(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 106411521 B
(45)授权公告日 2020.02.18

(21)申请号 201510463392.X
(22)申请日 2015.07.31
(65)同一申请的已公布的文献号
申请公布号 CN 106411521 A
(43)申请公布日 2017.02.15
(73)专利权人 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
(74)专利代理机构 北京清源汇知识产权代理事务所(特殊普通合伙) 11644
代理人 冯德魁
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)
审查员 陈娟

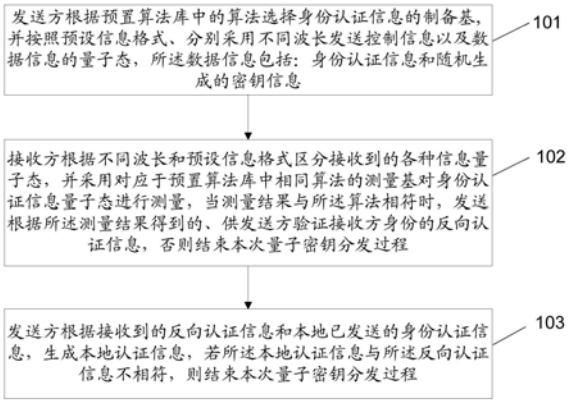
权利要求书8页 说明书24页 附图8页

(54)发明名称

用于量子密钥分发过程的身份认证方法、装置及系统

(57)摘要

本申请公开了一种用于量子密钥分发过程的身份认证方法，同时公开了另外两种身份认证方法及相应装置，以及一种身份认证系统。所述方法包括：发送方根据算法库中的算法选择身份认证信息的制备基，并按照预设信息格式分别采用不同波长发送控制信息以及数据信息的量子态；接收方区分接收到的量子态，并采用对应于相同算法的测量基对身份认证信息量子态进行测量，当测量结果与所述算法相符时发送反向认证信息，否则结束本次分发过程；发送方则在本地认证信息与反向认证信息不相符时，结束本次分发过程。采用本技术方案，可以实时确认通信方身份的合法性，有效防御中间人攻击和DDoS攻击，而且采用基于算法的方式生成身份认证信息，避免对量子密钥的浪费。



CN 106411521 B

1.一种用于量子密钥分发过程的身份认证方法，其特征在于，所述方法在参与量子密钥分发过程的收发双方量子通信设备中实施，包括：

发送方根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息；

接收方根据所述不同波长和所述预设信息格式区分接收到的各种信息量子态，并采用对应于预置算法库中相同算法的测量基对其中的身份认证信息量子态进行测量，当测量结果与所述算法对应的预期信息相符时，发送根据所述测量结果得到的、供发送方验证接收方身份的反向认证信息，否则结束本次量子密钥分发过程；

发送方根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，若所述本地认证信息与所述反向认证信息不相符，则结束本次量子密钥分发过程。

2.根据权利要求1所述的用于量子密钥分发过程的身份认证方法，其特征在于，当所述接收方判断出测量结果与所述算法对应的预期信息相符时，所述接收方还执行下述操作：

通过经典信道公开用于测量密钥信息量子态的测量基；

相应的，当所述发送方判断出所述本地认证信息与所述反向认证信息相符时，所述发送方执行下述操作：

确定密钥信息量子态的正确测量基，筛选原始密钥；

通过经典信道公布所述密钥信息量子态的正确测量基；

相应的，在上述发送方公布所述密钥信息量子态的正确测量基的步骤之后，执行下述操作：

接收方筛选原始密钥；以及，

收发双方通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

3.根据权利要求1所述的用于量子密钥分发过程的身份认证方法，其特征在于，在所述发送方根据预置算法库中的算法选择身份认证信息的制备基的步骤之前，执行下述操作：

收发双方通过经典信道协商算法编号；

相应的，收发双方所采用的算法是根据所述协商确定的算法编号从各自预置算法库中选取的。

4.根据权利要求3所述的用于量子密钥分发过程的身份认证方法，其特征在于，收发双方的预置算法库中的算法编号是按照预设策略同步变换的。

5.根据权利要求3所述的用于量子密钥分发过程的身份认证方法，其特征在于，在收发双方通过经典信道协商算法编号的过程中，所述编号是采用双方预置共享密钥加密传输的。

6.根据权利要求1所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述预设信息格式包括：身份认证信息和密钥信息分别有各自的控制信息作为前缀。

7.根据权利要求6所述的用于量子密钥分发过程的身份认证方法，其特征在于，承载作为身份认证信息前缀的控制信息量子态的波长、与承载作为密钥信息前缀的控制信息量子态的波长不同。

8.根据权利要求6所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述预设信息格式包括：作为身份认证信息前缀的控制信息与作为密钥信息前缀的控制信息分别

采用不同编码；

所述不同编码是收发双方预先设定的、或者通过经典信道预先协商确定的；收发双方用于制备或者测量控制信息量子态的基矢是收发双方预先设定的、或者通过经典信道预先协商确定的。

9.所述权利要求1所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述预设信息格式包括：身份认证信息和密钥信息采用共同的控制信息作为前缀；

相应的，在所述发送方根据预置算法库中的算法选择身份认证信息的制备基之前，执行下述操作：

收发双方通过经典信道协商位于控制信息与密钥信息之间的身份认证信息的长度。

10.根据权利要求1所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述根据所述测量结果得到的、供发送方验证接收方身份的反向认证信息包括：

接收方从所述测量结果中选取接收方认证密钥的位置信息，以及，所述接收方认证密钥或者接收方认证密钥的散列值；

相应的，所述发送方根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，包括：

所述发送方根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥，并相应地将所述发送方认证密钥或者所述发送方认证密钥的散列值作为所述本地认证信息。

11.根据权利要求1所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述由所述测量结果得到的、供发送方验证接收方身份的反向认证信息包括：

接收方从所述测量结果中选取接收方认证密钥的位置信息，用所述接收方认证密钥加密的、本地生成的辅助认证信息的密文，以及由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

相应的，所述发送方根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，包括：

所述发送方根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥；

利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息；

计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息。

12.根据权利要求11所述的用于量子密钥分发过程的身份认证方法，其特征在于，当所述发送方判断出所述本地认证信息与所述反向认证信息相符时，执行下述操作：

所述发送方采用所述发送方认证密钥加密所述通过解密操作获取的辅助认证信息的变体；

并通过经典信道发送执行上述加密操作后的密文；

相应的，所述接收方在接收所述密文后，执行下述操作：

采用所述接收方认证密钥解密接收到的密文；

判断执行所述解密操作后得到的信息是否与所述本地生成的辅助认证信息的变体一致；

若不一致，则结束本次量子密钥分发过程。

13.根据权利要求1-12任一项所述的用于量子密钥分发过程的身份认证方法，其特征在于，在所述发送方根据预置算法库中的算法选择身份认证信息的制备基的步骤之前，执行下述操作：

收发双方通过经典信道，利用预置的账户信息与对端设备相互进行身份验证，若其中任一设备未通过所述身份验证，则结束本次量子密钥分发过程。

14.根据权利要求1-12任一项所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述预置算法库中的算法包括：

根据身份验证信息中每个比特在数据信息中的位置，选择相应的制备基或者测量基。

15.根据权利要求14所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述根据身份验证信息中每个比特在数据信息中的位置，选择相应的制备基或者测量基，具体是指：

根据所述每个比特在数据信息中的位置信息与4取模的不同结果，选择相应的水平偏振基、垂直偏振基、左旋偏振基、或者右旋偏振基。

16.一种用于量子密钥分发过程的身份认证方法，其特征在于，所述方法在参与量子密钥分发过程的发送方量子通信设备上实施，包括：

根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长向参与量子密钥分发过程的对端设备发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息；

接收所述对端设备返回的反向认证信息；

根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息；

判断所述本地认证信息是否与接收到的反向认证信息相符；若否，则结束本次量子密钥分发过程。

17.根据权利要求16所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述对端设备返回的信息不仅包括：所述反向认证信息，还包括：测量密钥信息量子态所采用的测量基；

相应的，当所述判断所述本地认证信息是否与接收到的反向认证信息相符的结果为是时，执行下述操作：

确定密钥信息量子态的正确测量基，筛选原始密钥；

通过经典信道公布所述密钥信息量子态的正确测量基；

通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

18.根据权利要求16所述的用于量子密钥分发过程的身份认证方法，其特征在于，在所述根据预置算法库中的算法选择身份认证信息的制备基的步骤之前，执行下述操作：

与所述对端设备通过经典信道协商算法编号；

相应的，所述根据预置算法库中的算法选择身份认证信息的制备基包括：

根据协商确定的算法编号从所述预置算法库中选择算法；

根据所述算法选择所述身份认证信息的制备基。

19.根据权利要求16所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述预设信息格式包括：身份认证信息和密钥信息分别有各自的控制信息作为前缀。

20.根据权利要求16所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述预设信息格式包括：身份认证信息和密钥信息采用共同的控制信息作为前缀；

相应的，在所述根据预置算法库中的算法选择身份认证信息的制备基的步骤之前，执行下述操作：

与所述对端设备通过经典信道协商位于控制信息与密钥信息之间的身份认证信息的长度。

21.根据权利要求16所述的用于量子密钥分发过程的身份认证方法，其特征在于，接收到的所述反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、接收方认证密钥或接收方认证密钥的散列值；

相应的，所述根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，包括：

根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥，并相应地将所述发送方认证密钥或者所述发送方认证密钥的散列值作为所述本地认证信息。

22.根据权利要求16所述的用于量子密钥分发过程的身份认证方法，其特征在于，接收到的所述反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、辅助认证信息密文、以及由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

相应的，所述根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，包括：

根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥；

利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息；

计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息。

23.根据权利要求22所述的用于量子密钥分发过程的身份认证方法，其特征在于，当所述判断所述本地认证信息是否与接收到的反向认证信息相符的结果为是时，执行下述操作：

采用所述发送方认证密钥加密所述通过解密操作获取的辅助认证信息的变体；

通过经典信道将执行上述加密操作后的密文发送给所述对端设备。

24.一种用于量子密钥分发过程的身份认证装置，其特征在于，所述装置部署在参与量子密钥分发过程的发送方量子通信设备上，包括：

量子态发送单元，用于根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长向参与量子密钥分发过程的对端设备发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息；

响应信息接收单元，用于接收所述对端设备返回的反向认证信息；

本地认证信息生成单元，用于根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息；

发送方认证判断单元，用于判断所述本地认证信息是否与接收到的反向认证信息相符；

分发过程结束单元，用于当所述发送方认证判断单元的输出为否时，结束本次量子密钥分发过程。

25.根据权利要求24所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述响应信息接收单元接收到的信息不仅包括反向认证信息，还包括：测量密钥信息量子态所采用的测量基；

相应的，所述装置还包括：

原始密钥筛选单元，用于当所述发送方认证判断单元的输出结果为是时，确定密钥信息量子态的正确测量基，并筛选原始密钥；

正确测量基公布单元，用于通过经典信道公布所述密钥信息量子态的正确测量基；

发送方量子密钥获取单元，用于通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

26.根据权利要求24所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述装置还包括：

算法编号协商单元，用于在触发所述量子态发送单元工作之前，与所述对端设备通过经典信道协商算法编号；

相应的，所述量子态发送单元选择身份认证信息的制备基的功能具体通过如下方式实现：

根据所述算法编号协商单元确定的算法编号从所述预置算法库中选择算法，并根据所述算法选择所述身份认证信息的制备基。

27.根据权利要求24所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述量子态发送单元所采用的预设信息格式包括：身份认证信息和密钥信息分别有各自的控制信息作为前缀。

28.根据权利要求24所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述量子态发送单元所采用的预设信息格式包括：身份认证信息和密钥信息采用共同的控制信息作为前缀；

相应的，所述装置还包括：

认证信息长度协商单元，用于在触发所述量子态发送单元工作之前，与所述对端设备通过经典信道协商位于控制信息与密钥信息之间的身份认证信息的长度。

29.根据权利要求24所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述响应信息接收单元接收到的反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、接收方认证密钥或接收方认证密钥的散列值；

相应的，所述本地认证信息生成单元具体用于，根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥，并相应地将所述发送方认证密钥或者所述发送方认证密钥的散列值作为所述本地认证信息。

30.根据权利要求24所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述响应信息接收单元接收到的反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、辅助认证信息密文、以及由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

相应的，所述本地认证信息生成单元包括：

发送方认证密钥选取子单元，用于根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥；

辅助认证信息解密单元，用于利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息；

发送方散列值计算单元，用于计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息。

31.根据权利要求30所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述装置还包括：

变体信息加密单元，用于当所述发送方认证判断单元的输出为是时，采用所述发送方认证密钥加密所述通过解密操作获取的辅助认证信息的变体；

变体信息密文发送单元，用于通过经典信道将执行上述加密操作后的密文发送给所述对端设备。

32.一种用于量子密钥分发过程的身份认证方法，其特征在于，所述方法在参与量子密钥分发过程的接收方量子通信设备上实施，包括：

接收参与量子密钥分发过程的对端设备发送的量子态，并根据预先约定的不同波长和预设信息格式区分接收到的各种信息量子态；

根据从预置算法库中选取的、与所述对端设备相同的算法选择测量基，并用所述测量基对接收到的身份认证信息量子态进行测量；

判断测量结果是否与所选算法对应的预期信息相符；

若是，向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息；

若否，则结束本次量子密钥分发过程。

33.根据权利要求32所述的用于量子密钥分发过程的身份认证方法，其特征在于，当所述判断测量结果是否与所述算法对应的预期信息相符的结果为是时，还执行下述操作：

通过经典信道公开用于测量密钥信息量子态的测量基；

相应的，所述方法还包括：

接收所述对端设备通过经典信道发送的所述密钥信息量子态的正确测量基；

筛选原始密钥，并通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

34.根据权利要求32所述的用于量子密钥分发过程的身份认证方法，其特征在于，在所述接收参与量子密钥分发过程的对端设备发送的量子态的步骤之前，执行下述操作：

与所述对端设备通过经典信道协商算法编号；

相应的，所述根据从预置算法库中选取的、与对端设备相同的算法选择测量基包括：

根据协商确定的算法编号从所述预置算法库中选择算法；

根据所述算法选择所述测量基。

35.根据权利要求32所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息，包括：

从所述测量结果中选取接收方认证密钥；

将选取所述接收方认证密钥的位置信息、以及所述接收方认证密钥或者接收方认证密

钥的散列值发送给所述对端设备。

36.根据权利要求32所述的用于量子密钥分发过程的身份认证方法，其特征在于，所述向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息，包括：

