[19] Patents Registry
The Hong Kong Special Administrative Region
香港特別行政區
專利註冊處

[11] 1237156 B
CN 106656907 B

[12] **STANDARD PATENT (R) SPECIFICATION**
轉錄標準專利說明書

[21] Application no. 申請編號
17111024.8

[22] Date of filing 提交日期
30.10.2017

[51] Int. Cl.
H04L 29/06 (2006.01) H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

[54] AUTHENTICATION METHOD, APPARATUS, TERMINAL DEVICE AND SYSTEM
用於認證的方法、裝置、終端設備及系統

[43] Date of publication of application 申請發表日期
06.04.2018

[45] Date of publication of grant of patent 批予專利的發表日期
13.08.2021

CN Application no. & date 中國專利申請編號及日期
CN 201510713589.4 28.10.2015

CN Publication no. & date 中國專利申請發表編號及日期
CN 106656907 10.05.2017

Date of grant in designated patent office 指定專利當局批予專利日期
02.03.2021

[73] Proprietor 專利所有人
Alibaba Group Holding Limited
阿里巴巴集团控股有限公司
開曼群島
英属开曼群岛
大开曼资本大厦一座四层 847 号邮箱

[72] Inventor 發明人
FU, Yingfang 付颖芳

[74] Agent and / or address for service 代理人及/或送達地址
三友知識產權代理有限公司
香港
灣仔駱克道 160-174 號
越秀大廈 6 樓 601 室

(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 106656907 B
(45)授权公告日 2021.03.02

(21)申请号 201510713589.4

(22)申请日 2015.10.28

(65)同一申请的已公布的文献号
申请公布号 CN 106656907 A

(43)申请公布日 2017.05.10

(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 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 102946313 A,2013.02.27
CN 104579694 A,2015.04.29
CN 101741852 A,2010.06.16
CN 101222488 A,2008.07.16
US 2015288542 A1,2015.10.08
US 2008114983 A1,2008.05.15
谢巧玲."基于动态口令的双向身份认证识别系统的设计与实现".《中国优秀硕士学位论文全文数据库 信息科技辑》.2009,
谢巧玲."基于动态口令的双向身份认证识别系统的设计与实现".《中国优秀硕士学位论文全文数据库 信息科技辑》.2009,

审查员 曾康玲

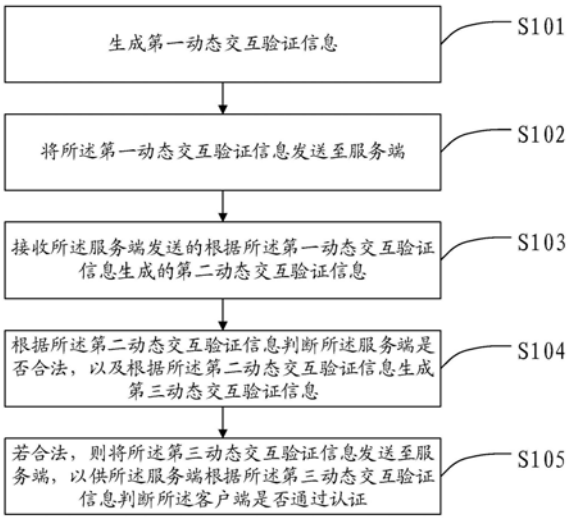
权利要求书12页 说明书33页 附图4页

(54)发明名称

用于认证的方法、装置、终端设备及系统

(57)摘要

本申请提供一种用于客户端的认证方法,首先客户端生成第一动态交互验证信息;然后将所述第一动态交互验证信息发送至服务端;再接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息;然后根据所述第二动态交互验证信息判断所述服务端是否合法,以及根据所述第二动态交互验证信息生成第三动态交互验证信息;若合法,则将所述第三动态交互验证信息发送至服务端,以供所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证。本方法的客户端和服务端均动态的利用对方的验证信息制作本方验证信息,再发给对方进行验证,实现了客户端与服务端的交互认证,可以防范假冒的服务器欺骗合法用户和抵御中间人攻击。



CN 106656907 B

1.一种用于客户端的认证方法,其特征在于,包括:

生成第一动态交互验证信息;

将所述第一动态交互验证信息发送至服务端;

接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息;

根据所述第二动态交互验证信息判断所述服务端是否合法,以及根据所述第二动态交互验证信息生成第三动态交互验证信息;

若合法,则将所述第三动态交互验证信息发送至服务端,以供所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证;

其中,所述第一动态交互验证信息、第二动态交互验证信息和第三动态交互验证信息采用量子态处理,所述第一动态交互验证信息包括:量子制备基标识和第一量子比特串长度;所述第二动态交互验证信息包括:根据所述第一量子比特串长度,通过所述量子态制备基标识在量子态库中查询的量子态制备基,生成的第一量子比特串;所述第三动态交互验证信息包括:随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量获得的比特值测量结果。

2.根据权利要求1所述的用于客户端的认证方法,其特征在于,客户端和所述服务端上均预先存储有相应的或相同的信息处理方法,所述客户端根据所述信息处理方法对动态交互验证信息的处理结果与所述服务端对所述动态交互验证信息的处理结果是相应的或相同的;

所述根据所述第二动态交互验证信息判断所述服务端是否合法的步骤,包括:

根据预先存储的信息处理方法对所述第二动态交互验证信息进行处理,根据处理结果是否符合预期判断所述服务端是否合法。

3.根据权利要求2所述的用于客户端的认证方法,其特征在于,所述客户端和所述服务端上均预先存储有多组相应的或相同的信息处理方法,且每组所述信息处理方法在所述客户端和所述服务端上均具有相应或相同的信息处理方法标识;

所述动态交互验证信息中包含有信息处理方法标识;

所述根据预先存储的信息处理方法对所述第二动态交互验证信息进行处理,根据处理结果判断所述服务端是否合法的步骤,包括:

根据所述第一动态交互验证信息中的信息处理方法标识查询对应的预先存储的信息处理方法;

根据所述信息处理方法对所述第二动态交互验证信息进行处理,根据处理结果是否符合预期判断所述服务端是否合法。

4.根据权利要求3所述的用于客户端的认证方法,其特征在于,所述信息处理方法标识在所述客户端与所述服务端之间同步且定时变更。

5.根据权利要求1所述的用于客户端的认证方法,其特征在于,客户端和所述服务端上均预先存储有相同的含有量子态制备基的量子态库,所述量子态制备基用于制备量子比特串或测量量子比特串,每个所述量子态制备基均有对应的量子态制备基标识,

所述根据所述第二动态交互验证信息判断所述服务端是否合法的步骤,包括:

采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值

进行测量，获得比特值测量结果；根据所述比特值测量结果是否符合预期判断所述服务端是否合法。

6.根据权利要求5所述的用于客户端的认证方法，其特征在于，所述生成第一动态交互验证信息的步骤，包括：

从量子态库中选择至少一种量子态制备基；

提取所述量子态制备基的量子态制备基标识；

生成包含所述量子态制备基标识的第一动态交互验证信息。

7.根据权利要求6所述的用于客户端的认证方法，其特征在于，所述从量子态库中选择至少一种量子态制备基采用随机选择的方式，每一次认证选择的量子态制备基均不相同。

8.根据权利要求5所述的用于客户端的认证方法，其特征在于，所述第一量子比特串通过所述量子态制备基发送至客户端。

9.根据权利要求7所述的用于客户端的认证方法，其特征在于，所述第二动态交互验证信息还包括将所述第一量子比特串进行十进制转换后获得的十进制第一量子比特串；

所述根据所述第二动态交互验证信息判断所述服务端是否合法的步骤，包括：

采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量，获得比特值测量结果；

将所述十进制第一量子比特串按照十进制转换方法转换为转换后的第一量子比特串；

测量所述第一量子比特串的长度，获得比特串长度测量结果，其中所述第一量子比特串的长度是根据所述第一量子比特串长度生成的；

根据所述比特值测量结果是否符合预期和所述比特串长度测量结果是否符合预期判断所述服务端是否合法。

10.根据权利要求5所述的用于客户端的认证方法，其特征在于，所述客户端与所述服务端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息

