子安全套接层终端给量子安全服务器发送数据时，所采用的第二量子密钥。一般情况下，量子安全套接层终端向量子安全服务器发送数据时，对该数据进行加密时所采用的量子密钥，是由量子安全服务器决定的，对量子安全服务器发送的密文解密后，可以获得标识该量子密钥的第二标识。

[0072] 量子安全套接层终端的服务器接口202，根据第二标识获得该第二标识所对应的第二量子密钥，利用该第二量子密钥对第二数据进行加密获得第二密文。第二数据是量子安全套接层终端要发送给量子安全服务器的数据。第二数据是用户终端发送给量子安全套接层终端的数据。可以理解的是，第二数据可以是用户终端对第一数据进行处理后所得的数据，也可以是用户终端给量子安全套接层终端发送的其他数据。

[0073] 量子安全套接层终端的服务器接口202，一方面，能够将量子安全服务器发送的第一密文，采用第一量子密钥进行解密，获得量子安全服务器给用户终端发送的第一数据，是提供量子安全服务器与用户终端进行数据交互的解密功能的接口；另一方面，能够将用户终端发送的第二数据，采用第二量子密钥进行加密，获得向量子安全服务器发送的第二密文，是提供量子安全服务器与用户终端进行数据交互的加密功能的接口。从而，用户终端可以直接处理第一数据，无需对量子安全服务器发送的第一密文进行解密，无需设置解密功能；用户终端仅需要将所要发送至量子安全服务器的第二数据发送至量子安全套接层终端，无需对第二数据进行加密，也无需设置加密功能。

[0074] 量子安全套接层终端中的处理器203，用于对第一数据进行处理。量子安全套接层终端与用户终端集成在同一物理实体中，该处理器203可以对第一数据进行处理生成第二数据。举例说明，第一数据是认证信息时，该处理器203可以根据第一数据进行认证操作。量子安全套接层终端与用户终端分别在不同的物理实体时，该处理器203对第一数据进行处理，则是将该第一数据发送至用户终端。用户终端对第一数据进行处理获得第二数据。

[0075] 量子安全套接层终端中的发送器204，将利用第二量子密钥对第二数据进行加密获得的第二密文，发送至量子安全服务器。

[0076] 在一个例子中，如图3所述量子安全套接层终端还包括：

[0077] 量子密钥存储设备301，用于存储多个量子密钥以及每个量子密钥对应的标识。

[0078] 量子安全套接层终端中的量子密钥存储设备301，存储有多个量子密钥，以及各个量子密钥对应的标识。一个量子密钥对应的标识，能够唯一标识该量子密钥。量子安全套接层终端的量子密钥存储设备301中，一个标识对应的量子密钥，与在量子安全服务器中该量子安全套接层终端对应的量子密钥集合中，同一个标识对应的量子密钥，是成对的量子密

钥。该量子密钥存储设备301与服务器接口202相连，服务器接口202从该量子密钥存储设备301中，根据标识查找该标识对应的量子密钥。

[0079] 为了进一步提高数据传输的安全性，量子密钥存储设备301中的量子密钥，作为给量子安全套接层终端和量子安全服务器交互的数据作为加密或者解密的密钥使用过一次后，则量子密钥存储设备301删除该量子密钥，以及该量子密钥对应的标识。因此，量子密钥存储设备301中的量子密钥，作为给量子安全套接层终端和量子安全服务器交互的数据的加密或者解密密钥，只能被使用一次，能够避免重放攻击，进一步提高互联网中数据传输的安全性。

[0080] 图3所示的量子密钥存储设备301，是集成在量子安全套接层终端中的量子密钥存储设备301。在实际应用中，量子密钥存储设备301还可以是量子安全套接层终端一个外接的物理实体，如图4所示，量子密钥存储设备301是一个可与量子安全套接层终端分离的外接的物理实体，例如采用UKey的形式，与量子安全套接层终端采用USB接口可拆卸式相连。当然，量子密钥存储设备301还可以采用其他可能的实现方式，这里不再一一赘述。

