(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116633530 A
(43)申请公布日 2023.08.22

(21)申请号 202210187877.0

(22)申请日 2022.02.28

(66)本国优先权数据
202210132323.0 2022.02.14 CN

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 谢天元 李民 张慧

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
专利代理师 郑晓玉

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/06(2006.01)
H04L 9/32(2006.01)

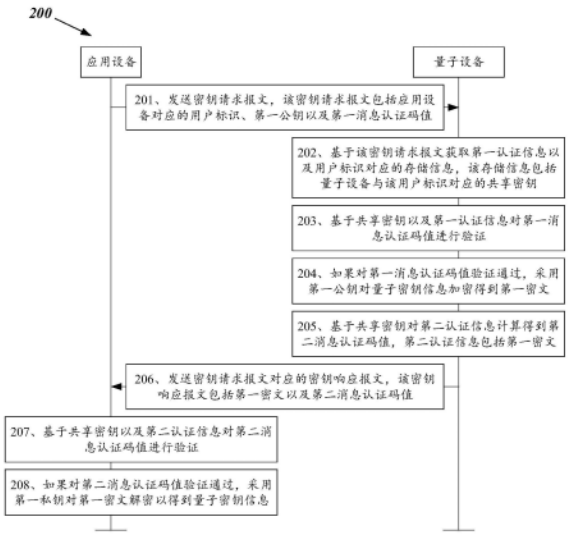
权利要求书9页 说明书26页 附图8页

(54)发明名称

量子密钥传输方法、装置及系统

(57)摘要

本申请公开了一种量子密钥传输方法、装置及系统，属于网络技术领域。应用设备向量子设备发送密钥请求报文，该密钥请求报文包括应用设备对应的用户标识、第一公钥和第一消息认证码值。如果量子设备对第一消息认证码值验证通过，量子设备向应用设备发送密钥响应报文，该密钥响应报文包括第一密文和第二消息认证码值。如果应用设备对第二消息认证码值验证通过，应用设备采用第一私钥对第一密文解密得到量子设备分配给该应用设备的量子密钥信息。第一公钥和第一私钥来自应用设备运行后量子密钥生成算法得到的密钥对。本申请实现了应用设备与量子设备之间的双向身份认证以及消息完整性验证，同时也保证了量子密钥的传输机密性。



CN 116633530 A

1.一种量子密钥传输方法,其特征在于,所述方法包括:

应用设备向量子设备发送密钥请求报文,所述密钥请求报文包括所述应用设备对应的用户标识、第一公钥以及第一消息认证码值,所述用户标识用于所述量子设备获取对应的存储信息,所述存储信息包括所述量子设备与所述用户标识对应的共享密钥,所述第一公钥用于所述量子设备对分配给所述应用设备的量子密钥信息加密,所述量子密钥信息包括量子密钥,所述第一公钥为所述应用设备运行后量子密钥生成算法得到的密钥对中的公钥,所述第一消息认证码值由所述应用设备基于所述共享密钥对第一认证信息计算得到,所述第一认证信息包括所述第一公钥;

所述应用设备接收来自所述量子设备的所述密钥请求报文对应的密钥响应报文,所述密钥响应报文包括第一密文以及第二消息认证码值;

所述应用设备基于所述共享密钥以及第二认证信息对所述第二消息认证码值进行验证,所述第二认证信息包括所述第一密文;

如果所述应用设备对所述第二消息认证码值验证通过,所述应用设备采用第一私钥对所述第一密文解密以得到量子密钥信息,所述第一私钥为所述密钥对中的私钥。

2.根据权利要求1所述的方法,其特征在于,所述应用设备对应的用户标识为所述应用设备的设备标识,或者,所述应用设备对应的用户标识为登录所述应用设备的用户账号。

3.根据权利要求1或2所述的方法,其特征在于,所述密钥请求报文还包括第一统计值,在所述应用设备向量子设备发送密钥请求报文之前,所述方法还包括:

所述应用设备获取包括所述用户标识的密钥请求报文的历史发送次数;

所述应用设备在所述历史发送次数上增加设定递增值,得到所述第一统计值。

4.根据权利要求3所述的方法,其特征在于,所述密钥响应报文还包括第二统计值,所述第二统计值为所述量子设备记录的包括所述用户标识的密钥请求报文的发送次数,在所述应用设备接收所述密钥请求报文对应的密钥响应报文之后,所述方法还包括:

如果所述第二统计值与所述第一统计值不相等,所述应用设备停止量子密钥传输流程。

5.根据权利要求3或4所述的方法,其特征在于,所述第一认证信息还包括所述量子设备的设备标识、所述用户标识或所述第一统计值中的一个或多个。

6.根据权利要求1至5任一所述的方法,其特征在于,在所述应用设备向量子设备发送密钥请求报文之前,所述方法还包括:

所述应用设备采用密钥派生函数基于目标口令生成派生密钥,所述共享密钥基于所述派生密钥得到。

7.根据权利要求6所述的方法,其特征在于,在所述应用设备向量子设备发送密钥请求报文之前,所述方法还包括:

响应于获取到输入的量子密钥获取指令,所述应用设备运行所述后量子密钥生成算法生成所述密钥对,所述量子密钥获取指令包括所述目标口令;

所述应用设备基于所述共享密钥对所述第一认证信息计算得到所述第一消息认证码值。

8.根据权利要求6或7所述的方法,其特征在于,在所述应用设备向量子设备发送密钥请求报文之前,所述方法还包括:

所述应用设备向所述量子设备发送注册请求报文；

所述应用设备接收来自所述量子设备的所述注册请求报文对应的注册响应报文，所述注册响应报文包括所述量子设备的证书，所述证书包括第二公钥；

如果所述应用设备对所述证书验证通过，所述应用设备采用所述第二公钥对注册信息加密得到第二密文，所述注册信息包括所述派生密钥以及所述用户标识；

所述应用设备向所述量子设备发送注册登记报文，所述注册登记报文包括所述第二密文。

9.根据权利要求8所述的方法，其特征在于，所述注册请求报文指示所述应用设备支持的密码算法，所述注册响应报文还指示所述量子设备从所述应用设备支持的密码算法中选择的目标密码算法，所述目标密码算法包括所述第一消息认证码值的生成算法、所述第二消息认证码值的生成算法或所述共享密钥的生成算法中的一个或多个。

10.根据权利要求8或9所述的方法，其特征在于，所述注册响应报文还包括密钥派生函数参数值，所述密钥派生函数参数值包括随机盐值和/或迭代次数，所述应用设备接收所述注册请求报文对应的注册响应报文之后，所述方法还包括：

所述应用设备获取所述用户标识以及所述目标口令；

所述应用设备采用密钥派生函数基于目标口令生成派生密钥，包括：

所述应用设备采用所述密钥派生函数基于所述目标口令以及所述密钥派生函数参数值生成所述派生密钥。

11.根据权利要求8至10任一所述的方法，其特征在于，所述注册登记报文还包括所述应用设备的设备标识，所述注册信息还包括所述应用设备的设备标识的哈希值。

12.根据权利要求8至11任一所述的方法，其特征在于，所述注册信息还包括所述应用设备生成的第一随机数，所述方法还包括：

所述应用设备接收来自所述量子设备的注册成功响应报文，所述注册成功响应报文用于指示所述用户标识已注册成功，所述注册成功响应报文包括第二随机数；

如果所述第二随机数与所述第一随机数相同，所述应用设备确定所述用户标识注册成功。

13.根据权利要求1至12任一所述的方法，其特征在于，所述应用设备基于所述共享密钥以及第二认证信息对所述第二消息认证码值进行验证，包括：

所述应用设备基于所述共享密钥对所述第二认证信息计算得到第三消息认证码值；

如果所述第三消息认证码值与所述第二消息认证码值相同，所述应用设备确定对所述第二消息认证码值验证通过。

14.根据权利要求1至13任一所述的方法，其特征在于，所述应用设备与所述量子设备通过经典网络通信。

15.一种量子密钥传输方法，其特征在于，所述方法包括：

量子设备接收来自应用设备的密钥请求报文，所述密钥请求报文包括所述应用设备对应的用户标识、第一公钥以及第一消息认证码值；

所述量子设备基于所述密钥请求报文获取第一认证信息以及所述用户标识对应的存储信息，所述存储信息包括所述量子设备与所述用户标识对应的共享密钥，所述第一认证信息包括所述第一公钥；

所述量子设备基于所述共享密钥以及所述第一认证信息对所述第一消息认证码值进行验证；

如果所述量子设备对所述第一消息认证码值验证通过，所述量子设备采用所述第一公钥对量子密钥信息加密得到第一密文，所述量子密钥信息包括量子密钥；

所述量子设备基于所述共享密钥对第二认证信息计算得到第二消息认证码值，所述第二认证信息包括所述第一密文；

所述量子设备向所述应用设备发送所述密钥请求报文对应的密钥响应报文，所述密钥响应报文包括所述第一密文以及所述第二消息认证码值。

16.根据权利要求15所述的方法，其特征在于，所述应用设备对应的用户标识为所述应用设备的设备标识，或者，所述应用设备对应的用户标识为登录所述应用设备的用户账号。

17.根据权利要求15或16所述的方法，其特征在于，所述密钥请求报文还包括第一统计值，所述第一统计值为所述应用设备记录的包括所述用户标识的密钥请求报文的发送次数，所述存储信息包括第二统计值，所述第二统计值为所述量子设备记录的包括所述用户标识的密钥请求报文的发送次数，在所述量子设备获取所述用户标识对应的存储信息之后，所述方法还包括：

如果所述第二统计值大于或等于所述第一统计值，所述量子设备停止量子密钥传输流程；

如果所述第二统计值小于所述第一统计值，所述量子设备更新所述第二统计值，使更新后的第二统计值等于所述第一统计值。

18.根据权利要求17所述的方法，其特征在于，所述密钥响应报文还包括所述更新后的第二统计值。

19.根据权利要求17或18所述的方法，其特征在于，所述第二认证信息还包括所述量子设备的设备标识、所述用户标识或所述更新后的第二统计值中的一个或多个。

20.根据权利要求15至19任一所述的方法，其特征在于，所述方法还包括：

所述量子设备接收来自所述应用设备的注册请求报文；

所述量子设备向所述应用设备发送注册响应报文，所述注册响应报文包括所述量子设备的证书，所述证书包括第二公钥，所述第二公钥为所述量子设备运行后量子密钥生成算法得到的密钥对中的公钥；

如果所述量子设备接收到来自所述应用设备的包括第二密文的注册登记报文，所述量子设备采用第二私钥对所述第二密文解密以得到注册信息，所述注册信息包括派生密钥以及所述应用设备对应的用户标识，所述第二私钥为所述密钥对中的私钥；

所述量子设备存储所述用户标识对应的存储信息，所述存储信息包括基于所述派生密钥得到的所述共享密钥以及所述用户标识。

21.根据权利要求20所述的方法，其特征在于，所述注册请求报文指示所述应用设备支持的密码算法，所述注册响应报文还指示所述量子设备从所述应用设备支持的密码算法中选择的目标密码算法，所述目标密码算法包括所述第一消息认证码值的生成算法、所述第二消息认证码值的生成算法或所述共享密钥的生成算法中的一个或多个。

22.根据权利要求20或21所述的方法，其特征在于，所述注册响应报文还包括第一密钥派生函数参数值，所述第一密钥派生函数参数值包括随机盐值和/或迭代次数，所述注册信

息还包括第二密钥派生函数参数值，在所述量子设备采用第二私钥对所述第二密文解密以得到注册信息之后，所述方法还包括：

所述量子设备比对所述第一密钥派生函数参数值与所述第二密钥派生函数参数值；

所述量子设备存储所述用户标识对应的存储信息，包括：

如果所述第一密钥派生函数参数值与所述第二密钥派生函数参数值相同，所述量子设备存储所述用户标识对应的存储信息。

23.根据权利要求20至22任一所述的方法，其特征在于，所述注册登记报文还包括所述应用设备的设备标识，所述注册信息还包括所述应用设备的设备标识的第一哈希值，在所述量子设备采用第二私钥对所述第二密文解密以得到注册信息之后，所述方法还包括：

所述量子设备计算所述应用设备的设备标识的第二哈希值；

所述量子设备比对所述第一哈希值与所述第二哈希值；

所述量子设备存储所述用户标识对应的存储信息，包括：

如果所述第一哈希值与所述第二哈希值相同，所述量子设备存储所述用户标识对应的存储信息。

24.根据权利要求20至23任一所述的方法，其特征在于，所述注册信息还包括所述应用设备生成的随机数，在所述量子设备存储所述用户标识对应的存储信息之后，所述方法还包括：

所述量子设备向所述应用设备发送注册成功响应报文，所述注册成功响应报文用于指示所述用户标识已注册成功，所述注册成功响应报文包括所述随机数。

25.根据权利要求15至24任一所述的方法，其特征在于，所述量子设备基于所述共享密钥以及所述第一认证信息对所述第一消息认证码值进行验证，包括：

所述量子设备基于所述共享密钥对所述第一认证信息计算得到第四消息认证码值；

如果所述第四消息认证码值与所述第一消息认证码值相同，所述量子设备确定对所述第一消息认证码值验证通过。

26.根据权利要求15至25任一所述的方法，其特征在于，所述应用设备与所述量子设备通过经典网络通信。

27.一种应用设备，其特征在于，包括：存储器、网络接口和至少一个处理器，

所述存储器用于存储程序指令，

所述至少一个处理器读取所述存储器中保存的程序指令后，使得所述应用设备执行以下操作：

向量子设备发送密钥请求报文，所述密钥请求报文包括所述应用设备对应的用户标识、第一公钥以及第一消息认证码值，所述用户标识用于所述量子设备获取对应的存储信息，所述存储信息包括所述量子设备与所述用户标识对应的共享密钥，所述第一公钥用于所述量子设备对分配给所述应用设备的量子密钥信息加密，所述量子密钥信息包括量子密钥，所述第一公钥为所述应用设备运行后量子密钥生成算法得到的密钥对中的公钥，所述第一消息认证码值由所述应用设备基于所述共享密钥对第一认证信息计算得到，所述第一认证信息包括所述第一公钥；

接收来自所述量子设备的所述密钥请求报文对应的密钥响应报文，所述密钥响应报文包括第一密文以及第二消息认证码值；

基于所述共享密钥以及第二认证信息对所述第二消息认证码值进行验证，所述第二认证信息包括所述第一密文；

如果所述应用设备对所述第二消息认证码值验证通过，采用第一私钥对所述第一密文解密以得到量子密钥信息，所述第一私钥为所述密钥对中的私钥。

28.根据权利要求27所述的应用设备，其特征在于，所述应用设备对应的用户标识为所述应用设备的设备标识，或者，所述应用设备对应的用户标识为登录所述应用设备的用户账号。

29.根据权利要求27或28所述的应用设备，其特征在于，所述密钥请求报文还包括第一统计值，所述程序指令被所述至少一个处理器读取后，使得所述应用设备还执行以下操作：

在向所述量子设备发送密钥请求报文之前，获取包括所述用户标识的密钥请求报文的历史发送次数；

在所述历史发送次数上增加设定递增值，得到所述第一统计值。

30.根据权利要求29所述的应用设备，其特征在于，所述密钥响应报文还包括第二统计值，所述第二统计值为所述量子设备记录的包括所述用户标识的密钥请求报文的发送次数，所述程序指令被所述至少一个处理器读取后，使得所述应用设备还执行以下操作：

在接收到所述密钥响应报文之后，如果所述第二统计值与所述第一统计值不相等，停止量子密钥传输流程。

31.根据权利要求29或30所述的应用设备，其特征在于，所述第一认证信息还包括所述量子设备的设备标识、所述用户标识或所述第一统计值中的一个或多个。

32.根据权利要求27至31任一所述的应用设备，其特征在于，所述程序指令被所述至少一个处理器读取后，使得所述应用设备还执行以下操作：

在向所述量子设备发送密钥请求报文之前，采用密钥派生函数基于目标口令生成派生密钥，所述共享密钥基于所述派生密钥得到。

33.根据权利要求32所述的应用设备，其特征在于，所述程序指令被所述至少一个处理器读取后，使得所述应用设备还执行以下操作：

在向所述量子设备发送密钥请求报文之前，响应于获取到输入的量子密钥获取指令，运行所述后量子密钥生成算法生成所述密钥对，所述量子密钥获取指令包括所述目标口令；

基于所述共享密钥对所述第一认证信息计算得到所述第一消息认证码值。

34.根据权利要求32或33所述的应用设备，其特征在于，所述程序指令被所述至少一个处理器读取后，使得所述应用设备还执行以下操作：

在向所述量子设备发送密钥请求报文之前，向所述量子设备发送注册请求报文；

接收来自所述量子设备的所述注册请求报文对应的注册响应报文，所述注册响应报文包括所述量子设备的证书，所述证书包括第二公钥；

如果所述应用设备对所述证书验证通过，采用所述第二公钥对注册信息加密得到第二密文，所述注册信息包括所述派生密钥以及所述用户标识；

向所述量子设备发送注册登记报文，所述注册登记报文包括所述第二密文。

35.根据权利要求34所述的应用设备，其特征在于，所述注册请求报文指示所述应用设备支持的密码算法，所述注册响应报文还指示所述量子设备从所述应用设备支持的密码算

法中选择的目标密码算法，所述目标密码算法包括所述第一消息认证码值的生成算法、所述第二消息认证码值的生成算法或所述共享密钥的生成算法中的一个或多个。

36.根据权利要求34或35所述的应用设备，其特征在于，所述注册响应报文还包括密钥派生函数参数值，所述密钥派生函数参数值包括随机盐值和/或迭代次数，所述程序指令被所述至少一个处理器读取后，使得所述应用设备还执行以下操作：

