(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 105991285 B
(45)授权公告日 2019.06.11

(21)申请号 201510084941.2

(22)申请日 2015.02.16

(65)同一申请的已公布的文献号
申请公布号 CN 105991285 A

(43)申请公布日 2016.10.05

(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 刘栓林

(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)

(56)对比文件
CN 102946313 A,2013.02.27,
CN 102946313 A,2013.02.27,
US 2013083926 A1,2013.04.04,
CN 102904726 A,2013.01.30,
CN 103338448 A,2013.10.02,
Olli Ahonen.“Entanglement-Enhanced Quantum Key Distribution”.《Phys.rev.a》.2008,

审查员 张翔宇

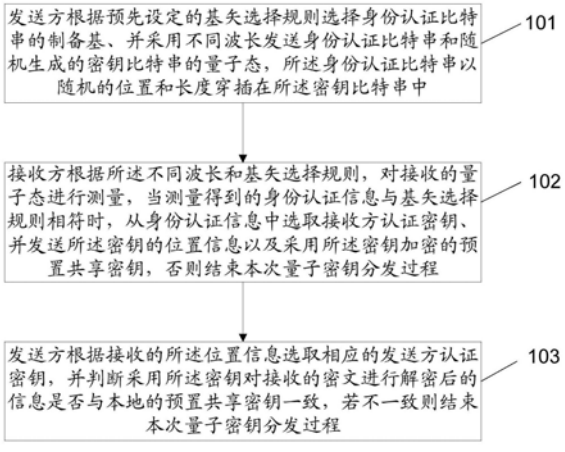
权利要求书7页 说明书19页 附图7页

(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。所述方法包括:发送方根据基矢选择规则选择身份认证比特串的制备基、并采用不同波长发送身份认证比特串和密钥比特串的量子态;接收方当测量得到的身份认证信息与基矢选择规则相符时,发送加密的预置共享密钥,否则结束量子密钥分发过程;发送方解密收到的密文并判断是否与本地的预置共享密钥一致,若不一致则结束量子密钥分发过程。采用本技术方案,可以在量子密钥分发过程中有效防御中间人攻击和DDoS攻击,保障量子密钥分发过程的安全性,而且不会造成身份识别率及量子密钥分发量的降低。



CN 105991285 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:

发送方根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用不同波长发送身份认证比特串和随机生成的密钥比特串的量子态,所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中;

接收方根据所述不同波长和基矢选择规则,对接收的量子态进行测量,当测量得到的身份认证信息与所述基矢选择规则相符时,从所述身份认证信息中选取接收方认证密钥、并发送所述接收方认证密钥的位置信息以及采用所述密钥加密的预置共享密钥,否则结束本次量子密钥分发过程;

发送方根据接收的所述位置信息选取相应的发送方认证密钥,并判断采用所述密钥对接收的密文进行解密后的信息是否与本地的预置共享密钥一致,若不一致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,当所述接收方测量得到的身份认证信息与所述基矢选择规则相符时,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量子态的测量基;

相应的,当所述发送方判断解密后的信息与本地的预置共享密钥一致时,所述发送方执行下述操作:

确定密钥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发送方认证密钥量子态的正确测量基;

相应的,在上述公布所述密钥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2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,在发送方发送身份认证比特串和随机生成的密钥比特串的量子态之前,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。

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,所述预置的账户信息包括:身份信息和证书。

5.根据权利要求2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,所述预先设定的基矢选择规则包括:

根据身份验证比特在量子态信息中的位置,选择相应的制备基或者测量基。

6.根据权利要求5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,所述根据身份验证比特在量子态信息中的位置,选择相应的制备基或者测量基,具体是指:

根据每个身份验证比特在量子态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。

7.根据权利要求2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,所述接收方根据所述不同波长和基矢选择规则,对接收的量子态进行测量,包括:

根据所述不同波长,区分身份认证量子态信息和密钥量子态信息;

按照所述预先设定的基矢选择规则选择身份认证量子态信息的测量基；

使用所选测量基测量所述身份认证量子态信息，并剔除其中未探测到光子的部分，获取所述测量得到的身份认证信息。

8.根据权利要求7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，所述接收方测量得到的身份认证信息与所述基矢选择规则相符是指，所述接收方测量得到的身份认证信息与遵循所述基矢选择规则的预期信息的差异，小于预先设定的阈值。

9.根据权利要求2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，所述接收方从所述身份认证信息中选取接收方认证密钥，包括：

所述接收方将所述身份认证信息作为所述接收方认证密钥；或者，

所述接收方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。

10.根据权利要求2-9任一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，所述接收方采用所述接收方认证密钥加密的信息不仅包括所述预置共享密钥，还包括本地生成的辅助认证信息；

相应的，发送方采用发送方认证密钥对接收的密文进行解密是指，所述发送方采用所述发送方认证密钥解密接收到的密文，获取解密后的预置共享密钥和解密后的辅助认证信息；

相应的，所述发送方判断解密后的信息是否与本地的预置共享密钥一致是指，所述发送方判断解密后的预置共享密钥是否与本地的预置共享密钥一致。

11.根据权利要求10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，当所述发送方判断解密后的预置共享密钥是否与本地的预置共享密钥一致的结果为是时，还执行下述操作：

所述发送方采用预设策略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正确测量基和所述密文后，执行下述操作：

采用与所述预设策略对应的方式，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；

若一致，则根据接收到的所述正确测量基执行所述筛选原始密钥的步骤，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。

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，所述预设策略包括：

采用本地的预置共享密钥执行所述加密操作；或者，

采用所述发送方认证密钥执行所述加密操作。

13.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，所述辅助认证信息的变体包括：

所述辅助认证信息本身；或者，

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。

14.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，所述

发送方根据所述接收方公布的部分密钥量子态的测量结果估算误码率后，采用所述发送方认证密钥加密所述误码率，并将加密后的信息发送给所述接收方；

相应的，所述接收方采用所述接收方认证密钥解密接收到的密文，获取解密后的误码率。

15.一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：

根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用预先设定的不同波长向参与量子密钥分发过程的对端设备发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中；

接收所述对端设备返回的认证密钥位置信息和待验证密文；

根据所述位置信息和已发送的量子态信息，选取认证密钥，并采用所述认证密钥对接收的待验证密文进行解密；

判断解密后的信息是否与本地的预置共享密钥一致；若否，则结束本次量子密钥分发过程。

16.根据权利要求15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：认证密钥位置信息和待验证密文，还包括：测量密钥量子态所采用的测量基；

相应的，当所述判断解密后的信息是否与本地的预置共享密钥一致的结果为是时，执行下述操作：

确定密钥量子态的正确测量基，并筛选原始密钥；

通过经典信道公布所述认证密钥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。

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，在所述发送身份认证比特串和随机生成的密钥密特串的量子态之前，执行下述操作：

向所述对端设备发送量子密钥协商请求，所述请求中包含发送方的账户信息；

接收所述对端设备发送的账户信息；

根据接收到的所述账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程。

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，所述预先设定的基矢选择规则包括：

根据身份验证比特在量子态信息中的位置，选择相应的制备基。

19.根据权利要求18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，所述根据身份验证比特在量子态信息中的位置，选择相应的制备基，具体是指：

根据每个身份验证比特在量子态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。

20.一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，用于根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用预先设定的不同波长向参与量子密钥分发过程的对端设备发送身份认证比特串和

随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中；

响应信息接收单元，用于接收所述对端设备返回的认证密钥位置信息和待验证密文；

信息解密单元，用于根据所述位置信息和已发送的量子态信息，选取认证密钥，并采用所述认证密钥对接收的待验证密文进行解密；

发送方认证判断单元，用于判断解密后的信息是否与本地的预置共享密钥一致；若否，则结束本次量子密钥分发过程。

21.根据权利要求20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：认证密钥位置信息和待验证密文，还包括：测量密钥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，用于当所述认证判断单元的输出结果为是时，确定密钥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认证密钥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。

22.根据权利要求21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：

协商请求发送单元，用于向所述对端设备发送量子密钥协商请求，所述请求中包含发送方的账户信息；

账户信息接收单元，用于接收所述对端设备发送的账户信息；

第一身份认证单元，用于根据所述账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程。

23.根据权利要求21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采用的预先设定的基矢选择规则包括：根据身份验证比特在量子态信息中的位置，选择相应的制备基。

24.根据权利要求23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采用的预先设定的基矢选择规则是指，根据每个身份验证比特在量子态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。

25.一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；

按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息；

判断所述身份认证信息与所述基矢选择规则是否相符；

若是，从所述身份认证信息中选取认证密钥、并向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥；

若否，结束本次量子密钥分发过程。

26.根据权利要求25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，当所述判断所述身份认证信息与所述基矢选择规则是否相符的结果为是时，还执行下述操作：

通过经典信道公开测量密钥量子态所采用的测量基；

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认证密钥量子态的正确测量基；

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

27.根据权利要求25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之前，执行下述操作：

接收所述对端设备发送的密钥协商请求；

根据所述请求中包含的账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程，否则向所述对端设备发送接收方的账户信息。

28.根据权利要求25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，所述预先设定的基矢选择规则包括：

根据身份认证比特在量子态信息中的位置，选择相应的测量基。

29.根据权利要求28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，所述根据身份验证比特在量子态信息中的位置，选择相应的测量基，具体是指：