还包括第一量子比特串长度代码；

所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在量子态库中查询相应的量子态制备基、根据所述第一量子比特串长度代码在量子串长度数据库中查询相应的第一量子比特串长度，然后根据所述第一量子比特串长度通过所述量子态制备基生成第一量子比特串，所述第一量子比特串通过所述量子态制备基发送至客户端。

11.根据权利要求5所述的用于客户端的认证方法，其特征在于，所述采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量的步骤，包括：

在量子态库中查找与所述量子态制备基标识对应的量子态制备基；

随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量。

12.根据权利要求5所述的用于客户端的认证方法，其特征在于，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的代码及第二量子比特串长度；

所述根据所述第二动态交互验证信息生成第三动态交互验证信息的步骤，包括：

在量子态库中查询与所述服务端选择的量子态制备基的代码相对应的量子态制备基；

根据所述第二量子比特串长度，通过所述量子态制备基生成第二量子比特串；

生成包含所述第二量子比特串的第三动态交互验证信息。

13.根据权利要求12所述的用于客户端的认证方法，其特征在于，所述根据所述第二动态交互验证信息生成第三动态交互验证信息的步骤，还包括：将所述第二量子比特串按照十进制转换方法进行转换，获得十进制第二量子比特串；

所述生成包含所述第二量子比特串的第三动态交互验证信息的步骤，包括：

生成包含所述第二量子比特串和所述十进制第二量子比特串的第三动态交互验证信息。

14.根据权利要求12或13所述的用于客户端的认证方法，其特征在于，所述若合法，则将所述第三动态交互验证信息发送至服务端的步骤，包括：

若合法，则将所述第二量子比特串采用所述量子态制备基发送至服务端。

15.根据权利要求5所述的用于客户端的认证方法，其特征在于，所述客户端的量子态库与所述服务端的量子态库同步且按照预定的规则定时变更。

16.根据权利要求1所述的用于客户端的认证方法，其特征在于，所述第一动态交互验证信息包括客户端的身份标识，所述身份标识用于服务端对所述客户端进行初步认证。

17.根据权利要求16所述的用于客户端的认证方法，其特征在于，所述客户端的身份标识包括客户端的用户识别码和身份证书。

18.根据权利要求1所述的用于客户端的认证方法，其特征在于，所述将所述第一动态交互验证信息发送至服务端的步骤，包括：

将全部或部分所述第一动态交互验证信息采用密钥加密后发送至服务端；

所述若合法，则将所述第三动态交互验证信息发送至服务端的步骤，包括：

若合法，则将全部或部分所述第三动态交互验证信息采用密钥加密后发送至服务端。

19.根据权利要求18所述的用于客户端的认证方法，其特征在于，所述密钥与所述服务端解密使用的密钥互为对称量子密钥，或互为公私密钥。

20.根据权利要求1所述的用于客户端的认证方法，其特征在于，所述接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息的步骤，包括：

接收所述服务端发送的至少部分信息已加密的根据所述第一动态交互验证信息生成的第二动态交互验证信息；

采用与所述服务端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

21.根据权利要求20所述的用于客户端的认证方法，其特征在于，所述解密密钥与所述服务端加密使用的密钥互为对称量子密钥，或互为公私密钥。

22.一种用于客户端的认证装置，其特征在于，包括：

第一动态交互验证信息生成单元，用于生成第一动态交互验证信息，所述第一动态交互验证信息包括：量子制备基标识和第一量子比特串长度；

第一动态交互验证信息发送单元，用于将所述第一动态交互验证信息发送至服务端；

第二动态交互验证信息接收单元，用于接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息，所述第二动态交互验证信息包括：根据所述第一量子比特串长度，通过所述量子态制备基标识在量子态库中查询的量子态制备基，生成的第一量子比特串；

第二动态交互验证信息验证单元，用于根据所述第二动态交互验证信息判断所述服务端是否合法，以及根据所述第二动态交互验证信息生成第三动态交互验证信息，所述第三

动态交互验证信息包括:随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量获得的比特值测量结果;

第三动态交互验证信息发送单元,用于若合法,则将所述第三动态交互验证信息发送至服务端,以供所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证。

23.根据权利要求22所述的用于客户端的认证装置,其特征在于,客户端和所述服务端上均预先存储有相应的或相同的信息处理方法,所述客户端根据所述信息处理方法对动态交互验证信息的处理结果与所述服务端对所述动态交互验证信息的处理结果是相应的或相同的;

所述第二动态交互验证信息验证单元包括:

处理判断子单元,用于根据预先存储的信息处理方法对所述第二动态交互验证信息进行处理,根据处理结果判断所述服务端是否合法。

24.根据权利要求23所述的用于客户端的认证装置,其特征在于,所述客户端和所述服务端上均预先存储有多组相应的或相同的信息处理方法,且每组所述信息处理方法在所述客户端和所述服务端上均具有相应或相同的信息处理方法标识;

所述动态交互验证信息中包含有信息处理方法标识;

所述处理判断子单元,包括:

处理方法查询子单元,用于根据所述第一动态交互验证信息中的信息处理方法标识查询对应的预先存储的信息处理方法;

处理方法处理子单元,用于根据所述信息处理方法对所述第二动态交互验证信息进行处理,根据处理结果判断所述服务端是否合法。

25.根据权利要求24所述的用于客户端的认证装置,其特征在于,所述信息处理方法标识在所述客户端与所述服务端之间同步且定时变更。

26.根据权利要求22所述的用于客户端的认证装置,其特征在于,客户端和所述服务端上均预先存储有相同的含有量子态制备基的量子态库,所述量子态制备基用于制备量子比特串或测量量子比特串,每个所述量子态制备基均有对应的量子态制备基标识,

所述第二动态交互验证信息验证单元包括:

第一量子测量子单元,用于采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量,获得比特值测量结果;

第一量子判断子单元,用于根据所述比特值测量结果是否符合预期判断所述服务端是否合法。

27.根据权利要求26所述的用于客户端的认证装置,其特征在于,所述第一动态交互验证信息生成单元包括:

第一制备基选择子单元,用于从量子态库中选择至少一种量子态制备基;

第一标识提取子单元,用于提取所述量子态制备基的量子态制备基标识;

第一动态交互验证信息生成子单元,用于生成包含所述量子态制备基标识的第一动态交互验证信息。

28.根据权利要求27所述的用于客户端的认证装置,其特征在于,所述从量子态库中选择至少一种量子态制备基采用随机选择的方式,每一次认证选择的量子态制备基均不相

同。

29.根据权利要求26所述的用于客户端的认证装置,其特征在于,

所述第一量子比特串通过所述量子态制备基发送至客户端。

30.根据权利要求29所述的用于客户端的认证装置,其特征在于,所述第二动态交互验证信息还包括将所述第一量子比特串进行十进制转换后获得的十进制第一量子比特串;

所述第二动态交互验证信息验证单元包括:

第二量子测量子单元,用于采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量,获得比特值测量结果;

第二转换子单元,用于将所述十进制第一量子比特串按照十进制转换方法转换为转换后的第一量子比特串;

第二长度测量子单元,用于测量所述第一量子比特串的长度,获得比特串长度测量结果,其中所述第一量子比特串的长度是根据所述第一量子比特串长度生成的;

第二判断子单元,用于根据所述比特值测量结果是否符合预期和所述比特串长度测量结果是否符合预期判断所述服务端是否合法。

31.根据权利要求26所述的用于客户端的认证装置,其特征在于,所述客户端与所述服务端上均预先存储有相同的量子串长度数据库,所述第一动态交互验证信息还包括第一量子比特串长度代码;

所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在量子态库中查询相应的量子态制备基、根据所述第一量子比特串长度代码在量子串长度数据库中查询相应的第一量子比特串长度,然后根据所述第一量子比特串长度通过所述量子态制备基生成第一量子比特串,所述第一量子比特串通过所述量子态制备基发送至客户端。