接收到所述注册响应报文之后，获取所述用户标识以及所述目标口令；

采用所述密钥派生函数基于所述目标口令以及所述密钥派生函数参数值生成所述派生密钥。

37.根据权利要求34至36任一所述的应用设备，其特征在于，所述注册登记报文还包括所述应用设备的设备标识，所述注册信息还包括所述应用设备的设备标识的哈希值。

38.根据权利要求34至37任一所述的应用设备，其特征在于，所述注册信息还包括所述应用设备生成的第一随机数，所述程序指令被所述至少一个处理器读取后，使得所述应用设备还执行以下操作：

接收来自所述量子设备的注册成功响应报文，所述注册成功响应报文用于指示所述用户标识已注册成功，所述注册成功响应报文包括第二随机数；

如果所述第二随机数与所述第一随机数相同，确定所述用户标识注册成功。

39.根据权利要求27至38任一所述的应用设备，其特征在于，所述程序指令被所述至少一个处理器读取后，使得所述应用设备执行以下操作：

基于所述共享密钥对所述第二认证信息计算得到第三消息认证码值；

如果所述第三消息认证码值与所述第二消息认证码值相同，确定对所述第二消息认证码值验证通过。

40.根据权利要求27至39任一所述的应用设备，其特征在于，所述应用设备与所述量子设备通过经典网络通信。

41.一种量子设备，其特征在于，包括：存储器、网络接口和至少一个处理器，

所述存储器用于存储程序指令，

所述至少一个处理器读取所述存储器中保存的程序指令后，使得所述量子设备执行以下操作：

接收来自应用设备的密钥请求报文，所述密钥请求报文包括所述应用设备对应的用户标识、第一公钥以及第一消息认证码值；

基于所述密钥请求报文获取第一认证信息以及所述用户标识对应的存储信息，所述存储信息包括所述量子设备与所述用户标识对应的共享密钥，所述第一认证信息包括所述第一公钥；

基于所述共享密钥以及所述第一认证信息对所述第一消息认证码值进行验证；

如果所述量子设备对所述第一消息认证码值验证通过，采用所述第一公钥对量子密钥信息加密得到第一密文，所述量子密钥信息包括量子密钥；

基于所述共享密钥对第二认证信息计算得到第二消息认证码值，所述第二认证信息包括所述第一密文；

向所述应用设备发送所述密钥请求报文对应的密钥响应报文，所述密钥响应报文包括所述第一密文以及所述第二消息认证码值。

42.根据权利要求41所述的量子设备，其特征在于，所述应用设备对应的用户标识为所述应用设备的设备标识，或者，所述应用设备对应的用户标识为登录所述应用设备的用户账号。

43.根据权利要求41或42所述的量子设备，其特征在于，所述密钥请求报文还包括第一统计值，所述第一统计值为所述应用设备记录的包括所述用户标识的密钥请求报文的发送次数，所述存储信息包括第二统计值，所述第二统计值为所述量子设备记录的包括所述用户标识的密钥请求报文的发送次数，所述程序指令被所述至少一个处理器读取后，使得所述量子设备还执行以下操作：

在获取所述用户标识对应的存储信息之后，如果所述第二统计值大于或等于所述第一统计值，停止量子密钥传输流程；

如果所述第二统计值小于所述第一统计值，更新所述第二统计值，使更新后的第二统计值等于所述第一统计值。

44.根据权利要求43所述的量子设备，其特征在于，所述密钥响应报文还包括所述更新后的第二统计值。

45.根据权利要求43或44所述的量子设备，其特征在于，所述第二认证信息还包括所述量子设备的设备标识、所述用户标识或所述更新后的第二统计值中的一个或多个。

46.根据权利要求41至45任一所述的量子设备，其特征在于，所述程序指令被所述至少一个处理器读取后，使得所述量子设备还执行以下操作：

接收来自所述应用设备的注册请求报文；

向所述应用设备发送注册响应报文，所述注册响应报文包括所述量子设备的证书，所述证书包括第二公钥，所述第二公钥为所述量子设备运行后量子密钥生成算法得到的密钥对中的公钥；

如果接收到来自所述应用设备的包括第二密文的注册登记报文，采用第二私钥对所述第二密文解密以得到注册信息，所述注册信息包括派生密钥以及所述应用设备对应的用户标识，所述第二私钥为所述密钥对中的私钥；

存储所述用户标识对应的存储信息，所述存储信息包括基于所述派生密钥得到的所述共享密钥以及所述用户标识。

47.根据权利要求46所述的量子设备，其特征在于，所述注册请求报文指示所述应用设备支持的密码算法，所述注册响应报文还指示所述量子设备从所述应用设备支持的密码算法中选择的目标密码算法，所述目标密码算法包括所述第一消息认证码值的生成算法、所述第二消息认证码值的生成算法或所述共享密钥的生成算法中的一个或多个。

48.根据权利要求46或47所述的量子设备，其特征在于，所述注册响应报文还包括第一密钥派生函数参数值，所述第一密钥派生函数参数值包括随机盐值和/或迭代次数，所述注册信息还包括第二密钥派生函数参数值，所述程序指令被所述至少一个处理器读取后，使得所述量子设备还执行以下操作：

在得到所述注册信息之后，比对所述第一密钥派生函数参数值与所述第二密钥派生函数参数值；

如果所述第一密钥派生函数参数值与所述第二密钥派生函数参数值相同，存储所述用户标识对应的存储信息。

49.根据权利要求46至48任一所述的量子设备，其特征在于，所述注册登记报文还包括所述应用设备的设备标识，所述注册信息还包括所述应用设备的设备标识的第一哈希值，所述程序指令被所述至少一个处理器读取后，使得所述量子设备还执行以下操作：

在得到所述注册信息之后，计算所述应用设备的设备标识的第二哈希值；

比对所述第一哈希值与所述第二哈希值；

如果所述第一哈希值与所述第二哈希值相同，存储所述用户标识对应的存储信息。

50.根据权利要求46至49任一所述的量子设备，其特征在于，所述注册信息还包括所述应用设备生成的随机数，所述程序指令被所述至少一个处理器读取后，使得所述量子设备还执行以下操作：

在存储所述用户标识对应的存储信息之后，向所述应用设备发送注册成功响应报文，所述注册成功响应报文用于指示所述用户标识已注册成功，所述注册成功响应报文包括所述随机数。

51.根据权利要求41至50任一所述的量子设备，其特征在于，所述程序指令被所述至少一个处理器读取后，使得所述量子设备执行以下操作：

基于所述共享密钥对所述第一认证信息计算得到第四消息认证码值；

如果所述第四消息认证码值与所述第一消息认证码值相同，确定对所述第一消息认证码值验证通过。

52.根据权利要求41至51任一所述的量子设备，其特征在于，所述应用设备与所述量子设备通过经典网络通信。

53.一种量子密钥传输系统，其特征在于，包括：第一应用设备和第一量子设备；

所述第一应用设备用于向所述第一量子设备发送密钥请求报文，所述密钥请求报文包括所述第一应用设备对应的用户标识、第一公钥以及第一消息认证码值，所述第一公钥为所述第一应用设备运行后量子密钥生成算法得到的密钥对中的公钥，所述第一消息认证码值由所述第一应用设备基于所述量子设备与所述用户标识对应的共享密钥对第一认证信息计算得到，所述第一认证信息包括所述第一公钥；

所述第一量子设备用于基于所述密钥请求报文获取所述第一认证信息以及所述用户标识对应的存储信息，所述存储信息包括所述共享密钥；

所述第一量子设备用于基于所述共享密钥以及所述第一认证信息对所述第一消息认证码值进行验证；

如果所述第一量子设备对所述第一消息认证码值验证通过，所述第一量子设备用于采用所述第一公钥对量子密钥信息加密得到第一密文，所述量子密钥信息包括量子密钥；

所述第一量子设备用于基于所述共享密钥对第二认证信息计算得到第二消息认证码值，所述第二认证信息包括所述第一密文；

所述第一量子设备用于向所述第一应用设备发送所述密钥请求报文对应的密钥响应报文，所述密钥响应报文包括所述第一密文以及所述第二消息认证码值；

所述第一应用设备用于基于所述密钥响应报文获取所述第二认证信息；

所述第一应用设备用于基于所述共享密钥以及所述第二认证信息对所述第二消息认证码值进行验证；

如果所述第一应用设备对所述第二消息认证码值验证通过，所述第一应用设备用于采

用第一私钥对所述第一密文解密以得到量子密钥信息,所述第一私钥为所述密钥对中的私钥。

54.根据权利要求53所述的系统,其特征在于,所述量子密钥信息还包括所述量子密钥的密钥标识,所述系统还包括第二应用设备和第二量子设备;

所述第一量子设备还用于向所述第二量子设备发送所述量子密钥信息;

所述第一应用设备还用于向所述第二应用设备发送所述密钥标识;

所述第二应用设备用于向所述第二量子设备发送密钥获取请求,所述密钥获取请求包括所述密钥标识;

所述第二量子设备用于基于所述密钥标识向所述第二应用设备发送所述量子密钥;

所述第一应用设备与所述第二应用设备用于基于所述量子密钥进行通信。

55.根据权利要求54所述的系统,其特征在于,所述第一量子设备与所述第二量子设备通过量子网络通信,所述第一量子设备与所述第一应用设备通过经典网络通信,所述第二量子设备与所述第二应用设备通过经典网络通信,所述第一应用设备与所述第二应用设备通过经典网络通信。

56.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有指令,当所述指令被应用设备的处理器执行时,实现如权利要求1至14任一所述的方法;或者,当所述指令被量子设备的处理器执行时,实现如权利要求15至26任一所述的方法。

量子密钥传输方法、装置及系统

[0001] 本申请要求于2022年02月14日提交的申请号为202210132323.0,发明名称为“一种密钥的传输方法、系统及相关装置”的中国专利申请的优先权,其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及网络技术领域,特别涉及一种量子密钥传输方法、装置及系统。

背景技术

[0003] 随着量子计算机的发展,量子攻击对当前广泛使用的密码体制造成了巨大的威胁。量子攻击是运行在量子计算机上的攻击算法,能够破解例如RSA(rivest-shamir-adleman)算法和椭圆曲线密码学(elliptic curves cryptography,ECC)算法等当前广泛使用的公钥密码算法。量子计算机预计在未来数十年时间内可实现。如果窃听者将使用当前加密算法加密后通过网络传输的数据保存下来,等到量子计算机实现后再通过量子攻击破解所保存的数据使用的加密算法,就可以得到解密后的明文数据。这对于需要长期保存的机密信息来说是一种巨大的威胁。因此设计能够抵抗量子攻击的密码技术成了刻不容缓的事情。

[0004] 量子密钥分发(quantum key distribution,QKD)是一种安全的密钥分发技术,能够在两个相距遥远的通信端之间实现密钥的安全传输。量子密钥分发的安全性由量子力学的基本原理保证。因此在量子网络中,量子密钥的传输理论上是无条件安全的。

[0005] 但是,对于使用量子密钥的应用设备和分发量子密钥的量子设备部署在不同安全域的情形,量子设备需要通过经典网络才能将量子密钥传输给应用设备。因此如何保障量子密钥在经典网络中传输的安全性和可靠性是目前亟需解决的问题。

发明内容

[0006] 本申请提供了一种量子密钥传输方法、装置及系统,能够实现量子密钥在经典网络中的安全传输。

[0007] 第一方面,提供了一种量子密钥传输方法。应用设备向量子设备发送密钥请求报文。密钥请求报文包括应用设备对应的用户标识、第一公钥以及第一消息认证码值。该用户标识用于量子设备获取对应的存储信息。该存储信息包括量子设备与用户标识对应的共享密钥。第一公钥用于量子设备对分配给应用设备的量子密钥信息加密。该量子密钥信息包括量子密钥。第一公钥为应用设备运行后量子密钥生成算法得到的密钥对中的公钥。第一消息认证码值由应用设备基于共享密钥对第一认证信息计算得到。第一认证信息包括第一公钥。应用设备接收来自量子设备的密钥请求报文对应的密钥响应报文。该密钥响应报文包括第一密文以及第二消息认证码值。应用设备基于共享密钥以及第二认证信息对第二消息认证码值进行验证。第二认证信息包括第一密文。如果应用设备对第二消息认证码值验证通过,应用设备采用第一私钥对第一密文解密以得到量子密钥信息。第一私钥为密钥对

中的私钥。

[0008] 其中，用户标识用于指示服务对象。该服务对象为应用设备或登录应用设备的用户账号。如果应用设备接收到的密钥响应报文确认来自量子设备并且未经篡改，则第一密文由量子设备采用第一公钥对量子密钥信息加密得到。第二消息认证码由量子设备基于共享密钥对第二认证信息计算得到。第二认证信息包括第一密文。

[0009] 由于量子设备用于加密量子密钥信息的第一公钥是应用设备运行后量子密钥生成算法得到的，因此量子设备会采用后量子加密算法对量子密钥加密后以密文的形式向应用设备传输量子密钥，保证了量子密钥的传输机密性。另外，由于传输的密文采用后量子加密算法加密得到，因此能够抵抗量子攻击，避免密文被量子计算机破解而造成量子密钥的泄露。第一消息认证码值能够用于量子设备对应用设备进行身份认证(即验证密钥请求报文的来源可靠性)，还能够用于量子设备对密钥请求报文进行消息完整性验证。第二消息认证码值能够用于应用设备对量子设备进行身份认证(即验证密钥响应报文的来源可靠性)，还能够用于应用设备对密钥响应报文进行消息完整性验证。因此本申请中，应用设备与量子设备之间能够进行双向身份认证，还能分别对各自接收到的报文进行消息完整性验证，同时也保证了量子密钥的传输机密性。进而实现了量子密钥在经典网络中传输的安全性和可靠性。另外，应用设备向量子设备请求获取量子密钥这个过程只需要两一轮报文交互就能完成量子密钥的传输以及双方身份认证，交互过程简单。

[0010] 可选地，应用设备对应的用户标识为该应用设备的设备标识，这种情况下，上述量子设备与用户标识对应的共享密钥为量子设备与该应用设备之间的共享密钥。或者，应用设备对应的用户标识为登录应用设备的用户账号，这种情况下，上述量子设备与用户标识对应的共享密钥为量子设备与该用户账号之间的共享密钥。

[0011] 可选地，密钥请求报文还包括第一统计值。在应用设备向量子设备发送密钥请求报文之前，应用设备获取包括用户标识的密钥请求报文的历史发送次数。应用设备在历史发送次数上增加设定递增值，得到第一统计值。

[0012] 本申请中，通过在应用设备发送的密钥请求报文中携带第一统计值，辅助量子设备侧实现重放攻击检测。

[0013] 可选地，密钥响应报文还包括第二统计值。第二统计值为量子设备记录的包括用户标识的密钥请求报文的发送次数。在应用设备接收到密钥请求报文对应的密钥响应报文之后，如果第二统计值与第一统计值不相等，应用设备停止量子密钥传输流程。

[0014] 由于量子设备在基于接收到的密钥请求报文更新存储的统计值之后，记录的密钥请求报文的发送次数理应等于应用设备记录的密钥请求报文的发送次数。如果密钥响应报文中携带的统计值不等于应用设备记录的统计值，那么说明该密钥响应报文有可能是攻击者重复发送的，也即是该密钥响应报文有可能是重放攻击报文，这样实现了应用设备侧的重放攻击检测。可选地，如果密钥响应报文中携带的统计值与应用设备记录的统计值不相等，应用设备还输出告警提示，该告警提示用于指示本次密钥请求异常，有助于相关人员对异常情况进行及时处理。

[0015] 可选地，第一认证信息还包括量子设备的设备标识、用户标识或第一统计值中的一个或多个。认证信息包含的内容越多，理论上认证的可靠性就越高。

[0016] 可选地，在应用设备向量子设备发送密钥请求报文之前，应用设备采用密钥派生

函数基于目标口令生成派生密钥，共享密钥基于派生密钥得到。

[0017] 本申请中，使用派生密钥代替目标口令得到共享密钥，这样应用设备与量子设备在同步共享密钥时，应用设备只需向量子设备发送基于目标口令得到的派生密钥。即使派生密钥在传输过程中或存储在量子设备中时被窃取，窃取者也无法还原出服务对象所使用的目标口令，进而能够避免窃取者仿冒服务对象向量子设备请求量子密钥。

[0018] 可选地，在应用设备向量子设备发送密钥请求报文之前，响应于获取到输入的量子密钥获取指令，应用设备运行后量子密钥生成算法生成密钥对，量子密钥获取指令包括目标口令。应用设备基于共享密钥对第一认证信息计算得到第一消息认证码值。

[0019] 本申请中，每当应用设备获取到量子密钥获取指令，都会运行后量子密钥生成算法生成临时密钥对，使得应用设备每次请求量子密钥时，量子设备都采用应用设备临时生成的公钥加密保护量子密钥信息，而非使用量子设备的私钥加密保护量子密钥信息。这样即使量子设备自身长期使用的私钥泄露，也不会造成量子设备与应用设备在之前通信过程中传递的量子密钥信息的泄露。保障了应用设备历史获取的量子密钥的安全性，从而保障了应用设备的历史通信安全性。

[0020] 可选地，在应用设备向量子设备发送密钥请求报文之前，应用设备向量子设备发送注册请求报文。应用设备接收来自量子设备的注册请求报文对应的注册响应报文。该注册响应报文包括量子设备的证书，该证书包括第二公钥。如果应用设备对证书验证通过，应用设备采用第二公钥对注册信息加密得到第二密文，该注册信息包括派生密钥以及用户标识。应用设备向量子设备发送注册登记报文。该注册登记报文包括第二密文。