根据每个身份验证比特在量子态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。

30.根据权利要求25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，所述按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息，包括：

根据所述预先设定的不同波长，区分身份认证量子态信息和密钥量子态信息；

按照所述预先设定的基矢选择规则选择身份认证量子态信息的测量基；

使用所选测量基测量所述身份认证量子态信息，并剔除其中未探测到光子的部分，获取所述身份认证信息。

31.根据权利要求25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，所述从所述身份认证信息中选取认证密钥，包括：

选取所述身份认证信息作为所述认证密钥；或者，

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认证密钥。

32.一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；

量子态测量单元，用于按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息；

接收方认证判断单元，用于判断所述身份认证信息与所述基矢选择规则是否相符，若否，则结束本次量子密钥分发过程；

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，从所述身份认证信息中选取认证密钥、并向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥

加密的预置共享密钥。

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装置，其特征在于，所述装置还包括：

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，通过经典信道公开测量密钥量子态所采用的测量基；

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认证密钥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。

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装置，其特征在于，所述装置还包括：

协商请求接收单元，用于接收所述对端设备发送的密钥协商请求；

第二身份认证单元，用于根据所述请求中包含的账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程，否则向所述对端设备发送接收方的账户信息。

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装置，其特征在于，所述量子态测量单元采用的预先设定的基矢选择规则包括：根据身份认证比特在量子态信息中的位置，选择相应的制备基。

36.根据权利要求35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，所述量子态测量单元采用的预先设定的基矢选择规则是指，根据每个身份认证比特在量子态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。

37.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装置，其特征在于，所述量子态测量单元包括：

信息区分子单元，用于根据所述预先设定的不同波长，区分身份认证量子态信息和密钥量子态信息；

身份认证测量基选择子单元，用于按照所述预先设定的基矢选择规则选择身份认证量子态信息的测量基；

身份认证信息获取子单元，用于使用所选测量基测量所述身份认证量子态信息，并剔除其中未探测到光子的部分，获取所述身份认证信息。

38.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装置，其特征在于，所述信息发送单元包括：

认证密钥选取子单元，用于从所述身份认证信息中选取认证密钥；

信息发送子单元，用于向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥；

其中，所述认证密钥选取子单元具体用于，

选取所述身份认证信息作为所述认证密钥；或者，

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认证密钥。

39.一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20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32所述的部署于接收方量子通信设备的身份认证装置；

所述部署于收发双方量子通信设备的身份认证装置，预置了相同的基矢选择规则、相同的共享密钥，并采用相同的、用于区分身份认证信息和密钥信息的波长设置。

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] 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。最初提出的量子密钥分配协议(如BB84)虽然能够检测出窃听者对密钥的窃取操作，但是这些协议没有提供有效的身份认证机制。

[0003] 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。由于传统的量子密钥分配协议不具备有效的身份认证机制，因此可能在量子密钥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，即使这些信息被修改也不会影响到安全。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密钥位，量子比特串中每4个比特位中有一个是特定的认证密钥位，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，同时量子力学基本原理又保证了绝对安全的密钥分配。

[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，但是由于该技术方案假设发送端的认证密钥量子态都能传输到接收端，接收端能按预设的认证密钥选择相应测量基去探测，探测结果一致就通过，否则认为对方是不合法的，终止量子密钥分发过程。该方案没有考虑光子在实际传输过程中的衰减(即：光子不一定能传输到对方，自然无法保证量子态的一致性)，也就是说该技术方案没有提供对信道衰减的容错能力，导致身份识别率以及量子密钥分发量的降低。

发明内容

[0010] 本申请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身份认证技术易遭受攻击、以及导致量子密钥分发量降低的问题。本申请另外提供两种用于量子密钥分发过程的身份认证方法及装置，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] 发送方根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用不同波长发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中；

[0013] 接收方根据所述不同波长和基矢选择规则，对接收的量子态进行测量，当测量得到的身份认证信息与所述基矢选择规则相符时，从所述身份认证信息中选取接收方认证密钥、并发送所述密钥的位置信息以及采用所述密钥加密的预置共享密钥，否则结束本次量子密钥分发过程；

[0014] 发送方根据接收的所述位置信息选取相应的发送方认证密钥，并判断采用所述密钥对接收的密文进行解密后的信息是否与本地的预置共享密钥一致，若不一致则结束本次量子密钥分发过程。

[0015] 可选的，当所述接收方测量得到的身份认证信息与所述基矢选择规则相符时，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量子态的测量基；

[0017] 相应的，当所述发送方判断解密后的信息与本地的预置共享密钥一致时，所述发送方执行下述操作：

[0018] 确定密钥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量子态的正确测量基；

[0020] 相应的，在上述公布所述密钥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，在发送方发送身份认证比特串和随机生成的密钥比特串的量子态之前，执行下述操作：

[0024] 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。

[0025] 可选的，所述预置的账户信息包括：身份信息和证书。

[0026] 可选的，所述预先设定的基矢选择规则包括：

[0027] 根据身份验证比特在量子态信息中的位置，选择相应的制备基或者测量基。

[0028] 可选的，所述根据身份验证比特在量子态信息中的位置，选择相应的制备基或者测量基，具体是指：

[0029] 根据每个身份验证比特在量子态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。

[0030] 可选的，所述接收方根据所述不同波长和基矢选择规则，对接收的量子态进行测

量，包括：

[0031] 根据所述不同波长，区分身份认证量子态信息和密钥量子态信息；

[0032] 按照所述预先设定的基矢选择规则选择身份认证量子态信息的测量基；

[0033] 使用所选测量基测量所述身份认证量子态信息，并剔除其中未探测到光子的部分，获取所述测量得到的身份认证信息。

[0034] 可选的，所述接收方测量得到的身份认证信息与所述基矢选择规则相符是指，所述接收方测量得到的身份认证信息与遵循所述基矢选择规则的预期信息的差异，小于预先设定的阈值。

[0035] 可选的，所述接收方从所述身份认证信息中选取接收方认证密钥，包括：

[0036] 所述接收方将所述身份认证信息作为所述接收方认证密钥；或者，

[0037] 所述接收方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。

[0038] 可选的，所述接收方采用所述接收方认证密钥加密的信息不仅包括所述预置共享密钥，还包括本地生成的辅助认证信息；

[0039] 相应的，发送方采用发送方认证密钥对接收的密文进行解密是指，所述发送方采用所述发送方认证密钥解密接收到的密文，获取解密后的预置共享密钥和解密后的辅助认证信息；

[0040] 相应的，所述发送方判断解密后的信息是否与本地的预置共享密钥一致是指，所述发送方判断解密后的预置共享密钥是否与本地的预置共享密钥一致。

[0041] 可选的，当所述发送方判断解密后的预置共享密钥是否与本地的预置共享密钥一致的结果为是时，还执行下述操作：

[0042] 所述发送方采用预设策略加密所述通过解密操作获取的辅助认证信息的变体；

[0043] 并通过经典信道发送执行上述加密操作后的密文；

[0044] 相应的，所述接收方在接收所述正确测量基和所述密文后，执行下述操作：

[0045] 采用与所述预设策略对应的方式，解密接收到的密文；

[0046] 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；

[0047] 若一致，则根据接收到的所述正确测量基执行所述筛选原始密钥的步骤，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。

[0048] 可选的，所述预设策略包括：

[0049] 采用本地的预置共享密钥执行所述加密操作；或者，

[0050] 采用所述发送方认证密钥执行所述加密操作。

[0051] 可选的，所述辅助认证信息的变体包括：

[0052] 所述辅助认证信息本身；或者，

[0053] 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。

[0054] 可选的，所述发送方根据所述接收方公布的部分密钥量子态的测量结果估算误码率后，采用所述发送方认证密钥加密所述误码率，并将加密后的信息发送给所述接收方；

[0055] 相应的，所述接收方采用所述接收方认证密钥解密接收到的密文，获取解密后的误码率。

[0056] 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：

[0057] 根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用预先设定的不同波长向参与量子密钥分发过程的对端设备发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中；

[0058] 接收所述对端设备返回的认证密钥位置信息和待验证密文；

[0059] 根据所述位置信息和已发送的量子态信息，选取认证密钥，并采用所述认证密钥对接收的待验证密文进行解密；

[0060] 判断解密后的信息是否与本地的预置共享密钥一致；若否，则结束本次量子密钥分发过程。

[0061] 可选的，所述对端设备返回的信息不仅包括：认证密钥位置信息和待验证密文，还包括：测量密钥量子态所采用的测量基；

[0062] 相应的，当所述判断解密后的信息是否与本地的预置共享密钥一致的结果为是时，执行下述操作：

[0063] 确定密钥量子态的正确测量基，并筛选原始密钥；

[0064] 通过经典信道公布所述密钥量子态的正确测量基；

[0065] 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。

[0066] 可选的，在所述发送身份认证比特串和随机生成的密钥密特串的量子态之前，执行下述操作：

[0067] 向所述对端设备发送量子密钥协商请求，所述请求中包含发送方的账户信息；

[0068] 接收所述对端设备发送的账户信息；

[0069] 根据接收到的所述账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程。

[0070] 可选的，所述预先设定的基矢选择规则包括：

[0071] 根据身份验证比特在量子态信息中的位置，选择相应的制备基。

[0072] 可选的，所述根据身份验证比特在量子态信息中的位置，选择相应的制备基，具体是指：

[0073] 根据每个身份验证比特在量子态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。

[0074] 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：

[0075] 量子态发送单元，用于根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用预先设定的不同波长向参与量子密钥分发过程的对端设备发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中；