从所述测量结果中选取接收方认证密钥；

用所述接收方认证密钥对本地生成的辅助认证信息加密；

计算由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

将选取所述接收方认证密钥的位置信息、所述辅助认证信息密文、以及所述散列值发送给所述对端设备。

37.根据权利要求36所述的用于量子密钥分发过程的身份认证方法，其特征在于，在所述向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息的步骤之后，执行下述操作：

接收所述对端设备发送的辅助认证信息变体的密文；

采用所述接收方认证密钥解密接收到的所述密文；

判断执行所述解密操作后得到的信息是否与所述本地生成的辅助认证信息的变体一致；

若不一致，则结束本次量子密钥分发过程。

38.一种用于量子密钥分发过程的身份认证装置，其特征在于，所述装置部署在参与量子密钥分发过程的接收方量子通信设备上，包括：

量子态接收单元，用于接收参与量子密钥分发过程的对端设备发送的量子态，并根据预先约定的不同波长和预设信息格式区分接收到的各种信息量子态；

量子态测量单元，用于根据从预置算法库中选取的、与对端设备相同的算法选择测量基，并用所述测量基对接收到的身份认证信息量子态进行测量；

接收方认证判断单元，用于判断测量结果是否与所选算法对应的预期信息相符；

反向认证信息发送单元，用于当所述接收方认证判断单元的输出为是时，向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息；

分发过程结束单元，用于当所述接收方认证判断单元的输出为否时，结束本次量子密钥分发过程。

39.根据权利要求38所述的用于量子密钥分发过程的身份认证装置，其特征在于，还包括：

测量基公布单元，用于当所述接收方认证判断单元的输出为是时，通过经典信道公开用于测量密钥信息量子态的测量基；

相应的，所述装置还包括：

正确测量基接收单元，用于接收所述对端设备通过经典信道发送的所述密钥信息量子态的正确测量基；

接收方量子密钥获取单元，用于筛选原始密钥，并通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

40.根据权利要求38所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述装置还包括：

算法编号协商单元，用于在触发所述量子态接收单元工作之前，与所述对端设备通过经典信道协商算法编号；

相应的，所述量子态测量单元选择身份认证信息的测量基的功能具体通过如下方式实现：

根据协商确定的算法编号从所述预置算法库中选择算法，并根据所述算法选择所述测量基。

41.根据权利要求38所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述反向认证信息发送单元包括：

接收方认证密钥选取子单元，用于从所述测量结果中选取接收方认证密钥；

第一信息发送执行子单元，用于将选取所述接收方认证密钥的位置信息、以及所述接收方认证密钥或者接收方认证密钥的散列值发送给所述对端设备。

42.根据权利要求38所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述反向认证信息发送单元包括：

接收方认证密钥选取子单元，用于从所述测量结果中选取接收方认证密钥；

辅助认证信息加密子单元，用于用所述接收方认证密钥对本地生成的辅助认证信息加密；

接收方散列值计算子单元，计算由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

第二信息发送执行子单元，用于将选取所述接收方认证密钥的位置信息、所述辅助认证信息密文、以及所述散列值发送给所述对端设备。

43.根据权利要求42所述的用于量子密钥分发过程的身份认证装置，其特征在于，所述装置还包括：

变体信息密文接收单元，用于在所述反向认证信息发送单元完成发送操作后，接收所述对端设备发送的辅助认证信息变体的密文；

变体信息密文解密单元，用于采用所述接收方认证密钥解密接收到的所述密文；

变体信息判断单元，用于判断执行所述解密操作后得到的信息是否与所述本地生成的辅助认证信息的变体一致，若不一致，则触发所述分发过程结束单元工作。

44.一种用于量子密钥分发过程的身份认证系统，其特征在于，包括：如上述权利要求24所述的部署于发送方量子通信设备的身份认证装置、以及如上述权利要求38所述的部署于接收方量子通信设备的身份认证装置。

用于量子密钥分发过程的身份认证方法、装置及系统

技术领域

[0001] 本申请涉及身份认证技术，具体涉及一种用于量子密钥分发过程的身份认证方法。本申请同时涉及另外两种用于量子密钥分发过程的身份认证方法及相应装置，以及一种用于量子密钥分发过程的身份认证系统。

背景技术

[0002] 身份认证是保证网络安全的一个重要环节，通过认证可以保障通信双方的真实性、消息的完整性和来源可靠性，以防止非法方对信息进行伪造、修改和延迟等攻击。密码学中通常利用私钥密码机制和公钥密码机制保证通信中身份信息的安全性、完整性、不可否认性和抵抗身份冒充攻击。

[0003] 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本原理保证，与攻击者的计算能力和存储能力无关，被证明具有无条件安全性和对窃听者的可检测性。然而传统的量子密钥分配协议却没有提供有效的身份认证机制，因此可能在量子密钥分配过程(也称分发过程)中受到中间人攻击或者分布式拒绝服务(Distributed Denial of Service—DDoS)攻击。

[0004] 针对上述问题，现有技术提出了如下两种解决方案：

[0005] (一)M.Dusek等认为在通信过程中不需要认证全部的经典信息，仅需要对影响正确判断量子态错误率的经典信息进行认证，其他的经典信息不需要认证。因此M.Dusek提出了结合经典消息认证算法的量子身份认证协议，其实质就是用经典的认证算法对尽量少的经典消息进行认证。

[0006] (二)采用带身份认证的BB84协议。该协议与原BB84协议的主要不同点是将随机发送的量子比特串中某些比特位设定为特定的认证位，其具体的位置由认证密钥决定，通过此认证位的比特所代表的测量基矢以及光量子的偏振态来实现通信双方的身份认证，认证位的量子态信息不可随机发送，而应根据特定的规则由双方共享的认证密钥决定。收发双方通过将每次协商获取的共享量子密钥中的一部分设定为认证密钥，从而实现认证密钥的动态更新。

[0007] 上述两种方案由于都采用了身份认证机制，在一定程度上可以加强量子密钥分发过程的安全性，但是各自都存在一定的缺陷：

[0008] (一)M.Dusek方案，通信双方事先共享的认证密钥数量有限，易遭受中间人攻击和DDoS攻击，而且该方案没有充分利用量子的优越性，依然采用的是经典认证技术，存在被破解的风险。

[0009] (二)带身份认证的BB84协议虽然将共享认证密钥信息以量子态形式发送，提高了密钥分发的安全性，但是该技术方案需要从每次协商获取的共享量子密钥中选取一部分作为认证密钥，导致这部分量子密钥无法用于业务数据加密，浪费量子密钥资源。

发明内容

[0010] 本申请实施例提出的一种用于量子密钥分发过程的身份认证方法，不仅提供了一种在量子密钥分发过程中进行身份认证的新思路，而且可以有效解决现有量子密钥分发过程采用的身份认证机制存在的不安全、以及浪费量子密钥资源的问题。本申请实施例还提供另外两种用于量子密钥分发过程的身份认证方法及相应装置，以及一种用于量子密钥分发过程的身份认证系统。

[0011] 本申请提供一种用于量子密钥分发过程的身份认证方法，所述方法在参与量子密钥分发过程的收发双方量子通信设备中实施，包括：

[0012] 发送方根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息；

[0013] 接收方根据所述不同波长和所述预设信息格式区分接收到的各种信息量子态，并采用对应于预置算法库中相同算法的测量基对其中的身份认证信息量子态进行测量，当测量结果与所述算法相符时，发送根据所述测量结果得到的、供发送方验证接收方身份的反向认证信息，否则结束本次量子密钥分发过程；

[0014] 发送方根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，若所述本地认证信息与所述反向认证信息不相符，则结束本次量子密钥分发过程。

[0015] 可选的，当所述接收方判断出测量结果与所述算法相符时，所述接收方还执行下述操作：

[0016] 通过经典信道公开用于测量密钥信息量子态的测量基；

[0017] 相应的，当所述发送方判断出所述本地认证信息与所述反向认证信息相符时，所述发送方执行下述操作：

[0018] 确定密钥信息量子态的正确测量基，筛选原始密钥；

[0019] 通过经典信道公布所述密钥信息量子态的正确测量基；

[0020] 相应的，在上述发送方公布所述密钥信息量子态的正确测量基的步骤之后，执行下述操作：

[0021] 接收方筛选原始密钥；以及，

[0022] 收发双方通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0023] 可选的，在所述发送方根据预置算法库中的算法选择身份认证信息的制备基的步骤之前，执行下述操作：

[0024] 收发双方通过经典信道协商算法编号；

[0025] 相应的，收发双方所采用的算法是根据所述协商确定的算法编号从各自预置算法库中选取的。

[0026] 可选的，收发双方的预置算法库中的算法编号是按照预设策略同步变换的。

[0027] 可选的，在收发双方通过经典信道协商算法编号的过程中，所述编号是采用双方预置共享密钥加密传输的。

[0028] 可选的，所述预设信息格式包括：身份认证信息和密钥信息分别有各自的控制信息作为前缀。

[0029] 可选的，承载作为身份认证信息前缀的控制信息量子态的波长、与承载作为密钥

信息前缀的控制信息量子态的波长不同。

[0030] 可选的，所述预设信息格式包括：作为身份认证信息前缀的控制信息与作为密钥信息前缀的控制信息分别采用不同编码；

[0031] 所述不同编码是收发双方预先设定的、或者通过经典信道预先协商确定的；收发双方用于制备或者测量控制信息量子态的基矢是收发双方预先设定的、或者通过经典信道预先协商确定的。

[0032] 可选的，所述预设信息格式包括：身份认证信息和密钥信息采用共同的控制信息作为前缀；

[0033] 相应的，在所述发送方根据预置算法库中的算法选择身份认证信息的制备基之前，执行下述操作：

[0034] 收发双方通过经典信道协商位于控制信息与密钥信息之间的身份认证信息的长度。

[0035] 可选的，所述根据所述测量结果得到的、供发送方验证接收方身份的反向认证信息包括：

[0036] 接收方从所述测量结果中选取接收方认证密钥的位置信息，以及，所述接收方认证密钥或者接收方认证密钥的散列值；

[0037] 相应的，所述发送方根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，包括：

[0038] 所述发送方根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥，并相应地将所述发送方认证密钥或者所述发送方认证密钥的散列值作为所述本地认证信息。

[0039] 可选的，所述由所述测量结果得到的、供发送方验证接收方身份的反向认证信息包括：

[0040] 接收方从所述测量结果中选取接收方认证密钥的位置信息，用所述接收方认证密钥加密的、本地生成的辅助认证信息的密文，以及由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

[0041] 相应的，所述发送方根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，包括：

[0042] 所述发送方根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥；

[0043] 利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息；

[0044] 计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息。

[0045] 可选的，当所述发送方判断出所述本地认证信息与所述反向认证信息相符时，执行下述操作：

[0046] 所述发送方采用所述发送方认证密钥加密所述通过解密操作获取的辅助认证信息的变体；

[0047] 并通过经典信道发送执行上述加密操作后的密文；

[0048] 相应的，所述接收方在接收所述密文后，执行下述操作：

[0049] 采用所述接收方认证密钥解密接收到的密文；

[0050] 判断执行所述解密操作后得到的信息是否与所述本地生成的辅助认证信息的变体一致；

[0051] 若不一致，则结束本次量子密钥分发过程。

[0052] 可选的，在所述发送方根据预置算法库中的算法选择身份认证信息的制备基的步骤之前，执行下述操作：

[0053] 收发双方通过经典信道，利用预置的账户信息与对端设备相互进行身份验证，若其中任一设备未通过所述身份验证，则结束本次量子密钥分发过程。

[0054] 可选的，所述预置算法库中的算法包括：

[0055] 根据身份验证信息中每个比特在数据信息中的位置，选择相应的制备基或者测量基。

[0056] 可选的，所述根据身份验证信息中每个比特在数据信息中的位置，选择相应的制备基或者测量基，具体是指：

[0057] 根据所述每个比特在数据信息中的位置信息与4取模的不同结果，选择相应的水平偏振基、垂直偏振基、左旋偏振基、或者右旋偏振基。

[0058] 此外，本申请还提供另一种用于量子密钥分发过程的身份认证方法，所述方法在参与量子密钥分发过程的发送方量子通信设备上实施，包括：

[0059] 根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长向参与量子密钥分发过程的对端设备发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息；

[0060] 接收所述对端设备返回的反向认证信息；

[0061] 根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息；

[0062] 判断所述本地认证信息是否与接收到的反向认证信息相符；若否，则结束本次量子密钥分发过程。

[0063] 可选的，所述对端设备返回的信息不仅包括：所述反向认证信息，还包括：测量密钥信息量子态所采用的测量基；

[0064] 相应的，当所述判断所述本地认证信息是否与接收到的反向认证信息相符的结果为是时，执行下述操作：

[0065] 确定密钥信息量子态的正确测量基，筛选原始密钥；

[0066] 通过经典信道公布所述密钥信息量子态的正确测量基；

[0067] 通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0068] 可选的，在所述根据预置算法库中的算法选择身份认证信息的制备基的步骤之前，执行下述操作：

[0069] 与所述对端设备通过经典信道协商算法编号；

[0070] 相应的，所述根据预置算法库中的算法选择身份认证信息的制备基包括：

[0071] 根据协商确定的算法编号从所述预置算法库中选择算法；

[0072] 根据所述算法选择所述身份认证信息的制备基。

[0073] 可选的，所述预设信息格式包括：身份认证信息和密钥信息分别有各自的控制信

息作为前缀。

[0074] 可选的，所述预设信息格式包括：身份认证信息和密钥信息采用共同的控制信息作为前缀；

[0075] 相应的，在所述根据预置算法库中的算法选择身份认证信息的制备基的步骤之前，执行下述操作：

[0076] 与所述对端设备通过经典信道协商位于控制信息与密钥信息之间的身份认证信息的长度。

[0077] 可选的，接收到的所述反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、接收方认证密钥或接收方认证密钥的散列值；

[0078] 相应的，所述根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，包括：

[0079] 根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥，并相应地将所述发送方认证密钥或者所述发送方认证密钥的散列值作为所述本地认证信息。

[0080] 可选的，接收到的所述反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、辅助认证信息密文、以及由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

[0081] 相应的，所述根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，包括：

[0082] 根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥；

[0083] 利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息；

[0084] 计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息。

[0085] 可选的，当所述判断所述本地认证信息是否与接收到的反向认证信息相符的结果为是时，执行下述操作：

[0086] 采用所述发送方认证密钥加密所述通过解密操作获取的辅助认证信息的变体；

[0087] 通过经典信道将执行上述加密操作后的密文发送给所述对端设备。

[0088] 相应的，本申请还提供一种用于量子密钥分发过程的身份认证装置，所述装置部署在参与量子密钥分发过程的发送方量子通信设备上，包括：

[0089] 量子态发送单元，用于根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长向参与量子密钥分发过程的对端设备发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息；