[0021] 本申请中，在注册阶段，量子设备的身份认证依赖于证书，应用设备的身份认证依赖于基于口令得到的派生密钥，应用设备与量子设备实现了互相身份认证。另外，注册信息是加密传输的，保证了注册信息的传输机密性。

[0022] 可选地，注册请求报文指示应用设备支持的密码算法。注册响应报文还指示量子设备从应用设备支持的密码算法中选择的目标密码算法。目标密码算法包括第一消息认证码值的生成算法、第二消息认证码值的生成算法或共享密钥的生成算法中的一个或多个。

[0023] 可选地，注册响应报文还包括密钥派生函数参数值。密钥派生函数参数值包括随机盐值和/或迭代次数。应用设备接收到注册请求报文对应的注册响应报文之后，应用设备获取用户标识以及目标口令。应用设备采用密钥派生函数基于目标口令以及该密钥派生函数参数值生成派生密钥。

[0024] 可选地，注册登记报文还包括应用设备的设备标识。注册信息还包括应用设备的设备标识的哈希值。

[0025] 本申请中，通过在应用设备发送的注册登记报文中携带应用设备的设备标识，并且使注册信息包括应用设备的设备标识的哈希值，辅助量子设备侧实现对应用设备向量子设备发送的报文的消息完整性验证。

[0026] 可选地，注册信息还包括应用设备生成的第一随机数。应用设备接收来自量子设备的注册成功响应报文。该注册成功响应报文用于指示用户标识已注册成功。注册成功响应报文包括第二随机数。如果第二随机数与第一随机数相同，应用设备确定用户标识注册成功。

[0027] 如果量子设备与应用设备之间传输的报文未经篡改，那么第一随机数与第二随机

数理应相同。这样能够实现应用设备对来自量子设备的报文的消息完整性验证。

[0028] 可选地，应用设备基于共享密钥以及第二认证信息对第二消息认证码值进行验证的实现方式，包括：应用设备基于共享密钥对第二认证信息计算得到第三消息认证码值。如果第三消息认证码值与第二消息认证码值相同，应用设备确定对第二消息认证码值验证通过。

[0029] 可选地，上述应用设备与量子设备通过经典网络通信。

[0030] 第二方面，提供了一种量子密钥传输方法。量子设备接收来自应用设备的密钥请求报文。该密钥请求报文包括应用设备对应的用户标识、第一公钥以及第一消息认证码值。量子设备基于密钥请求报文获取第一认证信息以及用户标识对应的存储信息。该存储信息包括量子设备与用户标识对应的共享密钥。第一认证信息包括第一公钥。量子设备基于共享密钥以及第一认证信息对第一消息认证码值进行验证。如果量子设备对第一消息认证码值验证通过，量子设备采用第一公钥对量子密钥信息加密得到第一密文。量子密钥信息包括量子密钥。量子设备基于共享密钥对第二认证信息计算得到第二消息认证码值。第二认证信息包括第一密文。量子设备向应用设备发送密钥请求报文对应的密钥响应报文，密钥响应报文包括第一密文以及第二消息认证码值。

[0031] 其中，用户标识用于指示服务对象。该服务对象为应用设备或登录应用设备的用户账号。如果量子设备接收到的密钥请求报文确认来自应用设备并且未经篡改，则第一公钥为应用设备运行后量子密钥生成算法得到的密钥对中的公钥。第一消息认证码由应用设备基于共享密钥对第一认证信息计算得到。

[0032] 可选地，应用设备对应的用户标识为应用设备的设备标识。或者，应用设备对应的用户标识为登录应用设备的用户账号。

[0033] 可选地，密钥请求报文还包括第一统计值。第一统计值为应用设备记录的包括用户标识的密钥请求报文的发送次数。用户标识对应的存储信息包括第二统计值。第二统计值为量子设备记录的包括用户标识的密钥请求报文的发送次数。在量子设备获取用户标识对应的存储信息之后，如果第二统计值大于或等于第一统计值，量子设备停止量子密钥传输流程。如果第二统计值小于第一统计值，量子设备更新第二统计值，使更新后的第二统计值等于第一统计值。

[0034] 由于量子设备在基于接收到的密钥请求报文更新存储的统计值之前，记录的密钥请求报文的发送次数理应小于应用设备记录的密钥请求报文的发送次数。如果密钥请求报文中携带的第一统计值小于或等于量子设备存储的第二统计值，那么说明该密钥请求报文有可能是攻击者重复发送的，也即是该密钥请求报文有可能是重放攻击报文，这样实现了量子设备侧的重放攻击检测。可选地，如果第二统计值大于或等于第一统计值，量子设备还输出告警提示，该告警提示用于指示本次密钥请求异常，有助于相关人员对异常情况进行及时处理。

[0035] 可选地，密钥响应报文还包括更新后的第二统计值。

[0036] 本申请中，通过在量子设备发送的密钥响应报文中携带更新后的第二统计值，辅助应用设备侧实现重放攻击检测。

[0037] 可选地，第二认证信息还包括量子设备的设备标识、用户标识或更新后的第二统计值中的一个或多个。

[0038] 可选地，量子设备接收来自应用设备的注册请求报文。量子设备向应用设备发送注册响应报文。该注册响应报文包括量子设备的证书。该证书包括第二公钥。第二公钥为量子设备运行后量子密钥生成算法得到的密钥对中的公钥。如果量子设备接收到来自应用设备的包括第二密文的注册登记报文，量子设备采用第二私钥对第二密文解密以得到注册信息。该注册信息包括派生密钥以及应用设备对应的用户标识。第二私钥为密钥对中的私钥。量子设备存储用户标识对应的存储信息。该存储信息包括基于派生密钥得到的共享密钥以及用户标识。

[0039] 本申请中，由于应用设备用于加密注册信息的第二公钥是量子设备运行后量子密钥生成算法得到的，因此应用设备会采用后量子加密算法对注册信息加密后以密文的形式向量子设备传输注册信息，保证了注册信息的传输机密性。另外，由于第二密文采用后量子加密算法加密得到，因此能够抵抗量子攻击，避免第二密文被量子计算机破解而造成注册信息的泄露。

[0040] 可选地，注册请求报文指示应用设备支持的密码算法。注册响应报文还指示量子设备从应用设备支持的密码算法中选择的目标密码算法。目标密码算法包括第一消息认证码值的生成算法、第二消息认证码值的生成算法或共享密钥的生成算法中的一个或多个。

[0041] 可选地，注册响应报文还包括第一密钥派生函数参数值。第一密钥派生函数参数值包括随机盐值和/或迭代次数。注册信息还包括第二密钥派生函数参数值。在量子设备采用第二私钥对第二密文解密以得到注册信息之后，量子设备比对第一密钥派生函数参数值与第二密钥派生函数参数值。如果第一密钥派生函数参数值与第二密钥派生函数参数值相同，量子设备存储用户标识对应的存储信息。

[0042] 由于应用设备在注册登记报文中携带的第二密钥派生函数参数值来自该应用设备接收到的注册响应报文中的第一密钥派生函数参数值，因此第一密钥派生函数参数值与第二密钥派生函数参数值理应相同。如果量子设备接收到注册登记报文之后，发现来自应用设备的注册登记报文中携带的第二密钥派生函数参数值与量子设备发出的注册响应报文中携带的第一密钥派生函数参数值不同，那么说明注册登记报文和/或注册响应报文在传输过程中被篡改过。本申请通过量子设备比对第一密钥派生函数参数值与第二密钥派生函数参数值，能够实现对量子设备与应用设备之间的双向传输报文的消息完整性验证。

[0043] 可选地，注册登记报文还包括应用设备的设备标识。注册信息还包括应用设备的设备标识的第一哈希值。在量子设备采用第二私钥对第二密文解密以得到注册信息之后，量子设备计算应用设备的设备标识的第二哈希值。量子设备比对第一哈希值与第二哈希值。如果第一哈希值与第二哈希值相同，量子设备存储用户标识对应的存储信息。

[0044] 如果量子设备接收到的注册登记报文中携带的第一哈希值与量子设备计算得到的第二哈希值不同，那么说明注册登记报文在传输过程中被篡改过。本申请通过量子设备比对第一哈希值和第二哈希值，能够实现对应用设备向量子设备发送的报文的消息完整性验证。

[0045] 可选地，注册信息还包括应用设备生成的随机数。在量子设备存储用户标识对应的存储信息之后，量子设备向应用设备发送注册成功响应报文。该注册成功响应报文用于指示用户标识已注册成功。该注册成功响应报文包括该随机数。

[0046] 本申请中，通过在量子设备发送的注册成功响应报文中携带注册信息中的随机

数，辅助应用设备实现对来自量子设备的报文的消息完整性验证。

[0047] 可选地，量子设备基于共享密钥以及第一认证信息对第一消息认证码值进行验证的实现方式，包括：量子设备基于共享密钥对第一认证信息计算得到第四消息认证码值。如果第四消息认证码值与第一消息认证码值相同，量子设备确定对第一消息认证码值验证通过。

[0048] 可选地，应用设备与量子设备通过经典网络通信。

[0049] 第三方面，提供了一种应用设备。所述应用设备包括多个功能模块，所述多个功能模块相互作用，实现上述第一方面及其各实施方式中的方法。所述多个功能模块可以基于软件、硬件或软件和硬件的结合实现，且所述多个功能模块可以基于具体实现进行任意组合或分割。

[0050] 第四方面，提供了一种量子设备。所述量子设备包括多个功能模块，所述多个功能模块相互作用，实现上述第二方面及其各实施方式中的方法。所述多个功能模块可以基于软件、硬件或软件和硬件的结合实现，且所述多个功能模块可以基于具体实现进行任意组合或分割。

[0051] 第五方面，提供了一种应用设备，包括：存储器、网络接口和至少一个处理器。所述存储器用于存储程序指令，所述至少一个处理器读取所述存储器中保存的程序指令后，使得所述应用设备执行上述第一方面及其各实施方式中的方法。

[0052] 第六方面，提供了一种量子设备，包括：存储器、网络接口和至少一个处理器。所述存储器用于存储程序指令，所述至少一个处理器读取所述存储器中保存的程序指令后，使得所述应用设备执行上述第二方面及其各实施方式中的方法。

[0053] 第七方面，提供了一种量子密钥传输系统，包括：应用设备和量子设备。应用设备用于执行上述第一方面及其各实施方式中的方法。量子设备用于执行上述第二方面及其各实施方式中的方法。

[0054] 第八方面，提供了一种量子密钥传输系统，包括：第一应用设备和第一量子设备。第一应用设备用于向第一量子设备发送密钥请求报文，密钥请求报文包括第一应用设备对应的用户标识、第一公钥以及第一消息认证码值，第一公钥为第一应用设备运行后量子密钥生成算法得到的密钥对中的公钥，第一消息认证码值由第一应用设备基于量子设备与用户标识对应的共享密钥对第一认证信息计算得到，第一认证信息包括第一公钥。第一量子设备用于基于密钥请求报文获取第一认证信息以及用户标识对应的存储信息，存储信息包括共享密钥。第一量子设备用于基于共享密钥以及第一认证信息对第一消息认证码值进行验证。如果第一量子设备对第一消息认证码值验证通过，第一量子设备用于采用第一公钥对量子密钥信息加密得到第一密文，量子密钥信息包括量子密钥。第一量子设备用于基于共享密钥对第二认证信息计算得到第二消息认证码值，第二认证信息包括第一密文。第一量子设备用于向第一应用设备发送密钥请求报文对应的密钥响应报文，密钥响应报文包括第一密文以及第二消息认证码值。第一应用设备用于基于密钥响应报文获取第二认证信息。第一应用设备用于基于共享密钥以及第二认证信息对第二消息认证码值进行验证。如果第一应用设备对第二消息认证码值验证通过，第一应用设备用于采用第一私钥对第一密文解密以得到量子密钥信息，第一私钥为密钥对中的私钥。

[0055] 可选地，量子密钥信息还包括量子密钥的密钥标识。该系统还包括第二应用设备

和第二量子设备。第一量子设备还用于向第二量子设备发送量子密钥信息。第一应用设备还用于向第二应用设备发送密钥标识。第二应用设备用于向第二量子设备发送密钥获取请求，密钥获取请求包括密钥标识。第二量子设备用于基于密钥标识向第二应用设备发送量子密钥。第一应用设备与第二应用设备用于基于量子密钥进行通信。

[0056] 可选地，第一量子设备与第二量子设备通过量子网络通信。第一量子设备与第一应用设备通过经典网络通信。第二量子设备与第二应用设备通过经典网络通信。第一应用设备与第二应用设备通过经典网络通信。

[0057] 第九方面，提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有指令，当所述指令被应用设备的处理器执行时，实现上述第一方面及其各实施方式中的方法；或者，当所述指令被量子设备的处理器执行时，实现上述第二方面及其各实施方式中的方法。

[0058] 第十方面，提供了一种计算机程序产品，包括计算机程序，所述计算机程序被应用设备的处理器执行时，实现上述第一方面及其各实施方式中的方法；或者，所述计算机程序被量子设备的处理器执行时，实现上述第二方面及其各实施方式中的方法。

[0059] 第十一方面，提供了一种芯片，芯片包括可编程逻辑电路和/或程序指令，当芯片运行时，实现上述第一方面及其各实施方式中的方法或上述第二方面及其各实施方式中的方法。

附图说明

[0060] 图1是本申请实施例提供的一种应用场景示意图；

[0061] 图2是本申请实施例提供的一种量子密钥传输方法的实现流程示意图；

[0062] 图3是本申请实施例提供的另一种量子密钥传输方法的实现流程示意图；

[0063] 图4是本申请实施例提供的一种应用设备中的密钥管理器的结构示意图；

[0064] 图5是本申请实施例提供的一种量子设备中的密钥管理器的结构示意图；

[0065] 图6是本申请实施例提供的一种量子密钥传输系统的结构示意图；

[0066] 图7是本申请实施例提供的一种应用设备的硬件结构示意图；

[0067] 图8是本申请实施例提供的一种量子设备的硬件结构示意图；

[0068] 图9是本申请实施例提供的一种应用设备的结构示意图；

[0069] 图10是本申请实施例提供的一种量子设备的结构示意图。

具体实施方式

[0070] 为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

[0071] 为了便于读者对本申请方案的理解，以下首先对一些名词进行解释。

[0072] 1、经典计算机：是采用二进制(0或1)存储和处理数据的物理装置。本申请涉及的应用设备属于经典计算机。

[0073] 2、量子计算机：是遵循量子力学规律，基于量子计算原理进行信息处理的物理装置。量子计算机采用量子比特存储和处理数据。量子比特相比于二进制有更多状态。量子计算机具备经典计算机的能力。量子计算机能够更高效地求解某些经典计算机难以求解的问

题。本申请涉及的量子设备属于量子计算机。

[0074] 3、经典网络:是由经典计算机构成的通信网络。

[0075] 4、量子网络:是新型的安全通信网络,其利用量子纠缠和量子隐形传态给网络带来真正意义上的安全,以及计算和科学领域质的飞跃。通信节点间通过量子网络通信,可理解为,通信节点间利用量子密钥分发技术实现通信节点间的量子密钥的共享,并基于量子密钥进行通信。在量子密钥分发过程中,量子密钥是以量子态的形式传输的。由于量子通信线路无法通过挂接旁路窃听或拦截窃听,只要被窃听就会让量子态发生变化从而改变通信内容,防止原文被侦知,因此能够实现量子密钥的安全传输。量子计算机之间能够通过量子网络通信。

[0076] 5、量子攻击:是运行在量子计算机上的攻击算法,例如包括Shor算法(秀尔算法)、Grover算法等能够高效地破解某些密码的算法。

[0077] 6、量子密钥分发(QKD):是利用量子力学的海森堡不确定性原理和量子态不可克隆定理实现的一种安全的密钥分发技术。在量子密钥分发过程中,由一台量子设备生成量子密钥,并通过量子网络传输给另一台量子设备,这样两台量子设备之间就形成了共享的量子密钥。

[0078] 7、非对称密码算法:指发送方与接收方采用不同的密钥进行加解密的算法,也称为公钥密码算法。在非对称密码技术中,有一对密钥,分别为私钥和公钥。私钥由密钥对所有者秘密保存,不可公布。公钥由密钥对持有者公布给他人。用公钥加密的数据只能使用对应的私钥解密。用私钥签名的数据也只能使用对应的公钥验签。目前常用的非对称密码算法包括RSA算法和ECC算法等。

[0079] 8、后量子密码(post quantum cryptography,PQC)体制:是一种包含密钥生成算法、加密算法和解密算法的公钥密码体制。后量子密码体制所包含的算法统称为后量子密码算法。后量子密码算法是能够运行在经典计算机上的非对称密码算法。后量子密码算法具有抗量子性,也即能够抗量子攻击,无法被量子计算机破解。后量子密码算法的抗量子性不依赖于量子力学,而是基于目前无法被量子计算机破解的数学难题实现。后量子密码算法包括基于格、基于编码、基于同源或基于多变量等细分种类实现的算法。

[0080] 9、数字签名(简称签名):是一种针对发送方数据的保护手段。发送方使用私钥对消息进行签名。没有私钥的任何第三方无法伪造签名。拥有发送方所持有的私钥对应的公钥的任何第三方都可以对签名进行验签,以确认消息的来源和完整性。

[0081] 10、签名验证(简称验签):接收方接收到数据后,采用公钥对签名进行验签,输出一个布尔值,表明签名合法(验签通过)或不合法(验签不通过)。如果验签通过,则说明数据没有被篡改。如果验签不通过,则说明数据被篡改。签名验证能够用于验证数据的完整性(未经篡改)和数据来源的可靠性(不是虚假数据或伪造数据)。