[0076] 响应信息接收单元，用于接收所述对端设备返回的认证密钥位置信息和待验证密文；

[0077] 信息解密单元，用于根据所述位置信息和已发送的量子态信息，选取认证密钥，并采用所述认证密钥对接收的待验证密文进行解密；

[0078] 发送方认证判断单元，用于判断解密后的信息是否与本地的预置共享密钥一致；若否，则结束本次量子密钥分发过程。

[0079] 可选的，所述响应信息接收单元接收到的信息不仅包括：认证密钥位置信息和待验证密文，还包括：测量密钥量子态所采用的测量基；

[0080] 相应的，所述装置还包括：

[0081] 原始密钥筛选单元，用于当所述认证判断单元的输出结果为是时，确定密钥量子态的正确测量基，并筛选原始密钥；

[0082] 正确测量基公布单元，用于通过经典信道公布所述密钥量子态的正确测量基；

[0083] 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。

[0084] 可选的，所述装置还包括：

[0085] 协商请求发送单元，用于向所述对端设备发送量子密钥协商请求，所述请求中包含发送方的账户信息；

[0086] 账户信息接收单元，用于接收所述对端设备发送的账户信息；

[0087] 第一身份认证单元，用于根据所述账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程。

[0088] 可选的，所述量子态发送单元采用的预先设定的基矢选择规则包括：根据身份验证比特在量子态信息中的位置，选择相应的制备基。

[0089] 可选的，所述量子态发送单元采用的预先设定的基矢选择规则是指，根据每个身份验证比特在量子态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。

[0090] 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：

[0091] 接收参与量子密钥分发过程的对端设备发送的量子态；

[0092] 按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息；

[0093] 判断所述身份认证信息与所述基矢选择规则是否相符；

[0094] 若是，从所述身份认证信息中选取认证密钥、并向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥；

[0095] 若否，结束本次量子密钥分发过程。

[0096] 可选的，当所述判断所述身份认证信息与所述基矢选择规则是否相符的结果为是时，还执行下述操作：

[0097] 通过经典信道公开测量密钥量子态所采用的测量基；

[0098] 相应的，所述方法还包括：

[0099] 接收所述对端设备通过经典信道发送的所述密钥量子态的正确测量基；

[0100] 筛选原始密钥，并通过获取误码率、纠错和隐私放大过程，获取最终的共享量子密钥。

[0101] 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之前，执行下述操作：

[0102] 接收所述对端设备发送的密钥协商请求；

[0103] 根据所述请求中包含的账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程，否则向所述对端设备发送接收方的账户信息。

[0104] 可选的，所述预先设定的基矢选择规则包括：

[0105] 根据身份认证比特在量子态信息中的位置，选择相应的测量基。

[0106] 可选的，所述根据身份验证比特在量子态信息中的位置，选择相应的测量基，具体是指：

[0107] 根据每个身份验证比特在量子态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。

[0108] 可选的，所述按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息，包括：

[0109] 根据所述预先设定的不同波长，区分身份认证量子态信息和密钥量子态信息；

[0110] 按照所述预先设定的基矢选择规则选择身份认证量子态信息的测量基；

[0111] 使用所选测量基测量所述身份认证量子态信息，并剔除其中未探测到光子的部分，获取所述身份认证信息。

[0112] 可选的，所述从所述身份认证信息中选取认证密钥，包括：

[0113] 选取所述身份认证信息作为所述认证密钥；或者，

[0114] 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认证密钥。

[0115] 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：

[0116] 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；

[0117] 量子态测量单元，用于按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息；

[0118] 接收方认证判断单元，用于判断所述身份认证信息与所述基矢选择规则是否相符，若否，则结束本次量子密钥分发过程；

[0119] 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，从所述身份认证信息中选取认证密钥、并向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥。

[0120] 可选的，所述装置还包括：

[0121] 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，通过经典信道公开测量密钥量子态所采用的测量基；

[0122] 相应的，所述装置还包括：

[0123] 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量子态的正确测量基；

[0124] 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。

[0125] 可选的，所述装置还包括：

[0126] 协商请求接收单元，用于接收所述对端设备发送的密钥协商请求；

[0127] 第二身份认证单元，用于根据所述请求中包含的账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程，否则向所述对端设备发送接收方的账户信息。

[0128] 可选的，所述量子态测量单元采用的预先设定的基矢选择规则包括：根据身份认证比特在量子态信息中的位置，选择相应的制备基。

[0129] 可选的，所述量子态测量单元采用的预先设定的基矢选择规则是指，根据每个身份认证比特在量子态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。

[0130] 可选的，所述量子态测量单元包括：

[0131] 信息区分子单元，用于根据所述预先设定的不同波长，区分身份认证量子态信息和密钥量子态信息；

[0132] 身份认证测量基选择子单元，用于按照所述预先设定的基矢选择规则选择身份认证量子态信息的测量基；

[0133] 身份认证信息获取子单元，用于使用所选测量基测量所述身份认证量子态信息，并剔除其中未探测到光子的部分，获取所述身份认证信息。

[0134] 可选的，所述信息发送单元包括：

[0135] 认证密钥选取子单元，用于从所述身份认证信息中选取认证密钥；

[0136] 信息发送子单元，用于向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥；

[0137] 其中，所述认证密钥选取子单元具体用于，

[0138] 选取所述身份认证信息作为所述认证密钥；或者，

[0139] 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认证密钥。

[0140] 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：如上述任一项所述的部署于发送方量子通信设备的身份认证装置、以及如上述任一项所述的部署于接收方量子通信设备的身份认证装置；

[0141] 所述部署于收发双方量子通信设备的身份认证装置，预置了相同的基矢选择规则、相同的共享密钥，并采用相同的、用于区分身份认证信息和密钥信息的波长设置。

[0142] 与现有技术相比，本申请具有以下优点：

[0143] 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，采用在密钥量子态中随机穿插身份认证信息量子态、以及利用特定波长来区分量子密钥信息和身份认证信息的方式，当参与量子密钥分发过程的量子通信设备检测到身份认证信息与双方预先设定的基矢选择规则不相符、或者检测到双方的预置共享密钥不一致时，则判定对端设备未通过身份认证并结束本次的量子密钥分发过程。上述技术方案，实现了量子态零知识证明的身份验证方法，可以在量子密钥分发过程中实时地进行身份验证，从而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，而且不会造成身份识别率及量子密钥分发量的降低。

附图说明

[0144] 图1是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；

[0145] 图2是本实施例提供的接收方根据测量结果验证发送方身份的处理流程图；

[0146] 图3是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；

[0147] 图4是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；

[0148] 图5是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；

[0149] 图6是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；

[0150] 图7是本申请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；

[0151] 图8是本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

[0152] 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。

[0153] 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。

[0154] 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作简要说明。

[0155] 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信息的设备，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信息进行测量的设备，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。下面对本实施例作详细说明。

[0156] 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：

[0157] 步骤101：发送方根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用不同波长发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中。

[0158] 本实施例提供的技术方案，可以在量子密钥分发过程(也称为量子密钥协商过程)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执行量子密钥分发过程，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方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。

[0159] 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，可以首先发起量子密钥协商请求，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。

[0160] 同样的道理，所述发送方接受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。

[0161] 若发送方和接收方都通过了上述身份验证过程，则继续后续的量子密钥分发过程。本技术方案为了在量子密钥分发过程中动态地进行身份验证，收发双方预置了相同的共享密钥，发送方在密钥比特串的任意位置穿插长度随机的身份认证比特串，并且采用预先设定的不同波长区分上述两种信息的量子态(简称密钥量子态和身份认证量子态)，其中，身份认证量子态对应的制备基遵循收发双发预置的基矢选择规则。

[0162] 例如，发送方要在时间点t_1、t_2...t_n发送长度为n的二进制比特串的量子态，该二进制比特串包含两部分，一部分是随机生成的经典二进制比特串，作为密钥比特串，另外一部分是与预先设定的基矢选择规则对应的身份认证比特串。发送方可以按照一定的策略选择小于n的随机数m，作为身份认证比特串的长度，然后再从1到n-m的自然数中随机选择自然数i，作为位于身份认证比特串之前的密钥比特串的长度，即，从位置i+1开始插入身份认证比特串，从而得到如下所示的二进制比特串，在该比特串中，$x_{i+1}\cdots x_{i+m}$为身份认证比特串，其余的为密钥比特串信息：

[0163] $x_1,x_2\cdots x_i,x_{i+1}\cdots x_{i+m},x_{i+m+1}\cdots x_n(x_i\in\{0,1\},=1,\cdots,n-)$

[0164] 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，$j_1,j_2,\cdots j_i$和$j_{i+m+1},\cdots j_n$是密钥比特串所对应的随机量子态制备基，$j_{i+1}\cdots j_{i+m}$是按照预先设定的基矢选择规则选取的身份认证比特串的量子态制备基。