32.根据权利要求26所述的用于客户端的认证装置,其特征在于,所述第一量子测量子单元包括:

第一量子查询子单元,用于在量子态库中查找与所述量子态制备基标识对应的量子态制备基;

第一随机测量子单元,用于随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量。

33.根据权利要求26所述的用于客户端的认证装置,其特征在于,所述第二动态交互验证信息还包括所述服务端选择的量子态制备基标识及第二量子比特串长度;

所述第二动态交互验证信息验证单元包括:

第二量子查询子单元,用于在量子态库中查询与所述服务端选择的量子态制备基标识相对应的量子态制备基;

第二量子制备子单元,用于根据所述第二量子比特串长度,通过所述量子态制备基生成第二量子比特串;

第三信息生成子单元,用于生成包含所述第二量子比特串的第三动态交互验证信息。

34.根据权利要求33所述的用于客户端的认证装置,其特征在于,所述第二动态交互验证信息验证单元还包括:

十进制转换子单元,用于将所述第二量子比特串按照十进制转换方法进行转换,获得十进制第二量子比特串;

所述第三信息生成子单元包括：

十进制第三信息生成子单元，用于生成包含所述第二量子比特串和所述十进制第二量子比特串的第三动态交互验证信息。

35.根据权利要求33或34所述的用于客户端的认证装置，其特征在于，所述第三动态交互验证信息发送单元包括：

第三动态交互验证信息量子发送子单元，用于若合法，则将所述第二量子比特串采用所述量子态制备基发送至服务端。

36.根据权利要求26所述的用于客户端的认证装置，其特征在于，所述客户端的量子态库与所述服务端的量子态库同步且按照预定的规则定时变更。

37.根据权利要求22所述的用于客户端的认证装置，其特征在于，所述第一动态交互验证信息包括客户端的身份标识，所述身份标识用于服务端对所述客户端进行初步认证。

38.根据权利要求37所述的用于客户端的认证装置，其特征在于，所述客户端的身份标识包括客户端的用户识别码和身份证书。

39.根据权利要求22所述的用于客户端的认证装置，其特征在于，所述第一动态交互验证信息发送单元包括：

第一动态交互验证信息加密子单元，用于将全部或部分所述第一动态交互验证信息采用密钥加密后发送至服务端；

所述第三动态交互验证信息发送单元包括：

第三动态交互验证信息加密子单元，用于若合法，则将全部或部分所述第三动态交互验证信息采用密钥加密后发送至服务端。

40.根据权利要求39所述的用于客户端的认证装置，其特征在于，所述密钥与所述服务端解密使用的密钥互为对称量子密钥，或互为公私密钥。

41.根据权利要求22所述的用于客户端的认证装置，其特征在于，所述第二动态交互验证信息接收单元包括：

加密第二动态交互验证信息接收子单元，用于接收所述服务端发送的至少部分信息已加密的根据所述第一动态交互验证信息生成的第二动态交互验证信息；

第二动态交互验证信息解密子单元，用于采用与所述服务端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

42.根据权利要求41所述的用于客户端的认证装置，其特征在于，所述解密密钥与所述服务端加密使用的密钥互为对称量子密钥，或互为公私密钥。

43.一种用于服务端的认证方法，其特征在于，包括：

接收客户端发送的第一动态交互验证信息；

根据所述第一动态交互验证信息生成第二动态交互验证信息；

将所述第二动态交互验证信息发送至所述客户端；

接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

根据所述第三动态交互验证信息判断所述客户端是否通过认证；

其中，所述第一动态交互验证信息、第二动态交互验证信息和第三动态交互验证信息采用量子态处理，所述第一动态交互验证信息包括：量子制备基标识和第一量子比特串长

度;所述第二动态交互验证信息包括:根据所述第一量子比特串长度,通过所述量子态制备基标识在量子态库中查询的量子态制备基,生成的第一量子比特串;所述第三动态交互验证信息包括:随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量获得的比特值测量结果。

44.根据权利要求43所述的用于服务端的认证方法,其特征在于,服务端和所述客户端上均预先存储有相应的或相同的信息处理方法,所述服务端根据所述信息处理方法对动态交互验证信息的处理结果与所述客户端对所述动态交互验证信息的处理结果是相应的或相同的;

所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤,包括:

采用与所述客户端相应的或相同的信息处理方法对所述第三动态交互验证信息进行处理,根据处理结果是否符合预期判断所述客户端是否通过认证。

45.根据权利要求44所述的用于服务端的认证方法,其特征在于,所述服务端和所述客户端上均预先存储有多组相应的或相同的信息处理方法,且每组所述信息处理方法在所述服务端和所述客户端上均具有相应或相同的信息处理方法标识;

所述动态交互验证信息中包含有信息处理方法标识;

所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤,包括:

根据所述第一动态交互验证信息中的信息处理方法标识查找对应的信息处理方法;

采用所述信息处理方法对所述第一动态交互验证信息进行处理,生成第二动态交互验证信息。

46.根据权利要求45所述的用于服务端的认证方法,其特征在于,所述信息处理方法标识在所述服务端与所述客户端之间同步且定时变更。

47.根据权利要求43所述的用于服务端的认证方法,其特征在于,服务端和所述客户端上均预先存储有相同的含有量子态制备基的量子态库,所述量子态制备基用于制备量子比特串或测量量子比特串,每个所述量子态制备基均有对应的量子态制备基标识。

48.根据权利要求47所述的用于服务端的认证方法,其特征在于,所述将所述第二动态交互验证信息发送至所述客户端的步骤,包括:

将所述第一量子比特串采用所述量子态制备基发送至所述客户端。

49.根据权利要求47所述的用于服务端的认证方法,其特征在于,将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串;

生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

50.根据权利要求47所述的用于服务端的认证方法,其特征在于,所述服务端与所述客户端上均预先存储有相同的量子串长度数据库,所述第一动态交互验证信息还包括第一量子比特串长度代码;

所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤,包括:

根据所述量子态制备基标识在量子态库中查找相应的量子态制备基;以及

根据所述第一量子比特串长度代码在所述量子串长度数据库中查找相应的第一量子比特串长度;

根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串;

将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

51.根据权利要求47所述的用于服务端的认证方法，其特征在于，

所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

采用所述量子位标识对应的量子态测量所述第一量子比特串的比特值，获得服务端比特值测量结果；

比较所述比特值测量结果与所述服务端比特值测量结果，根据比较结果是否符合预设的判断条件判断所述客户端是否通过认证。

52.根据权利要求47所述的用于服务端的认证方法，其特征在于，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串；

所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

根据所述第二量子比特值测量结果是否符合预期判断所述客户端是否通过认证。

53.根据权利要求47所述的用于服务端的认证方法，其特征在于，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串，以及将所述第二量子比特串进行十进制转换获得的十进制第二量子比特串；