[0082] 11、数字证书(简称证书):是设备、用户或应用在数字世界的身份证。证书包含申请者信息以及证书管理机构(certificate authority,CA)对申请者信息的签名。申请者信息包括申请者所持有的密钥对中的公钥。可选地,申请者信息还包括申请者的身份信息。例如申请者为一台设备,申请者的身份信息为能够唯一标识该设备的设备标识。可选地,一台设备的设备标识包括但不限于设备序列号、设备的媒体访问控制(Media Access Control,MAC)地址或设备的互联网协议(Internet Protocol,IP)地址中的一种或多种。接收方接收

到来自发送方的证书后，使用证书管理机构的“统一密钥对”中的公钥(也称为CA根证书)对证书验签，就能确认证书中的公钥是否来自发送方。

[0083] 12、消息认证码(message authentication code，MAC)：用于验证消息完整性(未经篡改)和消息来源的可靠性(不是虚假数据或伪造数据)。消息认证码的鉴权原理是：发送方和接收方事先协商好共享密钥，发送方使用共享密钥生成任意长度的消息的MAC值，再向接收方传输该消息以及该MAC值。接收方使用共享密钥生成该消息的MAC值，并将自己生成的MAC值与从发送方接收到的MAC值进行比对。若MAC值一致，则接收方判定该消息的确来自发送方且未经篡改(验证通过)。反之，若MAC值不一致，则接收方可以判定该消息不是来自发送方或传输过程中被篡改过(验证不通过)。

[0084] 量子密钥由量子设备生成和分发。对于应用设备和量子设备部署在不同安全域的情形，如果应用设备要使用量子密钥，则量子密钥需要从量子设备经过经典网络传输到应用设备上。这种情形下，为了使应用设备能够基于量子密钥安全地通信，首先需要解决量子密钥传输的“最后一公里”问题，即保障量子密钥在经典网络中传输的安全性和可靠性。而为了保障量子密钥在经典网络中传输的安全性和可靠性，需要解决以下三个问题。

[0085] 第一，身份认证问题。量子密钥需要传递给正确的目标用户，目标用户需要确认量子密钥的正确来源。因此量子设备与应用设备需要能够互相进行身份认证，以在交互过程中抵抗仿冒攻击。仿冒攻击例如包括，恶意的应用设备冒充合法的应用设备与量子设备交互，进而窃取量子密钥。

[0086] 第二，传输机密性问题。量子密钥需要以密文的形式在经典网络中传输。因此量子设备需要采用加密算法对量子密钥进行加密保护。并且选用的加密算法必须具有抗量子性，以避免加密算法被量子计算机破解，造成量子密钥的泄露。

[0087] 第三，消息完整性问题。应用设备和量子设备都需要确保接收到的消息是未经篡改的。因此量子设备与应用设备都需要能够对接收到的报文内容进行消息完整性验证。

[0088] 基于此，本申请提出了一种传输量子密钥的技术方案。应用设备和量子设备配合实施本技术方案。应用设备向量子设备发送密钥请求报文，该密钥请求报文包括应用设备对应的用户标识、第一公钥和第一消息认证码值。如果量子设备对第一消息认证码值验证通过，量子设备向应用设备发送密钥响应报文，该密钥响应报文包括第一密文和第二消息认证码值。如果应用设备对第二消息认证码值验证通过，应用设备采用第一私钥对第一密文解密得到量子设备分配给该应用设备的量子密钥信息。

[0089] 其中，第一公钥和第一私钥来自应用设备运行后量子密钥生成算法得到的密钥对。第一密文由量子设备采用第一公钥对分配给应用设备的量子密钥信息加密得到。量子密钥信息包括量子密钥。由于量子设备用于加密量子密钥信息的第一公钥是应用设备运行后量子密钥生成算法得到的，因此量子设备会采用后量子加密算法对量子密钥加密后以密文的形式向应用设备传输量子密钥，保证了量子密钥的传输机密性。另外，由于传输的密文采用后量子加密算法加密得到，因此能够抵抗量子攻击，避免密文被量子计算机破解而造成量子密钥的泄露。

[0090] 第一消息认证码值由应用设备基于量子设备与用户标识对应的共享密钥对第一认证信息计算得到，第一认证信息包括第一公钥。量子设备接收到来自应用设备的密钥请求报文之后，基于密钥请求报文获取第一认证信息以及密钥请求报文中的用户标识对应的

存储信息，该存储信息包括量子设备与该用户标识对应的共享密钥。然后量子设备基于获取的共享密钥以及第一认证信息对第一消息认证码值进行验证。如果量子设备对第一消息认证码值验证通过，则表示该密钥请求报文来自持有共享密钥的另一方，且第一认证信息中由密钥请求报文携带的内容(包括第一公钥)在传输过程中未被篡改。因此第一消息认证码值能够用于量子设备对应用设备进行身份认证(即验证密钥请求报文的来源可靠性)，还能够用于量子设备对密钥请求报文进行消息完整性验证。

[0091] 第二消息认证码值由量子设备基于量子设备与用户标识对应的共享密钥对第二认证信息计算得到，第二认证信息包括第一密文。应用设备接收到来自量子设备的密钥响应报文之后，基于密钥响应报文获取第二认证信息。然后应用设备基于量子设备与用户标识对应的共享密钥以及第二认证信息对第二消息认证码值进行验证。如果应用设备对第二消息认证码值验证通过，则表示该密钥响应报文来自持有共享密钥的另一方，且第二认证信息中由密钥响应报文携带的内容(包括第一密文)在传输过程中未被篡改。因此第二消息认证码值能够用于应用设备对量子设备进行身份认证(即验证密钥响应报文的来源可靠性)，还能够用于应用设备对密钥响应报文进行消息完整性验证。

[0092] 基于上述论述可知，通过实施本技术方案来传输量子密钥，应用设备与量子设备之间能够进行双向身份认证，还能分别对各自接收到的报文进行消息完整性验证，同时也保证了量子密钥的传输机密性。进而实现了量子密钥在经典网络中传输的安全性和可靠性。

[0093] 本申请实施例提供的量子密钥传输方法具有两种实施场景。在一种实施场景中，以具体的应用设备为服务对象，量子设备用于为该应用设备分配量子密钥。这种实施场景下，上述应用设备对应的用户标识为应用设备的设备标识。量子设备与用户标识对应的共享密钥为量子设备与具体的应用设备之间的共享密钥，也即是，持有共享密钥的一方为量子设备，另一方为具体的应用设备。在另一种实施场景中，以用户账号为服务对象，量子设备用于为该用户账号所登录的应用设备分配量子密钥。这种实施场景下，上述应用设备对应的用户标识为登录该应用设备的用户账号。量子设备与用户标识对应的共享密钥为量子设备与用户账号之间的共享密钥，持有共享密钥的一方为量子设备，另一方为用户账号所登录的任意应用设备。

[0094] 下面从应用场景、方法流程、功能模块、系统、硬件装置、软件装置等多个角度，对本技术方案进行详细介绍。

[0095] 下面对本申请实施例的应用场景举例说明。

[0096] 例如，图1是本申请实施例提供的一种应用场景示意图。如图1所示，该应用场景主要涉及到两类设备，分别是应用设备和量子设备。可选地，一台量子设备用于为一台或多台应用设备提供量子服务，即一台量子设备能够为一台或多台应用设备分配量子密钥。可选地，量子设备与应用设备之间通过经典网络通信。例如，量子设备与应用设备之间基于传输控制协议/互联网协议(Transmission Control Protocol/Internet Protocol，TCP/IP)进行通信。

[0097] 可选地，应用设备包括但不限于路由器、交换机、或防火墙等网络设备。或者，应用设备为电脑、手机、或物联网(internet of things，IoT)终端等终端设备。又或者，应用设备为服务器或云平台等具有通信需求的其它设备。量子设备为能够生成或存储量子密钥的

量子计算机。本申请实施例中的量子设备也可称为量子密钥分发设备。

[0098] 下面对本申请实施例的方法流程举例说明。

[0099] 例如，图2是本申请实施例提供的一种量子密钥传输方法200的实现流程示意图。如图2所示，方法200包括步骤201至步骤208。可选地，方法200中的量子设备为图1中的量子设备。方法200中的应用设备为图1中的任一应用设备。

[0100] 步骤201、应用设备向量子设备发送密钥请求报文，该密钥请求报文包括应用设备对应的用户标识、第一公钥以及第一消息认证码值。

[0101] 密钥请求报文中的应用设备对应的用户标识用于指示量子设备的服务对象，以使量子设备能够获取该服务对象对应的存储信息，也即是，应用设备对应的用户标识用于量子设备获取对应的存储信息。该存储信息包括量子设备与用户标识对应的共享密钥。可选地，应用设备对应的用户标识为应用设备的设备标识，则量子设备与用户标识对应的共享密钥为量子设备与该应用设备之间的共享密钥。这种情况下，共享密钥是预先存储在应用设备中的，应用设备能够直接获取存储的共享密钥。或者，应用设备对应的用户标识为登录该应用设备的用户账号，则量子设备与用户标识对应的共享密钥为量子设备与该用户账号之间的共享密钥。这种情况下，共享密钥与用户账号绑定，用户账号在应用设备上登录之后，应用设备能够获取与该用户账号绑定的共享密钥。

[0102] 密钥请求报文中的第一公钥用于量子设备对分配给发送该密钥请求报文的应用设备的量子密钥信息加密。量子密钥信息包括量子密钥。可选地，量子密钥信息还包括量子密钥的密钥标识。本申请实施例中，将第一公钥对应的私钥称为第一私钥。第一公钥和第一私钥分别为应用设备运行后量子密钥生成算法得到的密钥对中的公钥和私钥。

[0103] 密钥请求报文中的第一消息认证码值由应用设备基于量子设备与用户标识对应的共享密钥对第一认证信息计算得到。第一认证信息包括第一公钥。可选地，第一认证信息还包括量子设备的设备标识和/或密钥请求报文中携带的用户标识。第一消息认证码值用于量子设备对应用设备进行身份认证以及对密钥请求报文进行消息完整性认证。

[0104] 可选地，一台量子设备用于为一个或多个服务对象分配量子密钥。不同的服务对象使用不同的口令供量子设备进行身份认证。可选地，上述量子设备与用户标识对应的共享密钥基于目标口令得到，目标口令为该用户标识所指示的服务对象所使用的口令。

[0105] 可选地，在执行步骤201之前，响应于获取到输入的量子密钥获取指令，应用设备运行后量子密钥生成算法生成密钥对。该量子密钥获取指令包括目标口令。然后应用设备基于共享密钥对包含第一公钥的第一认证信息计算得到第一消息认证码值。例如，当用户在应用设备上输入目标口令时，应用设备确定获取到量子密钥获取指令。可选地，当应用设备上的口令输入错误次数达到预设的次数阈值时，应用设备锁定口令输入界面。本申请实施例通过限制口令的错误输入次数来限制攻击者的试错次数，能够抵抗在线字典攻击。

[0106] 可选地，第一消息认证码值为哈希消息认证码(HMAC)值。

[0107] 本申请实施例中，每当应用设备获取到量子密钥获取指令，都会运行后量子密钥生成算法生成临时密钥对，使得应用设备每次请求量子密钥时，量子设备都采用应用设备临时生成的公钥加密保护量子密钥信息，而非使用量子设备的私钥加密保护量子密钥信息。这样即使量子设备自身长期使用的私钥泄露，也不会造成量子设备与应用设备在之前通信过程中传递的量子密钥信息的泄露。保障了应用设备历史获取的量子密钥的安全性，

从而保障了应用设备的历史通信安全性。

[0108] 或者,应用设备请求量子密钥时使用固定的密钥对,这样应用设备在获取到量子密钥获取指令后无需生成密钥对,从而能够提高应用设备获取量子密钥的效率。例如,当服务对象为应用设备时,应用设备预先生成并存储密钥对,响应于获取到量子密钥获取指令,应用设备从存储的密钥对中直接获取公钥并计算得到消息认证码值。当服务对象为用户账号时,用户账号预先绑定密钥对,响应于获取到量子密钥获取指令,登录该用户账号的应用设备从该用户账号绑定的密钥对中直接获取公钥并计算得到消息认证码值。

[0109] 可选地,在执行步骤201之前,应用设备采用密钥派生函数(key derivation function,KDF)基于目标口令生成派生密钥。密钥派生函数用于使用伪随机函数从秘密值导出一个或多个密钥。秘密值为原始密钥,导出的密钥为派生密钥。例如,密钥派生函数的使用表示为:DK=KDF(Key,Salt,Iterations)。其中,DK是派生密钥。KDF是密钥派生函数。Key是原始密钥。Salt是作为密码盐的随机数(以下简称为随机盐值)。Iterations指迭代次数。随机盐值和迭代次数可统称为密钥派生函数参数值。本申请实施例中,目标口令用作密钥派生函数使用的原始密钥的部分或全部。量子设备与用户标识对应的共享密钥基于该派生密钥得到。可选地,共享密钥基于派生密钥得到,包括:共享密钥是派生密钥,或者,共享密钥是派生密钥的哈希值。

[0110] 本申请实施例中,使用派生密钥代替目标口令得到共享密钥,这样应用设备与量子设备在同步共享密钥时,应用设备只需向量子设备发送基于目标口令得到的派生密钥。即使派生密钥在传输过程中或存储在量子设备中时被窃取,窃取者也无法还原出服务对象所使用的目标口令,进而能够避免窃取者仿冒服务对象向量子设备请求量子密钥。

[0111] 可选地,应用设备采用的密钥派生函数包括但不限于哈希函数或基于口令的密钥派生函数(password-based key derivation function 2,PBKDF2)。例如,应用设备采用PBKDF2作为密钥派生函数,目标口令记为pwd,随机盐值记为salt,迭代次数记为i,则基于目标口令得到的派生密钥UK满足:UK=PBKDF2(pwd||secret,salt,i)。其中,“secret”为应用设备自行生成和维护的秘密。本申请实施例中的符号“||”表示“和”或“并”。应用设备将pwd和secret共同作为原始密钥来生成派生密钥,能够降低基于派生密钥破解还原得到目标口令的可能性,在一定程度上能够抵抗离线字典攻击,从而进一步提高目标口令的机密性和使用安全性。

[0112] 步骤202、量子设备接收到来自应用设备的密钥请求报文之后,基于该密钥请求报文获取第一认证信息以及用户标识对应的存储信息,该存储信息包括量子设备与该用户标识对应的共享密钥。

[0113] 量子设备基于密钥请求报文获取第一认证信息,包括量子设备从密钥请求报文中获取第一公钥。可选地,量子设备中存储有一个或多个用户标识对应的存储信息。每个用户标识对应的存储信息包括量子设备与该用户标识对应的共享密钥以及该用户标识。量子设备基于密钥请求报文获取用户标识对应的存储信息,也即是,量子设备获取密钥请求报文所携带的用户标识对应的存储信息。

[0114] 步骤203、量子设备基于共享密钥以及第一认证信息对第一消息认证码值进行验证。

[0115] 步骤203中的第一认证信息为步骤202中量子设备基于接收到的密钥请求报文获

取的认证信息。如果步骤201中应用设备发送的密钥请求报文在传输过程中未经篡改，那么步骤202中量子设备获取的第一认证信息与步骤201中应用设备用于计算第一消息认证码值所使用的第一认证信息的内容是一致的。可选地，步骤203的实现方式为：量子设备基于共享密钥对第一认证信息计算得到第四消息认证码值。如果第四消息认证码值与第一消息认证码值相同，量子设备确定对第一消息认证码值验证通过。反之，如果第四消息认证码值与第一消息认证码值不同，量子设备确定对第一消息认证码值验证不通过。

[0116] 如果量子设备对第一消息认证码值验证通过，则表示量子设备接收到的密钥请求报文来自持有共享密钥的另一方，且第一认证信息中由密钥请求报文携带的内容(至少包括第一公钥)在传输过程中未被篡改，这种情况下，量子设备向请求方提供量子密钥。如果量子设备对第一消息认证码值验证不通过，则表示量子设备接收到的密钥请求报文并非来自持有共享密钥的另一方，或者第一认证信息中由密钥请求报文携带的内容在传输过程中被篡改过，这种情况下，量子设备不向请求方提供量子密钥。本申请实施例中，通过在应用设备发送的密钥请求报文中携带第一消息认证码值，使得量子设备能够对应用设备进行身份认证(即验证密钥请求报文的来源可靠性)以及对密钥请求报文进行消息完整性验证。

[0117] 步骤204、如果量子设备对第一消息认证码值验证通过，量子设备采用第一公钥对量子密钥信息加密得到第一密文。

[0118] 量子密钥信息包括量子密钥。可选地，量子密钥信息还包括量子密钥的密钥标识。

[0119] 由于量子设备用于加密量子密钥信息的第一公钥是应用设备运行后量子密钥生成算法得到的，因此量子设备会采用后量子加密算法对量子密钥加密后以密文的形式向应用设备传输量子密钥，保证了量子密钥的传输机密性。另外，由于第一密文采用后量子加密算法加密得到，因此能够抵抗量子攻击，避免第一密文被量子计算机破解而造成量子密钥的泄露。

[0120] 可选地，量子设备在确定分配给应用设备的量子密钥信息之后，将该量子密钥信息添加到该应用设备对应的用户标识所对应的存储信息中，以便其它应用设备需要与该应用设备基于量子密钥通信时，量子设备能够直接或间接地向其它应用设备提供该应用设备所使用的量子密钥，从而实现应用设备之间的安全通信。