[0165] 相应的，在后续步骤102中，接收方采用测量基序列$k_1,k_2\cdots k_i,k_{i+1}\cdots k_{i+m},k_{i+m+1}\cdots k_n$对接收的量子态进行测量，其中，$k_1,k_2,\cdots k_i$和$k_{i+m+1},\cdots k_n$为密钥量子态对应的随机量子态测量基，$k_{i+1}\cdots k_{i+m}$为身份认证量子态对应的测量基，该测量基也是按照预先设定的基矢选择规则选取的。

[0166] 在具体实施中，可以采用不同的策略设定收发双方设备遵循的基矢选择规则，例如，可以根据身份验证比特在量子态信息中的位置，选择相应的制备基或者测量基，在本实施例的一个具体例子中，设定了如下规则：根据每个身份验证比特在量子态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。

[0167] 仍沿用上述对二进制比特串的描述方式，令i+m＝1，那么在所述具体例子中，身份认证量子态所对应的制备基和测量基满足如下条件：

[0168] $$f(l)=\begin{cases}\text{水平偏振态H}, & l\bmod 4=0\\ \text{垂直偏振态V}, & l\bmod 4=1\\ +45^{\circ}\text{偏振态}+, & l\bmod 4=2\\ -45^{\circ}\text{偏振态}-, & l\bmod 4=3\end{cases}$$

[0169] 上面给出了预先设定的基矢选择规则的一个具体例子，在具体实施本技术方案时，可以为收发双方预置不同于上述规则的其他基矢选择规则，例如可以采用不同算法，只要收发双方采用同样的规则选择身份认证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。

[0170] 在本步骤中，发送方根据预先设定的基矢选择规则选择身份认证比特串的量子态制备基，然后采用预先设定的不同波长承载身份认证比特串的量子态、以及随机生成的密钥比特串的量子态，并将上述量子态发送给参与量子密钥分发过程的对端设备。由于身份认证比特串以随机的位置和长度穿插在所述密钥比特串中，从而可以有效避免身份认证信息被窃听，避免量子密钥分发过程中的中间人攻击和DDoS攻击。

[0171] 步骤102：接收方根据所述不同波长和基矢选择规则，对接收的量子态进行测量，当测量得到的身份认证信息与所述基矢选择规则相符时，从所述身份认证信息中选取接收方认证密钥、并发送所述密钥的位置信息以及采用所述密钥加密的预置共享密钥，否则结束本次量子密钥分发过程。

[0172] 在发送方执行步骤101发送量子态信息后，收发双方可以通过交互过程根据身份验证量子态的测量结果以及双方预置的共享密钥的验证，完成收发双方的身份认证过程，然后再按照量子密钥分配协议继续后续的密钥协商过程。为了提高密钥分发的执行效率，减少交互次数，本实施例提供一种在密钥协商各阶段穿插进行身份认证的优选实施方式。

[0173] 在本步骤中，接收方不仅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102-7，下面结合图2作进一步说明。

[0174] 步骤102-1：根据所述不同波长，区分身份认证量子态信息和密钥量子态信息。

[0175] 由于发送方采用不同的波长发送身份认证量子态和密钥量子态，因此接收方可以按照与发送方同样的波长设置，从接收到的量子态信息中区分上述两种信息。

[0176] 步骤102-2：随机选择密钥量子态信息的测量基，并按照预先设定的基矢选择规则选择身份认证量子态信息的测量基。

[0177] 对于密钥量子态部分，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，对于身份验证量子态部分，则按照预先设定的基矢选择规则选择相应的测量基，关于这部分内容，在步骤101中已经进行了相关说明，此处不再赘述。

[0178] 步骤102-3：测量接收到的量子态信息，获取身份认证信息。

[0179] 本步骤测量密钥量子态，获取关于密钥信息的原始测量结果。

[0180] 本步骤还使用在步骤102-2中按照预先设定的基矢选择规则选择的测量基，测量接收的身份认证量子态信息，考虑到量子信道可能存在衰减，因此将其中未探测到光子的部分剔除，获取测量得到的身份认证信息。

[0181] 步骤102-4：判断测量得到的身份认证信息与预先设定的基矢选择规则是否相符，

若相符执行步骤102-5，否则结束本次量子密钥分发过程。

[0182] 由于参与量子密钥分发过程的收发双方，针对身份认证信息预置了相同的基矢选择规则，发送方遵循该规则选取制备基发送身份认证信息的量子态，接收方也遵循该规则选择测量相应量子态的测量基，因此，在剔除因为衰减而未探测到的光子后，接收方测量得到的身份认证信息应该与对应的预期信息是一致的。

[0183] 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，可以认为发送方针对身份认证信息采用的基矢选择规则与自己是相同的，而只有身份合法的发送方才可能获知该规则，因此可以判定发送方通过身份认证。

[0184] 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遵循所述基矢选择规则的预期信息的差异小于预先设定的阈值，例如，测量结果与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。

[0185] 步骤102-5：从身份认证信息中选取接收方认证密钥。

[0186] 在上面的步骤102-4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发送方比对预置共享密钥的方式实现上述验证功能。接收方可以采用从量子态中获取的身份认证信息加密本地预置的共享密钥，并提供给发送方进行验证，也就是说直接采用身份认证信息作为所述接收方认证密钥IDkey。

[0187] 为了避免恶意中间人或者攻击者也仿照上述方式采用窃取的身份认证信息对窃取的共享密钥进行加密传输，因此接收方可以不直接使用所述身份认证信息作为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。

[0188] 步骤102-6：采用接收方认证密钥加密本地预置的共享密钥。

[0189] 接收方采用在步骤102-5中选取的IDkey，加密本地预置的共享密钥。

[0190] 为了在后续的量子密钥分发的其他阶段，例如：公布正确测量基时，依然能够对信息发布者的身份进行验证，进一步保证密钥分发过程的安全性，本实施例还提供一种优选实施方式：接收方采用IDkey加密的信息不仅包括所述预置共享密钥，还包括本地生成的辅助认证信息m。

[0191] 步骤102-7：通过经典信道发送所述接收方认证密钥的位置信息，以及加密后的密文，同时公开密钥量子态信息的测量基。

[0192] 接收方通过经典信道发送在步骤102-5中选取IDkey所对应的位置信息，以及执行步骤102-6得到的密文。

[0193] 同时按照量子密钥分配协议，还可以通过经典信道公开接收方测量密钥量子态所采用的测量基。

[0194] 步骤103：发送方根据接收的所述位置信息选取相应的发送方认证密钥，并判断采用所述密钥对接收的密文进行解密后的信息是否与本地的预置共享密钥一致，若不一致则

结束本次量子密钥分发过程。

[0195] 发送方通过经典信道接收到了接收方公开的测量基、选取IDkey的位置信息以及加密后的密文。

[0196] 发送方根据所述位置信息、以及自己在步骤101中发送的量子态信息，获得发送方认证密钥，即，发送方的IDkey。并采用所述IDkey解密接收到的密文，获取解密后的预置共享密钥和辅助认证信息。

[0197] 然后判断解密后的预置共享密钥是否与本地的预置共享密钥一致。对于发送方来说，如果用自己的IDkey解密接收方发送的密文、所得到的预置共享密钥信息与本地的预置共享密钥一致，一方面说明接收方的预置共享密钥与自己本地的预置共享密钥是相同的，而只有身份合法的接收方才可能具有该共享密钥，另一方面说明接收方遵循与自己相同的基矢选择规则选择测量基，并采用正确的IDkey执行的加密操作，从而发送方才能够解密出与本地一致的预置共享密钥，因此可以判定接收方通过身份认证。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。

[0198] 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。

[0199] 至此，通过上述步骤101-步骤103，接收方通过判断身份认证量子态信息是否符合基矢选择规则，验证了发送方的身份；发送方则通过预置共享密钥的比对，验证了接收方的身份。如果收发双方都通过了上述验证，那么后续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。

[0200] 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。

[0201] 1)发送方加密辅助认证信息的变体，并发送密文。

[0202] 在上述步骤103中发送方获取了解密后的辅助认证信息，当发送方验证接收方的身份合法后，可以先采用预设策略加密所述解密后的辅助认证信息的变体，然后在通过经典信道公布密钥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。

[0203] 所述预设策略可以是收发双方预置的，也可以是通过协商确定的。所述预设策略包括：采用预置共享密钥执行加密操作；或者，采用IDkey执行加密操作。

[0204] 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。

[0205] 2)接收方接收所述正确测量基和所述密文后，通过解密密文验证发送方身份。

[0206] 首先，接收方采用与发送方所采用的预设策略对应的方式，解密接收到的密文，例如，发送方采用IDkey执行的加密操作，则接收方也采用自己的IDkey执行解密操作；若发送方采用本地的预置共享密钥执行的加密操作，则接收方也采用本地的预置共享密钥执行解密操作。

[0207] 然后，判断执行所述解密操作后得到的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，通过经典信息以加密形式发送给

发送方，发送方解密还原后，又采用预设策略加密该信息的变体，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，而且其采用的加密方式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量子态的正确测量基是可信的。