[0090] 响应信息接收单元，用于接收所述对端设备返回的反向认证信息；

[0091] 本地认证信息生成单元，用于根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息；

[0092] 发送方认证判断单元，用于判断所述本地认证信息是否与接收到的反向认证信息相符；

[0093] 分发过程结束单元，用于当所述发送方认证判断单元的输出为否时，结束本次量子密钥分发过程。

[0094] 可选的，所述响应信息接收单元接收到的信息不仅包括反向认证信息，还包括：测量密钥信息量子态所采用的测量基；

[0095] 相应的，所述装置还包括：

[0096] 原始密钥筛选单元，用于当所述发送方认证判断单元的输出结果为是时，确定密钥信息量子态的正确测量基，并筛选原始密钥；

[0097] 正确测量基公布单元，用于通过经典信道公布所述密钥信息量子态的正确测量基；

[0098] 发送方量子密钥获取单元，用于通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0099] 可选的，所述装置还包括：

[0100] 算法编号协商单元，用于在触发所述量子态发送单元工作之前，与所述对端设备通过经典信道协商算法编号；

[0101] 相应的，所述量子态发送单元选择身份认证信息的制备基的功能具体通过如下方式实现：

[0102] 根据所述算法编号协商单元确定的算法编号从所述预置算法库中选择算法，并根据所述算法选择所述身份认证信息的制备基。

[0103] 可选的，所述量子态发送单元所采用的预设信息格式包括：身份认证信息和密钥信息分别有各自的控制信息作为前缀。

[0104] 可选的，所述量子态发送单元所采用的预设信息格式包括：身份认证信息和密钥信息采用共同的控制信息作为前缀；

[0105] 相应的，所述装置还包括：

[0106] 认证信息长度协商单元，用于在触发所述量子态发送单元工作之前，与所述对端设备通过经典信道协商位于控制信息与密钥信息之间的身份认证信息的长度。

[0107] 可选的，所述响应信息接收单元接收到的反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、接收方认证密钥或接收方认证密钥的散列值；

[0108] 相应的，所述本地认证信息生成单元具体用于，根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥，并相应地将所述发送方认证密钥或者所述发送方认证密钥的散列值作为所述本地认证信息。

[0109] 可选的，所述响应信息接收单元接收到的反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、辅助认证信息密文、以及由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

[0110] 相应的，所述本地认证信息生成单元包括：

[0111] 发送方认证密钥选取子单元，用于根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥；

[0112] 辅助认证信息解密单元，用于利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息；

[0113] 发送方散列值计算单元，用于计算由所述获取的辅助认证信息与发送方认证密钥

拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息。

[0114] 可选的，所述装置还包括：

[0115] 变体信息加密单元，用于当所述发送方认证判断单元的输出为是时，采用所述发送方认证密钥加密所述通过解密操作获取的辅助认证信息的变体；

[0116] 变体信息密文发送单元，用于通过经典信道将执行上述加密操作后的密文发送给所述对端设备。

[0117] 此外，本申请还提供第三种用于量子密钥分发过程的身份认证方法，所述方法在参与量子密钥分发过程的接收方量子通信设备上实施，包括：

[0118] 接收参与量子密钥分发过程的对端设备发送的量子态，并根据预先约定的不同波长和预设信息格式区分接收到的各种信息量子态；

[0119] 根据从预置算法库中选取的、与所述对端设备相同的算法选择测量基，并用所述测量基对接收到的身份认证信息量子态进行测量；

[0120] 判断测量结果是否与所选算法相符；

[0121] 若是，向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息；

[0122] 若否，则结束本次量子密钥分发过程。

[0123] 可选的，当所述判断测量结果是否与所述算法相符的结果为是时，还执行下述操作：

[0124] 通过经典信道公开用于测量密钥信息量子态的测量基；

[0125] 相应的，所述方法还包括：

[0126] 接收所述对端设备通过经典信道发送的所述密钥信息量子态的正确测量基；

[0127] 筛选原始密钥，并通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0128] 可选的，在所述接收参与量子密钥分发过程的对端设备发送的量子态的步骤之前，执行下述操作：

[0129] 与所述对端设备通过经典信道协商算法编号；

[0130] 相应的，所述根据从预置算法库中选取的、与对端设备相同的算法选择测量基包括：

[0131] 根据协商确定的算法编号从所述预置算法库中选择算法；

[0132] 根据所述算法选择所述测量基。

[0133] 可选的，所述向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息，包括：

[0134] 从所述测量结果中选取接收方认证密钥；

[0135] 将选取所述接收方认证密钥的位置信息、以及所述接收方认证密钥或者接收方认证密钥的散列值发送给所述对端设备。

[0136] 可选的，所述向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息，包括：

[0137] 从所述测量结果中选取接收方认证密钥；

[0138] 用所述接收方认证密钥对本地生成的辅助认证信息加密；

[0139] 计算由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

[0140] 将选取所述接收方认证密钥的位置信息、所述辅助认证信息密文、以及所述散列值发送给所述对端设备。

[0141] 可选的，在所述向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息的步骤之后，执行下述操作：

[0142] 接收所述对端设备发送的辅助认证信息变体的密文；

[0143] 采用所述接收方认证密钥解密接收到的所述密文；

[0144] 判断执行所述解密操作后得到的信息是否与所述本地生成的辅助认证信息的变体一致；

[0145] 若不一致，则结束本次量子密钥分发过程。

[0146] 相应的，本申请还提供一种用于量子密钥分发过程的身份认证装置，所述装置部署在参与量子密钥分发过程的接收方量子通信设备上，包括：

[0147] 量子态接收单元，用于接收参与量子密钥分发过程的对端设备发送的量子态，并根据预先约定的不同波长和预设信息格式区分接收到的各种信息量子态；

[0148] 量子态测量单元，用于根据从预置算法库中选取的、与对端设备相同的算法选择测量基，并用所述测量基对接收到的身份认证信息量子态进行测量；

[0149] 接收方认证判断单元，用于判断测量结果是否与所选算法相符；

[0150] 反向认证信息发送单元，用于当所述接收方认证判断单元的输出为是时，向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息；

[0151] 分发过程结束单元，用于当所述接收方认证判断单元的输出为否时，结束本次量子密钥分发过程。

[0152] 可选的，所述装置还包括：

[0153] 测量基公布单元，用于当所述接收方认证判断单元的输出为是时，通过经典信道公开用于测量密钥信息量子态的测量基；

[0154] 相应的，所述装置还包括：

[0155] 正确测量基接收单元，用于接收所述对端设备通过经典信道发送的所述密钥信息量子态的正确测量基；

[0156] 接收方量子密钥获取单元，用于筛选原始密钥，并通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0157] 可选的，所述装置还包括：

[0158] 算法编号协商单元，用于在触发所述量子态接收单元工作之前，与所述对端设备通过经典信道协商算法编号；

[0159] 相应的，所述量子态测量单元选择身份认证信息的测量基的功能具体通过如下方式实现：

[0160] 根据协商确定的算法编号从所述预置算法库中选择算法，并根据所述算法选择所述测量基。

[0161] 可选的，所述反向认证信息发送单元包括：

[0162] 接收方认证密钥选取子单元，用于从所述测量结果中选取接收方认证密钥；

[0163] 第一信息发送执行子单元，用于将选取所述接收方认证密钥的位置信息、以及所述接收方认证密钥或者接收方认证密钥的散列值发送给所述对端设备。

[0164] 可选的，所述反向认证信息发送单元包括：

[0165] 接收方认证密钥选取子单元，用于从所述测量结果中选取接收方认证密钥；

[0166] 辅助认证信息加密子单元，用于用所述接收方认证密钥对本地生成的辅助认证信息加密；

[0167] 接收方散列值计算子单元，计算由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

[0168] 第二信息发送执行子单元，用于将选取所述接收方认证密钥的位置信息、所述辅助认证信息密文、以及所述散列值发送给所述对端设备。

[0169] 可选的，所述装置还包括：

[0170] 变体信息密文接收单元，用于在所述反向认证信息发送单元完成发送操作后，接收所述对端设备发送的辅助认证信息变体的密文；

[0171] 变体信息密文解密单元，用于采用所述接收方认证密钥解密接收到的所述密文；

[0172] 变体信息判断单元，用于判断执行所述解密操作后得到的信息是否与所述本地生成的辅助认证信息的变体一致，若不一致，则触发所述分发过程结束单元工作。

[0173] 此外，本申请还提供一种用于量子密钥分发过程的身份认证系统，包括：根据上述任意一项所述的部署于发送方量子通信设备的身份认证装置，以及根据上述任意一项所述的部署于接收方量子通信设备的身份认证装置。

[0174] 与现有技术相比，本申请具有以下优点：

[0175] 本申请提供的一种用于量子密钥分发过程的身份认证方法，发送方根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长发送控制信息以及包含身份认证信息和密钥信息的数据信息的量子态；接收方根据所述不同波长和所述预设信息格式区分接收到的各种信息量子态，并采用相应的测量基对其中的身份认证信息量子态进行测量，当测量结果与所述算法相符时，发送反向认证信息，否则结束本次量子密钥分发过程；发送方判断出本地认证信息与接收到的反向认证信息不相符时，结束本次量子密钥分发过程。上述技术方案，收发双方通过控制信息以及不同波长在密钥信息量子态中穿插或者区分身份认证信息量子态，并且依据预置算法库中的算法选择身份认证信息量子态的制备基以及测量基、根据测量得到的身份认证信息是否与算法相符进行身份验证，从而在量子密钥分发过程中实现了量子态零知识证明的动态身份认证机制，可以实时确认通信方身份的合法性，有效防御中间人攻击和DDoS攻击，保障了量子密钥分发过程的安全性，而且采用基于算法的方式动态生成身份认证信息，避免对量子密钥资源的浪费。

附图说明

[0176] 图1是本申请提供的一种用于量子密钥分发过程的身份认证方法的实施例的流程图；

[0177] 图2是本申请实施例提供的第一种信息格式的示意图；

[0178] 图3是本申请实施例提供的第二种信息格式的示意图；

[0179] 图4是本申请实施例提供的第三种信息格式的示意图；

[0180] 图5是本申请实施例提供的接收方执行身份认证操作的处理流程图；

[0181] 图6是本申请实施例提供的接收方发送反向认证信息的处理流程图；

[0182] 图7是本申请实施例提供的发送方执行身份认证操作的处理流程图；

[0183] 图8是本申请提供的另一种用于量子密钥分发过程的身份认证方法的实施例的流程图；

[0184] 图9是本申请提供的一种用于量子密钥分发过程的身份认证装置的实施例的示意图；

[0185] 图10是本申请提供的第三种用于量子密钥分发过程的身份认证方法的实施例的流程图；

[0186] 图11是本申请提供的一种用于量子密钥分发过程的身份认证装置的实施例的示意图；

[0187] 图12是本申请提供的一种用于量子密钥分发过程的身份认证系统的实施例示意图；

[0188] 图13是本申请实施例提供的身份认证系统的交互处理流程示意图。

具体实施方式

[0189] 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。

[0190] 在本申请中，分别提供了一种用于量子密钥分发过程的身份认证方法、另外两种用于量子密钥分发过程的身份认证方法以及相应的装置、以及一种用于量子密钥分发过程的身份认证系统，在下面的实施例中逐一进行详细说明。

[0191] 请参考图1，其为本申请的一种用于量子密钥分发过程的身份认证方法的实施例的流程图，所述方法在参与量子密钥分发过程的收发双方量子通信设备中实施。在详细描述本实施例的具体步骤之前，先对本技术方案涉及的收发双方量子通信设备以及本实施例作简要说明。

[0192] 本技术方案在量子密钥分发过程中动态地对参与分发过程的双方量子通信设备的身份进行验证。其中，选取制备基向对端设备发送量子态的设备，即通常所述的Alice一方，在本技术方案中称为发送方量子通信设备，简称发送方；选取测量基对接收到的量子态进行测量的设备，即通常所述的Bob一方，在本技术方案中称为接收方量子通信设备，简称接收方。

[0193] 量子密钥分发过程包括：发送方发送量子态、接收方测量量子态、收发双方比对测量基并筛选原始密钥、估算误码率、纠错、隐私放大这样几个阶段，本技术方案在上述过程中实现动态身份认证。在具体实施时，发送方在发送的量子态中穿插身份认证信息后，接收方可以通过测量量子态与发送方相互验证身份，并在完成身份认证后再继续后续比对测量基等各阶段的处理流程；也可以将相互验证身份的处理过程穿插在各阶段中完成。在具体实施时，上述两种方式都是可行的，其中第二种方式可以简化交互过程，提高执行效率，是优选实施方式，因此下面的实施例中描述基于上述第二种方式的实施方式。下面对本实施例作详细说明。

[0194] 所述用于量子密钥分发过程的身份认证方法包括如下步骤：

[0195] 步骤101、发送方根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息。

[0196] 在发送方通过量子信道向接收方发送量子态之前，可以先通过经典信道与接收方相互进行身份认证，并且协商与双方选择基矢相关的算法编号，并在完成上述两个处理后，启动量子密钥分发过程(也称为量子密钥协商过程)，下面先对上述两个处理过程进行说明。

[0197] 1)收发双方通过经典信道进行身份认证。

[0198] 本实施例提供的技术方案，可以在量子密钥分发过程中动态地进行身份认证。同时为了避免在不合法的量子通信设备之间启动量子密钥分发过程，本实施例提供了一种优选实施方式：在发送方启动量子密钥分发过程之前，收发双发的量子通信设备先通过经典信道对对端设备的身份进行验证，只有双方设备都通过验证，才能够继续后续的量子密钥分发过程。

[0199] 具体说，量子密钥协商过程的发起方，即本申请所述的发送方，可以首先发送量子密钥协商请求，所述请求中包含所述发送方的账户信息，所述账户信息可以包含发送方的身份信息和签名证书。参与量子密钥协商过程的对端设备，即本申请所述的接收方收到上述账户信息后，用其中的身份信息对所述证书进行验证，若通过验证，则向发送方返回响应信息，其中包含接收方的账户信息，若未通过验证，则结束本次量子密钥分发过程。

[0200] 同样的道理，所述发送方接收来自所述接收方的账户信息后，可以采用上述同样的方式对接收方身份进行验证，若通过验证，则可以执行后续的量子密钥分发过程，否则，结束本次量子密钥分发过程。