[0121] 步骤205、量子设备基于共享密钥对第二认证信息计算得到第二消息认证码值，第二认证信息包括第一密文。

[0122] 可选地，第二认证信息还包括量子设备的设备标识和/或密钥请求报文中携带的用户标识。可选地，第二消息认证码值为哈希消息认证码(HMAC)值。

[0123] 步骤206、量子设备向应用设备发送密钥请求报文对应的密钥响应报文，该密钥响应报文包括第一密文以及第二消息认证码值。

[0124] 步骤207、应用设备接收到来自量子设备的密钥响应报文之后，基于共享密钥以及第二认证信息对第二消息认证码值进行验证。

[0125] 步骤207中的第二认证信息为应用设备基于接收到的密钥响应报文获取的认证信息。如果步骤206中量子设备发送的密钥响应报文在传输过程中未经篡改，那么应用设备基于密钥响应报文获取的认证信息与步骤205中应用设备用于计算第二消息认证码值所使用的第二认证信息的内容是一致的。可选地，步骤207的实现方式为：应用设备基于共享密钥对第二认证信息计算得到第三消息认证码值。如果第三消息认证码值与第二消息认证码值

相同，应用设备确定对第二消息认证码值验证通过。反之，如果第三消息认证码值与第二消息认证码值不同，应用设备确定对第二消息认证码值验证不通过。

[0126] 如果应用设备对第二消息认证码值验证通过，则表示应用设备接收到的密钥响应报文来自持有共享密钥的另一方，且第二认证信息中由密钥响应报文携带的内容(至少包括第一密文)在传输过程中未被篡改，这种情况下，说明密钥响应报文中携带的量子密钥信息是可靠的，应用设备进一步提取该密钥响应报文中携带的量子密钥信息。如果应用设备对第二消息认证码值验证不通过，则表示应用设备接收到的密钥响应报文并非来自持有共享密钥的另一方，或者第二认证信息中由密钥响应报文携带的内容在传输过程中被篡改过，这种情况下，说明密钥响应报文中携带的量子密钥信息是不可靠的，应用设备不再对该密钥响应报文中的信息进行处理。本申请实施例中，通过在量子设备发送的密钥响应报文中携带第二消息认证码值，使得应用设备能够对量子设备进行身份认证(即验证密钥响应报文的来源可靠性)以及对密钥响应报文进行消息完整性验证。

[0127] 步骤208、如果应用设备对第二消息认证码值验证通过，应用设备采用第一私钥对第一密文解密以得到量子密钥信息。

[0128] 可选地，量子设备中用户标识对应的存储信息包括第二统计值，该第二统计值为量子设备记录的包括该用户标识的密钥请求报文的发送次数。密钥请求报文还包括第一统计值，该第一统计值为应用设备记录的包括用户标识的密钥请求报文的发送次数。可选地，第一认证信息还包括第一统计值。如果服务对象为应用设备，则第一统计值为该应用设备发送的包括该应用设备的设备标识(用户标识)的密钥请求报文的次数。具体实现时，通过在应用设备中设置计数器记录密钥请求报文的发送次数。应用设备每发送一次密钥请求报文，使计数器增加设定递增值。如果服务对象为用户账号，则第一统计值为该用户账号登录过的所有应用设备发送的包括该用户账号(用户标识)的密钥请求报文的次数。

[0129] 可选地，在应用设备向量子设备发送包括用户标识的密钥请求报文之前(即执行步骤201之前)，应用设备获取包括该用户标识的密钥请求报文的历史发送次数。应用设备在该历史发送次数上增加设定递增值，得到第一统计值。也即是，应用设备计算的第一统计值是算上本次发送的密钥请求报文的。可选地，设定递增值为1。相应地，量子设备在接收到密钥请求报文之后，如果获取的用户标识对应的存储信息中的第二统计值大于或等于第一统计值，量子设备停止量子密钥传输流程。如果第二统计值小于第一统计值，量子设备更新第二统计值，使更新后的第二统计值等于第一统计值。量子设备在基于接收到的密钥请求报文更新存储的统计值之前，记录的密钥请求报文的发送次数理应小于应用设备记录的密钥请求报文的发送次数。如果密钥请求报文中携带的第一统计值小于或等于量子设备存储的第二统计值，那么说明该密钥请求报文有可能是攻击者重复发送的，也即是该密钥请求报文有可能是重放攻击报文，这样实现了量子设备侧的重放攻击检测。可选地，如果获取的用户标识对应的存储信息中的第二统计值大于或等于第一统计值，量子设备还输出告警提示，该告警提示用于指示本次密钥请求异常，有助于相关人员对异常情况进行及时处理。

[0130] 可选地，量子设备在确定第二统计值小于第一统计值的情况下，再对第一消息认证码值进行验证(即执行步骤203)。

[0131] 可选地，密钥响应报文还包括更新后的第二统计值。可选地，第二认证信息还包括更新后的第二统计值。应用设备在接收到密钥响应报文之后，如果密钥响应报文中携带的

统计值(更新后的第二统计值)与应用设备记录的统计值(第一统计值)不相等,应用设备停止量子密钥传输流程。量子设备在基于接收到的密钥请求报文更新存储的统计值之后,记录的密钥请求报文的发送次数理应等于应用设备记录的密钥请求报文的发送次数。如果密钥响应报文中携带的统计值不等于应用设备记录的统计值,那么说明该密钥响应报文有可能是攻击者重复发送的,也即是该密钥响应报文有可能是重放攻击报文,这样实现了应用设备侧的重放攻击检测。可选地,如果密钥响应报文中携带的统计值与应用设备记录的统计值不相等,应用设备还输出告警提示,该告警提示用于指示本次密钥请求异常,有助于相关人员对异常情况进行及时处理。

[0132] 可选地,应用设备在更新后的第二统计值与第一统计值相等的情况下,再对第二消息认证码值进行验证(即执行步骤207)。

[0133] 本申请实施例提供的量子密钥传输方法,在应用设备向量子设备请求获取量子密钥的过程中,应用设备与量子设备之间能够进行双向身份认证,还能分别对各自接收到的报文进行消息完整性验证,同时也保证了量子密钥的传输机密性。进而实现了量子密钥在经典网络中传输的安全性和可靠性。另外,应用设备向量子设备请求获取量子密钥这个过程只需要一轮报文(密钥请求报文和密钥响应报文)交互就能完成量子密钥的传输以及双方身份认证,交互过程简单。另外,本申请实施例中应用设备与量子设备之间的双向身份认证以及消息完整性验证都是基于消息认证码实现的。而现有的基于通信双方的证书的认证密钥交换的方案,如传输层安全(transport layer security,TLS)双向认证,握手阶段通信方需使用私钥对报文进行签名,另一通信方需使用对应的公钥进行签名验证,以保障报文来源的合法性和内容的完整性。一方面,由于消息认证码的运算效率高于签名的运算效率,因此本申请方案相较于现有的认证密钥交换方案,应用设备对密钥的获取效率会更高。另一方面,由于消息认证码这类原语能够抵抗量子攻击,而现有的通信方所使用的签名算法通常不具备抗量子性,因此本申请方案相较于现有的认证密钥交换方案,对通信双方进行身份认证以及消息完整性验证的可靠性更高。

[0134] 可选地,本申请技术方案分为两个实现阶段,分别为注册阶段和量子密钥获取阶段。服务对象在注册阶段完成在量子设备上的注册以与量子设备建立首次互信。其中,服务对象在量子设备上完成注册,包括服务对象与量子设备之间完成共享密钥的同步。服务对象在量子密钥获取阶段完成与量子设备的互相身份认证以及量子密钥的传输。例如,上述方法200描述了量子密钥获取阶段的实现流程。注册阶段与量子密钥获取阶段是相互独立的,服务对象完成一次注册后,能够多次向量子设备请求获取量子密钥。例如服务对象为应用设备,应用设备在量子设备上注册完成之后,该应用设备能够多次执行量子密钥获取流程以从量子设备处获取量子密钥。又例如,服务对象为用户账号,用户账号登录一台应用设备以在量子设备上完成注册,之后,该用户账号能够多次登录该应用设备或其它应用设备,使能每次登录的应用设备执行量子密钥获取流程以从量子设备处获取量子密钥。值得说明的是,在服务对象为应用设备的情况下,与量子设备完成注册流程的应用设备跟向量子设备请求获取量子密钥的应用设备只能是同一台应用设备。这种情况下,上述方法200中的应用设备与下述方法300中的应用设备为同一台应用设备。在服务对象为用户账号的情况下,与量子设备完成注册流程的应用设备跟向量子设备请求获取量子密钥的应用设备为登录同一用户账号的同一台应用设备或不同应用设备。这种情况下,上述方法200中的应用设备

与下述方法300中的应用设备为登录同一用户账号的应用设备(同一台设备或不同设备)。

[0135] 本申请以下实施例对注册阶段的实现流程进行说明。例如,图3是本申请实施例提供的一种量子密钥传输方法300的实现流程示意图。该方法300仅示出了注册阶段的实现流程,应用设备在量子设备上完成注册之后,向量子设备请求获取量子密钥的过程可参考上述方法200,本申请实施例在此不再赘述。如图3所示,方法300包括步骤301至步骤310。

[0136] 步骤301、应用设备向量子设备发送注册请求报文。

[0137] 注册请求报文用于向量子设备申请发起注册流程。可选地,注册请求报文指示应用设备支持的密码算法。例如,注册请求报文指示应用设备支持的消息认证码生成算法、密钥派生函数算法或后量子密码算法等。

[0138] 步骤302、量子设备接收到来自应用设备的注册请求报文之后,向应用设备发送注册响应报文,该注册响应报文包括量子设备的证书,该证书包括第二公钥。

[0139] 第二公钥为量子设备所持有的密钥对中的公钥。本申请实施例中,将第二公钥对应的私钥称为第二私钥。第二公钥和第二私钥分为量子设备运行后量子密钥生成算法得到的密钥对中的公钥和私钥。

[0140] 可选地,注册响应报文还指示量子设备从应用设备支持的密码算法中选择的目标密码算法。目标密码算法包括第一消息认证码值的生成算法(即上述步骤201中应用设备计算第一消息认证码值所使用的算法)、第二消息认证码值的生成算法(即上述步骤205中量子设备计算第二消息认证码值所使用的算法)或共享密钥的生成算法(即上述步骤201中基于派生密钥得到共享密钥的算法)中的一个或多个。可选地,目标密钥算法还包括应用设备生成第一公钥和第一私钥所使用的后量子密码算法(步骤201),和/或,量子设备生成第二公钥和第二私钥所使用的后量子密码算法(步骤302)。以使应用设备能够使用配套的后量子加密算法或后量子解密算法对密文加解密。

[0141] 步骤303、应用设备接收到来自量子设备的注册请求报文对应的注册响应报文之后,如果应用设备对量子设备的证书验证通过,应用设备获取用户标识和目标口令。

[0142] 量子设备的证书还包括第三方认证机构(例如CA)的签名。应用设备基于量子设备的证书对量子设备进行身份认证。应用设备对量子设备的证书验证通过,即应用设备使用第三方认证机构提供的公钥对量子设备的证书验签通过。这样应用设备就能确认证书中的公钥的确是来自该量子设备的,进而能够避免仿冒攻击。应用设备获取的目标口令为该应用设备获取的用户标识对应的口令。本申请实施例中,用户标识对应的口令用作该用户标识所指示的服务对象向量子设备请求服务的通行密码。

[0143] 可选地,如果注册请求报文用于请求将发送该注册请求报文的应用设备作为服务对象,则应用设备将自身的设备标识作为用户标识。如果注册请求报文用于请求注册一个用户账号作为服务对象,则应用设备在接收到注册响应报文之后创建一个用户账号,并将创建的用户账号作为用户标识。

[0144] 可选地,目标口令由用户输入。应用设备在接收到注册响应报文之后,显示口令输入界面以提示用户输入口令。然后应用设备将用户输入的内容作为目标口令。

[0145] 步骤304、应用设备采用密钥派生函数基于目标口令生成派生密钥。

[0146] 可选地,注册响应报文还包括密钥派生函数参数值,该密钥派生函数参数值包括随机盐值和/或迭代次数。量子设备通过在注册响应报文中携带密钥派生函数参数值,以指

示应用设备在采用密钥派生函数生成派生密钥时所使用的随机盐值和/或迭代次数。这种情况下，步骤304的实现方式为，应用设备采用密钥派生函数基于目标口令以及注册响应报文中的密钥派生函数参数值生成派生密钥。此步骤304的具体实现方式可参考上述步骤201中的相关描述，本申请实施例在此不再赘述。

[0147] 步骤305、应用设备采用第二公钥对注册信息加密得到第二密文，该注册信息包括派生密钥以及用户标识。

[0148] 可选地，在注册响应报文包括密钥派生函数参数值的情况下，应用设备将从注册响应报文中获取的密钥派生函数参数值作为注册信息的一部分，即注册信息包括密钥派生函数参数值。为了便于描述上的区分，本申请实施例将注册响应报文中的密钥派生函数参数值称为第一密钥派生函数参数值，将注册信息中的密钥派生函数参数值称为第二密钥派生函数参数值。

[0149] 由于应用设备用于加密注册信息的第二公钥是量子设备运行后量子密钥生成算法得到的，因此应用设备会采用后量子加密算法对注册信息加密后以密文的形式向量子设备传输注册信息，保证了注册信息的传输机密性。另外，由于第二密文采用后量子加密算法加密得到，因此能够抵抗量子攻击，避免第二密文被量子计算机破解而造成注册信息的泄露。

[0150] 可选地，注册信息还包括密钥派生函数参数值、量子设备的设备标识、应用设备的设备标识的哈希值或应用设备生成的随机数中的一个或多个。

[0151] 步骤306、应用设备向量子设备发送注册登记报文，注册登记报文包括第二密文。

[0152] 可选地，注册登记报文还包括应用设备的设备标识。注册信息还包括应用设备的设备标识的第一哈希值。

[0153] 步骤307、量子设备接收到来自应用设备的注册登记报文之后，采用第二私钥对第二密文解密以得到注册信息。

[0154] 步骤308、量子设备存储用户标识对应的存储信息。

[0155] 步骤308中的用户标识为量子设备从步骤307中解密得到的注册信息中获取的用户标识。用户标识对应的存储信息包括用户标识以及该用户标识对应的共享密钥。该共享密钥基于注册信息中的派生密钥得到。例如，量子设备将注册信息中的派生密钥作为该量子设备与注册信息中的用户标识对应的共享密钥。或者，量子设备将注册信息中的派生密钥的哈希值作为该量子设备与注册信息中的用户标识对应的共享密钥。只需保证应用设备与量子设备双方基于派生密钥得到共享密钥的处理方式相同即可。可选地，注册信息中的用户标识对应的存储信息还包括注册信息中除用户标识以外的部分或全部内容。例如，量子设备中存储的用户标识对应的存储信息包括用户标识、用户标识对应的共享密钥、应用设备计算派生密钥所使用的随机盐值和迭代次数以及量子设备记录的包括用户标识的密钥请求报文的发送次数。该发送次数的初始值为0。

[0156] 可选地，当注册响应报文包括第一密钥派生函数参数值，注册信息包括第二密钥派生函数参数值时，量子设备先比对第一密钥派生函数参数值与第二密钥派生函数参数值。如果第一密钥派生函数参数值与第二密钥派生函数参数值相同，量子设备存储注册信息中的用户标识对应的存储信息。

[0157] 由于应用设备在注册登记报文中携带的第二密钥派生函数参数值来自该应用设

备接收到的注册响应报文中的第一密钥派生函数参数值，因此第一密钥派生函数参数值与第二密钥派生函数参数值理应相同。如果量子设备接收到注册登记报文之后，发现来自应用设备的注册登记报文中携带的第二密钥派生函数参数值与量子设备发出的注册响应报文中携带的第一密钥派生函数参数值不同，那么说明注册登记报文和/或注册响应报文在传输过程中被篡改过。本申请实施例通过量子设备比对第一密钥派生函数参数值与第二密钥派生函数参数值，能够实现对量子设备与应用设备之间的双向传输报文的消息完整性验证。

[0158] 可选地，当注册登记报文包括应用设备的设备标识，注册信息包括应用设备的设备标识的第一哈希值时，量子设备得到注册信息之后，计算注册信息中的应用设备的设备标识的第二哈希值。然后量子设备比对注册登记报文中携带的第一哈希值与计算得到的第二哈希值。如果第一哈希值与第二哈希值相同，量子设备存储用户标识对应的存储信息。

[0159] 如果量子设备接收到的注册登记报文中携带的第一哈希值与量子设备计算得到的第二哈希值不同，那么说明注册登记报文在传输过程中被篡改过。本申请实施例通过量子设备比对第一哈希值和第二哈希值，能够实现对应用设备向量子设备发送的报文的消息完整性验证。

[0160] 可选地，注册信息还包括应用设备生成的第一随机数。在量子设备存储注册信息中的用户标识对应的存储信息之后，继续执行以下步骤309至步骤310。

[0161] 步骤309、量子设备向应用设备发送注册成功响应报文，该注册成功响应报文用于指示注册信息中的用户标识已注册成功，该注册成功响应报文包括第二随机数，第二随机数来自注册信息。

[0162] 量子设备从注册信息中获取第一随机数之后，将第一随机数携带在注册成功响应报文中。为了便于描述上的区分，本申请实施例将注册信息中的随机数称为第一随机数，将注册成功响应报文中的随机数称为第二随机数。如果量子设备与应用设备之间传输的报文未经篡改，那么第一随机数与第二随机数理应相同。