[0081] 当量子密钥存储设备301中存储的量子密钥，满足量子密钥更新条件时，需要对量子密钥存储设备301中的量子密钥进行更新。该量子密钥更新条件有多种可能的实现形式：第一种可能的实现形式，作为给量子安全套接层终端和量子安全服务器交互的数据的加密或者解密密钥，都已经使用过一次；第二种可能的实现形式，作为给量子安全套接层终端和量子安全服务器交互的数据的加密或者解密密钥，使用数量或使用次数大于预设阈值时；第三种可能的实现形式，达到预设更新时间，该预设更新时间指的是对量子密钥存储设备301中的量子密钥进行更新的时间间隔。

[0082] 当然，量子密钥更新条件并不仅限于上述所述的三种可能的实现形式，还可以根据实际需要自行设定。

[0083] 此时，如图5所示，量子密钥存储设备301向与其通信的第一量子设备请求量子数据，第一量子设备向量子密钥存储设备301发送量子数据，量子密钥存储设备301利用该量子数据生成多个新的量子密钥以及每个新的量子密钥对应的标识。于此同时，量子安全服务器向与其通信的第二量子设备请求量子数据，第二量子设备向量子安全服务器发送量子数据，量子安全服务器利用该量子数据生成多个新的量子密钥以及每个新的量子密钥对应的标识。其中，第一量子设备和第二量子设备具有对称的量子数据。

[0084] 第一量子设备和第二量子设备都是量子密钥分发设备时，第一量子设备和第二量子设备采用量子密钥分发技术生成对称的量子数据。第一量子设备和第二量子设备都是量子密钥管理设备时，第一量子设备接入的量子密钥分发设备与第二量子设备接入的量子密钥分发设备采用量子密钥分发技术生成对称的量子数据，第一量子设备接收其所接入的量子密钥分发设备发送的量子数据，第二量子设备也接收其所接入的量子密钥分发设备发送的量子数据。

[0085] 量子密钥存储设备301获得量子密钥以后，采用与量子安全服务器预先协商的预设的处理逻辑对该量子数据进行处理，获得多个新的量子密钥以及每个新的量子密钥对应的标识。量子安全服务器也采用相同的预设的处理逻辑对量子安全服务器获得的量子数据进行处理。从而，量子安全套接层终端的量子密钥存储设备301与量子安全服务器，同时更新各自的量子密钥，获得新的对称的量子密钥，同一标识对应的量子密钥是一对对称的量

子密钥。其中，预设的处理逻辑，规定了量子密钥的长度，生成量子密钥的算法等内容。

[0086] 实际应用中，量子安全套接层终端也可以直接与第一量子设备进行通信，由第一量子设备直接给量子安全套接层终端提供量子密钥。

[0087] 在图3所示的实例中，量子密钥存储设备301，是集成在量子安全套接层终端中的量子密钥存储设备301，量子密钥存储设备301向与其通信的第一量子设备请求量子数据时，该量子密钥存储设备301是通过量子安全套接层终端向第一量子设备请求量子数据，即量子安全套接层终端与第一量子设备进行通信。

[0088] 而在图4所示的实例中，量子密钥存储设备301是一个可与量子安全套接层终端分离的外接的物理实体时，该量子密钥存储设备301可以通过量子安全套接层终端向第一量子设备请求量子数据，也可以通过其他的终端设备向第一量子设备请求量子数据。只要确保量子密钥存储设备301相连的终端设备与第一量子设备进行通信即可。

[0089] 在一个例子中，所述量子安全套接层终端还包括：

[0090] 告警器，用于满足预设的告警条件时，获得所述预设的告警条件对应的告警信息，所述预设的告警条件包括量子密钥废弃，票据错误，或者票据过期；

[0091] 所述发送器，还用于将所述告警信息发送至所述量子安全服务器。

[0092] 量子安全套接层终端与量子安全服务器进行通信会话时，若会话过程出现错误，则需要立即中断会话，并删除缓冲区的会话记录。当量子安全套接层终端发现会话错误时，需要在中断会话前，向量子安全服务器发送告警信息。

[0093] 量子安全套接层终端的告警器，检测量子安全套接层终端的会话过程的数据是否错误，当会话过程中的数据满足预设的告警条件时，表示当前会话错误。在实际应用中，一种预设的告警条件对应于一种告警信息，当会话过程的数据满足一种预设的告警条件时，获取该预设的告警条件对应的告警信息。量子安全套接层终端的发送器204将该告警信息发送至量子安全服务器。