[0201] 2)收发双方通过经典信道协商算法编号。

[0202] 若发送方和接收方都通过了上述身份验证过程，则可以协商双方采用的算法编号。在本申请的技术方案中，为了有效抵御中间人攻击和DDoS攻击，收发双方都预置相同的算法库，在每次的量子密钥分发过程中，发送方根据算法库中的算法动态确定身份认证信息量子态的制备基，接收方则根据算法库中的算法动态确定身份认证信息量子态的测量基。为了正确实现身份认证，收发双方需要采用相同的算法，在具体实施时，收发双方可以在每次的量子密钥分发过程中采用相同的预设规则选择预置算法库中的算法，例如，可以按照预设的顺序表依次选取，只要能够保证收发双方采用相同的算法即可。

[0203] 为了保证收发双方采用算法的一致性，也可以在启动量子密钥分发过程之前，收发双方通过协商过程确定共同采用的算法的编号。由于该协商过程是通过经典信道完成的，为了避免攻击者获取算法编号、并根据算法编号推测出具体算法，可以采用如下两种方式：

[0204] a)收发双方按照预设策略对各自算法库中的算法编号进行同步变换，在协商算法编号的过程中可以采用明文方式。具体实施时，收发双方可以按照预设周期定期对算法库中的算法编号进行同步变换，也可以在每次启动量子密钥分发过程之前触发一次同步变换，具体的编号变换方式则可以采用多种算法，只要保证变换后收发双方算法库中的相同算法具有相同编号即可。例如：算法库中有5个算法，原编号分别为1、2、3、4、5，进行变换后，

收发双方算法库中上述5个算法的编号都同步调整为2、3、4、5、1。

[0205] b)如果收发双方不具备a)中描述的同步变换机制，那么在协商算法编号的过程中可以采用加密传输的方式。例如，发送方将拟采用的算法编号采用双方预置共享密钥加密后发送给接收方，接收方采用同样的预置共享密钥解密，从而获知采用的算法编号，并给发送方返回确认应答。在具体实施时，也可以用上一次量子密钥协商过程获取的量子密钥对算法编号加密。

[0206] 通过上面的描述可以看出，由于采用了协商算法编号的匿名方式进行算法协商，而且算法编号是同步变换的、或者是采用密钥加密传输的，从而攻击者即使通过对经典信道的监控获取了上述协商信息，也无法获知收发双方采用的具体算法内容，在确保收发双方采用相同算法的同时，也能够避免受到中间人攻击或者DDoS攻击。

[0207] 完成上述交互处理流程后，可以启动后续的量子密钥分发过程。本步骤中，发送方根据预置算法库中的算法(例如，由协商确定的算法编号确定的算法)选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息，该发送过程是通过量子信道完成的。

[0208] 在具体实施中，所述预置算法库中可以包含各种不同的算法，例如，可以根据身份验证信息中每个比特在数据信息中的位置，选择相应的制备基(对于发送方)或者测量基(对于接收方)，在本实施例的一个具体例子中，所述预置算法库中包含如下算法：根据所述每个比特在数据信息中的位置信息与4取模的不同结果，选择相应的水平偏振基、垂直偏振基、左旋偏振基、或者右旋偏振基。具体说，如果身份验证信息中某个比特处于数据信息中的第l个比特，那么该比特量子态所对应的制备基和测量基满足如下条件：

[0209] $$f(l)=\begin{cases}\text{水平偏振态H}, & l \bmod 4=0\\ \text{垂直偏振态V}, & l \bmod 4=1\\ +45°\text{偏振态}+, & l \bmod 4=2\\ -45°\text{偏振态}-, & l \bmod 4=3\end{cases}$$

[0210] 上面给出了所述预置算法库中算法的一个具体例子，在具体实施本技术方案时，可以在预置算法库中包含上述算法，也可以包含不同于上述算法的其它算法，只要收发双方从预置算法库中选用相同算法选择身份认证信息量子态的制备基和测量基，就都可以实现本申请的技术方案，都在本申请的保护范围之内。

[0211] 发送方采用上述方式选择身份认证信息的制备基，并向接收方发送控制信息和数据信息(包括身份认证信息和密钥信息)的量子态。为了避免攻击者进行有针对性的监测，所有数据信息的量子态都采用相同波长发送，即：身份认证信息量子态和密钥信息量子态采用相同的波长；为了便于接收方从接收到的量子态中区分身份认证信息量子态和密钥信息量子态、从而选择正确的测量基进行探测，承载控制信息量子态的波长与承载数据信息量子态的波长是不同的。所述不同的波长可以是收发双方预先设定的，也可以是在启动量子密钥分发过程之前通过经典信道协商确定的。

[0212] 在约定上述波长特征的基础上，收发双方可以预设相同的信息格式，发送方按照该格式发送控制信息、密钥信息和身份认证信息的量子态，而接收方则按照约定波长、以及

所述信息格式，区分接收到的各种信息量子态。所述信息格式可以采用多种定义方式，只要接收方能够正确区分就都是可以的。下面给出几种具体的例子。

[0213] 例1：身份认证信息和密钥信息分别有各自的控制信息作为前缀(以下分别简称为：身份认证控制信息和密钥控制信息)，且承载两种控制信息量子态的波长不同，请参见图2给出的信息格式示意图。承载数据信息(包括身份认证信息和密钥信息)量子态的波长为λ_1，承载身份认证控制信息量子态的波长为λ_2，承载密钥控制信息量子态的波长为λ_3，λ_1、λ_2及λ_3都互不相同。其中，λ_2和λ_3可以是收发双方预先设定的、也可以是在启动量子密钥协商过程之前协商确定的。采用这种方式，发送方可以随机选择两类控制信息的量子态，而接收方则可以直接根据波长区分身份认证控制信息和密钥控制信息。

[0214] 例2：身份认证信息和密钥信息分别有各自的控制信息作为前缀，且两种控制信息编码不同，请参见图3给出的信息格式示意图。承载数据信息(包括身份认证信息和密钥信息)量子态的波长为λ_1，承载身份认证控制信息量子态的波长、与承载密钥控制信息量子态的波长都为λ_2(不同于λ_1)，但是两类控制信息的编码不同，例如，00000为身份认证控制信息的编码，11111为密钥控制信息的编码。其中，所述不同编码是收发双方预先设定的、或者在启动量子密钥分发过程之前通过经典信道协商确定的；收发双方用于制备或者测量上述两种控制信息量子态的基矢也可以是收发双方预先设定的、或者是在启动量子密钥分发过程之前通过经典信道协商确定的。

[0215] 例3：身份认证信息和密钥信息采用共同的控制信息作为前缀，请参见图4给出的信息格式示意图。承载数据信息(包括身份认证信息和密钥信息)量子态的波长为λ_1，身份认证信息和密钥信息共用同一个控制信息前缀，承载控制信息量子态的波长为λ_2，λ_2不同于λ_1。采用这种方式，由于接收方可以根据波长区分控制信息和数据信息，发送方可以随机选择控制信息量子态，然而位于控制信息和密钥信息之间的身份认证信息的长度应该是收发双方约定好的，这样接收方才能够正确区分数据信息中的身份认证信息和密钥信息，在具体实施时，所述身份认证信息的长度可以是收发双方预先设定的，也可以是在启动量子密钥分发过程之前通过经典信道协商确定的。

[0216] 需要说明的是，上面给出的例子以及相关图示中，给出的都只是信息格式的一部分，在具体实施时，每种信息格式可以多次重复并串接在一起。例如，对于例3中给出的信息格式，可以扩展为：控制信息|身份认证信息|密钥信息|.....|控制信息|身份认证信息|密钥信息；当然也可以采用不同于上述三个例子的其他信息格式，只要控制信息和数据信息采用不同的波长、并且接收方能够按照约定好的波长特征和信息格式区分接收到的量子态中的各种信息，就都是可以的，也都在本申请的保护范围之内。

[0217] 在本步骤中，发送方按照与接收方约定好的波长特征和信息格式，发送控制信息、身份认证信息以及密钥信息的量子态。为了便于理解，下面采用上述例子3中的信息格式举例说明。

[0218] 例如，发送方在时间点t_1、t_2...t_n发送长度为n的二进制比特串的量子态，所述二进制比特串如下所示：

[0219] $x_1, x_2 \cdots x_i, x_{i+1} \cdots x_{i+m}, x_{i+m+1} \cdots x_n$

[0220] 该二进制比特串包含三部分，第一部分是控制信息，第二部分是身份认证信息，第三部分是密钥信息。其中，控制信息为随机选择的二进制比特串，长度为i；身份认证信息则

是根据预置算法库中所选算法对应的制备基确定的身份认证比特串，其长度m可以由发送方和接收方预先通过经典信道协商确定；密钥信息是随机生成的二进制比特串，其长度为n-m-i。

[0221] 发送方在时间点t_1、t_2、.....t_n发送上述二进制比特串的编码量子态（$|\varphi_{j_1}^{x_1}, |\varphi_{j_2}^{x_2} \ldots |\varphi_{j_i}^{x_i}, |\varphi_{j_i+1}^{x_{i+1}} \ldots |\varphi_{j_i+m}^{x_{i+m}}, |\varphi_{j_i+m+1}^{x_{i+m+1}} \ldots |\varphi_{j_n}^{x_n}$）给接收方，$j_1, j_2, \cdots j_i$，$j_{i+1} \cdots j_{i+m}, j_{i+m+1}, \cdots j_n$是发送方采用的制备基序列，其中，$j_1, j_2, \cdots j_i$是控制信息比特串对应的随机量子态制备基，波长为$\lambda_2$，$j_{i+1} \cdots j_{i+m}$是按照所述算法选取的身份认证信息比特串的量子态制备基，$j_{i+m+1}, \cdots j_n$是密钥信息比特串对应的随机量子态制备基，身份认证信息比特串和密钥信息比特串的制备基的波长都为λ_1，λ_1与λ_2不同。

[0222] 相应的，在本例的后续步骤102中，接收方可以根据波长区分控制信息和数据信息，根据长度m区分数据信息中的身份认证信息和密钥信息，并采用测量基序列$k_{i+1} \cdots k_{i+m}$，$k_{i+m+1} \cdots k_n$对接收的数据信息量子态进行测量，其中，$k_{i+1} \cdots k_{i+m}$为身份认证信息量子态对应的测量基，该测量基是遵循与发送方相同的算法选取的，$k_{i+m+1}, \cdots k_n$为密钥信息量子态对应的随机量子态测量基。

[0223] 在本步骤中，发送方由于采用根据算法库中的算法选择身份认证比特串制备基的方式，并且采用不同波长发送控制信息以及数据信息(包括身份认证信息和密钥信息)的量子态，一方面便于接收方进行区分，另一方面可以有效抵御量子密钥分发过程中的中间人攻击和DDoS攻击，而且采用基于算法的方式生成身份认证信息，可以避免对量子密钥资源的浪费。

[0224] 步骤102、接收方根据所述不同波长和所述预设信息格式区分接收到的各种信息量子态，并采用对应于预置算法库中相同算法的测量基对其中的身份认证信息量子态进行测量，当测量结果与所述算法相符时，发送根据所述测量结果得到的、供发送方验证接收方身份的反向认证信息，否则结束本次量子密钥分发过程。

[0225] 在本步骤中，接收方不仅按照量子密钥分配协议(例如BB84协议)完成常规的密钥量子态的测量，并且根据身份认证量子态信息的测量结果完成对发送方身份的验证。该处理过程包括子步骤102-1至102-4，下面结合图5作进一步说明。

[0226] 步骤102-1：根据所述不同波长和所述预设信息格式区分接收到的各种信息量子态。

[0227] 在本步骤中，接收方针对从量子信道接收到的各种信息量子态，可以采用与发送方预先约定好的波长特征和信息格式区分其中的控制信息、身份认证信息以及密钥信息的量子态。在具体实施时，可以根据不同的波长区分控制信息和数据信息的量子态，并进一步结合预设信息格式区分身份认证信息和密钥信息的量子态。

[0228] 例如，发送方和接收方预先约定了如步骤101中例1所述的波长特征和信息格式，那么在本步骤中，接收方如果接收到波长为λ_2的量子态，则可获知为身份认证控制信息量子态，随后接收到的波长为λ_1的量子态为身份认证信息量子态，应该采用与发送方相同算法对应的测量基进行测量；如果接收到波长为λ_3的量子态，则可获知随后接收到的波长为λ_1的量子态为密钥信息量子态，可以采用随机选取的测量基进行测量。

[0229] 再例如，发送方和接收方预先约定了如步骤101中例2所述的波长特征和信息格

式，那么在本步骤中，接收方如果接收到波长为λ_2的量子态，则可获知为控制信息量子态，采用与发送方预先约定的(预先设定或者协商确定的)测量基进行测量，通过将测量结果与预先约定的编码值进行比对，从而获知接收到的控制信息类型：身份认证控制信息、或者密钥控制信息，后续接收到波长为λ_1的量子态时，则可以采用与所述类型对应的测量基进行测量。

[0230] 对于步骤101中例3所述的波长特征和信息格式，以及其他发送方可能采用的波长特征和信息格式，接收方也可以采用类似方式区分各种信息量子态，此处不再赘述。

[0231] 步骤102-2：采用随机选择的测量基测量密钥信息量子态，采用与发送方相同算法对应的测量基测量身份认证信息量子态，获取身份认证信息。

[0232] 对于密钥信息量子态部分，可以依然按照量子密钥分配协议(例如BB84协议)随机选择测量基进行测量，获取量子密钥信息的原始测量结果。

[0233] 对于身份认证信息量子态部分，则可以采用与发送方相同算法对应的测量基进行测量。发送方与接收方通常预置相同的算法库，接收方可以在每次的量子密钥分发过程中采用与发送方相同的预设规则选择预置算法库中的算法、或者在启动量子密钥分发过程之前与发送方协商所采用的算法编号，从而保证选用与发送方相同的算法，并采用根据所述算法所选的测量基对接收到的身份认证信息量子态进行测量，获取测量结果，即测量得到的身份认证信息。

[0234] 考虑到量子信道可能存在衰减，因此可以将在测量过程中未探测到光子的部分剔除，仅保留测量得到的信息，作为身份认证信息量子态的测量结果。

[0235] 步骤102-3：判断测量得到的身份认证信息与所采用的算法是否相符，若相符执行步骤102-4，否则结束本次量子密钥分发过程。

[0236] 由于收发双方预置了相同的算法库，并遵循该算法库中的相同算法选择身份认证信息量子态的制备基以及测量基，因此，接收方测量得到的身份认证信息应该与所选算法对应的预期信息是一致的。

[0237] 对于接收方来说，如果测量得到的身份认证信息与对应的预期信息一致，可以认为发送方选择身份认证信息量子态制备基所遵循的算法与自己是相同的，而只有身份合法的发送方才可能获知该算法，因此可以判定发送方通过身份认证。