[0163] 步骤310、应用设备接收到来自量子设备的注册成功响应报文之后，如果第二随机数与应用设备生成的第一随机数相同，应用设备确定该用户标识注册成功。

[0164] 应用设备确定用户标识注册成功，也即是，应用设备确定该用户标识所指示的服务对象在量子设备上注册完成。

[0165] 本申请实施例中，应用设备的身份认证是基于口令的方式。量子设备在注册阶段的身份认证依赖于证书，在量子密钥获取阶段的身份认证依赖于基于口令得到的派生密钥。无论是注册阶段还是量子密钥获取阶段，应用设备与量子设备都实现了互相身份认证，从而保障了量子密钥传输的安全性和可靠性。另外，在注册阶段，应用设备采用量子设备运行后量子加密算法得到的公钥对注册信息加密后以密文的形式向量子设备传输注册信息。在量子密钥获取阶段，量子设备采用应用设备运行后量子密钥生成算法得到的公钥对量子密钥加密后以密文的形式向应用设备传输量子密钥。实现了量子设备与应用设备之间消息传输的机密性，同时，传输的密文能够抵抗量子攻击，因此降低了消息泄露的风险。

[0166] 本申请实施例提供的上述量子密钥传输方法的步骤的先后顺序能够进行适当调整，步骤也能够根据情况进行相应增减。任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化的方法，都应涵盖在本申请的保护范围之内。

[0167] 下面对量子设备和应用设备的功能模块举例说明。

[0168] 本申请实施例提供的量子设备和应用设备都配置有密钥管理器，本申请方案的核心功能分别由量子设备和应用设备的密钥管理器实现。

[0169] 例如，图4是本申请实施例提供的一种应用设备中的密钥管理器的结构示意图。如图4所示，应用设备中的密钥管理器包括量子服务注册模块和量子密钥请求模块。量子服务注册模块负责向量子设备申请注册服务对象，并向量子设备提供必要的身份材料，具体执行例如上述步骤301、步骤303至步骤306以及步骤310。量子密钥请求模块包括身份认证模块和量子密钥解封装模块。其中，身份认证模块负责在量子密钥获取过程中对交互的量子设备进行身份认证，具体执行例如上述步骤207。量子密钥解封装模块负责对量子设备发送的量子密钥信息进行解封装，以提取出真正的量子密钥，具体执行例如上述步骤208。

[0170] 例如，图5是本申请实施例提供的一种量子设备中的密钥管理器的结构示意图。如图5所示，量子设备中的密钥管理器包括注册请求处理模块和量子密钥请求处理模块。注册请求处理模块负责处理来自应用设备的注册请求，具体执行例如上述步骤302以及步骤307至步骤309。量子密钥请求处理模块包括身份认证模块和量子密钥封装模块。其中，身份认证模块负责对交互的应用设备进行身份认证，具体执行例如上述步骤203。量子密钥请求处理模块负责封装量子密钥信息，具体执行例如上述步骤204，以保障量子密钥在经典网络中的传输机密性。

[0171] 下面对本申请实施例涉及的系统举例说明。

[0172] 本申请实施例还提供了一种量子密钥传输系统，包括：应用设备和量子设备。应用设备与量子设备交互，使得应用设备能够从量子设备上获取量子密钥。应用设备和量子设备的详细工作过程请参照前面方法200中描述的量子密钥获取阶段的实现流程。例如，应用设备用于执行上述方法200中的步骤201以及步骤207至步骤208。量子设备用于执行上述方法200中的步骤202至步骤206。

[0173] 可选地，应用设备还与量子设备交互，使得应用设备能够在量子设备上完成服务对象的注册。应用设备和量子设备的详细工作过程请参照前面方法300中描述的注册阶段的实现流程。例如，应用设备用于执行上述方法300中的步骤301、步骤303至步骤306以及步骤310。量子设备用于执行上述方法300中的步骤302以及步骤307至步骤309。

[0174] 例如，图6是本申请实施例提供的一种量子密钥传输系统的结构示意图。如图6所示，该系统包括第一应用设备和第一量子设备。第一应用设备在第一量子设备上完成了注册，或者，登录第一应用设备的用户账号在第一量子设备上完成了注册，具体注册过程可参考上述方法300中的描述。第一量子设备能够向第一应用设备提供量子服务。可选地，当第一应用设备为通信发起方时，第一应用设备向第一量子设备请求获取量子密钥。第一应用设备向第一量子设备请求获取量子密钥的过程可参考上述方法200中的描述。

[0175] 例如，第一应用设备用于向第一量子设备发送密钥请求报文。该密钥请求报文包括第一应用设备对应的用户标识、第一公钥以及第一消息认证码值。第一公钥为第一应用设备运行后量子密钥生成算法得到的密钥对中的公钥。第一消息认证码值由第一应用设备基于量子设备与用户标识对应的共享密钥对第一认证信息计算得到。第一认证信息包括第一公钥。第一量子设备用于基于密钥请求报文获取第一认证信息以及用户标识对应的存储信息，该存储信息包括共享密钥。第一量子设备用于基于共享密钥以及第一认证信息对第

一消息认证码值进行验证。如果第一量子设备对第一消息认证码值验证通过，第一量子设备用于采用第一公钥对量子密钥信息加密得到第一密文。该量子密钥信息包括量子密钥。第一量子设备用于基于共享密钥对第二认证信息计算得到第二消息认证码值。第二认证信息包括第一密文。第一量子设备用于向第一应用设备发送密钥请求报文对应的密钥响应报文。该密钥响应报文包括第一密文以及第二消息认证码值。第一应用设备用于基于密钥响应报文获取第二认证信息。第一应用设备用于基于共享密钥以及第二认证信息对第二消息认证码值进行验证。如果第一应用设备对第二消息认证码值验证通过，第一应用设备用于采用第一私钥对第一密文解密以得到量子密钥信息。第一私钥为第一应用设备运行后量子密钥生成算法得到的密钥对中的私钥。第一私钥为第一公钥对应的私钥。

[0176] 可选地，第一量子设备为第一应用设备分配的量子密钥信息还包括量子密钥的密钥标识。

[0177] 可选地，请继续参见图6，该系统还包括第二应用设备和第二量子设备。第二应用设备在第二量子设备上完成了注册，或者，登录第二应用设备的用户账号在第二量子设备上完成了注册，具体注册过程可参考上述方法300中的描述。第二量子设备能够向第二应用设备提供量子服务。可选地，当第二应用设备为通信接收方时，第二应用设备向第二量子设备请求获取通信发起方的量子密钥。

[0178] 例如，第一量子设备还用于向第二量子设备发送量子密钥信息。第一应用设备还用于向第二应用设备发送密钥标识。第二应用设备用于向第二量子设备发送密钥获取请求，该密钥获取请求包括密钥标识。第二量子设备用于基于密钥标识向第二应用设备发送量子密钥。第一应用设备与第二应用设备用于基于量子密钥进行通信。

[0179] 其中，第二应用设备向第二量子设备发送密钥获取请求的方式可参考上述方法200中应用设备向量子设备发送密钥请求报文的方式，具体过程可参考上述方法200中的步骤201。例如密钥获取请求所包含的内容相较于密钥请求报文多了密钥标识，以指示第二量子设备获取该密钥标识所指示的量子密钥。第二量子设备对密钥获取请求的处理方式可参考上述方法200中量子设备对密钥请求报文的处理方式，具体过程可参考上述方法200中的步骤202至步骤206，区别在于，此处第二量子设备的加密对象为密钥标识所指示的量子密钥。相应地，第二应用设备对来自第二量子设备的对量子密钥加密得到的密文的处理方式可参考上述方法200中应用设备对密钥响应报文的处理方式，具体过程可参考上述方法200中的步骤207至步骤208。

[0180] 可选地，请继续参见图6，第一量子设备与第二量子设备通过量子网络通信。第一量子设备与第一应用设备通过经典网络通信。第二量子设备与第二应用设备通过经典网络通信。第一应用设备与第二应用设备通过经典网络通信。

[0181] 图6示出的系统以向第一应用设备提供量子服务的量子设备(第一量子设备)与向第二应用设备提供量子服务的量子设备(第二量子设备)不同为例进行说明。如果第一应用设备与第二应用设备由同一台量子设备提供量子服务，那么在实现技术方案时，则省略两个量子设备之间同步量子密钥信息的步骤。

[0182] 本申请实施例提供的量子密钥传输系统，实现了将量子密钥从量子设备跨安全域安全可靠地传输到应用设备上。当通过经典网络通信的两个应用设备需要使用量子密钥进行通信时，通信发起方从对应的量子设备获取量子密钥和密钥标识。然后通信发起方通过

经典网络向通信接收方同步密钥标识。如果通信发起方和通信接收方由不同的量子设备提供量子服务，通信发起方对应的量子设备还向通信接收方对应的量子设备同步量子密钥和密钥标识。这样，通信接收方就能够向对应的量子设备请求到密钥标识对应的量子密钥，进而通信双方能够基于量子密钥进行通信。由于量子密钥从量子设备传输到应用设备的过程是安全可靠的，量子密钥通过量子网络传输始终是安全的，而两个应用设备之间传输的是量子密钥的密钥标识并非是量子密钥，使得窃取者无法从两个应用设备的通信过程中窃取量子密钥，因此通信双方获取量子密钥的整个过程都是安全可靠的，进而能够提高通信安全性和可靠性。

[0183] 下面对量子设备的基本硬件结构举例说明。

[0184] 例如，图7是本申请实施例提供的一种应用设备的硬件结构示意图。如图7所示，应用设备700包括处理器701和存储器702，存储器701与存储器702通过总线703连接。图7以处理器701和存储器702相互独立说明。可选地，处理器701和存储器702集成在一起。可选地，结合图1来看，图7中的应用设备700是图1所示的任一应用设备。

[0185] 其中，存储器702用于存储计算机程序，计算机程序包括操作系统和程序代码。存储器702是各种类型的存储介质，例如只读存储器(read-only memory，ROM)、随机存取存储器(random access memory，RAM)、电可擦可编程只读存储器(electrically erasable programmable read-only memory，EEPROM)、只读光盘(compact disc read-only memory，CD-ROM)、闪存、光存储器、寄存器、光盘存储、光碟存储、磁盘或者其它磁存储设备。

[0186] 其中，处理器701是通用处理器或专用处理器。处理器701可能是单核处理器或多核处理器。处理器701包括至少一个电路，以执行本申请实施例提供的上述方法200或方法300中应用设备执行的动作。

[0187] 可选地，应用设备700还包括网络接口704，网络接口704通过总线703与处理器701和存储器702连接。网络接口704能够实现应用设备700与量子设备或其它应用设备通信。处理器701能够通过网络接口704与量子设备交互来注册服务对象和获取量子密钥等，以及与其它应用设备通信等。

[0188] 可选地，应用设备700还包括输入/输出(input/output，I/O)接口705，I/O接口705通过总线703与处理器701和存储器702连接。处理器701能够通过I/O接口705接收输入的命令或数据等。I/O接口705用于应用设备700连接输入设备，这些输入设备例如是键盘、鼠标等。可选地，在一些可能的场景中，上述网络接口704和I/O接口705被统称为通信接口。

[0189] 可选地，应用设备700还包括显示器706，显示器706通过总线703与处理器701和存储器702连接。显示器706能够用于显示处理器701执行上述方法产生的中间结果和/或最终结果等，例如显示告警提示。在一种可能的实现方式中，显示器706是触控显示屏，以提供人机交互接口。

[0190] 其中，总线703是任何类型的，用于实现应用设备700的内部器件互连的通信总线。例如系统总线。本申请实施例以应用设备700内部的上述器件通过总线703互连为例说明，可选地，应用设备700内部的上述器件采用除了总线703之外的其他连接方式彼此通信连接，例如应用设备700内部的上述器件通过应用设备700内部的逻辑接口互连。

[0191] 上述器件可以分别设置在彼此独立的芯片上，也可以至少部分的或者全部的设置在同一块芯片上。将各个器件独立设置在不同的芯片上，还是整合设置在一个或者多个芯

片上，往往取决于产品设计的需要。本申请实施例对上述器件的具体实现形式不做限定。

[0192] 图7所示的应用设备700仅仅是示例性的，在实现过程中，应用设备700包括其他组件，本文不再一一列举。图7所示的应用设备700可以通过执行上述实施例提供的方法的全部或部分步骤来实现量子密钥的传输。

[0193] 下面对应用设备的基本硬件结构举例说明。

[0194] 例如，图8是本申请实施例提供的一种量子设备的硬件结构示意图。如图8所示，量子设备800包括处理器801和存储器802，存储器801与存储器802通过总线803连接。图8以处理器801和存储器802相互独立说明。可选地，处理器801和存储器802集成在一起。可选地，结合图1来看，图8中的量子设备800是图1所示的量子设备。

[0195] 其中，存储器802用于存储计算机程序，计算机程序包括操作系统和程序代码。存储器802是各种类型的存储介质，例如ROM、RAM、EEPROM、CD-ROM、闪存、光存储器、寄存器、光盘存储、光碟存储、磁盘或者其它磁存储设备。

[0196] 其中，处理器801是通用处理器或专用处理器。处理器801可能是单核处理器或多核处理器。处理器801包括至少一个电路，以执行本申请实施例提供的上述方法200或方法300中量子设备执行的动作。

[0197] 可选地，量子设备800还包括网络接口804，网络接口804通过总线803与处理器801和存储器802连接。网络接口804能够实现量子设备800与应用设备或其它量子设备通信。处理器801能够通过网络接口804与应用设备交互来注册服务对象和提供量子密钥等，以及与其它量子设备交互来同步量子密钥信息等。

[0198] 可选地，量子设备800还包括I/O接口805，I/O接口805通过总线803与处理器801和存储器802连接。处理器801能够通过I/O接口805接收输入的命令或数据等。I/O接口805用于量子设备800连接输入设备，这些输入设备例如是键盘、鼠标等。可选地，在一些可能的场景中，上述网络接口804和I/O接口805被统称为通信接口。

[0199] 可选地，量子设备800还包括显示器806，显示器806通过总线803与处理器801和存储器802连接。显示器806能够用于显示处理器801执行上述方法产生的中间结果和/或最终结果等，例如显示告警提示。在一种可能的实现方式中，显示器806是触控显示屏，以提供人机交互接口。

[0200] 其中，总线803是任何类型的，用于实现量子设备800的内部器件互连的通信总线。例如系统总线。本申请实施例以量子设备800内部的上述器件通过总线803互连为例说明，可选地，量子设备800内部的上述器件采用除了总线803之外的其他连接方式彼此通信连接，例如量子设备800内部的上述器件通过量子设备800内部的逻辑接口互连。

[0201] 上述器件可以分别设置在彼此独立的芯片上，也可以至少部分的或者全部的设置在同一块芯片上。将各个器件独立设置在不同的芯片上，还是整合设置在一个或者多个芯片上，往往取决于产品设计的需要。本申请实施例对上述器件的具体实现形式不做限定。

[0202] 图8所示的量子设备800仅仅是示例性的，在实现过程中，量子设备800包括其他组件，本文不再一一列举。图8所示的量子设备800可以通过执行上述实施例提供的方法的全部或部分步骤来实现量子密钥的传输。

[0203] 下面对本申请实施例的虚拟装置举例说明。

[0204] 图9是本申请实施例提供的一种应用设备的结构示意图。具有图9所示结构的应用

设备实现上述实施例描述的方案中应用设备的功能。可选地，图9所示的应用设备是图1或图6所示的应用场景中的任一应用设备、图4所示的应用设备或图7所示的应用设备，执行图2或图3所示实施例中描述的应用设备的功能。如图9所示，应用设备900包括发送模块901、接收模块902和处理模块903。

[0205] 发送模块901，用于向量子设备发送密钥请求报文，密钥请求报文包括应用设备对应的用户标识、第一公钥以及第一消息认证码值，用户标识用于量子设备获取对应的存储信息，存储信息包括量子设备与用户标识对应的共享密钥，第一公钥用于量子设备对分配给应用设备的量子密钥信息加密，量子密钥信息包括量子密钥，第一公钥为应用设备运行后量子密钥生成算法得到的密钥对中的公钥，第一消息认证码值由应用设备基于共享密钥对第一认证信息计算得到，第一认证信息包括第一公钥。

[0206] 接收模块902，用于接收来自量子设备的密钥请求报文对应的密钥响应报文，密钥响应报文包括第一密文以及第二消息认证码值。

[0207] 处理模块903，用于基于共享密钥以及第二认证信息对第二消息认证码值进行验证，第二认证信息包括第一密文。

[0208] 处理模块903，还用于如果应用设备对第二消息认证码值验证通过，采用第一私钥对第一密文解密以得到量子密钥信息，第一私钥为密钥对中的私钥。

[0209] 这里，发送模块901、接收模块902和处理模块903的详细工作过程请参照前面方法实施例中的描述。例如，发送模块901采用方法200中的步骤201向量子设备发送密钥请求报文。接收模块902采用方法200中的步骤206接收来自量子设备的密钥响应报文。处理模块903采用方法200中的步骤207和步骤208处理来自量子设备的密钥响应报文。本申请实施例在此不再重复描述。

[0210] 可选地，应用设备对应的用户标识为应用设备的设备标识，或者，应用设备对应的用户标识为登录应用设备的用户账号。

[0211] 可选地，密钥请求报文还包括第一统计值。处理模块903，还用于在向量子设备发送密钥请求报文之前，获取包括用户标识的密钥请求报文的历史发送次数。在历史发送次数上增加设定递增值，得到第一统计值。这里，处理模块903的详细工作过程可参考方法200中的相关描述。

[0212] 可选地，密钥响应报文还包括第二统计值。第二统计值为量子设备记录的包括用户标识的密钥请求报文的发送次数。处理模块903，还用于在接收到密钥响应报文之后，如果第二统计值与第一统计值不相等，停止量子密钥传输流程。这里，处理模块903的详细工作过程可参考方法200中的相关描述。

[0213] 可选地，第一认证信息还包括量子设备的设备标识、用户标识或第一统计值中的一个或多个。

[0214] 可选地，处理模块903，还用于在发送模块901向量子设备发送密钥请求报文之前，采用密钥派生函数基于目标口令生成派生密钥，共享密钥基于派生密钥得到。这里，处理模块903的详细工作过程可参考方法200中步骤201的相关描述。