所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

将所述十进制第二量子比特串按照十进制转换方法转换为转换后的第二量子比特串；

测量所述第二量子比特串的长度，获得第二量子比特串长度测量结果；

根据所述第二量子比特值测量结果是否符合预期和所述第二量子比特串长度测量结果是否符合预期判断所述服务端是否通过认证。

54.根据权利要求47所述的用于服务端的认证方法，其特征在于，所述服务端的量子态库与所述客户端的量子态库同步且按照预定的规则定时变更。

55.根据权利要求43所述的用于服务端的认证方法，其特征在于，所述第一动态交互验证信息包括客户端的身份标识；

所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

根据所述客户端的身份标识对所述客户端进行初步认证；

若初步认证通过，则根据所述第一动态交互验证信息生成第二动态交互验证信息。

56.根据权利要求55所述的用于服务端的认证方法，其特征在于，所述客户端的身份标

识包括客户端的用户识别码和身份证书。

57.根据权利要求43所述的用于服务端的认证方法，其特征在于，所述将所述第二动态交互验证信息发送至所述客户端的步骤，包括：

将全部或部分所述第二动态交互验证信息采用密钥加密后发送至服务端。

58.根据权利要求57所述的用于服务端的认证方法，其特征在于，所述密钥与所述客户端解密使用的密钥互为对称量子密钥，或互为公私密钥。

59.根据权利要求43所述的用于服务端的认证方法，其特征在于，所述接收客户端发送的第一动态交互验证信息的步骤，包括：

接收客户端发送的至少部分信息已加密的第一动态交互验证信息；

采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密；

所述接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息的步骤，包括：

接收所述客户端发送的至少部分信息已加密的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

60.根据权利要求59所述的用于服务端的认证方法，其特征在于，所述解密密钥与所述客户端加密使用的密钥互为对称量子密钥，或互为公私密钥。

61.一种用于服务端的认证装置，其特征在于，包括：

第一动态交互验证信息接收单元，用于接收客户端发送的第一动态交互验证信息，所述第一动态交互验证信息包括：量子制备基标识和第一量子比特串长度；

第二动态交互验证信息生成单元，用于根据所述第一动态交互验证信息生成第二动态交互验证信息，所述第二动态交互验证信息包括：根据所述第一量子比特串长度，通过所述量子态制备基标识在量子态库中查询的量子态制备基，生成的第一量子比特串；

第二动态交互验证信息发送单元，用于将所述第二动态交互验证信息发送至所述客户端；

第三动态交互验证信息接收单元，用于接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息，所述第三动态交互验证信息包括：随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量获得的比特值测量结果；

第三动态交互验证信息判断单元，用于根据所述第三动态交互验证信息判断所述客户端是否通过认证。

62.根据权利要求61所述的用于服务端的认证装置，其特征在于，服务端和所述客户端上均预先存储有相应的或相同的信息处理方法，所述服务端根据所述信息处理方法对动态交互验证信息的处理结果与所述客户端对所述动态交互验证信息的处理结果是相应的或相同的；

所述第三动态交互验证信息判断单元包括：

第三动态交互验证信息处理子单元，用于采用与所述客户端相应的或相同的信息处理方法对所述第三动态交互验证信息进行处理，根据处理结果是否符合预期判断所述客户端是否通过认证。

63.根据权利要求62所述的用于服务端的认证装置，其特征在于，所述服务端和所述客

户端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述服务端和所述客户端上均具有相应或相同的信息处理方法标识；

所述动态交互验证信息中包含有信息处理方法标识；

所述第二动态交互验证信息生成单元包括：

处理方法查询子单元，用于根据所述第一动态交互验证信息中的信息处理方法标识查找对应的信息处理方法；

第一信息处理子单元，用于采用所述信息处理方法对所述第一动态交互验证信息进行处理，生成第二动态交互验证信息。

64.根据权利要求63所述的用于服务端的认证装置，其特征在于，所述信息处理方法标识在所述服务端与所述客户端之间同步且定时变更。

65.根据权利要求61所述的用于服务端的认证装置，其特征在于，服务端和所述客户端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识。

66.根据权利要求65所述的用于服务端的认证装置，其特征在于，所述第二动态交互验证信息发送单元包括：

第一量子比特串发送子单元，用于将所述第一量子比特串采用所述量子态制备基发送至所述客户端。

67.根据权利要求65所述的用于服务端的认证装置，其特征在于，

所述第二动态交互验证信息生成单元包括：

第二十进制转换子单元，用于将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

第二服务端动态交互验证信息生成子单元，用于生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

68.根据权利要求65所述的用于服务端的认证装置，其特征在于，所述服务端与所述客户端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码；

所述第二动态交互验证信息生成单元包括：

第三服务端量子查询子单元，根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

第三服务端长度查询子单元，根据所述第一量子比特串长度代码在所述量子串长度数据库中查找相应的第一量子比特串长度；

第三服务端比特串生成子单元，用于根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

第三十进制转换子单元，用于将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

第三服务端动态交互验证信息生成子单元，用于生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

69.根据权利要求65所述的用于服务端的认证装置，其特征在于，

所述第三动态交互验证信息判断单元包括：

服务端第一量子串测量子单元，用于采用所述量子位标识对应的量子态测量所述第一量子比特串的比特值，获得服务端比特值测量结果；

服务端测量比较子单元，用于比较所述比特值测量结果与所述服务端比特值测量结果，根据比较结果是否符合预设的判断条件判断所述客户端是否通过认证。

70.根据权利要求65所述的用于服务端的认证装置，其特征在于，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串；

所述第三动态交互验证信息判断单元包括：

第一服务端比特串测量子单元，用于采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；第一服务端测量判断子单元，用于根据所述第二量子比特值测量结果是否符合预期判断所述客户端是否通过认证。

71.根据权利要求65所述的用于服务端的认证装置，其特征在于，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串，以及将所述第二量子比特串进行十进制转换获得的十进制第二量子比特串；

所述第三动态交互验证信息判断单元包括：

第二服务端比特串测量子单元，用于采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

第二服务端十进制转换子单元，用于将所述十进制第二量子比特串按照十进制转换方法转换为转换后的第二量子比特串；

第二服务端长度判断子单元，用于测量所述第二量子比特串的长度，获得第二量子比特串长度测量结果；

第二服务端测量判断子单元，用于根据所述第二量子比特值测量结果是否符合预期和所述第二量子比特串长度测量结果是否符合预期判断所述服务端是否通过认证。

72.根据权利要求65所述的用于服务端的认证装置，其特征在于，所述服务端的量子态库与所述客户端的量子态库同步且按照预定的规则定时变更。

73.根据权利要求61所述的用于服务端的认证装置，其特征在于，所述第一动态交互验证信息包括客户端的身份标识；

所述第二动态交互验证信息生成单元包括：

初步认证子单元，用于根据所述客户端的身份标识对所述客户端进行初步认证；

第二动态交互验证信息生成子单元，用于若初步认证通过，则根据所述第一动态交互验证信息生成第二动态交互验证信息。

74.根据权利要求73所述的用于服务端的认证装置，其特征在于，所述客户端的身份标识包括客户端的用户识别码和身份证书。

75.根据权利要求61所述的用于服务端的认证装置，其特征在于，所述第二动态交互验

证信息发送单元包括：

加密第二动态交互验证信息发送子单元，用于将全部或部分所述第二动态交互验证信息采用密钥加密后发送至服务端。

76.根据权利要求75所述的用于服务端的认证装置，其特征在于，所述密钥与所述客户端解密使用的密钥互为对称量子密钥，或互为公私密钥。

77.根据权利要求61所述的用于服务端的认证装置，其特征在于，所述第一动态交互验证信息接收单元包括：

加密第一动态交互验证信息接收子单元，用于接收客户端发送的至少部分信息已加密的第一动态交互验证信息；

第一动态交互验证信息解密子单元，用于采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密；

所述第三动态交互验证信息接收单元包括：

加密第三动态交互验证信息接收子单元，用于接收所述客户端发送的至少部分信息已加密的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

第三动态交互验证信息解密子单元，用于采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

78.根据权利要求77所述的用于服务端的认证装置，其特征在于，所述解密密钥与所述客户端加密使用的密钥互为对称量子密钥，或互为公私密钥。

79.一种用于客户端的认证终端设备，其特征在于，包括：

中央处理器；

输入输出单元；

存储器；

所述存储器中存储有权利要求1至权利要求21所述的任一用于客户端的认证方法的程序；并在启动后能够根据上述方法的程序运行。

80.一种用于服务端的认证终端设备，其特征在于，包括：

中央处理器；

输入输出单元；

存储器；

所述存储器中存储有权利要求43至权利要求60所述的任一用于服务端的认证方法的程序；并在启动后能够根据上述方法的程序运行。

81.一种用于用户认证的系统，包括客户端和服务端，其特征在于，所述客户端配置有权利要求22至权利要求42所述的任一用于客户端的认证装置，所述服务端配置有权利要求61至权利要求78所述的任一用于服务端的认证装置。