[0238] 考虑到在量子信道传输过程中，可能因为噪声干扰等因素，导致个别量子态的测量结果与预期不符，如果在这种情况下，认为发送方未通过身份认证，并结束本次量子密钥分发过程，那么会造成量子密钥分发量的无谓减少。考虑上述情况，同时也兼顾防御中间人攻击和DDoS攻击的需求，可以采取设定阈值的方式，即：如果接收方测量得到的身份认证信息与所选算法对应的预期信息的差异小于预先设定的阈值，例如，测量得到的身份认证信息与所述预期信息不相符的比特位的个数小于预先设定的上限值，则接收方可以认为发送方通过身份认证。

[0239] 步骤102-4：发送根据所述身份认证信息得到的、供发送方验证接收方身份的反向认证信息。

[0240] 在上面的步骤102-3中，接收方已经验证了发送方的身份，接下来接收方需要向发送方证明自己身份的合法性，本技术方案采用了由接收方提供反向认证信息、发送方根据该信息验证接收方身份的方式实现上述验证功能。

[0241] 所述反向认证信息，是接收方从测量得到的身份认证信息中获取的、用于供发送方验证接收方身份的信息。例如，接收方可以从测量得到的身份认证信息中选取部分信息作为接收方认证密钥IDkey，并将选取所述密钥的位置信息、以及所述接收方认证密钥作为反向认证信息发送给发送方，发送方根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥，若所述发送方认证密钥与接收到的接收方认证密钥一致，则认为接收方通过身份认证。

[0242] 在具体实施中，可以对上述实施方式进行变更，例如：接收方发送的反向认证信息中可以包含所述位置信息以及接收方认证密钥的散列值，相应的发送方用发送方认证密钥的散列值进行比对验证，也同样可以实现对接收方身份的验证。下面给出本实施例提供的一种优选实施方式，包括步骤102-4-1至步骤102-4-4，下面结合图6进行说明。

[0243] 步骤102-4-1：从测量得到的身份认证信息中选取接收方认证密钥。

[0244] 在具体实施时，可以直接将所述测量得到的身份认证信息作为接收方认证密钥IDkey。为了进一步提高安全性，也可以不直接使用所述测量得到的身份认证信息作为IDkey，而是从所述身份认证信息中随机选择处于不同位置的比特，并将所选比特组成的比特串作为所述接收方认证密钥IDkey。

[0245] 步骤102-4-2：用所述接收方认证密钥对本地生成的辅助认证信息加密。

[0246] 所述辅助认证信息m，可以是接收方任意选取的一个自然数，也可以是采用随机数生成算法或者工具生成的随机数。本步骤采用之前选取的接收方IDkey对所述辅助认证信息m加密。

[0247] 步骤102-4-3：计算由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值。

[0248] 采用预设散列算法，例如：SHA-1、SHA-2、或者SHA-3，计算由所述辅助认证信息m和接收方IDkey拼接而成的字符串的散列值。在具体实施时，也可以采用此处未列出的其他散列算法，只要发送方也采用相同的算法验证接收方身份，就都是可以的。

[0249] 步骤102-4-4：通过经典信道发送选取所述接收方认证密钥的位置信息、所述辅助认证信息密文、以及所述散列值，并公开密钥信息量子态的测量基。

[0250] 执行完上述步骤102-4-1至步骤102-4-3后，可以将选取接收方认证密钥的位置信息、所述加密后的辅助认证信息、以及计算得到的散列值作为所述反向认证信息，一并通过经典信道发送给所述发送方，供所述发送方参照这些信息验证自己的身份。

[0251] 此外，还可以按照量子密钥分配协议，通过经典信道公开接收方测量密钥信息量子态所采用的测量基。

[0252] 步骤103、发送方根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息，若所述本地认证信息与所述反向认证信息不相符，则结束本次量子密钥分发过程。

[0253] 由于接收方是从测量得到的身份认证信息中、获取所述反向认证信息的，而收发双方采用相同的算法选择身份认证信息的制备基和测量基，因此双方所享有的身份认证信息通常是一致的，在此基础上，发送方通过将本地认证信息与接收到的反向认证信息进行比对，就可以识别发送所述反向认证信息的接收方的身份是否合法。

[0254] 具体实施时，发送方可以根据接收到的反向认证信息的内容执行相应的比对操

作,对于在步骤102-4给出的接收方发送反向认证信息的优选实施方式,发送方可以通过以下步骤103-1至步骤103-5完成对接收方的身份认证,下面结合图7作进一步说明。

[0255] 步骤103-1、发送方根据接收的位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥。

[0256] 发送方通过经典信道接收到了接收方公开的测量基、以及反向认证信息,所述反向认证信息包括:位置信息、辅助认证信息密文、以及由辅助认证信息和接收方认证密钥计算得到的散列值。

[0257] 发送方根据所述位置信息、从步骤101中发送的身份认证信息中选取与所述位置信息对应的比特位,从而得到发送方认证密钥,即,发送方IDkey。

[0258] 步骤103-2、利用所述发送方认证密钥对接收到的辅助认证信息密文解密,获取辅助认证信息。

[0259] 利用步骤103-1选取的发送方IDkey,对接收到的辅助认证信息密文解密,获取辅助认证信息m。

[0260] 步骤103-3、计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值,并将所述计算得到的散列值作为所述本地认证信息。

[0261] 将步骤103-2获取的辅助认证信息m、以及步骤103-1获取的发送方IDkey以字符串的形式拼接在一起,并采用与接收方相同的散列算法计算拼接得到的字符串的散列值,并将该散列值作为用于验证接收方身份的本地认证信息。

[0262] 步骤103-4、判断所述本地认证信息与所述反向认证信息是否相符,若是,执行步骤103-5,若否,则结束本次量子密钥分发过程。

[0263] 判断步骤103-3计算得到的散列值与接收到的反向认证信息中的散列值是否一致,若一致,即本地认证信息与反向认证信息相符,说明接收方在生成所述反向认证信息时采用的是正确的IDkey(与发送方IDkey相同),从而发送方才能够解密出与接收方相同的辅助认证信息m、并进一步计算得到相同的散列值,而只有身份合法的接收方才可能采用与发送方相同算法对应的测量基测量身份认证信息量子态并获取正确的接收方IDkey,因此可以判定接收方通过身份认证,继续执行步骤103-5。反之,如果两者不一致,则可以认为接收方可能是中间人或者攻击者,因此结束本次量子密钥分发过程。

[0264] 步骤103-5、筛选原始密钥,并通过经典信道公布密钥信息量子态的正确测量基。

[0265] 如果发送方判定接收方身份合法,则可以按照量子密钥分配协议的流程,将接收方公开的测量基与自己使用的制备基进行比较,从中选出正确的测量基,根据正确的测量基筛选出原始密钥,并通过经典信道向接收方公开正确的测量基。

[0266] 至此,通过上述步骤101-步骤103,接收方通过判断测量得到的身份认证信息与从预置算法库中所选算法相符,验证了发送方的身份;发送方则通过将接收方提供的反向认证信息与本地认证信息的比对,验证了接收方的身份。在收发双方都通过上述验证的条件下,就可以按照量子密钥分配协议的流程继续执行后续的密钥分发过程。

[0267] 为了进一步保证密钥分发过程的安全性,本实施例在后续分发过程中也穿插了身份认证以及数据加密处理流程,下面对这种优选实施方式作进一步说明。

[0268] 1)发送方采用发送方IDkey加密所述通过解密操作获取的辅助认证信息m的变体,并通过经典信道发送执行上述加密操作后的密文。

[0269] 在上述步骤103中发送方获取了解密后的辅助认证信息m，当发送方验证接收方的身份合法后，可以采用发送方IDkey加密所述解密后的信息m的变体，然后在通过经典信道公布密钥信息量子态的正确测量基时，一并发送执行上述加密操作后的密文信息。其中，发送方公布的密钥信息量子态的正确测量基信息可以采用发送方IDkey加密。

[0270] 所述辅助认证信息的变体，是指基于所述辅助认证信息生成的信息，例如，可以是所述辅助认证信息本身；或者，是采用预设的数学变换方法处理所述辅助认证信息得到的结果，例如：m+1。收发双发可以预置相同的变体生成算法或者函数，从而保证针对相同的辅助认证信息m，双方生成的变体信息是一致的。

[0271] 2)接收方接收所述正确测量基和所述密文后，通过解密密文再次验证发送方身份。

[0272] 首先，接收方采用发送方IDkey对接收到的密文执行解密操作，获得辅助认证信息m的变体信息。

[0273] 然后，判断执行所述解密操作后得到的m的变体信息是否与本地生成的辅助认证信息m的变体一致。所述辅助认证信息m最初是接收方本地生成的(参见步骤102-4-2)，通过经典信道以加密形式发送给发送方，发送方解密还原后，又采用发送方IDkey加密该信息的变体，并发送给接收方，那么如果接收方解密后的结果与其本地原始生成的辅助认证信息的变体一致，说明发送方不仅能够成功地解密还原m，而且其采用的发送方IDkey以及变体生成算法或者函数与接收方是相符的，从而接收方再次验证了发送方的身份，同时也说明发送方通过经典信道公布的密钥信息量子态的正确测量基是可信的。

[0274] 因此，如果上述判断结果为“是”，接收方可以根据经典信道公开的正确测量基，筛选原始密钥，并可以通过经典信道公布部分密钥量子态的测量结果，以便进行后续的误码率估算；如果上述判断结果为“否”，则说明发送方身份不可信，因此可以结束本次的量子密钥分发过程。

[0275] 3)收发双方通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0276] 如果在上述2)中接收方再次成功地验证了发送方的身份，并且完成了筛选原始密钥的操作，那么之后收发双方就可以按照量子密钥分配协议的规定继续执行后续的处理，包括误码率估算、纠错和隐私放大等处理，上述处理过程是收发双方通过经典信道共同协商完成的，协商过程中所涉及的信息都可以采用收发双方相应的IDkey进行加解密。

[0277] 综上所述，本实施例提供的身份认证方法，收发双方通过控制信息以及不同波长在密钥信息量子态中穿插或者区分身份认证信息量子态，并且依据预置算法库中的算法选择身份认证信息量子态的制备基以及测量基、根据测量得到的身份认证信息是否与算法相符进行身份验证，从而在量子密钥分发过程中实现了量子态零知识证明的动态身份认证机制，可以实时确认通信方身份的合法性，有效防御中间人攻击和DDoS攻击，保障了量子密钥分发过程的安全性，而且采用基于算法的方式动态生成身份认证信息，避免对量子密钥资源的浪费。

[0278] 此外，本申请还提供了另一种用于量子密钥分发过程的身份认证方法，所述方法在参与量子密钥分发过程的发送方量子通信设备上实施。请参考图8，其为本申请的另一种用于量子密钥分发过程的身份认证方法的实施例的流程图，本实施例与上述实施例步骤相同的部分不再赘述，下面重点描述不同之处。所述方法包括如下步骤：

[0279] 步骤801、根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长向参与量子密钥分发过程的对端设备发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息。

[0280] 在执行本步骤之前，可以与所述对端设备通过经典信道协商算法编号。相应的，所述根据预置算法库中的算法选择身份认证信息的制备基包括：根据协商确定的算法编号从所述预置算法库中选择算法；根据所述算法选择所述身份认证信息的制备基。

[0281] 所述预设信息格式可以包括：身份认证信息和密钥信息分别有各自的控制信息作为前缀；所述预设信息格式也可以包括：身份认证信息和密钥信息采用共同的控制信息作为前缀，若采用这种信息格式，那么执行本步骤之前，可以与所述对端设备通过经典信道协商位于控制信息与密钥信息之间的身份认证信息的长度。

[0282] 步骤802、接收所述对端设备返回的反向认证信息。

[0283] 此处列举接收到的所述反向认证信息的两种例子：

[0284] 第一种，所述反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、接收方认证密钥或接收方认证密钥的散列值。

[0285] 第二种，所述反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、辅助认证信息密文、以及由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值。

[0286] 所述对端设备返回的信息可以不仅包括所述反向认证信息，还包括：测量密钥信息量子态所采用的测量基。

[0287] 步骤803、根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息。

[0288] 如果步骤802接收到第一种反向认证信息，则本步骤可以根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥，并相应地将所述发送方认证密钥或者所述发送方认证密钥的散列值作为所述本地认证信息。

[0289] 如果步骤802接收到第二种反向认证信息，则本步骤可以执行如下操作：根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥；利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息；计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息。

[0290] 步骤804、判断所述本地认证信息是否与接收到的反向认证信息相符；若否，执行步骤805。

[0291] 如果本步骤的判断结果为是，则可以采用所述发送方认证密钥加密所述通过解密操作获取的辅助认证信息的变体；通过经典信道将执行上述加密操作后的密文发送给所述对端设备。还可以按照量子密钥分配协议继续执行后续的操作：

[0292] 确定密钥信息量子态的正确测量基，筛选原始密钥；

[0293] 通过经典信道公布所述密钥信息量子态的正确测量基；

[0294] 通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0295] 步骤805、结束本次量子密钥分发过程。

[0296] 在上述的实施例中，提供了另一种用于量子密钥分发过程的身份认证方法，与之

相对应的，本申请还提供一种用于量子密钥分发过程的身份认证装置，所述装置部署在参与量子密钥分发过程的发送方量子通信设备上。请参看图9，其为本申请的一种用于量子密钥分发过程的身份认证装置的实施例示意图。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。

[0297] 本实施例的一种用于量子密钥分发过程的身份认证装置，包括：量子态发送单元901，用于根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长向参与量子密钥分发过程的对端设备发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息；响应信息接收单元902，用于接收所述对端设备返回的反向认证信息；本地认证信息生成单元903，用于根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息；发送方认证判断单元904，用于判断所述本地认证信息是否与接收到的反向认证信息相符；分发过程结束单元905，用于当所述发送方认证判断单元的输出为否时，结束本次量子密钥分发过程。

[0298] 可选的，所述响应信息接收单元接收到的信息不仅包括反向认证信息，还包括：测量密钥信息量子态所采用的测量基；

[0299] 相应的，所述装置还包括：

[0300] 原始密钥筛选单元，用于当所述发送方认证判断单元的输出结果为是时，确定密钥信息量子态的正确测量基，并筛选原始密钥；

[0301] 正确测量基公布单元，用于通过经典信道公布所述密钥信息量子态的正确测量基；

[0302] 发送方量子密钥获取单元，用于通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0303] 可选的，所述装置还包括：