[0094] 在实际应用中，预设的告警条件包括量子密钥废弃，量子密钥废弃对应的告警信息为certificate_revoked；预设的告警条件包括票据错误，票据错误对应的告警信息为bad_certificate；预设的告警条件包括票据过期，票据过期对应的告警信息为certificate_expired。

[0095] 除此以外，量子安全套接层终端中的预设告警条件还可以包括：接收到不合适的报文，对应的告警信息为unexpected_message；接收到不正确的MAC，对应的告警信息为bad_record_mac；解压缩函数收到不适当的输入，对应的告警信息为decompression_failure；握手报文中的一个字段超出范围或与其他字段不兼容，对应的告警信息为illegal_parameter；以及握手过程失败，对应的告警信息为handshake_failure。当然，量子安全套接层终端中的预设告警条件还可以包括其他内容，这里不再一一赘述。

[0096] 量子安全服务器接收到量子安全套接层终端发送的告警信息后，即可获知量子安全套接层终端中断会话的原因。

[0097] 图6为本发明实施例提供的量子安全服务器结构示意图，包括：

[0098] 终端接口601，用于获得第一标识和第二标识，采用第一标识对应的第一量子密钥，对第一数据和第二标识进行加密获得第一密文，第一数据是发送给量子安全套接层终端的数据；采用第二标识对应的第二量子密钥，对量子安全套接层终端发送的第二密文进

行解密获得第二数据。

[0099] 处理器602，用于处理第二数据。

[0100] 第一发送器603，用于将第一标识和第一密文发送至量子安全套接层终端。

[0101] 第一接收器604，用于接收量子安全套接层终端发送的第二密文。

[0102] 量子安全服务器中的终端接口601，是实现与量子安全套接层终端进行数据交互的接口。终端接口601获取第一标识和第二标识，第一标识用于唯一标识第一量子密钥，第一量子密钥用于给第一数据进行加密，第一数据是量子安全服务器发送至量子安全套接层终端的数据。第二标识用于唯一标识第二量子密钥，而第二量子密钥用于给第二数据进行加密，第二数据是量子安全套接层终端发送至量子安全服务器的数据。

[0103] 也就是说，量子安全服务器中的终端接口601，不仅要确定其自身对第一数据加密时所采用的第一量子密钥，还要确定量子安全套接层终端对第二数据进行加密时所采用的第二量子密钥。终端接口601采用第一量子密钥对第一数据和第二标识进行加密获得第一密文，第一密文中不仅有量子安全服务器发送给量子安全套接层终端的第一数据，还有唯一标识量子安全套接层终端加密时所采用的第二量子密钥的第二标识。

[0104] 量子安全服务器中的第一发送器603将第一密文和第一标识发送至量子安全套接层终端，量子安全套接层终端可以根据第一标识获得第一量子密钥，根据第一量子密钥对第一密文进行解密，进而获得第一数据和第二标识。此内容具体实现方式与图2所示的量子安全套接层终端中的描述类似，参考图2所示的量子安全套接层终端中的技术描述，这里不再赘述。

[0105] 量子安全服务器中的第一接收器604，接收量子安全套接层终端发送的第二密文。量子安全服务器中的终端接口601，已知该量子安全套接层终端发送的第二密文所采用的加密密钥是第二量子密钥，利用第二量子密钥对第二密文进行解密，获得量子安全套接层终端发送至量子安全服务器的第二数据。量子安全服务器中的处理器602对解密获得的第二数据进行处理。

[0106] 由此可知，量子安全服务器中的终端接口601，既提供对发送至量子安全套接层终端的第一数据的加密功能，又提供对量子安全套接层终端发送的第二密文的解密功能。实现量子安全服务器与量子安全套接层终端之间交互的数据，采用量子密钥进行加密，保证量子安全套接层终端与量子安全服务器之间数据交互的安全性。