[0208] 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。

[0209] 需要说明的是，发送方也可以采用动态变化的算法或者函数计算解密得到的辅助认证信息的变体，只要接收方知道计算所述变体的相应规则即可，同样可以实现本技术方案，而且能够进一步提高安全性。例如，发送方第一次采用如下方式计算所述变体：辅助认证信息+1，接收方则将解密后的信息与本地原始生成的辅助认证信息m的变体m+1进行比较；发送方第二次采用如下方式计算所述变体：辅助认证信息+2，接收方则将解密后的信息与本地原始生成的辅助认证信息m的变体m+2进行比较。

[0210] 3)发送方估算误码率后，用IDkey加密误码率并发送给接收方。

[0211] 所述发送方根据所述接收方公布的部分密钥量子态的测量结果，估算误码率，若误码率在一定的阈值范围内，就利用纠错技术进行纠错，然后进一步对纠错过的量子密钥进行隐私放大，从而消除通信过程和纠错过程中导致的信息泄露，最后提取到无条件安全的共享量子密钥。若误码率超过一定阈值，则放弃本次量子密钥分发过程。

[0212] 如果误码率没有超出阈值，那么发送方在完成上述操作后，可以将误码率发送给接收方，供接收方参考，以保证双方做出相同的判断、以及基于相同的策略执行后续的隐私放大等处理操作，从而获取相同的共享量子密钥。为了避免中间人或者攻击者窃取误码率信息，发送方可以采用IDkey加密所述误码率，并将加密后的信息发送给所述接收方。

[0213] 4)接收方解密接收到的信息，获取误码率，并执行相应的处理。

[0214] 接收方收到误码率的密文后，采用IDkey解密该信息，获取发送方估算的误码率，接收方可以根据该误码率执行与发送方同样的操作，也可以将自己估算的误码率与发送方发送的误码率进行比较，如果两者的差异在预先设定的范围内，也就说收发双方基于误码率的判断结果和后续处理策略都是相同的，则接收方可以继续执行后续操作，最终获取与发送方相同的无条件安全的共享量子密钥。

[0215] 至此，通过上述步骤101-103，在量子密钥分发过程中实现了对收发双方的身份认证。本技术方案采用不同波长区分密钥信息和身份认证信息，在密钥量子态中随机穿插长度可变的身份认证信息的量子态，收发双方通过检测对端设备在选择制备基或测量基时是否遵循同样的基矢选择规则，以及对端设备是否具有相同的预置共享密钥，从而完成身份认证过程。由于本技术方案充分利用了量子的安全性、通过量子态信息进行身份认证，而且不需要收发双方预置相同的身份认证信息，实现了量子态零知识证明身份验证方法，不仅可以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，而且不会造成量子密钥分发量的降低。

[0216] 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3，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，本实施例与上面第一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：

[0217] 步骤301：根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用预先设定的不同波长向参与量子密钥分发过程的对端设备发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中。

[0218] 在本步骤之前，可以先向所述对端设备发送量子密钥协商请求，所述请求中包含发送方的账户信息，供对端设备验证自己的身份，随后可以接收所述对端设备发送的账户信息，并根据所述账户信息验证对方的身份，若验证失败，则结束本次量子密钥分发过程；若验证成功，则可以执行本步骤进行量子态的发送。

[0219] 所述预先设定的基矢选择规则包括：根据身份验证比特在量子态信息中的位置，选择相应的制备基，例如，根据每个身份验证比特在量子态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。

[0220] 步骤302：接收所述对端设备返回的认证密钥位置信息和待验证密文。

[0221] 作为一种优选实施方式，本方法可以在量子密钥分发过程中穿插执行，在这种方式下，所述对端设备返回的信息不仅包括：认证密钥位置信息和待验证密文，还包括：测量密钥量子态所采用的测量基。

[0222] 步骤303：根据所述位置信息和已发送的量子态信息，选取认证密钥，并采用所述认证密钥对接收的待验证密文进行解密。

[0223] 步骤304：判断解密后的信息是否与本地的预置共享密钥一致，若不一致，则结束本次量子密钥分发过程。

[0224] 如果本步骤的判断结果为是，则可以按照量子密钥分配协议继续执行后续的操作：

[0225] 确定密钥量子态的正确测量基，筛选原始密钥；

[0226] 通过经典信道公布所述密钥量子态的正确测量基；

[0227] 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。

[0228] 如果在步骤302中还接收到了接收方发送的辅助认证信息，那么在本步骤的判断结果为“是”时，还可以加密所述辅助认证信息的变体，在上述公布正确测量基的同时，发送所述辅助认证信息的变体的密文，供接收方做进一步的验证；此外，在估算误码率后，还可以采用步骤303选取的认证密钥加密所述误码率，并将其发送给接收方。

[0229] 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4，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。

[0230] 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401，用于根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用预先设定的

不同波长向参与量子密钥分发过程的对端设备发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中；响应信息接收单元402，用于接收所述对端设备返回的认证密钥位置信息和待验证密文；信息解密单元403，用于根据所述位置信息和已发送的量子态信息，选取认证密钥，并采用所述认证密钥对接收的待验证密文进行解密；发送方认证判断单元404，用于判断解密后的信息是否与本地的预置共享密钥一致；若否，则结束本次量子密钥分发过程。

[0231] 可选的，所述响应信息接收单元接收到的信息不仅包括：认证密钥位置信息和待验证密文，还包括：测量密钥量子态所采用的测量基；

[0232] 相应的，所述装置还包括：

[0233] 原始密钥筛选单元，用于当所述认证判断单元的输出结果为是时，确定密钥量子态的正确测量基，并筛选原始密钥；

[0234] 正确测量基公布单元，用于通过经典信道公布所述密钥量子态的正确测量基；

[0235] 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。

[0236] 可选的，所述装置还包括：

[0237] 协商请求发送单元，用于向所述对端设备发送量子密钥协商请求，所述请求中包含发送方的账户信息；

[0238] 账户信息接收单元，用于接收所述对端设备发送的账户信息；

[0239] 第一身份认证单元，用于根据所述账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程。

[0240] 可选的，所述量子态发送单元采用的预先设定的基矢选择规则包括：根据身份验证比特在量子态信息中的位置，选择相应的制备基。

[0241] 可选的，所述量子态发送单元采用的预先设定的基矢选择规则是指，根据每个身份验证比特在量子态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。

[0242] 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5，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，本实施例与上面第一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：

[0243] 步骤501：接收参与量子密钥分发过程的对端设备发送的量子态。

[0244] 在本步骤之前，可以接收所述对端设备发送的密钥协商请求，并根据所述请求中包含的账户信息验证对方的身份，若验证失败，则结束本次量子密钥分发过程；若验证成功，向所述对端设备发送接收方的账户信息，并可以执行本步骤接收所述对端设备发送的量子态。

[0245] 步骤502：按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息。

[0246] 所述预先设定的基矢选择规则包括：根据身份验证比特在量子态信息中的位置，选择相应的测量基，例如，根据每个身份验证比特在量子态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。

[0247] 具体说，本步骤包括以下处理过程：根据所述预先设定的不同波长，区分身份认证量子态信息和密钥量子态信息；按照所述预先设定的基矢选择规则选择身份认证量子态信息的测量基；使用所选测量基测量所述身份认证量子态信息，并剔除其中未探测到光子的部分，获取所述身份认证信息。

[0248] 步骤503：判断所述身份认证信息与所述基矢选择规则是否相符，若相符，执行步骤504，否则，结束本次的量子密钥分发过程。

[0249] 步骤504：从所述身份认证信息中选取认证密钥、并向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥。

[0250] 所述从所述身份认证信息中选取认证密钥，包括：选取所述身份认证信息作为所述认证密钥；或者，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认证密钥。

[0251] 在本步骤中，还可以用所述认证密钥加密本地生成的辅助认证信息m，并将加密后的密文与所述位置信息和加密后的预置共享密钥一起发送给所述对端设备。

[0252] 本身份认证方法可以在量子密钥分发过程中穿插执行，因此本步骤还可以通过经典信道公开测量密钥量子态所采用的测量基。

[0253] 在本步骤之后，还可以执行下述操作：

[0254] 1)接收所述对端设备通过经典信道发送的所述密钥量子态的正确测量基。

[0255] 如果同时还接收到了辅助认证信息的变体的密文，则执行解密操作，并验证所述辅助认证信息的变体是否与本地原始生成的辅助认证信息的变体一致，若一致，执行后续筛选原始密钥等操作，否则，结束本次量子密钥分发过程。

[0256] 2)筛选原始密钥，并通过获取误码率、纠错和隐私放大过程，获取最终的共享量子密钥。

[0257] 如果在筛选原始密钥后，接收到发送方发送的误码率密文，则可以采用步骤504选取的认证密钥解密，并根据该结果，执行后续的纠错、隐私放大等过程，获取最终的共享量子密钥。

[0258] 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6，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。

[0259] 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601，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；量子态测量单元602，用于按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息；接收方认证判断单元603，用于判断所述身份认证信息与所述基矢选择规则是否相符，若否，则结束本次量子密钥分发过程；信息发送单元604，用于当所述接收方认证判断单元的输出为是时，从所述身份认证信息中选取认证密钥、并向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥。

[0260] 可选的，所述装置还包括：

[0261] 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，通过经典信道公开测量密钥量子态所采用的测量基；