[0304] 算法编号协商单元，用于在触发所述量子态发送单元工作之前，与所述对端设备通过经典信道协商算法编号；

[0305] 相应的，所述量子态发送单元选择身份认证信息的制备基的功能具体通过如下方式实现：

[0306] 根据所述算法编号协商单元确定的算法编号从所述预置算法库中选择算法，并根据所述算法选择所述身份认证信息的制备基。

[0307] 可选的，所述量子态发送单元所采用的预设信息格式包括：身份认证信息和密钥信息分别有各自的控制信息作为前缀。

[0308] 可选的，所述量子态发送单元所采用的预设信息格式包括：身份认证信息和密钥信息采用共同的控制信息作为前缀；

[0309] 相应的，所述装置还包括：

[0310] 认证信息长度协商单元，用于在触发所述量子态发送单元工作之前，与所述对端设备通过经典信道协商位于控制信息与密钥信息之间的身份认证信息的长度。

[0311] 可选的，所述响应信息接收单元接收到的反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、接收方认证密钥或接收方认证密钥的散列值；

[0312] 相应的，所述本地认证信息生成单元具体用于，根据接收的所述位置信息从本地

已发送的身份认证信息中选取相应的发送方认证密钥，并相应地将所述发送方认证密钥或者所述发送方认证密钥的散列值作为所述本地认证信息。

[0313] 可选的，所述响应信息接收单元接收到的反向认证信息包括：所述对端设备选取接收方认证密钥的位置信息、辅助认证信息密文、以及用所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

[0314] 相应的，所述本地认证信息生成单元包括：

[0315] 发送方认证密钥选取子单元，用于根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥；

[0316] 辅助认证信息解密单元，用于利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息；

[0317] 发送方散列值计算单元，用于计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息。

[0318] 可选的，所述装置还包括：

[0319] 变体信息加密单元，用于当所述发送方认证判断单元的输出为是时，采用所述发送方认证密钥加密所述通过解密操作获取的辅助认证信息的变体；

[0320] 变体信息密文发送单元，用于通过经典信道将执行上述加密操作后的密文发送给所述对端设备。

[0321] 此外，本申请还提供了第三种用于量子密钥分发过程的身份认证方法，所述方法在参与量子密钥分发过程的接收方量子通信设备上实施。请参考图10，其为本申请的第三种用于量子密钥分发过程的身份认证方法的实施例的流程图，本实施例与上述各实施例步骤相同的部分不再赘述，下面重点描述不同之处。所述方法包括如下步骤：

[0322] 步骤1001、接收参与量子密钥分发过程的对端设备发送的量子态，并根据预先约定的不同波长和预设信息格式区分接收到的各种信息量子态。

[0323] 在执行本步骤之前，可以与所述对端设备通过经典信道协商算法编号。相应的，所述根据从预置算法库中选取的、与对端设备相同的算法选择测量基包括：根据协商确定的算法编号从所述预置算法库中选择算法；根据所述算法选择所述测量基。

[0324] 步骤1002、根据从预置算法库中选取的、与所述对端设备相同的算法选择测量基，并用所述测量基对接收到的身份认证信息量子态进行测量。

[0325] 步骤1003、判断测量结果是否与所选算法相符；若是，执行步骤1004，若否，执行步骤1005。

[0326] 步骤1004、向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息。

[0327] 本步骤可以采用如下实现方式：从所述测量结果中选取接收方认证密钥；将选取所述接收方认证密钥的位置信息、以及所述接收方认证密钥或者接收方认证密钥的散列值发送给所述对端设备。

[0328] 本步骤也可以采用如下实现方式：从所述测量结果中选取接收方认证密钥；用所述接收方认证密钥对本地生成的辅助认证信息加密；计算由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；将选取所述接收方认证密钥的位置信息、所述辅助认证信息密文、以及所述散列值发送给所述对端设备。

[0329] 本步骤除了向对端设备发送反向认证信息之外，还可以通过经典信道公开用于测量密钥信息量子态的测量基。

[0330] 此后，还可以执行下述操作：接收所述对端设备发送的辅助认证信息变体的密文；采用所述接收方认证密钥解密接收到的所述密文；判断执行所述解密操作后得到的信息是否与所述本地生成的辅助认证信息的变体一致；如果上述判断结果为“是”，接收方可以根据接收的正确测量基，筛选原始密钥，并通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥；如果上述判断结果为“否”，则说明发送方身份不可信，因此可以结束本次的量子密钥分发过程。

[0331] 步骤1005、结束本次量子密钥分发过程。

[0332] 在上述的实施例中，提供了第三种用于量子密钥分发过程的身份认证方法，与之相对应的，本申请还提供一种用于量子密钥分发过程的身份认证装置，所述装置部署在参与量子密钥分发过程的接收方量子通信设备上。请参看图11，其为本申请的一种用于量子密钥分发过程的身份认证装置的实施例示意图。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。

[0333] 本实施例的一种用于量子密钥分发过程的身份认证装置，包括：量子态接收单元1101，用于接收参与量子密钥分发过程的对端设备发送的量子态，并根据预先约定的不同波长和预设信息格式区分接收到的各种信息量子态；量子态测量单元1102，用于根据从预置算法库中选取的、与对端设备相同的算法选择测量基，并用所述测量基对接收到的身份认证信息量子态进行测量；接收方认证判断单元1103，用于判断测量结果是否与所选算法相符；反向认证信息发送单元1104，用于当所述接收方认证判断单元的输出为是时，向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息；分发过程结束单元1105，用于当所述接收方认证判断单元的输出为否时，结束本次量子密钥分发过程。

[0334] 可选的，所述装置还包括：

[0335] 测量基公布单元，用于当所述接收方认证判断单元的输出为是时，通过经典信道公开用于测量密钥信息量子态的测量基；

[0336] 相应的，所述装置还包括：

[0337] 正确测量基接收单元，用于接收所述对端设备通过经典信道发送的所述密钥信息量子态的正确测量基；

[0338] 接收方量子密钥获取单元，用于筛选原始密钥，并通过误码率估算、纠错和隐私放大过程，获取最终的共享量子密钥。

[0339] 可选的，所述装置还包括：

[0340] 算法编号协商单元，用于在触发所述量子态接收单元工作之前，与所述对端设备通过经典信道协商算法编号；

[0341] 相应的，所述量子态测量单元选择身份认证信息的测量基的功能具体通过如下方式实现：

[0342] 根据协商确定的算法编号从所述预置算法库中选择算法，并根据所述算法选择所述测量基。

[0343] 可选的，所述反向认证信息发送单元包括：

[0344] 接收方认证密钥选取子单元，用于从所述测量结果中选取接收方认证密钥；

[0345] 第一信息发送执行子单元，用于将选取所述接收方认证密钥的位置信息、以及所述接收方认证密钥或者接收方认证密钥的散列值发送给所述对端设备。

[0346] 可选的，所述反向认证信息发送单元包括：

[0347] 接收方认证密钥选取子单元，用于从所述测量结果中选取接收方认证密钥；

[0348] 辅助认证信息加密子单元，用于用所述接收方认证密钥对本地生成的辅助认证信息加密；

[0349] 接收方散列值计算子单元，计算由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值；

[0350] 第二信息发送执行子单元，用于将选取所述接收方认证密钥的位置信息、所述辅助认证信息密文、以及所述散列值发送给所述对端设备。

[0351] 可选的，所述装置还包括：

[0352] 变体信息密文接收单元，用于在所述反向认证信息发送单元完成发送操作后，接收所述对端设备发送的辅助认证信息变体的密文；

[0353] 变体信息密文解密单元，用于采用所述接收方认证密钥解密接收到的所述密文；

[0354] 变体信息判断单元，用于判断执行所述解密操作后得到的信息是否与所述本地生成的辅助认证信息的变体一致，若不一致，则触发所述分发过程结束单元工作。

[0355] 此外，本申请实施例还提供了一种用于量子密钥分发过程的身份认证系统，如图12所示，该系统包括：部署于发送方量子通信设备的身份认证装置1201，以及部署于接收方量子通信设备的身份认证装置1202。

[0356] 分别部署于收发双方量子通信设备的身份认证装置，采用本申请提供的身份认证方法，在量子密钥分发过程中实现对对端设备身份的动态验证。下面结合图13，对所述用于量子密钥分发过程的身份认证系统的交互处理流程作简要说明。其中，部署于发送方量子通信设备的身份认证装置，简称为A，部署于接收方量子通信设备的身份认证装置，简称为B，(message)key代表用key对message加密，hash()代表散列函数。

[0357] 1)A向B发送密钥协商请求，请求中携带A的账户信息；

[0358] 2)B验证A身份的合法性，向A发送B的账户信息；

[0359] 3)A根据接收到的账户信息验证B身份的合法性；A与B协商拟采用的预置算法库中的算法编号；

[0360] 4)A根据所述编号对应的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长发送控制信息以及数据信息的量子态，所述数据信息包括：身份认证信息和随机生成的密钥信息；

[0361] 5)B根据所述不同波长和所述预设信息格式区分接收到的各种信息量子态，并采用对应于预置算法库中相同编号算法的测量基对其中的身份认证信息量子态进行测量，当测量结果与所述算法相符时，发送选取接收方IDkey的位置信息、用接收方IDkey加密的辅助认证信息m的密文、以及由m和IDkey拼接而成的字符串的散列值，并公开密钥信息量子态的测量基，否则结束本次量子密钥分发过程；

[0362] 6)A根据接收的所述位置信息从本地已发送的身份认证信息中选取相应的发送方

IDkey，利用发送方IDkey对接收到的密文解密，获取辅助认证信息m，并计算由所述m与发送方IDkey拼接而成的字符串的散列值，然后判断计算得到的散列值是否与接收到的散列值一致，若一致，筛选原始密钥、公布密钥信息量子态的正确测量基、并发送用发送方IDkey加密的辅助认证信息m的变体的密文，若不一致则结束本次量子密钥分发过程；

[0363] 7)B采用接收方IDkey解密接收到的辅助认证信息的变体的密文，若解密后获取的信息与本地原始生成的辅助认证信息m的变体一致，则根据接收的正确测量基筛选原始密钥、并公布部分密钥量子态的测量结果，否则结束本次量子密钥分发过程；

[0364] 8)A与B通过计算误码率、纠错、隐私放大，获取最终的共享量子密钥，其中各协商过程中所涉及的信息都可以采用收发双方相应的IDkey进行加解密。

[0365] 需要说明的是，上述示出的是本系统的一种优选实施方式，在其他实施方式中可以采用不同的交互方式，例如，可以不执行其中1)、2)的基于预置账户信息的身份认证环节，可以不执行3)进行算法编号的协商，而是由收发双方在每次的量子密钥分发过程中采用相同的预设规则选择预置算法库中的算法也是可以的；在环节5)B向A发送的反向认证信息也可以采用不同于本实施例中的其他形式，只要A能够根据B提供的反向认证信息验证B的身份即可。这些都属于本系统交互流程的变更，都不偏离本申请的核心，都在本申请的保护范围之内。

[0366] 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申请的精神和范围内，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。