[0107] 在一个例子中，如图7所示，所述量子安全服务器还包括：

[0108] 量子密钥存储设备701，用于存储多个量子密钥以及每个量子密钥对应的标识。

[0109] 量子安全服务器中的量子密钥存储设备701，存储有多个量子密钥，以及各个量子密钥对应的标识。一个量子密钥对应的标识，能够唯一标识该量子密钥。量子安全服务器中的量子密钥存储设备701中，一个标识对应的量子密钥，与量子安全套接层终端中同一个标识对应的量子密钥，是成对的量子密钥。该量子密钥存储设备701与终端接口601相连，终端接口601从该量子密钥存储设备701中，根据标识查找该标识对应的量子密钥。

[0110] 为了进一步提高数据传输的安全性，量子安全服务器中的量子密钥存储设备701中的量子密钥，作为给量子安全套接层终端和量子安全服务器交互的数据作为加密或解密的密钥使用过一次后，则量子密钥存储设备701删除该量子密钥，以及该量子密钥对应的标识。因此，量子密钥存储设备701中的量子密钥，作为给量子安全套接层终端和量子安全服

务器交互的数据的加密或解密的密钥，只能被使用一次，能够避免重放攻击，进一步提高互联网中数据传输的安全性。

[0111] 当量子安全服务器中的量子密钥存储设备701中存储的量子密钥，满足量子密钥更新条件时，需要对量子密钥存储设备701中的量子密钥进行更新。该量子密钥更新条件有多种可能的实现形式：第一种可能的实现形式，作为给量子安全套接层终端和量子安全服务器交互的数据的加密或者解密密钥，都已经使用过一次；第二种可能的实现形式，作为给量子安全套接层终端和量子安全服务器交互的数据的加密或者解密密钥，使用数量或使用次数大于预设阈值时；第三种可能的实现形式，达到预设更新时间，该预设更新时间指的是对量子密钥存储设备701中的量子密钥进行更新的时间间隔。

[0112] 当然，量子密钥更新条件并不仅限于上述所述的三种可能的实现形式，还可以根据实际需要自行设定。

[0113] 量子安全服务器，一方面，可以提供与量子安全套接层终端实现数据交互的终端接口601；另一方面，还可以提供与不同类型的量子设备实现数据交互的量子设备接口，下面详细阐述。

[0114] 在一个例子中，如图8所示，所述量子安全服务器还包括：

[0115] 第二接收器801，用于接收第二量子设备发送的量子数据，第二量子设备与第一量子设备相连，第一量子设备给所述量子安全套接层终端提供量子数据。

[0116] 量子设备接口802，用于调用与设备标识和通信协议版本都适配的预设的处理逻辑，将量子数据利用预设的处理逻辑进行处理，获得多个新的量子密钥以及每个新的量子密钥对应的标识，将所获得的多个新的量子密钥以及每个新的量子密钥对应的标识发送至量子密钥存储设备701进行更新。

[0117] 第二发送器803，用于向所述第二量子设备发送响应信息。

[0118] 量子设备的生产厂家不同，以及所采用的通信协议的版本不同时，对该量子设备发送的量子数据所采用的预设的处理逻辑不同。举例说明，生产厂家不同时，量子安全服务器与量子设备之间所采用的通信协议类型可能不同；同一种通信协议下，通信协议版本不同，该通信协议版本的报文处理方式也可能不同。

[0119] 因此，量子安全服务器提供与量子设备进行通信的量子设备接口802。该量子设备接口802中存储有多种预设的处理逻辑，每种预设的处理逻辑可能对应一种设备标识和通信协议版本组合，也可能对应多种设备标识和通信协议版本组合，但是，一种设备标识和通信协议版本的组合只唯一的对应于一种预设的处理逻辑。量子设备接口802能够根据量子设备发送的通信请求中的设备标识，以及通信协议版本，调用与该设备标识和通信协议版本都适配的预设的处理逻辑。

[0120] 从而，量子安全服务器中的第二接收器801，接收第二量子设备发送的量子数据。可以理解的是，量子安全服务器对量子密钥存储设备701中的量子密钥进行更新时，该量子安全服务器与第二量子设备进行数据交互，于此同时，量子安全套接层终端的量子密钥存储设备301也需要进行量子密钥的更新，该量子安全套接层终端的量子密钥存储设备301与第一量子设备进行数据交互。

[0121] 第一量子设备和第二量子设备都是量子密钥分发设备时，第一量子设备和第二量子设备采用量子密钥分发技术生成对称的量子数据。第一量子设备和第二量子设备都是量