用于认证的方法、装置、终端设备及系统

技术领域

[0001] 本申请涉及电子技术领域，具体的说是一种用于客户端的认证方法、装置及终端设备，一种用于服务端的认证方法、装置及终端设备，以及一种用于用户认证的系统。

背景技术

[0002] 由于静态口令认证机制存在易遭受窃听攻击、口令猜测攻击、重放攻击及口令泄露等问题，而动态口令由于它使用便捷，能与各种业务系统快速无缝互操作，而成为身份认证技术的主流，被广泛应用于电子商务、网游、金融等领域。

[0003] 动态口令认证机制是基于某种密码算法，将用户的身份代码和某种不确定因素作为密码算法的输入参数，经过算法变换得到一个变化的结果，将其作为用户的登录口令。认证服务器端使用相应的算法进行计算，并将计算结果与用户的登录口令进行比对，若相同则接受登录。由此得到变化的、不重复的动态口令，且无需用户记忆，一个口令只能使用一次，重复使用将被拒绝接受登录。

[0004] 现有生成动态口令认证的终端有硬件令牌、短信密码、手机令牌、软件令牌四种，这四种存在如下不足：一是仅实现服务器对客户端的单向认证，无法防范假冒的服务器欺骗合法用户，如果攻击者截取服务器的认证信息，可以利用数据库，口令重放等手段冒充服务器欺骗客户端。二是容易遭受小数攻击，当客户端向认证服务器请求认证时，攻击者可通过网络窃听截获认证服务器传送的挑战信息(即Seed和Iteration)，并修改Iteration为较小值，然后假冒服务器将截获的Seed和较小的Iteration发给客户端。客户端利用攻击者传送的Seed和Iteration计算出一次性口令，并传送给服务器。攻击者再次截获客户端传来的一次性口令，并利用已知的单向散列函数依次计算较大Iteration的一次性口令，获得此用户后继的一系列口令，因此，攻击者可以冒充合法用户，发起小数攻击。三是难以抵御中间人攻击，中间人攻击的具体过程为：位于客户端和服务器端之间的攻击者可能截获认证信息，一方面假冒客户端与服务器端连接，另一方面假冒服务器端与客户端连接。客户端登录传送一次性口令给服务器端，攻击者可以截获一次性口令，使客户端无法登录，造成网络连接断开、连接超时等假象。同时，可以利用截获的一次性口令假冒客户端登录到服务器端。四是客户端和服务端的敏感保密数据(比如硬件令牌丢失，其PIN密码的保护)的存储缺乏安全手段。

发明内容

[0005] 鉴于上述问题，本申请提供一种用于客户端的认证方法、一种用于客户端的认证装置及一种用于客户端的认证终端设备，一种用于服务端的认证方法、一种用于服务端的认证装置及一种用于服务端的认证终端设备，以及一种用于用户认证的系统。

[0006] 本申请采用的技术方案是：

[0007] 本申请提供一种用于客户端的认证方法，包括：

[0008] 生成第一动态交互验证信息；

[0009] 将所述第一动态交互验证信息发送至服务端；

[0010] 接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息；

[0011] 根据所述第二动态交互验证信息判断所述服务端是否合法，以及根据所述第二动态交互验证信息生成第三动态交互验证信息；

[0012] 若合法，则将所述第三动态交互验证信息发送至服务端，以供所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0013] 可选的，客户端和所述服务端上均预先存储有相应的或相同的信息处理方法，所述客户端根据所述信息处理方法对动态交互验证信息的处理结果与所述服务端对所述动态交互验证信息的处理结果是相应的或相同的；

[0014] 所述根据所述第二动态交互验证信息判断所述服务端是否合法的步骤，包括：

[0015] 根据预先存储的信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果是否符合预期判断所述服务端是否合法。

[0016] 可选的，所述客户端和所述服务端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述客户端和所述服务端上均具有相应或相同的信息处理方法标识；

[0017] 所述动态交互验证信息中包含有信息处理方法标识；

[0018] 所述根据预先存储的信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果判断所述服务端是否合法的步骤，包括：

[0019] 根据所述第一动态交互验证信息中的信息处理方法标识查询对应的预先存储的信息处理方法；

[0020] 根据所述信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果是否符合预期判断所述服务端是否合法。

[0021] 可选的，所述信息处理方法标识在所述客户端与所述服务端之间同步且定时变更。

[0022] 可选的，客户端和所述服务端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识，所述第一动态交互验证信息包括所述量子态制备基标识；

[0023] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基，并通过所述量子态制备基生成第一量子比特串；

[0024] 所述根据所述第二动态交互验证信息判断所述服务端是否合法的步骤，包括：

[0025] 采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量，获得比特值测量结果；

[0026] 根据所述比特值测量结果是否符合预期判断所述服务端是否合法。

[0027] 可选的，所述生成第一动态交互验证信息的步骤，包括：

[0028] 从量子态库中选择至少一种量子态制备基；

[0029] 提取所述量子态制备基的量子态制备基标识；

[0030] 生成包含所述量子态制备基标识的第一动态交互验证信息。

[0031] 可选的，所述从量子态库中选择至少一种量子态制备基采用随机选择的方式，每

一次认证选择的量子态制备基均不相同。

[0032] 可选的，所述第一动态交互验证信息还包括第一量子比特串长度；

[0033] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基，并根据所述第一量子比特串长度通过所述量子态制备基生成的第一量子比特串，所述第一量子比特串通过所述量子态制备基发送至客户端。

[0034] 可选的，所述第二动态交互验证信息还包括将所述第一量子比特串进行十进制转换后获得的十进制第一量子比特串；

[0035] 所述根据所述第二动态交互验证信息判断所述服务端是否合法的步骤，包括：

[0036] 采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量，获得比特值测量结果；

[0037] 将所述十进制第一量子比特串按照十进制转换方法转换为转换后的第一量子比特串；

[0038] 测量所述第一量子比特串的长度，获得比特串长度测量结果；

[0039] 根据所述比特值测量结果是否符合预期和所述比特串长度测量结果是否符合预期判断所述服务端是否合法。

[0040] 可选的，所述客户端与所述服务端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码；

[0041] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在量子态库中查询相应的量子态制备基、根据所述第一量子比特串长度代码在量子串长度数据库中查询相应的第一量子比特串长度，然后根据所述第一量子比特串长度通过所述量子态制备基生成第一量子比特串，所述第一量子比特串通过所述量子态制备基发送至客户端。

[0042] 可选的，所述采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量的步骤，包括：

[0043] 在量子态库中查找与所述量子态制备基标识对应的量子态制备基；

[0044] 随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量。

[0045] 可选的，所述根据所述第二动态交互验证信息生成第三动态交互验证信息的步骤，包括：

[0046] 将所述比特值测量结果及测量时使用的量子态的量子位标识作为第三动态交互验证信息。

[0047] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的代码及第二量子比特串长度；

[0048] 所述根据所述第二动态交互验证信息生成第三动态交互验证信息的步骤，包括：

[0049] 在量子态库中查询与所述服务端选择的量子态制备基的代码相对应的量子态制备基；

[0050] 根据所述第二量子比特串长度，通过所述量子态制备基生成第二量子比特串；

[0051] 生成包含所述第二量子比特串的第三动态交互验证信息。

[0052] 可选的，所述根据所述第二动态交互验证信息生成第三动态交互验证信息的步骤，还包括：将所述第二量子比特串按照十进制转换方法进行转换，获得十进制第二量子比特串；