[0367] 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。

[0368] 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。

[0369] 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。

[0370] 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。

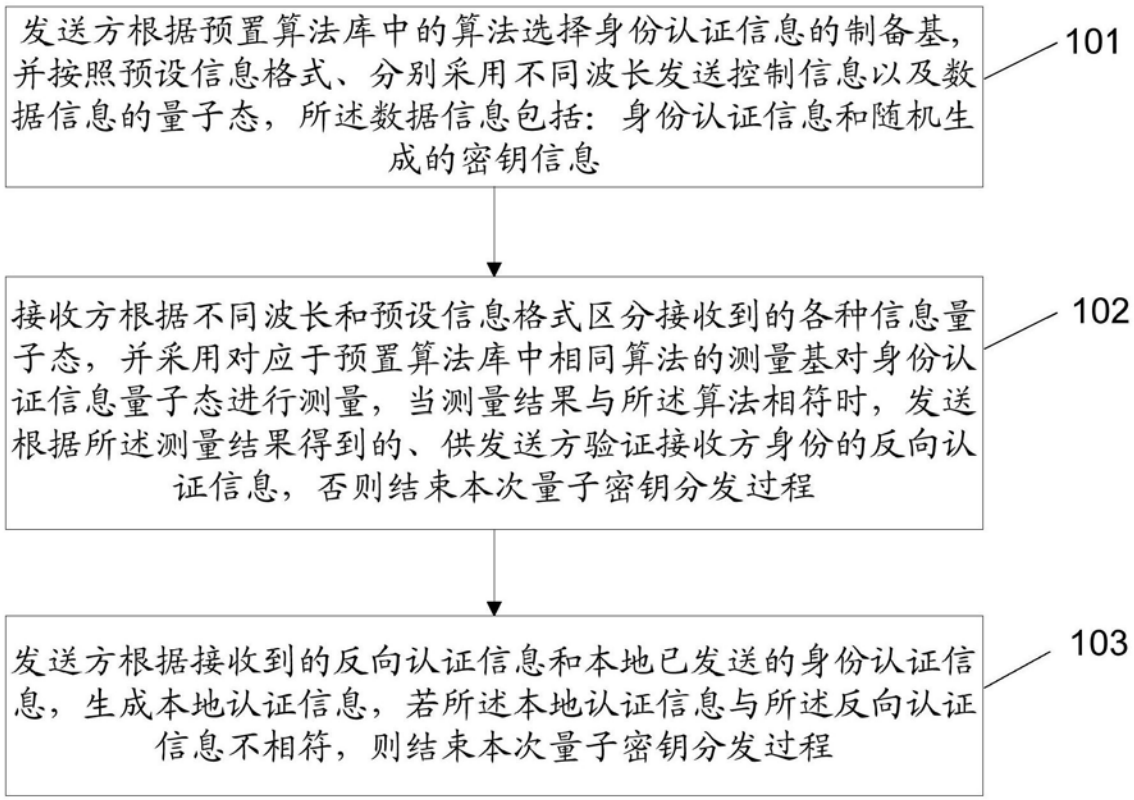


图1

身份认证控制信息	身份认证信息	密钥控制信息	密钥信息
λ_2	λ_1	λ_3	λ_1

图2

身份认证控制信息 00000	身份认证信息	密钥控制信息 11111	密钥信息
λ_2	λ_1	λ_2	λ_1

图3

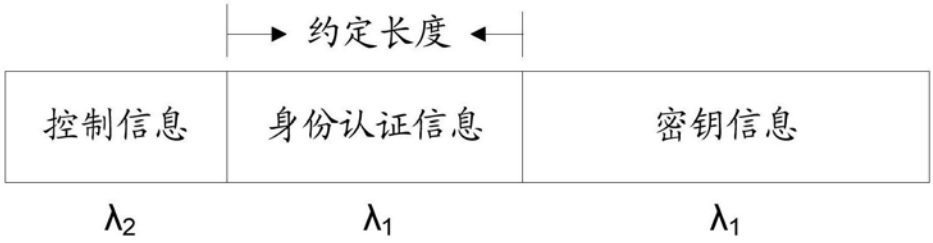

约定长度
控制信息
身份认证信息
密钥信息
λ2
λ1
λ1

图4

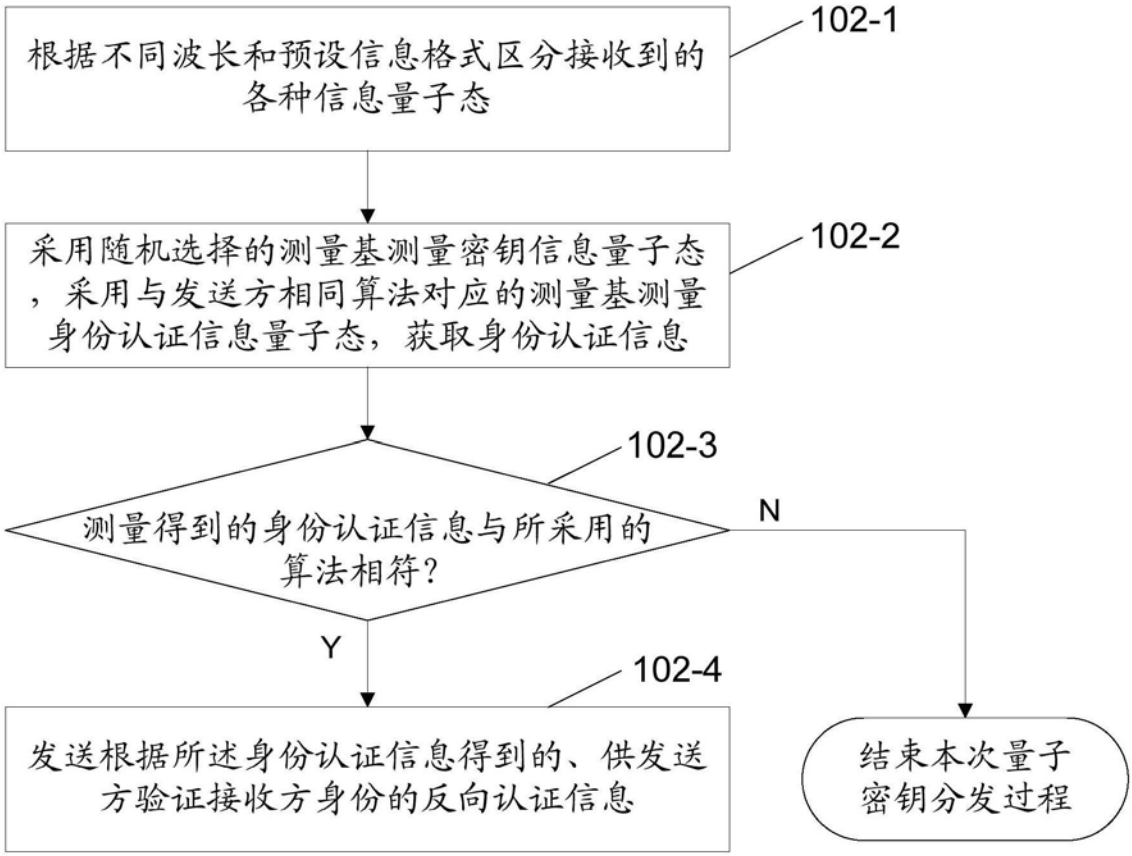

根据不同波长和预设信息格式区分接收到的各种信息量子态
102-1
采用随机选择的测量基测量密钥信息量子态，采用与发送方相同算法对应的测量基测量身份认证信息量子态，获取身份认证信息
102-2
测量得到的身份认证信息与所采用的算法相符?
102-3
N
Y
发送根据所述身份认证信息得到的、供发送方验证接收方身份的反向认证信息
102-4
结束本次量子密钥分发过程

图5

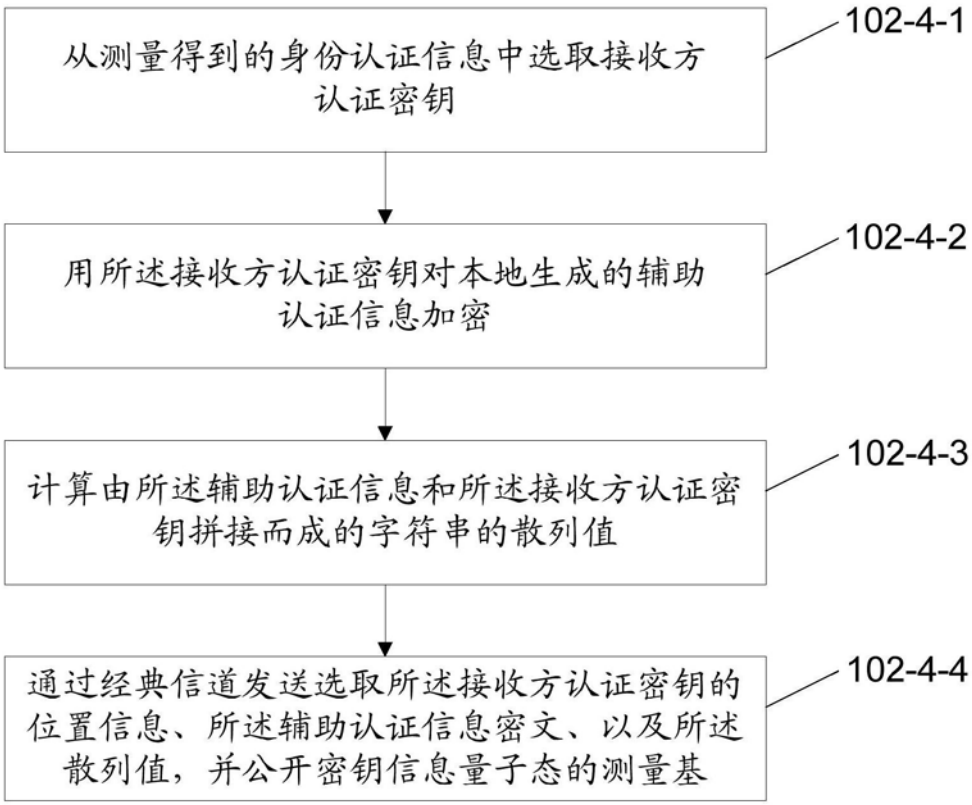

从测量得到的身份认证信息中选取接收方认证密钥
102-4-1
用所述接收方认证密钥对本地生成的辅助认证信息加密
102-4-2
计算由所述辅助认证信息和所述接收方认证密钥拼接而成的字符串的散列值
102-4-3
通过经典信道发送选取所述接收方认证密钥的位置信息、所述辅助认证信息密文、以及所述散列值，并公开密钥信息量子态的测量基
102-4-4

图6

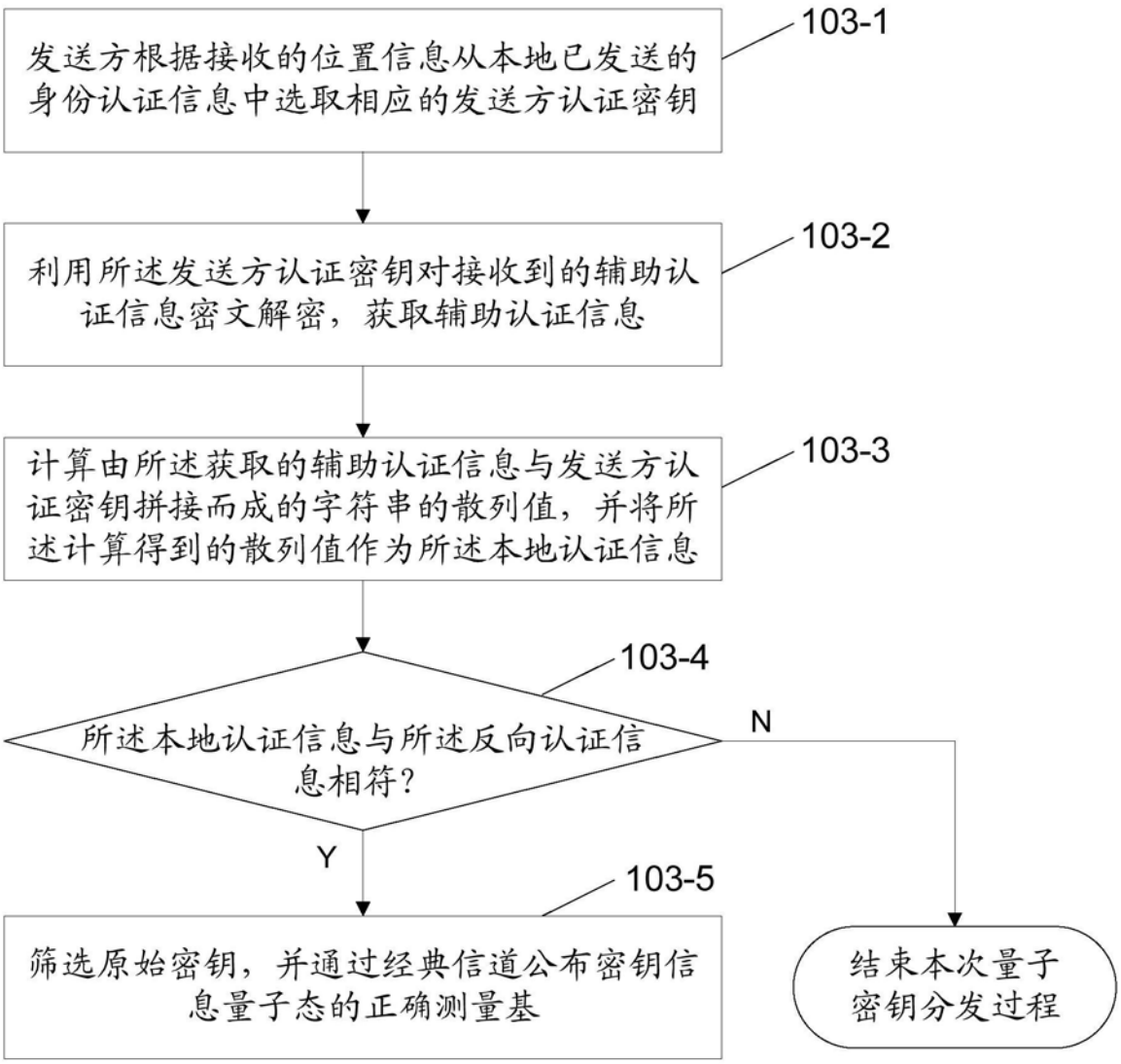

发送方根据接收的位置信息从本地已发送的身份认证信息中选取相应的发送方认证密钥
103-1
利用所述发送方认证密钥对接收到的辅助认证信息密文解密，获取辅助认证信息
103-2
计算由所述获取的辅助认证信息与发送方认证密钥拼接而成的字符串的散列值，并将所述计算得到的散列值作为所述本地认证信息
103-3
所述本地认证信息与所述反向认证信息相符?
103-4
N
Y
筛选原始密钥，并通过经典信道公布密钥信息量子态的正确测量基
103-5
结束本次量子密钥分发过程

图7

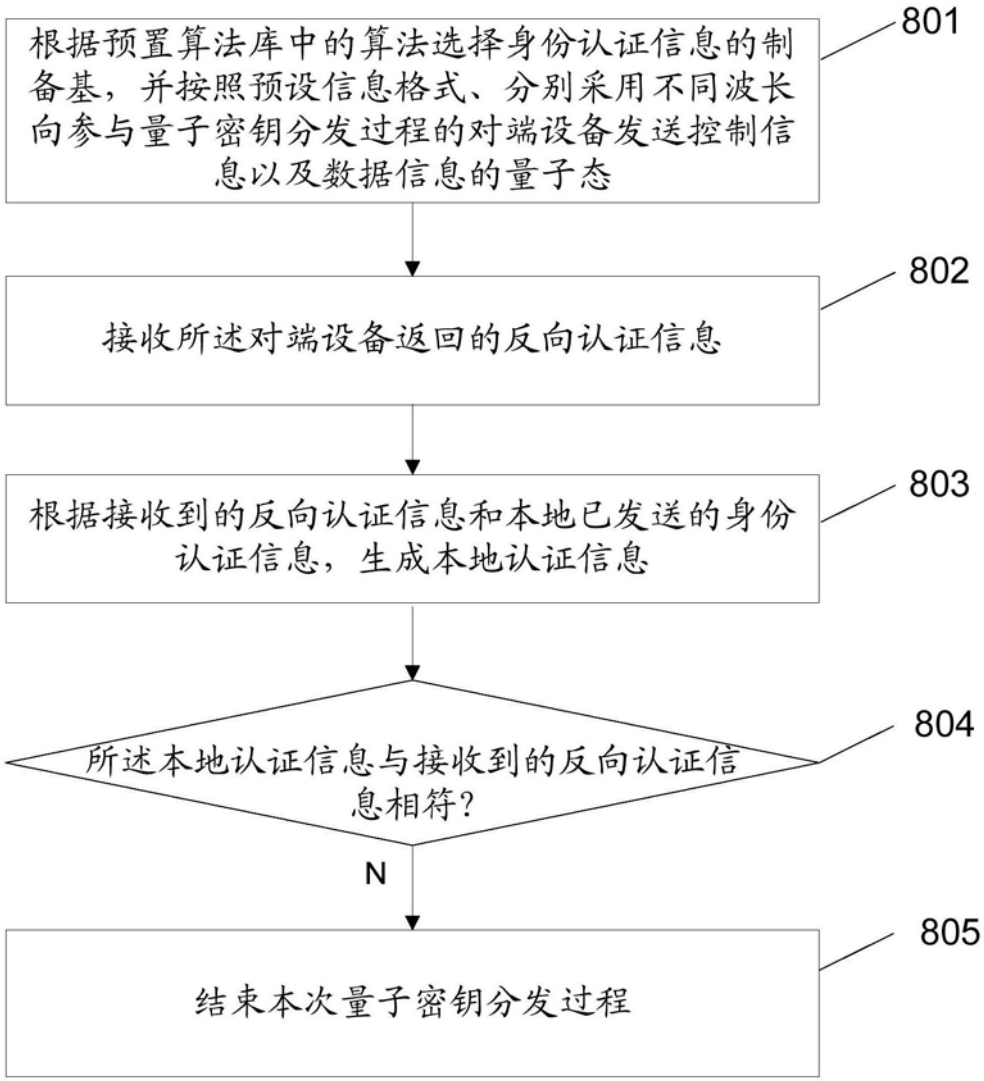

根据预置算法库中的算法选择身份认证信息的制备基，并按照预设信息格式、分别采用不同波长向参与量子密钥分发过程的对端设备发送控制信息以及数据信息的量子态
801
接收所述对端设备返回的反向认证信息
802
根据接收到的反向认证信息和本地已发送的身份认证信息，生成本地认证信息
803
所述本地认证信息与接收到的反向认证信息相符？
804
N
结束本次量子密钥分发过程
805