子密钥管理设备时，第一量子设备接入的量子密钥分发设备与第二量子设备接入的量子密钥分发设备采用量子密钥分发技术生成对称的量子数据，第一量子设备接收其所接入的量子密钥分发设备发送的量子数据，第二量子设备也接收其所接入的量子密钥分发设备发送的量子数据。

[0122] 量子安全服务器中的量子设备接口802，根据通信请求中的设备标识和通信协议，查找该设备标识和通信协议对应的预设的处理逻辑，调用该预设的处理逻辑处理量子设备发送的量子数据，获得多个新的量子密钥以及每个新的量子密钥对应的标识，将所获得的多个新的量子密钥以及每个新的量子密钥对应的标识发送至量子密钥存储设备701，对该量子密钥存储设备701中存储的量子密钥进行更新。。在进行量子密钥更新时，量子安全服务器中所采用的预设的处理逻辑与量子设备中所采用的预设的处理逻辑相同。量子安全服务器可以适用于不同类型的量子设备，能够处理不同类型的量子设备发送的量子数据。

[0123] 对量子数据处理结束后，量子安全服务器中的第二发送器803，向第二量子设备发送响应信息，即告知该第二量子设备对该量子数据的处理结果。

[0124] 由此可知，量子安全服务器中的量子设备接口802，能够实现该量子安全服务器与量子密钥分发网络中的量子设备进行数据交互。并且，提供了不同类型的量子设备的接入功能，实现了给不同类型的量子设备发送的数据，调用适配的预设的处理逻辑进行处理。

[0125] 在一个例子中，所述量子安全服务器还包括：

[0126] 告警器，用于满足预设的告警条件时，获得预设的告警条件对应的告警信息，预设的告警条件包括票据错误，或者票据过期；

[0127] 第一发送器603，还用于将告警信息发送至量子安全套接层终端。

[0128] 量子安全套接层终端与量子安全服务器进行通信会话时，若会话过程出现错误，则需要立即中断会话，并删除缓冲区的会话记录。当量子安全服务器发现会话错误时，需要在中断会话前，向量子安全套接层终端发送告警信息。

[0129] 量子安全服务器的告警器，检测量子安全服务器的会话过程的数据是否错误，当会话过程中的数据满足预设的告警条件时，表示当前会话错误。在实际应用中，一种预设的告警条件对应于一种告警信息，当会话过程的数据满足一种预设的告警条件时，获取该预设的告警条件对应的告警信息。量子安全服务器的第一发送器603将该告警信息发送至量子安全套接层终端。

[0130] 在实际应用中，预设的告警条件包括票据错误，票据错误对应的告警信息为bad_certificate；预设的告警条件包括票据过期，票据过期对应的告警信息为certificate_expired。

[0131] 除此以外，量子安全服务器中的预设告警条件还可以包括：解压缩函数收到不适当的输入，对应的告警信息为decompression_failure；握手报文中的一个字段超出范围或与其他字段不兼容，对应的告警信息为illegal_parameter。当然，量子安全服务器中的预设告警条件还可以包括其他内容，这里不再一一赘述。