[0053] 所述生成包含所述第二量子比特串的第三动态交互验证信息的步骤，包括：

[0054] 生成包含所述第二量子比特串和所述十进制第二量子比特串的第三动态交互验证信息。

[0055] 可选的，所述若合法，则将所述第三动态交互验证信息发送至服务端的步骤，包括：

[0056] 若合法，则将所述第二量子比特串采用所述量子态制备基发送至服务端。

[0057] 可选的，所述客户端的量子态库与所述服务端的量子态库同步且按照预定的规则定时变更。

[0058] 可选的，所述第一动态交互验证信息包括客户端的身份标识，所述身份标识用于服务端对所述客户端进行初步认证。

[0059] 可选的，所述客户端的身份标识包括客户端的用户识别码和身份证书。

[0060] 可选的，所述将所述第一动态交互验证信息发送至服务端的步骤，包括：

[0061] 将全部或部分所述第一动态交互验证信息采用密钥加密后发送至服务端；

[0062] 所述若合法，则将所述第三动态交互验证信息发送至服务端的步骤，包括：

[0063] 若合法，则将全部或部分所述第三动态交互验证信息采用密钥加密后发送至服务端。

[0064] 可选的，所述密钥与所述服务端解密使用的密钥互为对称量子密钥，或互为公私密钥。

[0065] 可选的，所述接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息的步骤，包括：

[0066] 接收所述服务端发送的至少部分信息已加密的根据所述第一动态交互验证信息生成的第二动态交互验证信息；

[0067] 采用与所述服务端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0068] 可选的，所述解密密钥与所述服务端加密使用的密钥互为对称量子密钥，或互为公私密钥。

[0069] 相应的，本申请还提供一种用于客户端的认证装置，包括：

[0070] 第一动态交互验证信息生成单元，用于生成第一动态交互验证信息；

[0071] 第一动态交互验证信息发送单元，用于将所述第一动态交互验证信息发送至服务端；

[0072] 第二动态交互验证信息接收单元，用于接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息；

[0073] 第二动态交互验证信息验证单元，用于根据所述第二动态交互验证信息判断所述服务端是否合法，以及根据所述第二动态交互验证信息生成第三动态交互验证信息；

[0074] 第三动态交互验证信息发送单元，用于若合法，则将所述第三动态交互验证信息发送至服务端，以供所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0075] 可选的，客户端和所述服务端上均预先存储有相应的或相同的信息处理方法，所述客户端根据所述信息处理方法对动态交互验证信息的处理结果与所述服务端对所述动态交互验证信息的处理结果是相应的或相同的；

[0076] 所述第二动态交互验证信息验证单元包括：

[0077] 处理判断子单元，用于根据预先存储的信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果判断所述服务端是否合法。

[0078] 可选的，所述客户端和所述服务端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述客户端和所述服务端上均具有相应或相同的信息处理方法标识；

[0079] 所述动态交互验证信息中包含有信息处理方法标识；

[0080] 所述处理判断子单元，包括：

[0081] 处理方法查询子单元，用于根据所述第一动态交互验证信息中的信息处理方法标识查询对应的预先存储的信息处理方法；

[0082] 处理方法处理子单元，用于根据所述信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果判断所述服务端是否合法。

[0083] 可选的，所述信息处理方法标识在所述客户端与所述服务端之间同步且定时变更。

[0084] 可选的，客户端和所述服务端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识，所述第一动态交互验证信息包括所述量子态制备基标识；

[0085] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基，并通过所述量子态制备基生成第一量子比特串；

[0086] 所述第二动态交互验证信息验证单元包括：

[0087] 第一量子测量子单元，用于采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量，获得比特值测量结果；

[0088] 第一量子判断子单元，用于根据所述比特值测量结果是否符合预期判断所述服务端是否合法。

[0089] 可选的，所述第一动态交互验证信息生成单元包括：

[0090] 第一制备基选择子单元，用于从量子态库中选择至少一种量子态制备基；

[0091] 第一标识提取子单元，用于提取所述量子态制备基的量子态制备基标识；

[0092] 第一验证信息生成子单元，用于生成包含所述量子态制备基标识的第一动态交互验证信息。

[0093] 可选的，所述从量子态库中选择至少一种量子态制备基采用随机选择的方式，每一次认证选择的量子态制备基均不相同。

[0094] 可选的，所述第一动态交互验证信息还包括第一量子比特串长度；

[0095] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基，并根据所述第一量子比特串长度通过所述量子态制备基生成的第一量子比特串，所述第一量子比特串通过所述量子态制备基发送至客户端。

[0096] 可选的，所述第二动态交互验证信息还包括将所述第一量子比特串进行十进制转换后获得的十进制第一量子比特串；

[0097] 所述第二动态交互验证信息验证单元包括：

[0098] 第二量子测量子单元，用于采用与所述量子态制备基标识对应的量子态制备基对

所述第一量子比特串的比特值进行测量，获得比特值测量结果；

[0099] 第二转换子单元，用于将所述十进制第一量子比特串按照十进制转换方法转换为转换后的第一量子比特串；

[0100] 第二长度测量子单元，用于测量所述第一量子比特串的长度，获得比特串长度测量结果；

[0101] 第二判断子单元，用于根据所述比特值测量结果是否符合预期和所述比特串长度测量结果是否符合预期判断所述服务端是否合法。

[0102] 可选的，所述客户端与所述服务端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码；

[0103] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在量子态库中查询相应的量子态制备基、根据所述第一量子比特串长度代码在量子串长度数据库中查询相应的第一量子比特串长度，然后根据所述第一量子比特串长度通过所述量子态制备基生成第一量子比特串，所述第一量子比特串通过所述量子态制备基发送至客户端。

[0104] 可选的，所述第一量子测量子单元包括：

[0105] 第一量子查询子单元，用于在量子态库中查找与所述量子态制备基标识对应的量子态制备基；

[0106] 第一随机测量子单元，用于随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量。

[0107] 可选的，所述第二动态交互验证信息验证单元包括：

[0108] 第三动态验证信息生成子单元，用于将所述比特值测量结果及测量时使用的量子态的量子位标识作为第三动态交互验证信息。

[0109] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基标识及第二量子比特串长度；

[0110] 所述第二动态交互验证信息验证单元包括：

[0111] 第二量子查询子单元，用于在量子态库中查询与所述服务端选择的量子态制备基标识相对应的量子态制备基；

[0112] 第二量子制备子单元，用于根据所述第二量子比特串长度，通过所述量子态制备基生成第二量子比特串；

[0113] 第三信息生成子单元，用于生成包含所述第二量子比特串的第三动态交互验证信息。

[0114] 可选的，所述第二动态交互验证信息验证单元还包括：

[0115] 十进制转换子单元，用于将所述第二量子比特串按照十进制转换方法进行转换，获得十进制第二量子比特串；

[0116] 所述第三信息生成子单元包括：

[0117] 十进制第三信息生成子单元，用于生成包含所述第二量子比特串和所述十进制第二量子比特串的第三动态交互验证信息。

[0118] 可选的，所述第三动态交互验证信息发送单元包括：

[0119] 第三动态交互验证信息量子发送子单元，用于若合法，则将所述第二量子比特串采用所述量子态制备基发送至服务端。

[0120] 可选的，所述客户端的量子态库与所述服务端的量子态库同步且按照预定的规则定时变更。

[0121] 可选的，所述第一动态交互验证信息包括客户端的身份标识，所述身份标识用于服务端对所述客户端进行初步认证。

[0122] 可选的，所述客户端的身份标识包括客户端的用户识别码和身份证书。

[0123] 可选的，所述第一动态交互验证信息发送单元包括：

[0124] 第一动态交互验证信息加密子单元，用于将全部或部分所述第一动态交互验证信息采用密钥加密后发送至服务端；

[0125] 所述第三动态交互验证信息发送单元包括：

[0126] 第三动态交互验证信息加密子单元，用于若合法，则将全部或部分所述第三动态交互验证信息采用密钥加密后发送至服务端。

[0127] 可选的，所述密钥与所述服务端解密使用的密钥互为对称量子密钥，或互为公私密钥。

[0128] 可选的，所述第二动态交互验证信息接收单元包括：

[0129] 加密第二动态交互验证信息接收子单元，用于接收所述服务端发送的至少部分信息已加密的根据所述第一动态交互验证信息生成的第二动态交互验证信息；

[0130] 第二动态交互验证信息解密子单元，用于采用与所述服务端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0131] 可选的，所述解密密钥与所述服务端加密使用的密钥互为对称量子密钥，或互为公私密钥。