[0262] 相应的，所述装置还包括：

[0263] 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量子态的正确测量基；

[0264] 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。

[0265] 可选的，所述装置还包括：

[0266] 协商请求接收单元，用于接收所述对端设备发送的密钥协商请求；

[0267] 第二身份认证单元，用于根据所述请求中包含的账户信息验证所述对端设备的身份，若验证失败，结束本次量子密钥分发过程，否则向所述对端设备发送接收方的账户信息。

[0268] 可选的，所述量子态测量单元采用的预先设定的基矢选择规则包括：根据身份认证比特在量子态信息中的位置，选择相应的制备基。

[0269] 可选的，所述量子态测量单元采用的预先设定的基矢选择规则是指，根据每个身份认证比特在量子态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。

[0270] 可选的，所述量子态测量单元包括：

[0271] 信息区分子单元，用于根据所述预先设定的不同波长，区分身份认证量子态信息和密钥量子态信息；

[0272] 身份认证测量基选择子单元，用于按照所述预先设定的基矢选择规则选择身份认证量子态信息的测量基；

[0273] 身份认证信息获取子单元，用于使用所选测量基测量所述身份认证量子态信息，并剔除其中未探测到光子的部分，获取所述身份认证信息。

[0274] 可选的，所述信息发送单元包括：

[0275] 认证密钥选取子单元，用于从所述身份认证信息中选取认证密钥；

[0276] 信息发送子单元，用于向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥；

[0277] 其中，所述认证密钥选取子单元具体用于，

[0278] 选取所述身份认证信息作为所述认证密钥；或者，

[0279] 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认证密钥。

[0280] 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7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701，以及部署于接收方量子通信设备的身份认证装置702；所述部署于收发双方量子通信设备的身份认证装置，预置了相同的基矢选择规则、相同的共享密钥，并采用相同的、用于区分身份认证信息和密钥信息的波长设置。

[0281] 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。下面结合附图8，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。

[0282] 1)A向B发送密钥协商请求，请求中携带A的账户信息；

[0283] 2)B验证A身份的合法性，向A发送B的账户信息；

[0284] 3)A据接收到的账户信息验证B身份的合法性；A按照预先设定的基矢选择规则选择身份认证比特串的制备基、并采用不同波长发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中；

[0285] 4)B根据所述不同波长和基矢选择规则，对接收的量子态进行测量，当测量得到的身份认证信息与所述基矢选择规则相符时，从所述身份认证信息中选取接收方认证密钥IDkey、发送所述密钥的位置信息以及采用所述密钥加密的预置共享密钥和本地辅助认证信息m、并公开密钥量子态的测量基，否则结束本次量子密钥分发过程。

[0286] 5)A根据接收的所述位置信息选取相应的发送方认证密钥，并判断采用所述密钥对接收的密文进行解密后的预置共享密钥是否与本地的预置共享密钥一致，若一致，筛选原始密钥、公布密钥量子态的正确测量基、以及获取的辅助认证信息的变体的密文，若不一致则结束本次量子密钥分发过程；

[0287] 6)B解密辅助认证信息的变体的密文，若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；

[0288] 7)A通过计算误码率、纠错、隐私放大，获取最终的共享量子密钥，并将用IDkey加密的误码率发送给B；B解密接收到的误码率，并根据该误码率执行相应的纠错、隐私放大，获取最终的共享量子密钥。

[0289] 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，在环节4)进行B对A的身份认证、以及环节5)进行A对B的身份认证的过程中，可以不采用辅助认证信息m，也不在后续环节继续利用m的变体信息进行身份认证，也可以不利用IDkey对误码率进行加、解密操作等。只要在3)、4)、5)环节利用身份认证量子态是否符合基矢选择规则，以及双方预置的共享密钥是否一致，完成A与B之间的相互认证，就不偏离本申请的核心，都在本申请的保护范围之内。

[0290] 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。

[0291] 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。

[0292] 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。

[0293] 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。

[0294] 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。

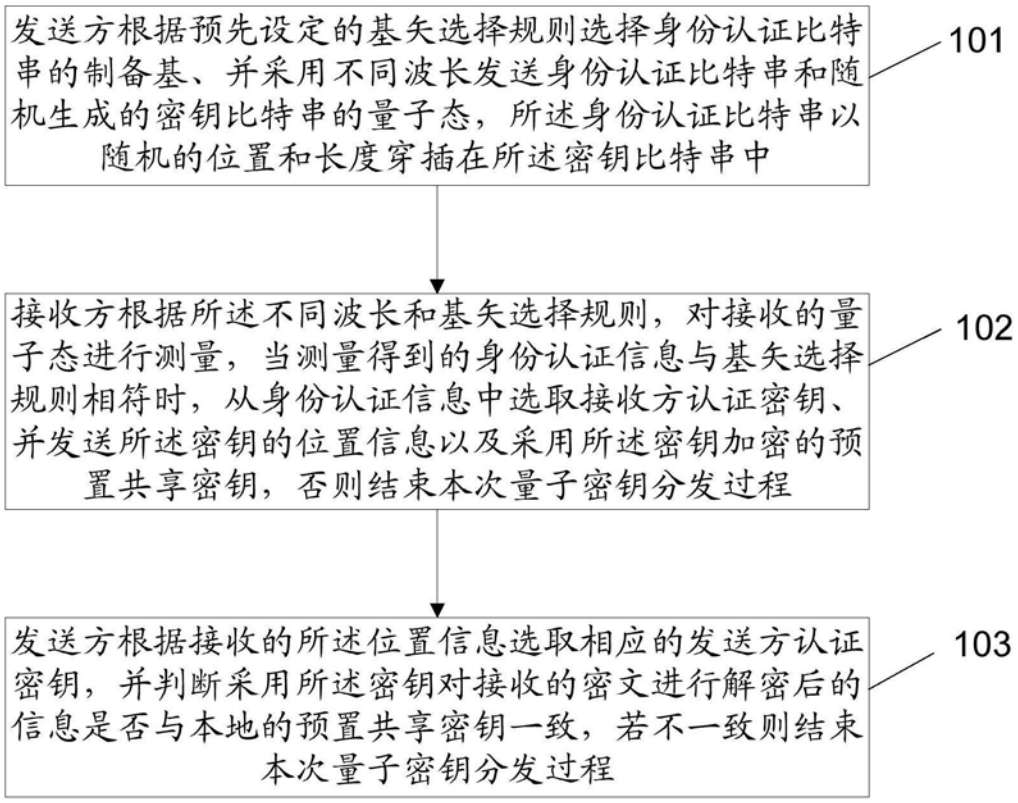

发送方根据预先设定的基矢选择规则选择身份认证比特串的制备基、并采用不同波长发送身份认证比特串和随机生成的密钥比特串的量子态，所述身份认证比特串以随机的位置和长度穿插在所述密钥比特串中
101
接收方根据所述不同波长和基矢选择规则，对接收的量子态进行测量，当测量得到的身份认证信息与基矢选择规则相符时，从身份认证信息中选取接收方认证密钥、并发送所述密钥的位置信息以及采用所述密钥加密的预置共享密钥，否则结束本次量子密钥分发过程
102
发送方根据接收的所述位置信息选取相应的发送方认证密钥，并判断采用所述密钥对接收的密文进行解密后的信息是否与本地的预置共享密钥一致，若不一致则结束本次量子密钥分发过程
103