[0132] 量子安全套接层终端接收到量子安全服务器发送的告警信息后，即可获知量子安全服务器中断会话的原因。

[0133] 图9为本发明实施例提供的量子安全套接层系统结构示意图，包括：

[0134] 上述内容所述的量子安全套接层终端901，以及上述内容所述的量子安全服务器

902。

[0135] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

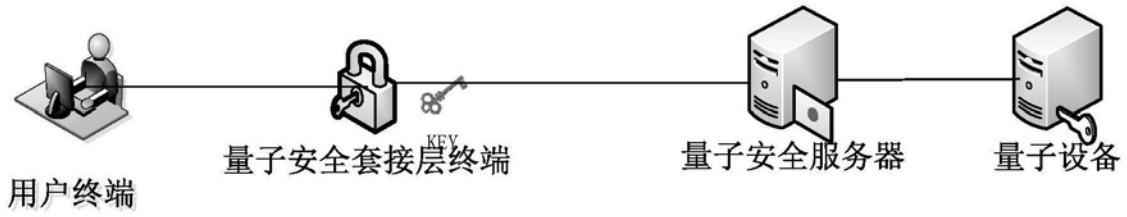

用户终端
KEY
量子安全套接层终端
量子安全服务器
量子设备

图1

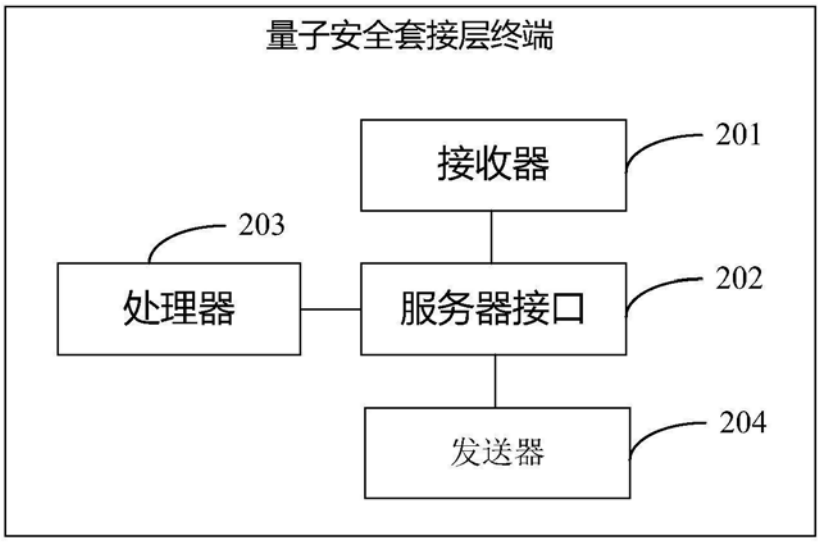

量子安全套接层终端
接收器
201
203
处理器
服务器接口