[0132] 本申请还提供一种用于服务端的认证方法，包括：

[0133] 接收客户端发送的第一动态交互验证信息；

[0134] 根据所述第一动态交互验证信息生成第二动态交互验证信息；

[0135] 将所述第二动态交互验证信息发送至所述客户端；

[0136] 接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

[0137] 根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0138] 可选的，服务端和所述客户端上均预先存储有相应的或相同的信息处理方法，所述服务端根据所述信息处理方法对动态交互验证信息的处理结果与所述客户端对所述动态交互验证信息的处理结果是相应的或相同的；

[0139] 所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

[0140] 采用与所述客户端相应的或相同的信息处理方法对所述第三动态交互验证信息进行处理，根据处理结果是否符合预期判断所述客户端是否通过认证。

[0141] 可选的，所述服务端和所述客户端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述服务端和所述客户端上均具有相应或相同的信息处理方法标识；

[0142] 所述动态交互验证信息中包含有信息处理方法标识；

[0143] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0144] 根据所述第一动态交互验证信息中的信息处理方法标识查找对应的信息处理方法；

[0145] 采用所述信息处理方法对所述第一动态交互验证信息进行处理，生成第二动态交互验证信息。

[0146] 可选的，所述信息处理方法标识在所述服务端与所述客户端之间同步且定时变更。

[0147] 可选的，服务端和所述客户端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识；

[0148] 所述第一动态交互验证信息包括所述客户端选择的至少一种量子态制备基的量子态制备基标识；

[0149] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0150] 根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0151] 采用所述量子态制备基生成第一量子比特串；

[0152] 生成包含所述第一量子比特串的第二动态交互验证信息。

[0153] 可选的，所述将所述第二动态交互验证信息发送至所述客户端的步骤，包括：

[0154] 将所述第一量子比特串采用所述量子态制备基发送至所述客户端。

[0155] 可选的，所述第一动态交互验证信息还包括第一量子比特串长度；

[0156] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0157] 根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0158] 根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

[0159] 将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

[0160] 生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

[0161] 可选的，所述服务端与所述客户端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码；

[0162] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0163] 根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；以及

[0164] 根据所述第一量子比特串长度代码在所述量子串长度数据库中查找相应的第一量子比特串长度；

[0165] 根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

[0166] 将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

[0167] 生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

[0168] 可选的，所述第三动态交互验证信息包括所述客户端测量所述第二动态交互验证信息时采用的量子态的量子位标识以及比特值测量结果；

[0169] 所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

[0170] 采用所述量子位标识对应的量子态测量所述第一量子比特串的比特值，获得服务

端比特值测量结果；

[0171] 比较所述比特值测量结果与所述服务端比特值测量结果，根据比较结果是否符合预设的判断条件判断所述客户端是否通过认证。

[0172] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0173] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串；

[0174] 所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

[0175] 采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

[0176] 根据所述第二量子比特值测量结果是否符合预期判断所述客户端是否通过认证。

[0177] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0178] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串，以及将所述第二量子比特串进行十进制转换获得的十进制第二量子比特串；

[0179] 所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

[0180] 采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

[0181] 将所述十进制第二量子比特串按照十进制转换方法转换为转换后的第二量子比特串；

[0182] 测量所述第二量子比特串的长度，获得第二量子比特串长度测量结果；

[0183] 根据所述第二量子比特值测量结果是否符合预期和所述第二量子比特串长度测量结果是否符合预期判断所述服务端是否通过认证。

[0184] 可选的，所述服务端的量子态库与所述客户端的量子态库同步且按照预定的规则定时变更。

[0185] 可选的，所述第一动态交互验证信息包括客户端的身份标识；

[0186] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0187] 根据所述客户端的身份标识对所述客户端进行初步认证；

[0188] 若初步认证通过，则根据所述第一动态交互验证信息生成第二动态交互验证信息。

[0189] 可选的，所述客户端的身份标识包括客户端的用户识别码和身份证书。

[0190] 可选的，所述将所述第二动态交互验证信息发送至所述客户端的步骤，包括：

[0191] 将全部或部分所述第二动态交互验证信息采用密钥加密后发送至服务端。

[0192] 可选的，所述密钥与所述客户端解密使用的密钥互为对称量子密钥，或互为公私密钥。

[0193] 可选的，所述接收客户端发送的第一动态交互验证信息的步骤，包括：

[0194] 接收客户端发送的至少部分信息已加密的第一动态交互验证信息；

[0195] 采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密；

[0196] 所述接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息的步骤，包括：

[0197] 接收所述客户端发送的至少部分信息已加密的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

[0198] 采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0199] 可选的，所述解密密钥与所述客户端加密使用的密钥互为对称量子密钥，或互为公私密钥。

[0200] 相应的，本申请还提供一种用于服务端的认证装置，包括：

[0201] 第一动态交互验证信息接收单元，用于接收客户端发送的第一动态交互验证信息；

[0202] 第二动态交互验证信息生成单元，用于根据所述第一动态交互验证信息生成第二动态交互验证信息；

[0203] 第二动态交互验证信息发送单元，用于将所述第二动态交互验证信息发送至所述客户端；

[0204] 第三动态交互验证信息接收单元，用于接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

[0205] 第三动态交互验证信息判断单元，用于根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0206] 可选的，服务端和所述客户端上均预先存储有相应的或相同的信息处理方法，所述服务端根据所述信息处理方法对动态交互验证信息的处理结果与所述客户端对所述动态交互验证信息的处理结果是相应的或相同的；

[0207] 所述第三动态交互验证信息判断单元包括：

[0208] 第三动态交互验证信息处理子单元，用于采用与所述客户端相应的或相同的信息处理方法对所述第三动态交互验证信息进行处理，根据处理结果是否符合预期判断所述客户端是否通过认证。

[0209] 可选的，所述服务端和所述客户端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述服务端和所述客户端上均具有相应或相同的信息处理方法标识；

[0210] 所述动态交互验证信息中包含有信息处理方法标识；

[0211] 所述第二动态交互验证信息生成单元包括：

[0212] 处理方法查询子单元，用于根据所述第一动态交互验证信息中的信息处理方法标识查找对应的信息处理方法；

[0213] 第一信息处理子单元，用于采用所述信息处理方法对所述第一动态交互验证信息进行处理，生成第二动态交互验证信息。

[0214] 可选的，所述信息处理方法标识在所述服务端与所述客户端之间同步且定时变更。

[0215] 可选的，服务端和所述客户端上均预先存储有相同的含有量子态制备基的量子态

库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识；

[0216] 所述第一动态交互验证信息包括所述客户端选择的至少一种量子态制备基的量子态制备基标识；

[0217] 所述第二动态交互验证信息生成单元包括：

[0218] 第一服务端量子查询子单元，用于根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0219] 第一服务端比特串生成子单元，用于采用所述量子态制备基生成第一量子比特串；

[0220] 第一服务端验证信息生成子单元，用于生成包含所述第一量子比特串的第二动态交互验证信息。

[0221] 可选的，所述第二动态交互验证信息发送单元包括：

[0222] 第一量子比特串发送子单元，用于将所述第一量子比特串采用所述量子态制备基发送至所述客户端。

[0223] 可选的，所述第一动态交互验证信息还包括第一量子比特串长度；

[0224] 所述第二动态交互验证信息生成单元包括：

[0225] 第二服务端量子查询子单元，用于根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0226] 第二服务端比特串生成子单元，用于根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

[0227] 第二十进制转换子单元，用于将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

[0228] 第二服务端验证信息生成子单元，用于生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

[0229] 可选的，所述服务端与所述客户端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码；

[0230] 所述第二动态交互验证信息生成单元包括：

[0231] 第三服务端量子查询子单元，根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0232] 第三服务端长度查询子单元，根据所述第一量子比特串长度代码在所述量子串长度数据库中查找相应的第一量子比特串长度；