图1

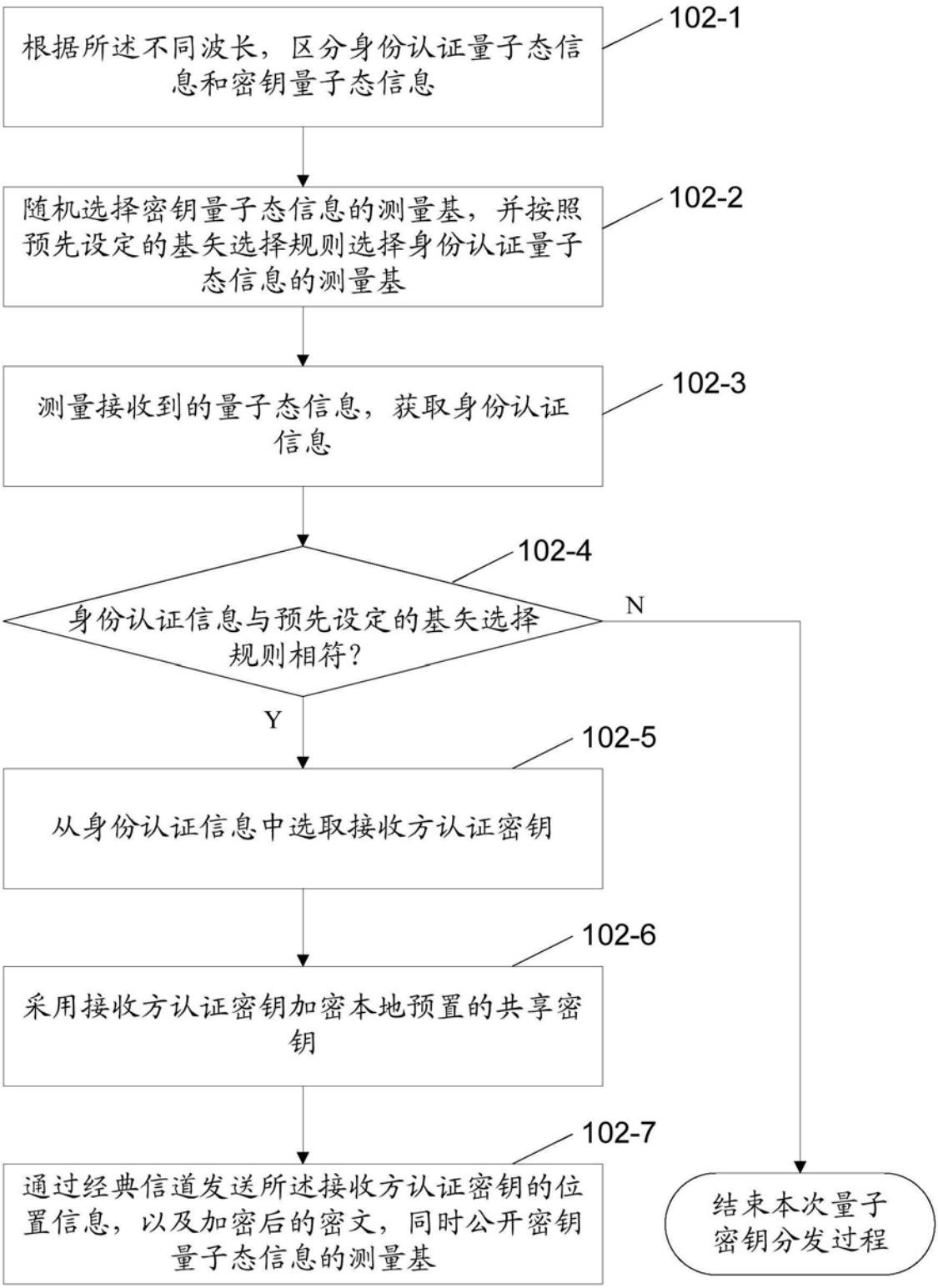

根据所述不同波长，区分身份认证量子态信息和密钥量子态信息
102-1
随机选择密钥量子态信息的测量基，并按照预先设定的基矢选择规则选择身份认证量子态信息的测量基
102-2
测量接收到的量子态信息，获取身份认证信息
102-3
身份认证信息与预先设定的基矢选择规则相符？
102-4
N
Y
从身份认证信息中选取接收方认证密钥
102-5
采用接收方认证密钥加密本地预置的共享密钥
102-6
通过经典信道发送所述接收方认证密钥的位置信息，以及加密后的密文，同时公开密钥量子态信息的测量基
102-7
结束本次量子密钥分发过程

图2

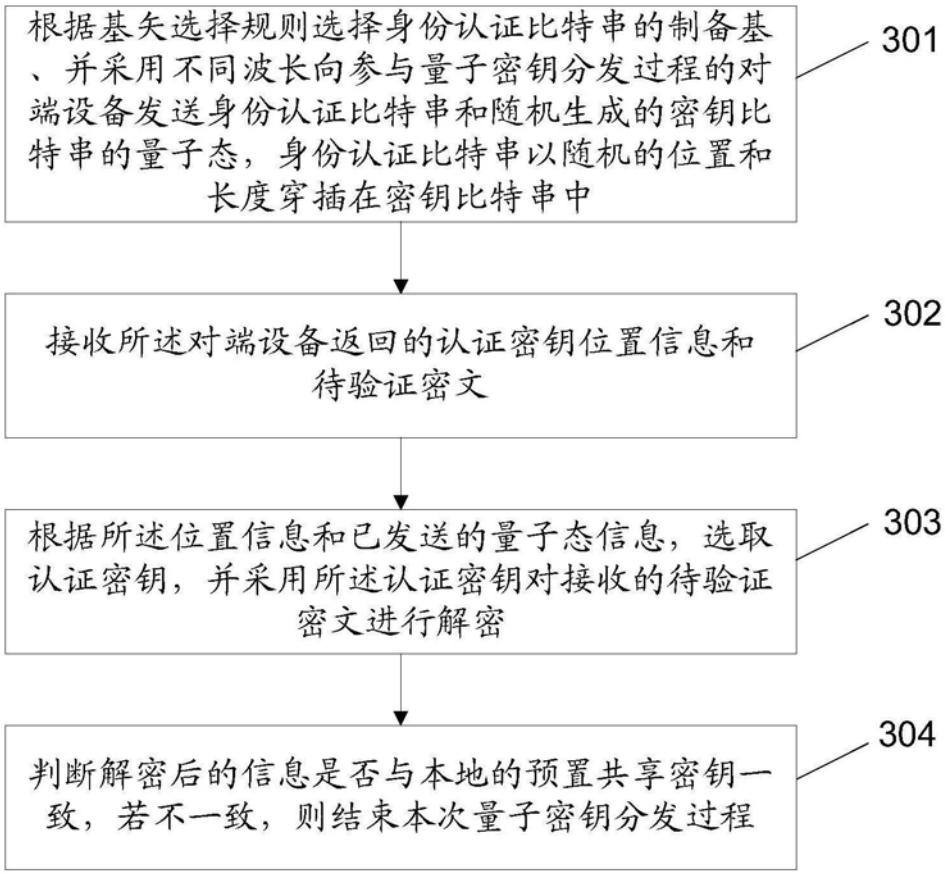

根据基矢选择规则选择身份认证比特串的制备基、并采用不同波长向参与量子密钥分发过程的对端设备发送身份认证比特串和随机生成的密钥比特串的量子态，身份认证比特串以随机的位置和长度穿插在密钥比特串中
301
接收所述对端设备返回的认证密钥位置信息和待验证密文
302
根据所述位置信息和已发送的量子态信息，选取认证密钥，并采用所述认证密钥对接收的待验证密文进行解密
303
判断解密后的信息是否与本地的预置共享密钥一致，若不一致，则结束本次量子密钥分发过程
304