202
发送器
204

图2

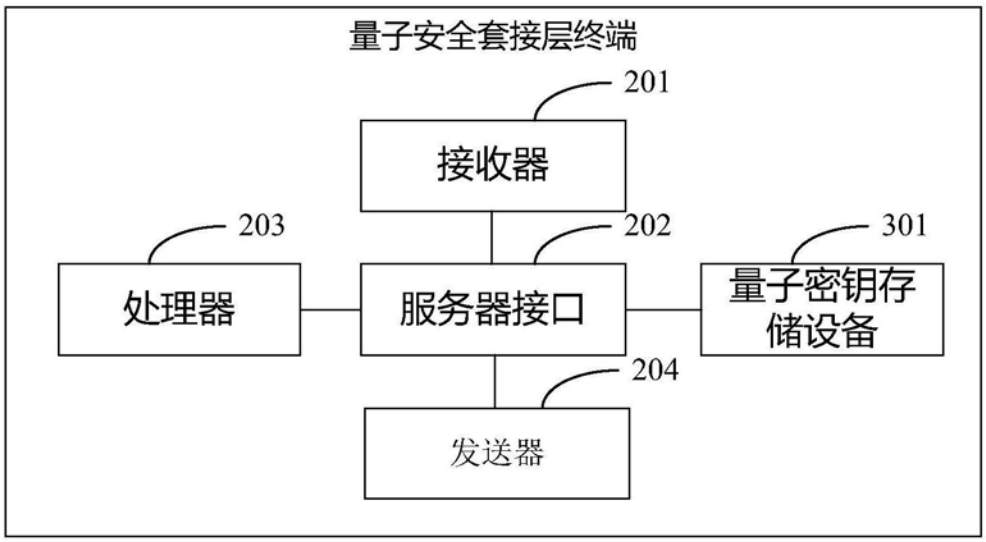

量子安全套接层终端
201
接收器
203
202
301
处理器
服务器接口
量子密钥存储设备
204
发送器

图3

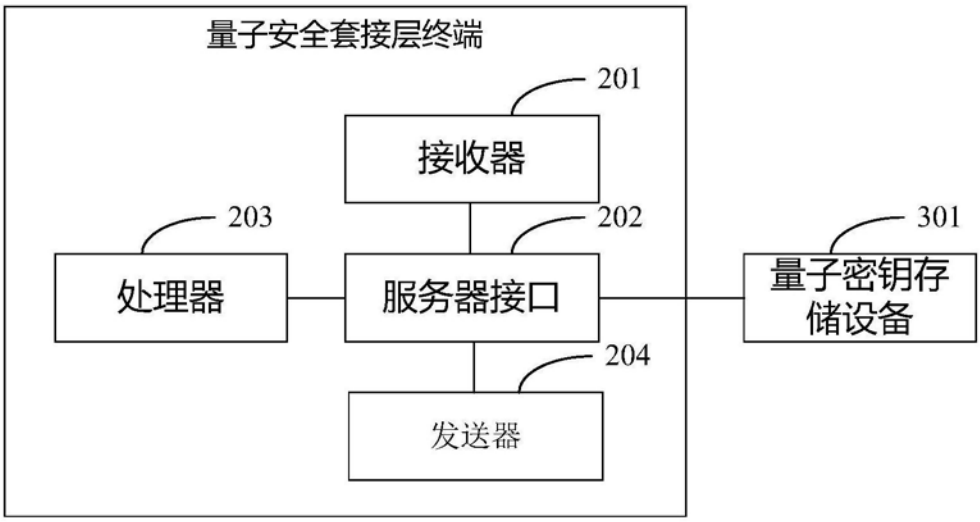

量子安全套接层终端
201
接收器
203
处理器
202
服务器接口
301
量子密钥存储设备
204
发送器

图4

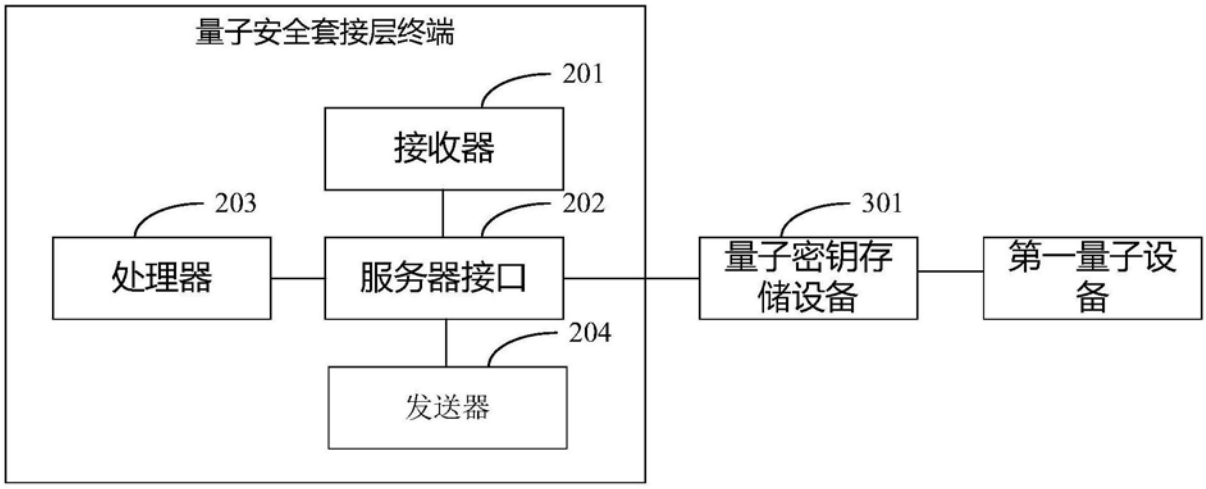

量子安全套接层终端
201
接收器
203
处理器
202
服务器接口
301
量子密钥存储设备
第一量子设备
204
发送器

图5

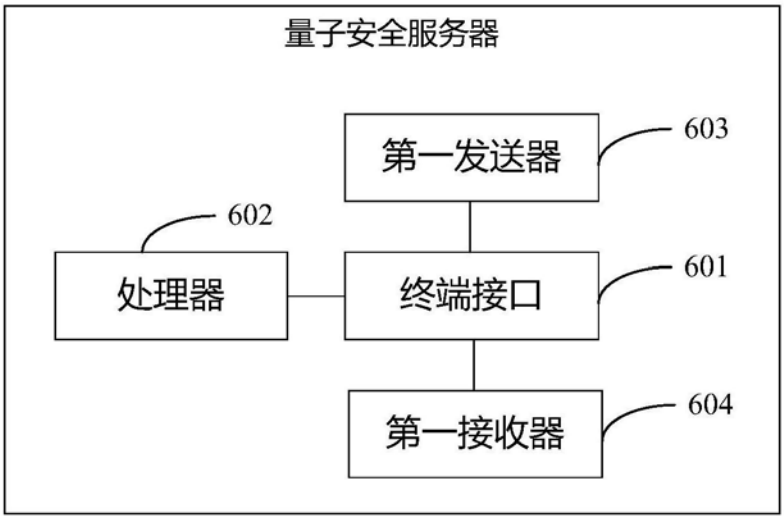