[0215] 可选地，处理模块903，还用于在发送模块901向量子设备发送密钥请求报文之前，响应于获取到输入的量子密钥获取指令，运行后量子密钥生成算法生成密钥对，量子密钥获取指令包括目标口令。基于共享密钥对第一认证信息计算得到第一消息认证码值。这里，

处理模块903的详细工作过程可参考方法200中步骤201的相关描述。

[0216] 可选地，发送模块901，还用于在向量子设备发送密钥请求报文之前，向量子设备发送注册请求报文。接收模块902，还用于接收来自量子设备的注册请求报文对应的注册响应报文，注册响应报文包括量子设备的证书，证书包括第二公钥。处理模块903还用于如果应用设备对证书验证通过，采用第二公钥对注册信息加密得到第二密文，注册信息包括派生密钥以及用户标识。发送模块901，还用于向量子设备发送注册登记报文，注册登记报文包括第二密文。这里，发送模块901的详细工作过程可参考方法300中步骤301和步骤306的相关描述。接收模块902的详细工作过程可参考方法300中步骤302的相关描述。处理模块903的详细工作过程可参考方法300中步骤305的相关描述。

[0217] 可选地，注册请求报文指示应用设备支持的密码算法，注册响应报文还指示量子设备从应用设备支持的密码算法中选择的目标密码算法，目标密码算法包括第一消息认证码值的生成算法、第二消息认证码值的生成算法或共享密钥的生成算法中的一个或多个。

[0218] 可选地，注册响应报文还包括密钥派生函数参数值，密钥派生函数参数值包括随机盐值和/或迭代次数。处理模块903，还用于在接收模块902接收到注册响应报文之后，获取用户标识以及目标口令，采用密钥派生函数基于目标口令以及密钥派生函数参数值生成派生密钥。这里，处理模块903的详细工作过程可参考方法300中步骤303和步骤304的相关描述。

[0219] 可选地，注册登记报文还包括应用设备的设备标识。注册信息还包括应用设备的设备标识的哈希值。

[0220] 可选地，注册信息还包括应用设备生成的第一随机数。接收模块902，还用于接收来自量子设备的注册成功响应报文，注册成功响应报文用于指示用户标识已注册成功，注册成功响应报文包括第二随机数。处理模块903，还用于如果第二随机数与第一随机数相同，确定用户标识注册成功。这里，接收模块902的详细工作过程可参考方法300中步骤309的相关描述。处理模块903的详细工作过程可参考方法300中步骤310的相关描述。

[0221] 可选地，处理模块903，用于基于共享密钥对第二认证信息计算得到第三消息认证码值。如果第三消息认证码值与第二消息认证码值相同，确定对第二消息认证码值验证通过。这里，处理模块903的详细工作过程可参考方法200中步骤207的相关描述。

[0222] 可选地，应用设备与量子设备通过经典网络通信。

[0223] 图10是本申请实施例提供的一种量子设备的结构示意图。具有图10所示结构的量子设备实现上述实施例描述的方案中量子设备的功能。可选地，图10所示的量子设备是图1或图6所示的应用场景中的量子设备、图5所示的量子设备或图8所示的量子设备，执行图2或图3所示实施例中描述的量子设备的功能。如图10所示，量子设备1000包括接收模块1001、处理模块1002和发送模块1003。

[0224] 接收模块1001，用于接收来自应用设备的密钥请求报文，密钥请求报文包括应用设备对应的用户标识、第一公钥以及第一消息认证码值。

[0225] 处理模块1002，用于基于密钥请求报文获取第一认证信息以及用户标识对应的存储信息，存储信息包括量子设备与用户标识对应的共享密钥，第一认证信息包括第一公钥。

[0226] 处理模块1002，还用于基于共享密钥以及第一认证信息对第一消息认证码值进行验证。

[0227] 处理模块1002，还用于如果量子设备对第一消息认证码值验证通过，采用第一公钥对量子密钥信息加密得到第一密文，量子密钥信息包括量子密钥。

[0228] 处理模块1002，还用于基于共享密钥对第二认证信息计算得到第二消息认证码值，第二认证信息包括第一密文。

[0229] 发送模块1003，用于向应用设备发送密钥请求报文对应的密钥响应报文，密钥响应报文包括第一密文以及第二消息认证码值。

[0230] 这里，接收模块1001、处理模块1002和发送模块1003的详细工作过程请参照前面方法实施例中的描述。例如，接收模块1001采用方法200中的步骤201接收来自应用设备的密钥请求报文。处理模块1002采用方法200中的步骤202至步骤205处理来自应用设备的密钥请求报文。发送模块1003采用方法200中的步骤206向应用设备发送密钥响应报文。本申请实施例在此不再重复描述。

[0231] 可选地，应用设备对应的用户标识为应用设备的设备标识，或者，应用设备对应的用户标识为登录应用设备的用户账号。

[0232] 可选地，密钥请求报文还包括第一统计值，第一统计值为应用设备记录的包括用户标识的密钥请求报文的发送次数，存储信息包括第二统计值，第二统计值为量子设备记录的包括用户标识的密钥请求报文的发送次数。处理模块1002，还用于在获取用户标识对应的存储信息之后，如果第二统计值大于或等于第一统计值，停止量子密钥传输流程。如果第二统计值小于第一统计值，更新第二统计值，使更新后的第二统计值等于第一统计值。这里，处理模块1002的详细工作过程可参考方法200中的相关描述。

[0233] 可选地，密钥响应报文还包括更新后的第二统计值。

[0234] 可选地，第二认证信息还包括量子设备的设备标识、用户标识或更新后的第二统计值中的一个或多个。

[0235] 可选地，接收模块1001，还用于接收来自应用设备的注册请求报文。发送模块1003，还用于向应用设备发送注册响应报文，注册响应报文包括量子设备的证书，证书包括第二公钥，第二公钥为量子设备运行后量子密钥生成算法得到的密钥对中的公钥。处理模块1002，还用于如果接收模块1001接收到来自应用设备的包括第二密文的注册登记报文，采用第二私钥对第二密文解密以得到注册信息，注册信息包括派生密钥以及应用设备对应的用户标识，所述第二私钥为密钥对中的私钥，并存储用户标识对应的存储信息，存储信息包括基于派生密钥得到的共享密钥以及用户标识。这里，接收模块1001的详细工作过程可参考方法300中步骤301和步骤306的相关描述。处理模块1002的详细工作过程可参考方法300中步骤307和步骤308的相关描述。发送模块1003的详细工作过程可参考方法300中步骤302的相关描述。

[0236] 可选地，注册请求报文指示应用设备支持的密码算法，注册响应报文还指示量子设备从应用设备支持的密码算法中选择的目标密码算法，目标密码算法包括第一消息认证码值的生成算法、第二消息认证码值的生成算法或共享密钥的生成算法中的一个或多个。

[0237] 可选地，注册响应报文还包括第一密钥派生函数参数值，第一密钥派生函数参数值包括随机盐值和/或迭代次数，注册信息还包括第二密钥派生函数参数值。处理模块1002，还用于在得到注册信息之后，比对第一密钥派生函数参数值与第二密钥派生函数参数值，如果第一密钥派生函数参数值与第二密钥派生函数参数值相同，存储用户标识对应

的存储信息。这里，处理模块1002的详细工作过程可参考方法300中步骤308的相关描述。

[0238] 可选地，注册登记报文还包括应用设备的设备标识，注册信息还包括应用设备的设备标识的第一哈希值。处理模块1002，还用于在得到注册信息之后，计算应用设备的设备标识的第二哈希值，比对第一哈希值与第二哈希值，如果第一哈希值与第二哈希值相同，存储用户标识对应的存储信息。这里，处理模块1002的详细工作过程可参考方法300中步骤308的相关描述。

[0239] 可选地，注册信息还包括应用设备生成的随机数。发送模块1003，还用于在处理模块1002存储用户标识对应的存储信息之后，向应用设备发送注册成功响应报文，注册成功响应报文用于指示用户标识已注册成功，注册成功响应报文包括随机数。这里，发送模块1003的详细工作过程可参考方法300中步骤309的相关描述。

[0240] 可选地，处理模块1002，用于基于共享密钥对第一认证信息计算得到第四消息认证码值。如果第四消息认证码值与第一消息认证码值相同，确定对第一消息认证码值验证通过。这里，处理模块1002的详细工作过程可参考方法200中步骤203的相关描述。

[0241] 可选地，应用设备与量子设备通过经典网络通信。

[0242] 本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有指令，当所述指令被应用设备的处理器执行时，实现上述方法200或方法300中应用设备执行的步骤。或者，当所述指令被量子设备的处理器执行时，实现上述方法200或方法300中量子设备执行的步骤。

[0243] 本申请实施例还提供了一种计算机程序产品，包括计算机程序，所述计算机程序被应用设备的处理器执行时，实现上述方法200或方法300中应用设备执行的步骤。或者，所述计算机程序被量子设备的处理器执行时，实现上述方法200或方法300中量子设备执行的步骤。

[0244] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0245] 在本申请实施例中，术语“第一”、“第二”和“第三”仅用于描述目的，而不能理解为指示或暗示相对重要性。

[0246] 本申请中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0247] 需要说明的是，本申请所涉及的信息(包括但不限于用户设备信息、用户个人信息等)、数据(包括但不限于用于分析的数据、存储的数据、展示的数据等)以及信号，均为经用户授权或者经过各方充分授权的，且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准。例如，本申请中涉及到的量子密钥信息、注册信息等都是在充分授权的情况下获取的。

[0248] 以上所述仅为本申请的可选实施例，并不用以限制本申请，凡在本申请的构思和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

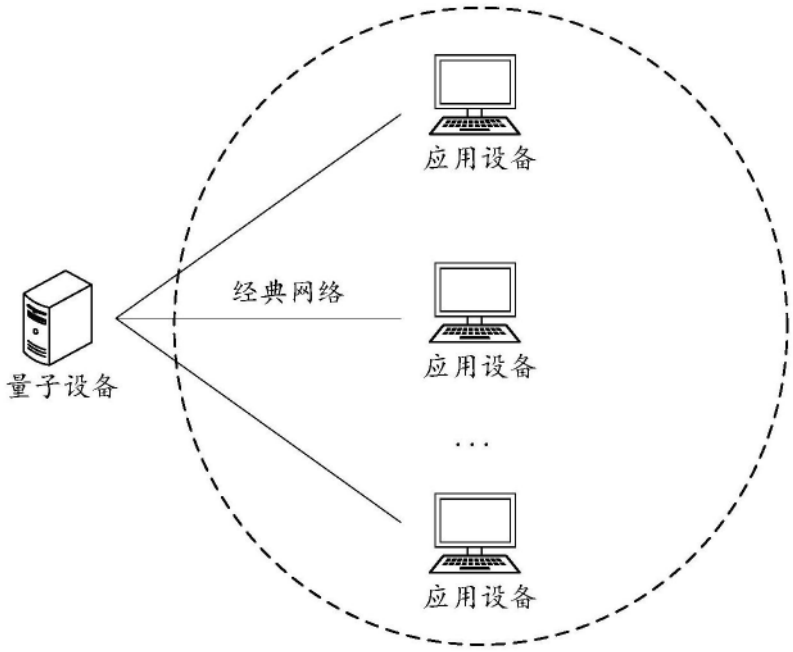


图1

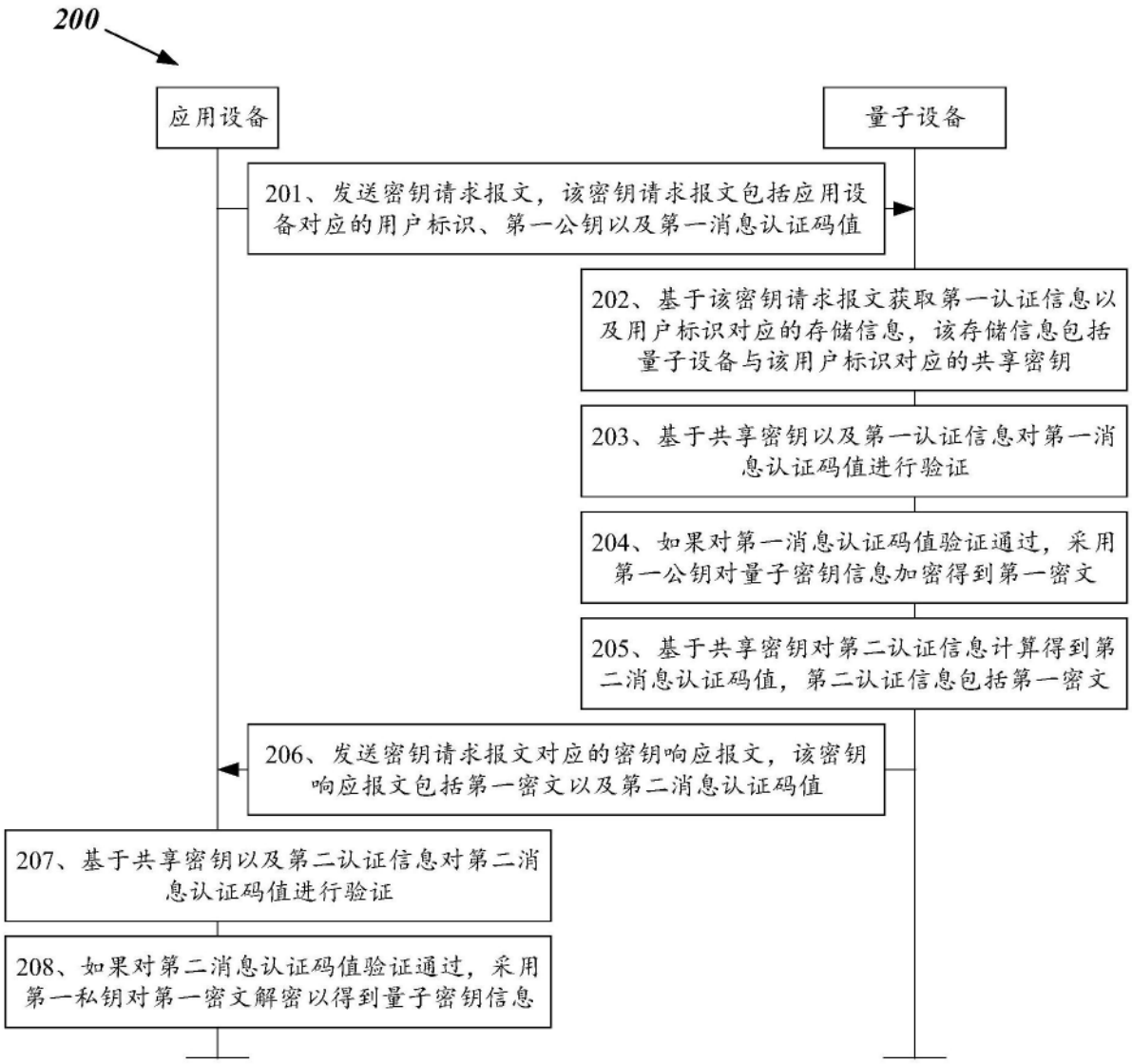

200
应用设备
量子设备
201、发送密钥请求报文，该密钥请求报文包括应用设备对应的用户标识、第一公钥以及第一消息认证码值
202、基于该密钥请求报文获取第一认证信息以及用户标识对应的存储信息，该存储信息包括量子设备与该用户标识对应的共享密钥
203、基于共享密钥以及第一认证信息对第一消息认证码值进行验证
204、如果对第一消息认证码值验证通过，采用第一公钥对量子密钥信息加密得到第一密文
205、基于共享密钥对第二认证信息计算得到第二消息认证码值，第二认证信息包括第一密文
206、发送密钥请求报文对应的密钥响应报文，该密钥响应报文包括第一密文以及第二消息认证码值
207、基于共享密钥以及第二认证信息对第二消息认证码值进行验证
208、如果对第二消息认证码值验证通过，采用第一私钥对第一密文解密以得到量子密钥信息