图3

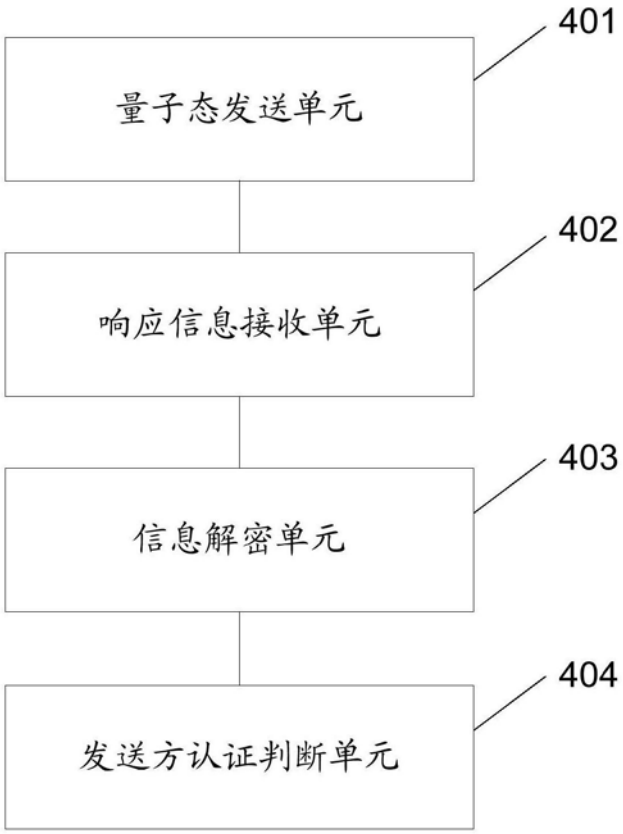


图4

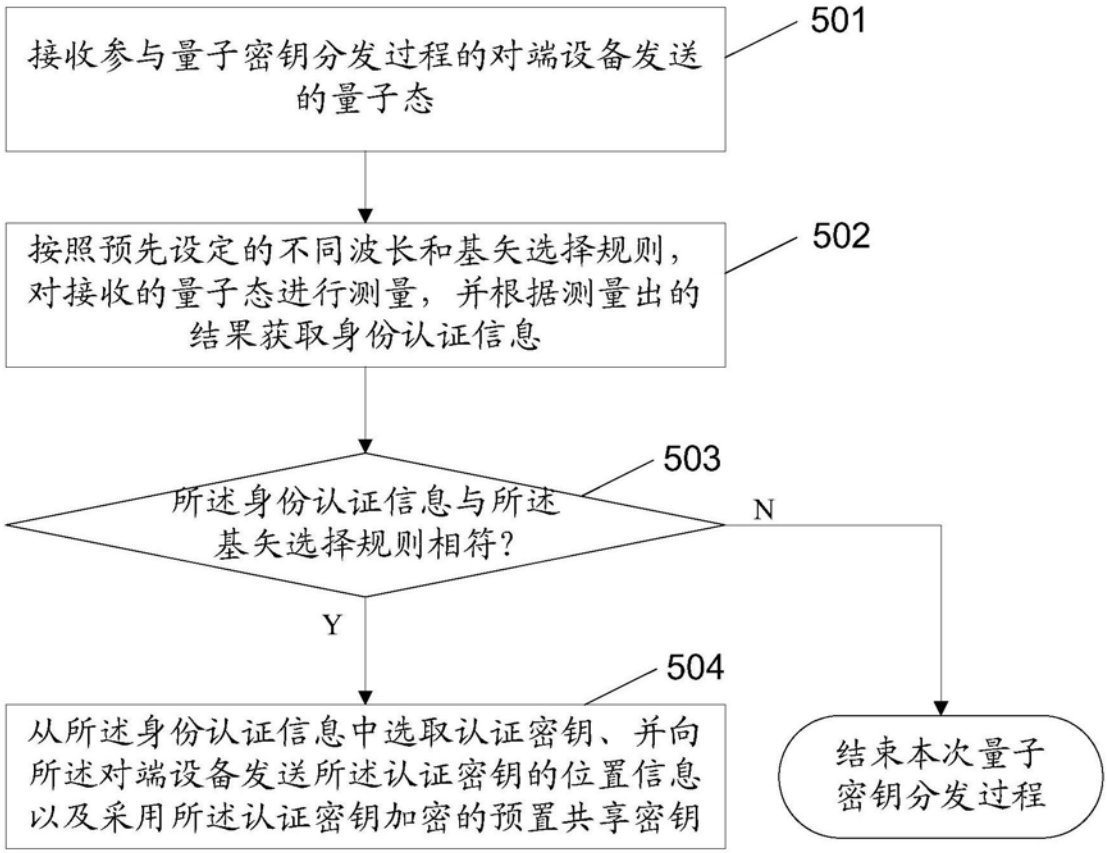

接收参与量子密钥分发过程的对端设备发送的量子态
501
按照预先设定的不同波长和基矢选择规则，对接收的量子态进行测量，并根据测量出的结果获取身份认证信息
502
所述身份认证信息与所述基矢选择规则相符?
503
N
Y
从所述身份认证信息中选取认证密钥、并向所述对端设备发送所述认证密钥的位置信息以及采用所述认证密钥加密的预置共享密钥
504
结束本次量子密钥分发过程

图5

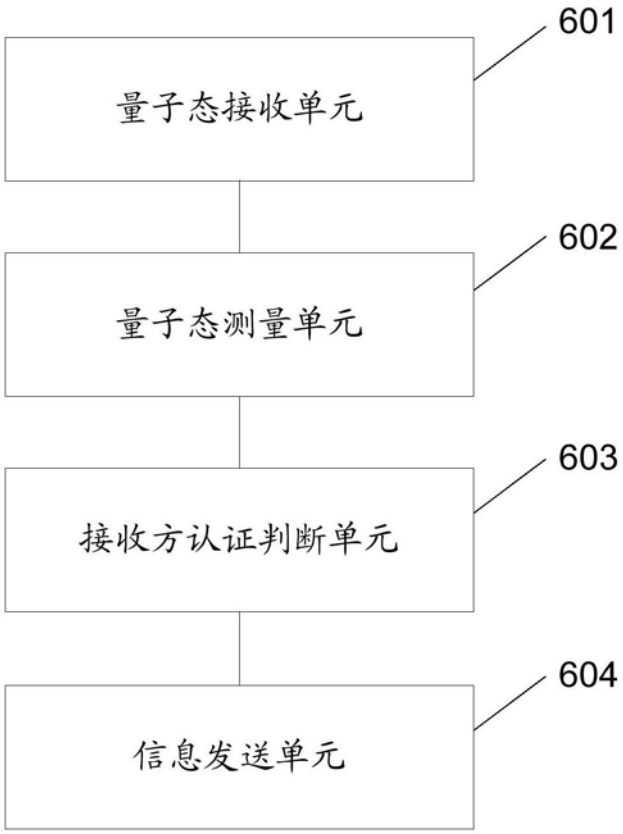

601
量子态接收单元
602
量子态测量单元
603
接收方认证判断单元
604
信息发送单元

图6

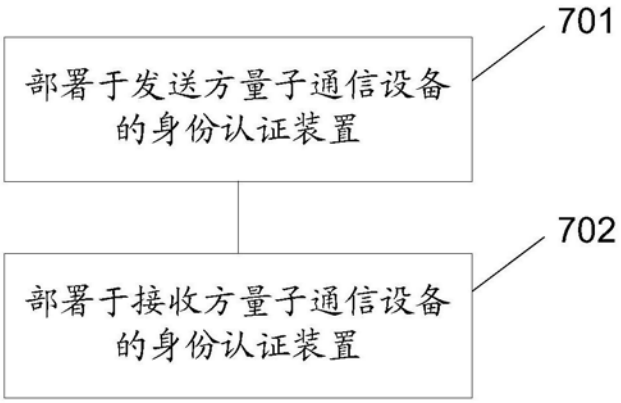

701
部署于发送方量子通信设备的身份认证装置
702
部署于接收方量子通信设备的身份认证装置

图7

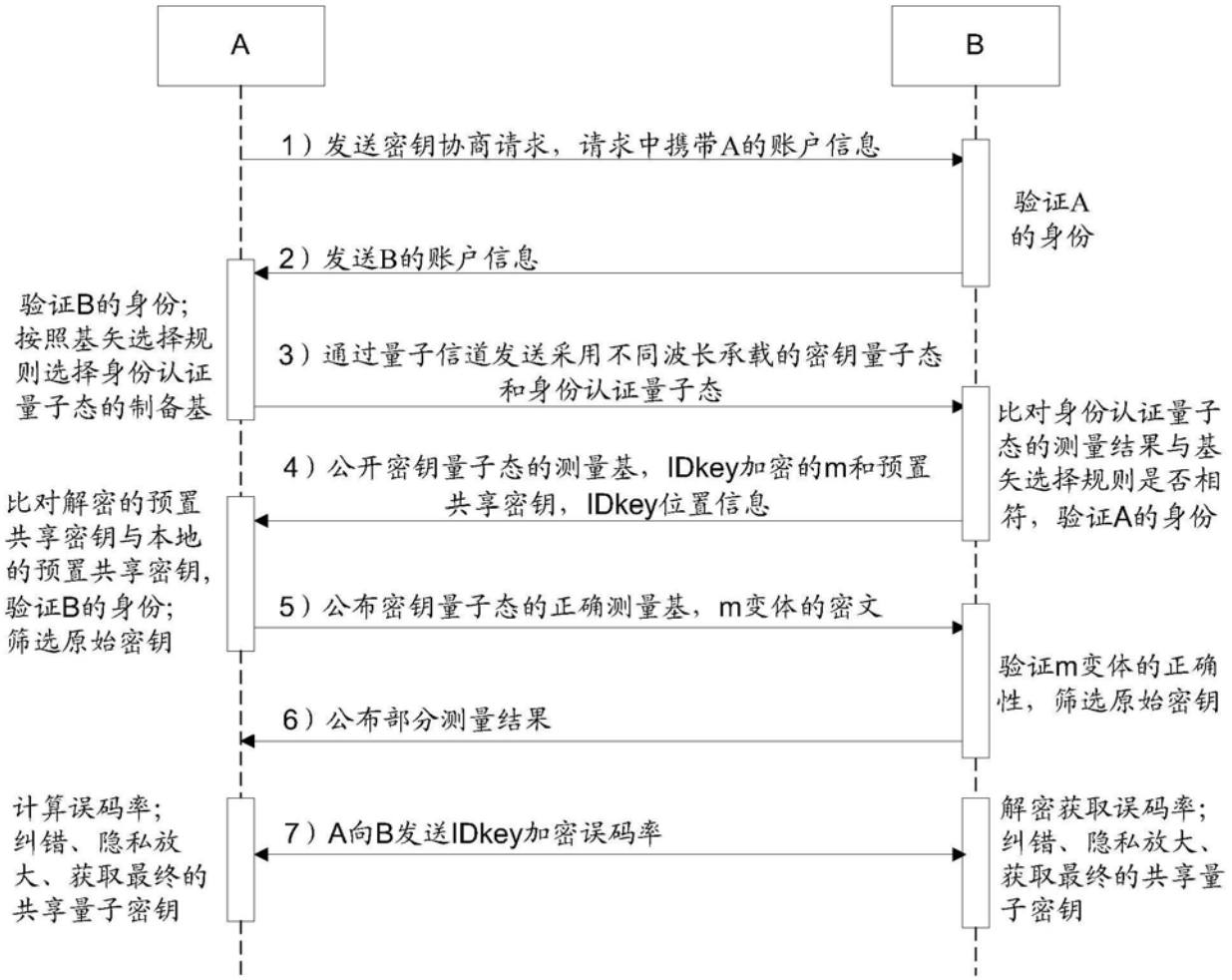

A
B
1）发送密钥协商请求，请求中携带A的账户信息
验证A的身份
2）发送B的账户信息
验证B的身份；按照基矢选择规则选择身份认证量子态的制备基
3）通过量子信道发送采用不同波长承载的密钥量子态和身份认证量子态
比对身份认证量子态的测量结果与基矢选择规则是否相符，验证A的身份
4）公开密钥量子态的测量基，IDkey加密的m和预置共享密钥，IDkey位置信息
比对解密的预置共享密钥与本地的预置共享密钥，验证B的身份；筛选原始密钥
5）公布密钥量子态的正确测量基，m变体的密文
验证m变体的正确性，筛选原始密钥
6）公布部分测量结果
计算误码率；纠错、隐私放大、获取最终的共享量子密钥
7）A向B发送IDkey加密误码率
解密获取误码率；纠错、隐私放大、获取最终的共享量子密钥

图8