量子安全服务器
第一发送器
603
602
处理器
终端接口
601
第一接收器
604

图6

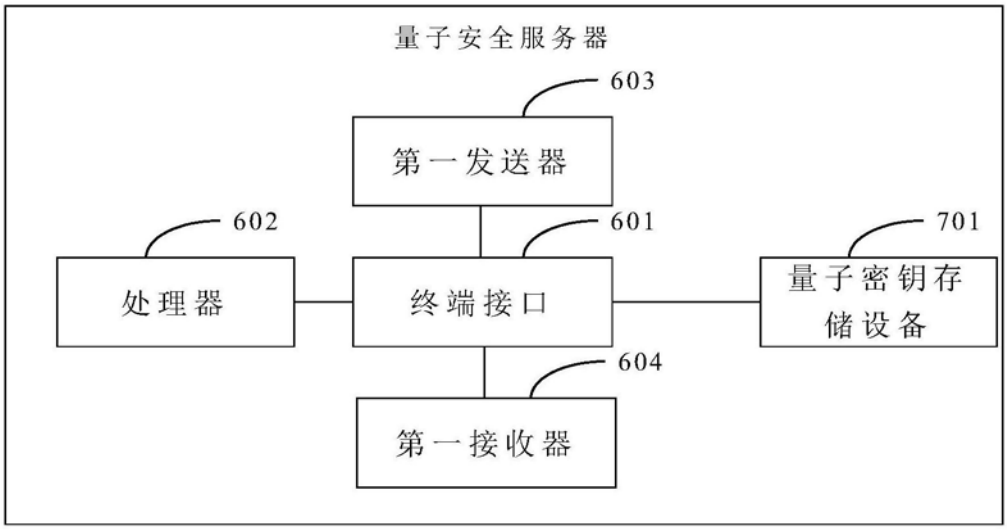

量子安全服务器
603
第一发送器
602
601
701
处理器
终端接口
量子密钥存储设备
604
第一接收器

图7

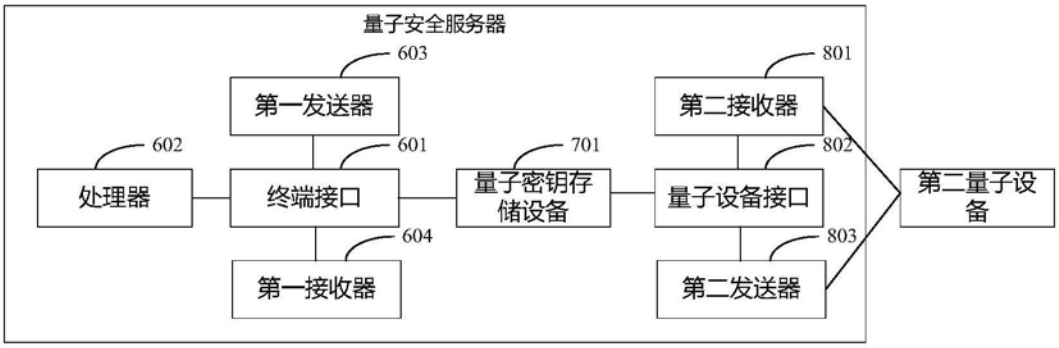

量子安全服务器
603
801
第一发送器
第二接收器
602
601
701
802
处理器
终端接口
量子密钥存储设备
量子设备接口
第二量子设备
604
803
第一接收器
第二发送器

图8

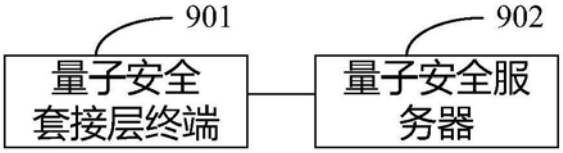



图9