图8

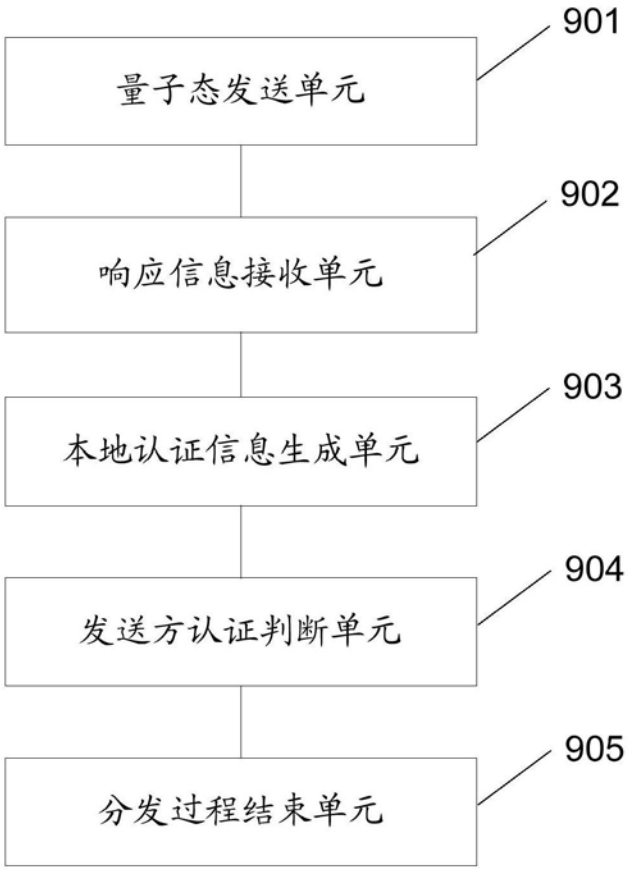

901
量子态发送单元
902
响应信息接收单元
903
本地认证信息生成单元
904
发送方认证判断单元
905
分发过程结束单元

图9

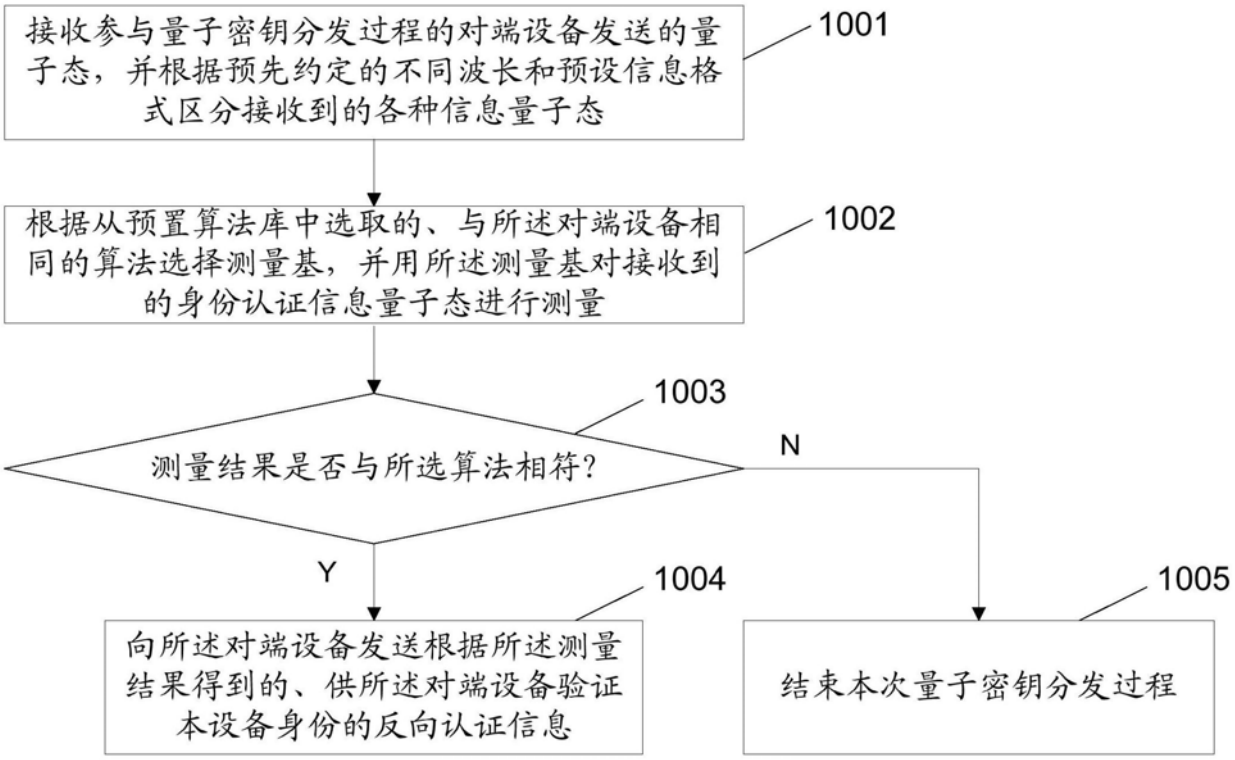

接收参与量子密钥分发过程的对端设备发送的量子态，并根据预先约定的不同波长和预设信息格式区分接收到的各种信息量子态
1001
根据从预置算法库中选取的、与所述对端设备相同的算法选择测量基，并用所述测量基对接收到的身份认证信息量子态进行测量
1002
测量结果是否与所选算法相符?
1003
N
Y
向所述对端设备发送根据所述测量结果得到的、供所述对端设备验证本设备身份的反向认证信息
1004
结束本次量子密钥分发过程
1005

图10

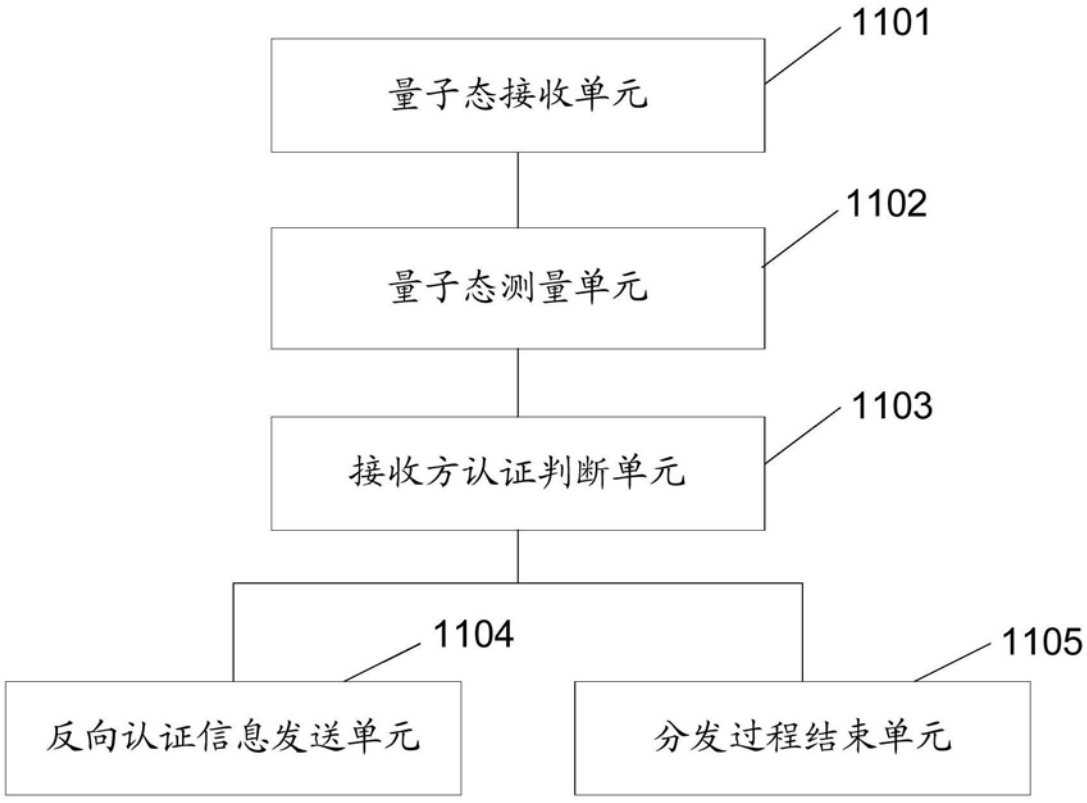

量子态接收单元
1101
量子态测量单元
1102
接收方认证判断单元
1103
反向认证信息发送单元
1104
分发过程结束单元
1105

图11

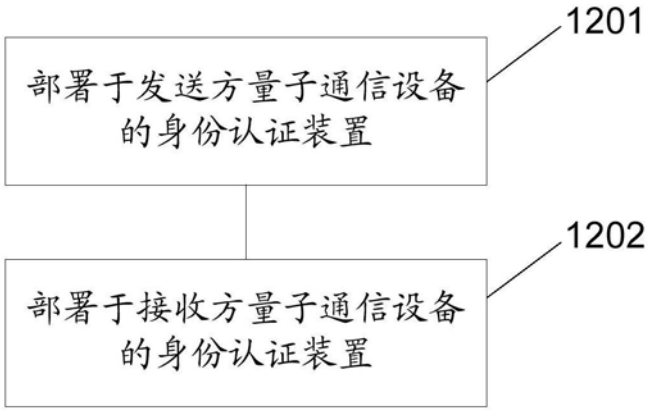

1201
部署于发送方量子通信设备的身份认证装置
1202
部署于接收方量子通信设备的身份认证装置

图12

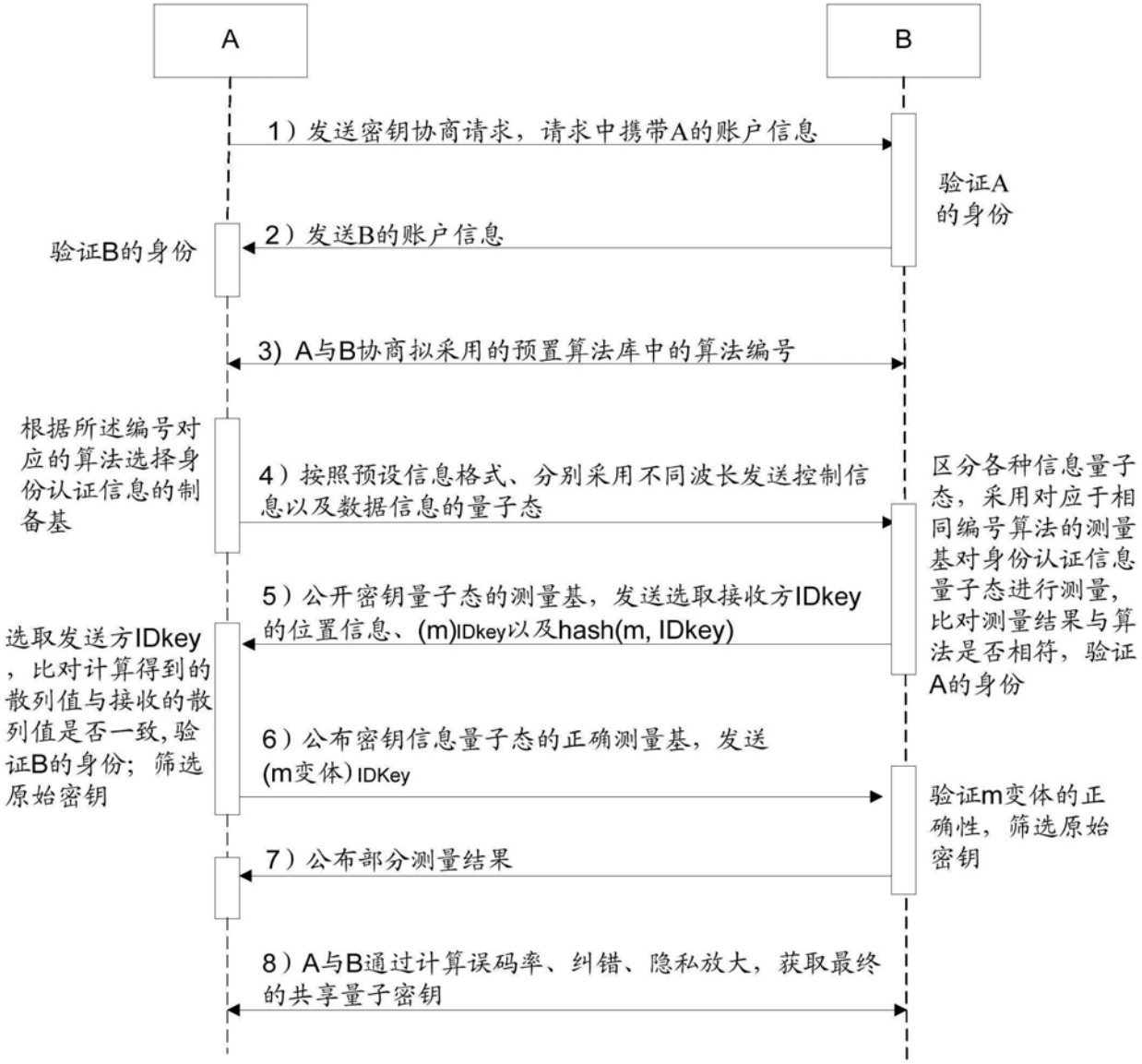

A
B
1）发送密钥协商请求，请求中携带A的账户信息
验证A的身份
验证B的身份
2）发送B的账户信息
3) A与B协商拟采用的预置算法库中的算法编号
根据所述编号对应的算法选择身份认证信息的制备基
4）按照预设信息格式、分别采用不同波长发送控制信息以及数据信息的量子态
区分各种信息量子态，采用对应于相同编号算法的测量基对身份认证信息量子态进行测量，比对测量结果与算法是否相符，验证A的身份
5）公开密钥量子态的测量基，发送选取接收方IDkey的位置信息、(m)IDkey以及hash(m, IDkey)
选取发送方IDkey，比对计算得到的散列值与接收的散列值是否一致,验证B的身份；筛选原始密钥
6）公布密钥信息量子态的正确测量基，发送(m变体)IDKey
验证m变体的正确性，筛选原始密钥
7）公布部分测量结果
8）A与B通过计算误码率、纠错、隐私放大，获取最终的共享量子密钥

图13