图2

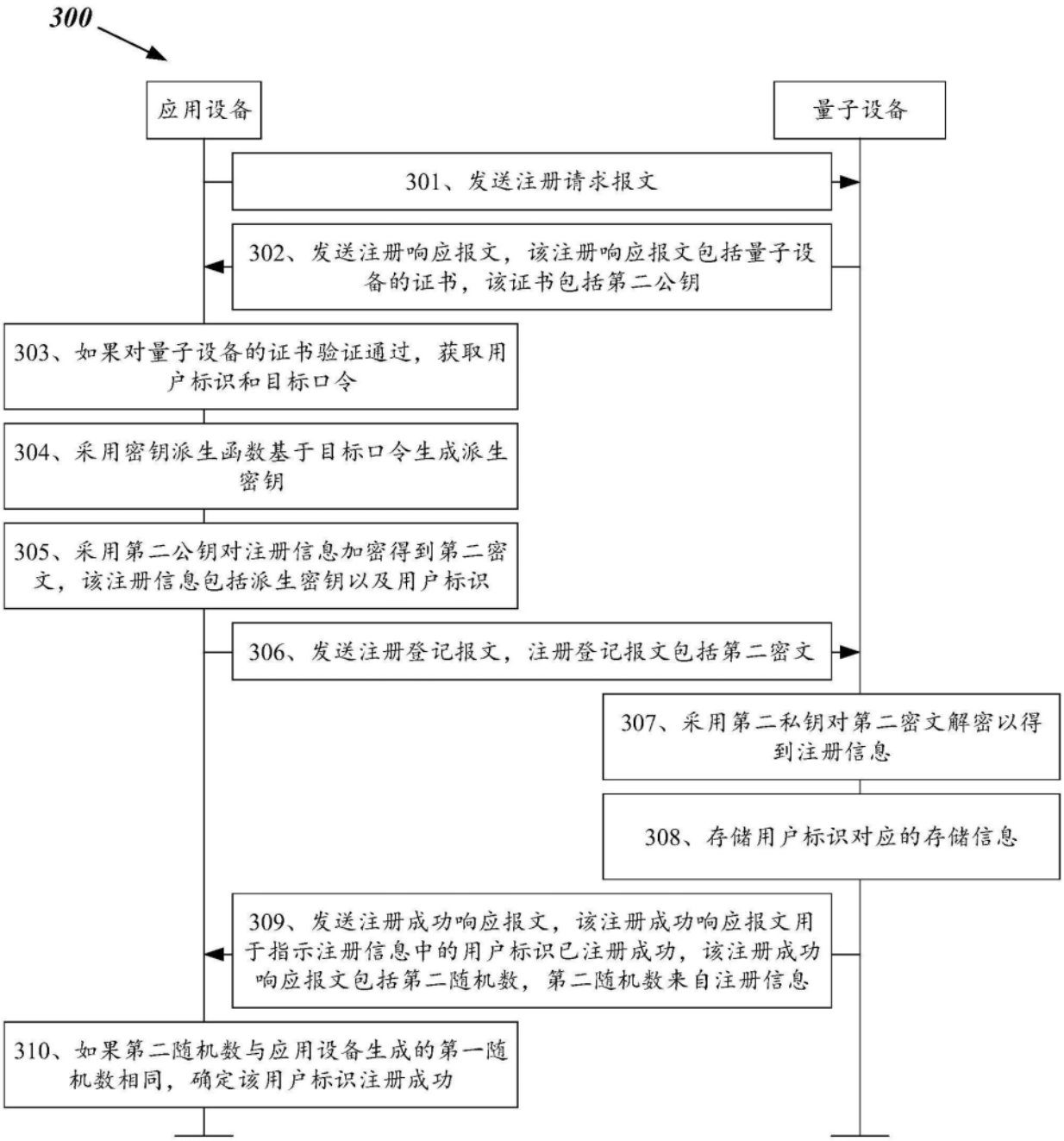

300
应用设备
量子设备
301、发送注册请求报文
302、发送注册响应报文，该注册响应报文包括量子设备的证书，该证书包括第二公钥
303、如果对量子设备的证书验证通过，获取用户标识和目标口令
304、采用密钥派生函数基于目标口令生成派生密钥
305、采用第二公钥对注册信息加密得到第二密文，该注册信息包括派生密钥以及用户标识
306、发送注册登记报文，注册登记报文包括第二密文
307、采用第二私钥对第二密文解密以得到注册信息
308、存储用户标识对应的存储信息
309、发送注册成功响应报文，该注册成功响应报文用于指示注册信息中的用户标识已注册成功，该注册成功响应报文包括第二随机数，第二随机数来自注册信息
310、如果第二随机数与应用设备生成的第一随机数相同，确定该用户标识注册成功

图3

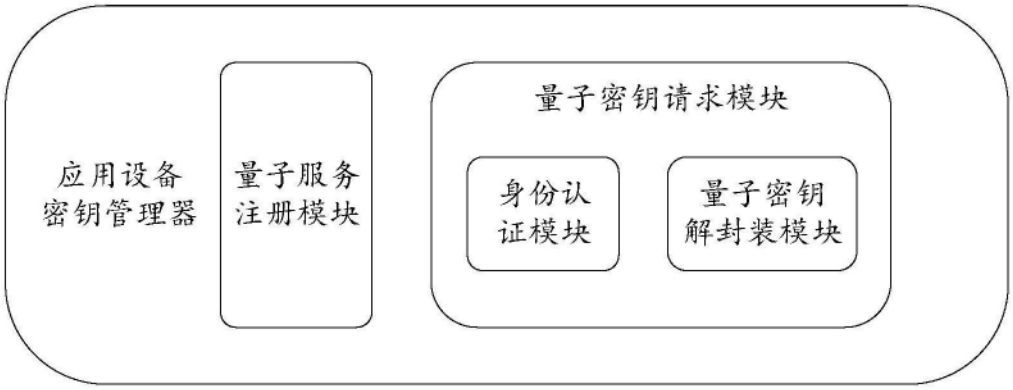

应用设备
密钥管理器
量子服务
注册模块
量子密钥请求模块
身份认
证模块
量子密钥
解封装模块

图4

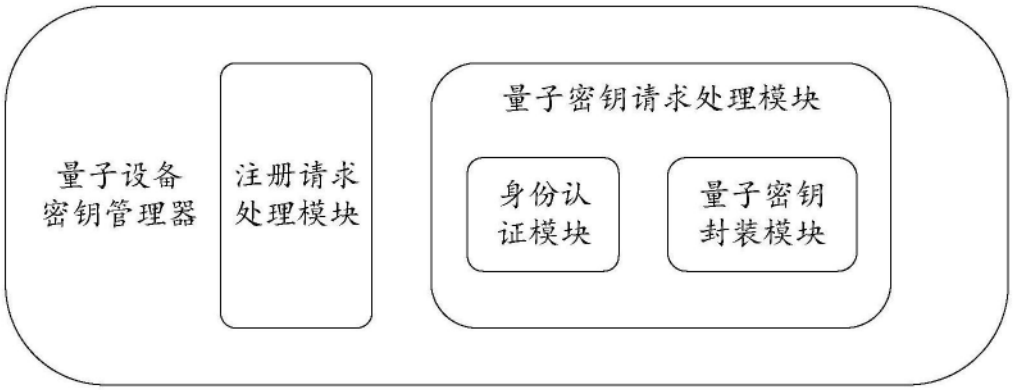

量子设备
密钥管理器
注册请求
处理模块
量子密钥请求处理模块
身份认
证模块
量子密钥
封装模块

图5

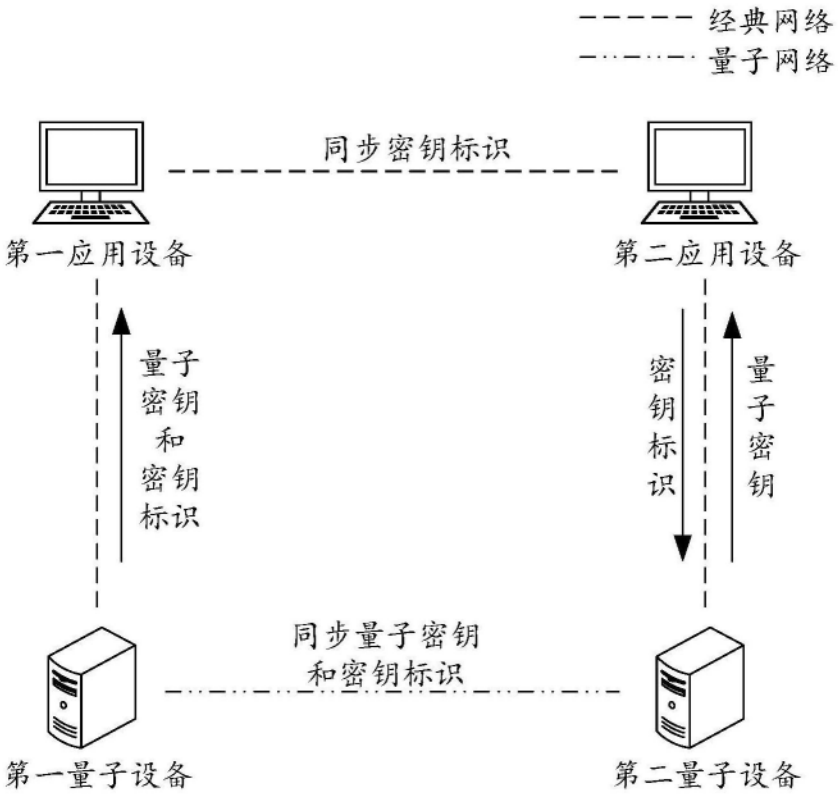

经典网络
量子网络
同步密钥标识
第一应用设备
第二应用设备
量子密钥和密钥标识
密钥标识
量子密钥
同步量子密钥和密钥标识
第一量子设备
第二量子设备

图6

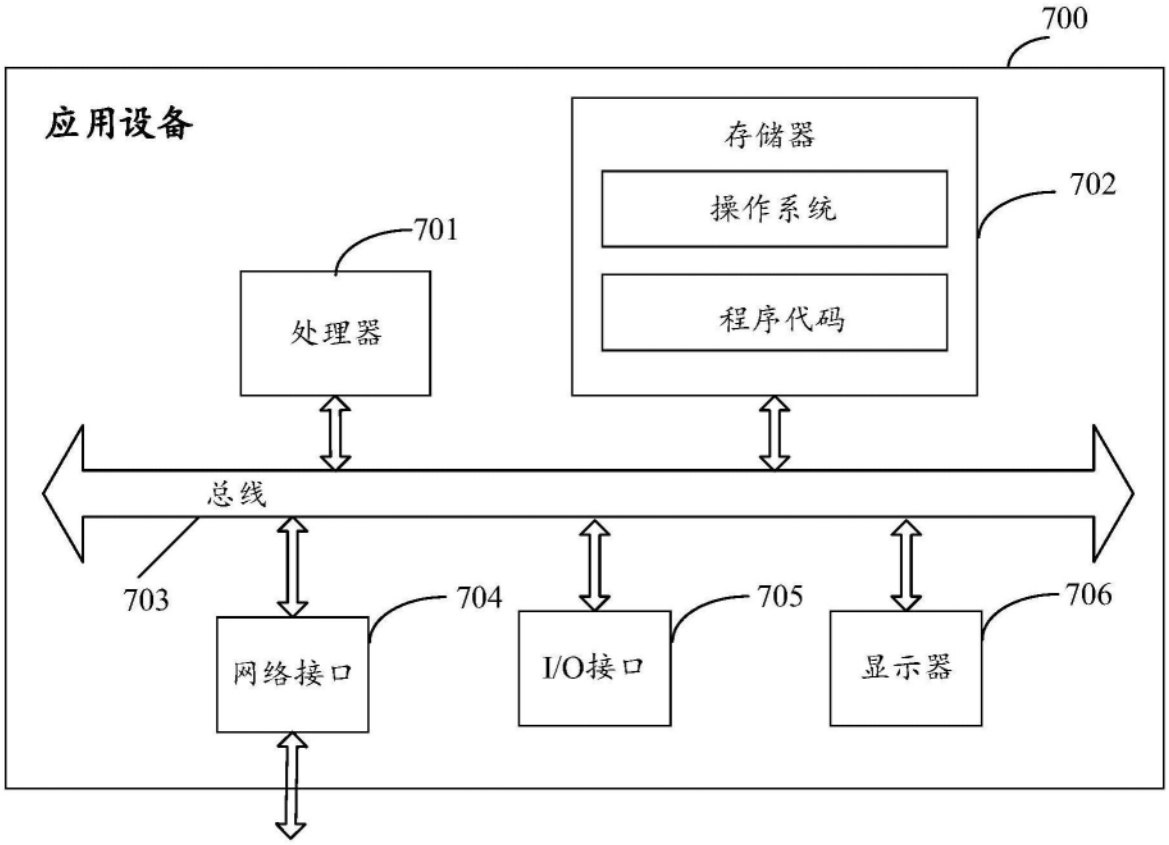

700
应用设备
存储器
操作系统
程序代码
702
701
处理器
总线
703
704
网络接口
705
I/O接口
706
显示器

图7

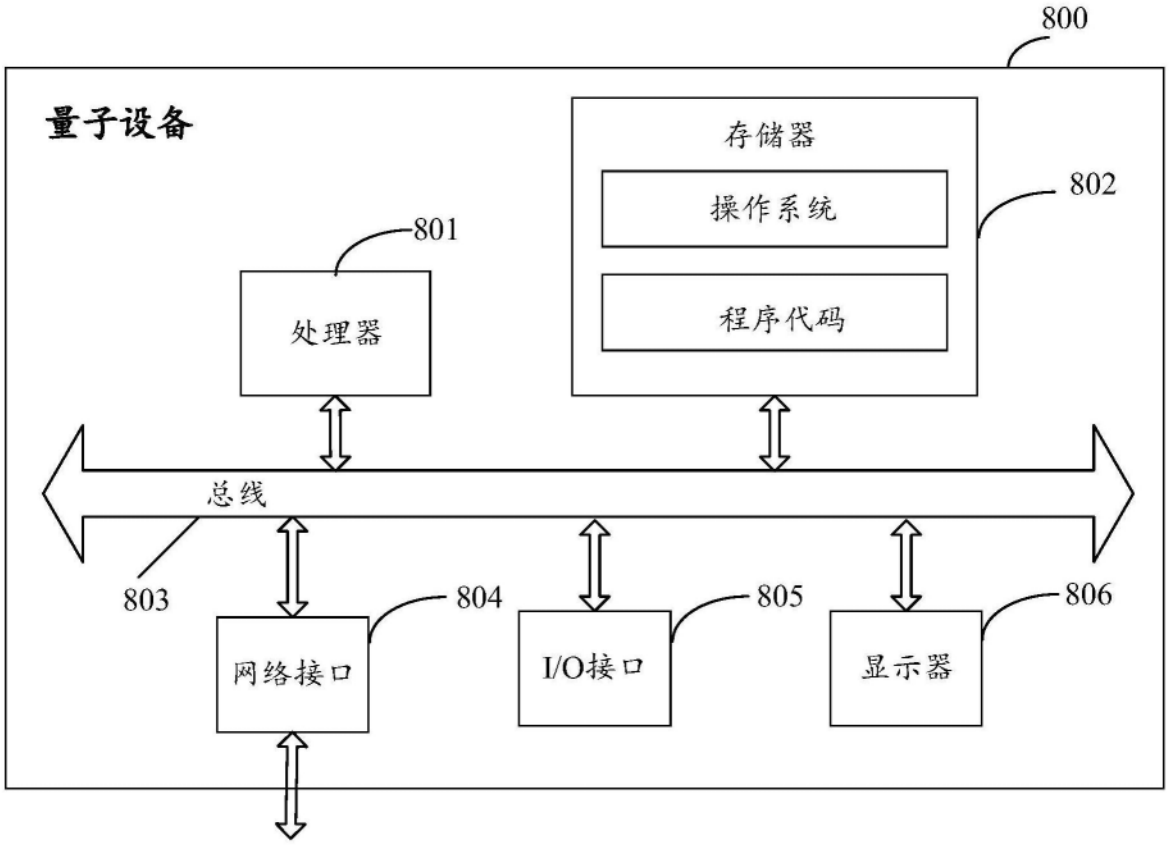

800
量子设备
存储器
操作系统
802
801
处理器
程序代码
总线
803
804
805
806
网络接口
I/O接口
显示器

图8

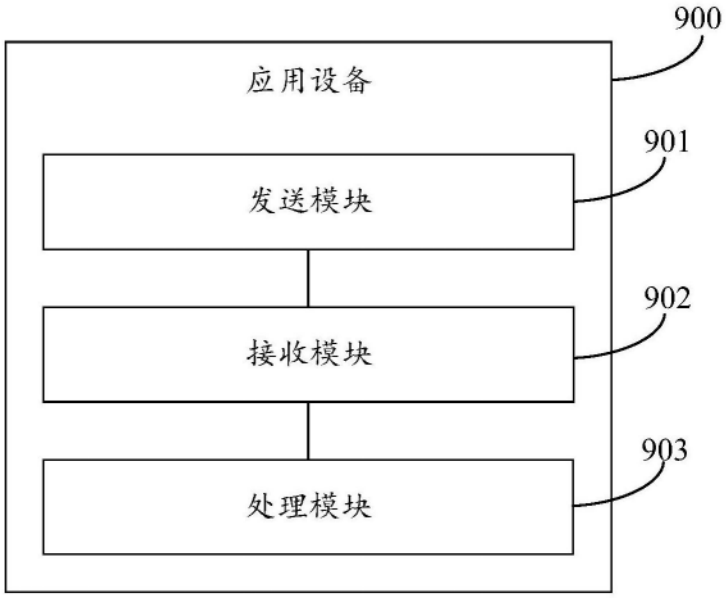

900
应用设备
901
发送模块
902
接收模块
903
处理模块

图9

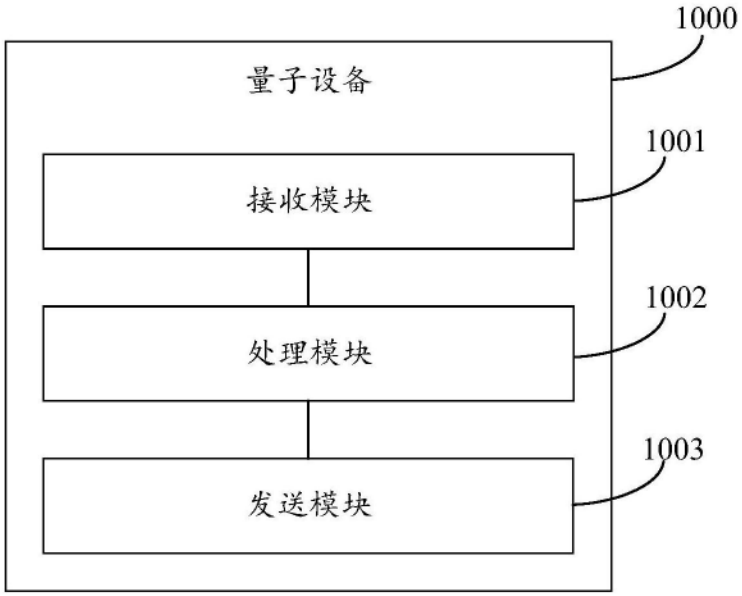


图10