[0233] 第三服务端比特串生成子单元，用于根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

[0234] 第三十进制转换子单元，用于将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

[0235] 第三服务端验证信息生成子单元，用于生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

[0236] 可选的，所述第三动态交互验证信息包括所述客户端测量所述第二动态交互验证信息时采用的量子态的量子位标识以及比特值测量结果；

[0237] 所述第三动态交互验证信息判断单元包括：

[0238] 服务端第一量子串测量子单元，用于采用所述量子位标识对应的量子态测量所述第一量子比特串的比特值，获得服务端比特值测量结果；

[0239] 服务端测量比较子单元，用于比较所述比特值测量结果与所述服务端比特值测量结果，根据比较结果是否符合预设的判断条件判断所述客户端是否通过认证。

[0240] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0241] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串；

[0242] 所述第三动态交互验证信息判断单元包括：

[0243] 第一服务端比特串测量子单元，用于采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；第一服务端测量判断子单元，用于根据所述第二量子比特值测量结果是否符合预期判断所述客户端是否通过认证。

[0244] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0245] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串，以及将所述第二量子比特串进行十进制转换获得的十进制第二量子比特串；

[0246] 所述第三动态交互验证信息判断单元包括：

[0247] 第二服务端比特串测量子单元，用于采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

[0248] 第二服务端十进制转换子单元，用于将所述十进制第二量子比特串按照十进制转换方法转换为转换后的第二量子比特串；

[0249] 第二服务端长度判断子单元，用于测量所述第二量子比特串的长度，获得第二量子比特串长度测量结果；

[0250] 第二服务端测量判断子单元，用于根据所述第二量子比特值测量结果是否符合预期和所述第二量子比特串长度测量结果是否符合预期判断所述服务端是否通过认证。

[0251] 可选的，所述服务端的量子态库与所述客户端的量子态库同步且按照预定的规则定时变更。

[0252] 可选的，所述第一动态交互验证信息包括客户端的身份标识；

[0253] 所述第二动态交互验证信息生成单元包括：

[0254] 初步认证子单元，用于根据所述客户端的身份标识对所述客户端进行初步认证；

[0255] 第二动态交互验证信息生成子单元，用于若初步认证通过，则根据所述第一动态交互验证信息生成第二动态交互验证信息。

[0256] 可选的，所述客户端的身份标识包括客户端的用户识别码和身份证书。

[0257] 可选的，所述第二动态交互验证信息发送单元包括：

[0258] 加密第二动态交互验证信息发送子单元，用于将全部或部分所述第二动态交互验证信息采用密钥加密后发送至服务端。

[0259] 可选的，所述密钥与所述客户端解密使用的密钥互为对称量子密钥，或互为公私密钥。

[0260] 可选的，所述第一动态交互验证信息接收单元包括：

[0261] 加密第一动态交互验证信息接收子单元，用于接收客户端发送的至少部分信息已加密的第一动态交互验证信息；

[0262] 第一动态交互验证信息解密子单元，用于采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密；

[0263] 所述第三动态交互验证信息接收单元包括：

[0264] 加密第三动态交互验证信息接收子单元，用于接收所述客户端发送的至少部分信息已加密的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

[0265] 第三动态交互验证信息解密子单元，用于采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0266] 可选的，所述解密密钥与所述客户端加密使用的密钥互为对称量子密钥，或互为公私密钥。

[0267] 本申请还提供一种用于客户端的认证终端设备，包括：

[0268] 中央处理器；

[0269] 输入输出单元；

[0270] 存储器；

[0271] 所述存储器中存储有本申请提供的用于客户端的认证方法；并在启动后能够根据上述方法运行。

[0272] 本申请还提供一种用于服务端的认证终端设备，包括：

[0273] 中央处理器；

[0274] 输入输出单元；

[0275] 存储器；

[0276] 所述存储器中存储有本申请提供的用于服务端的认证方法；并在启动后能够根据上述方法运行。

[0277] 本申请还提供一种用于用户认证的系统，包括客户端和服务端，所述客户端配置有本申请提供的用于客户端的认证装置，所述服务端配置有本申请提供的用于服务端的认证装置。

[0278] 与现有技术相比，本申请具有以下优点：

[0279] 本申请提供的一种用于客户端的认证方法，首先生成第一动态交互验证信息；然后将所述第一动态交互验证信息发送至服务端；接下来，接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息；然后根据所述第二动态交互验证信息判断所述服务端是否合法，以及根据所述第二动态交互验证信息生成第三动态交互验证信息；若合法，则将所述第三动态交互验证信息发送至服务端，以供所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证。相较于传统的动态口令认证，本方法通过客户端与服务端的交互通信，实现了客户端与服务端的交互认证，可以防范假冒的服务器欺骗合法用户，同时，由于客户端和服务端均动态的利用对方的验证信息制作本方验证信息，再发给对方进行验证，因此，可以抵御中间人攻击，且可防御小数攻击，将所述验证

信息采用量子态处理后，可以进一步提高验证信息传输及存储的安全性。

附图说明

[0280] 图1是本申请提供的一种用于客户端的认证方法实施例的流程图；

[0281] 图2是本申请提供的一种用于客户端的认证装置实施例的示意图；

[0282] 图3是本申请提供的一种用于服务端的认证方法实施例的流程图；

[0283] 图4是本申请提供的一种用于服务端的认证装置实施例的示意图。

具体实施方式

[0284] 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。

[0285] 本申请提供了一种用于客户端的认证方法、一种用于客户端的认证装置及一种用于客户端的认证终端设备，一种用于服务端的认证方法、一种用于服务端的认证装置及一种用于服务端的认证终端设备，以及一种用于用户认证的系统，下面依次结合附图对本申请的实施例进行详细说明。

[0286] 请参考图1，其为本申请提供的一种用于客户端的认证方法实施例的流程图，所述方法包括如下步骤：

[0287] 步骤S101：生成第一动态交互验证信息。

[0288] 本步骤，首先生成第一动态交互验证信息，所述第一动态交互验证信息用于发送给服务端，供服务端根据所述第一动态交互验证信息生成第二动态交互验证信息。

[0289] 在本申请提供的一个实施例中，客户端和所述服务端上均预先存储有相应的或相同的信息处理方法，所述客户端根据所述信息处理方法对动态交互验证信息的处理结果与所述服务端对所述动态交互验证信息的处理结果是相应的或相同的。所述生成第一动态交互验证信息的步骤，包括：生成可以使用所述信息处理方法处理的第一动态交互验证信息。

[0290] 在本申请提供的另一个实施例中，所述客户端和所述服务端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述客户端和所述服务端上均具有相应或相同的信息处理方法标识。所述生成第一动态交互验证信息的步骤，包括：生成包含所述信息处理方法标识的第一动态交互验证信息。所述信息处理方法标识用于所述服务端根据所述信息处理方法标识查找对应的信息处理方法。

[0291] 进一步的，在本申请提供的一个实施例中，所述信息处理方法标识在所述客户端与所述服务端之间同步且定时变更，这样，每一次认证时发送的所述信息处理方法标识对应的信息处理方法可能不同，从而增加破译的难度，有效避免所述第一动态交互验证信息被伪造或复制，提高安全性。

[0292] 在本申请提供的一个优选实施例中，所述客户端和所述服务端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识，所述第一动态交互验证信息包括所述量子态制备基标识。所述生成第一动态交互验证信息的步骤，包括：

[0293] 从量子态库中选择至少一种量子态制备基；

[0294] 提取所述量子态制备基的量子态制备基标识；

[0295] 生成包含所述量子态制备基标识的第一动态交互验证信息。

[0296] 考虑到所述量子态制备基制作量子比特串时的参数可以预先设定好，也可以由客户端指定，因此，在本申请提供的一个实施例中，所述第一动态交互验证信息还包括第一量子比特串长度，以供所述服务端根据所述第一量子比特串长度生成对应的第一量子比特串，提高认证的可依据性。

[0297] 在本申请提供的一个优选的具体实施例中，在所述客户端和服务端均安装一个轻量级的量子态库，所述量子态库中包含有多个不同的正交量子态制备基，每个量子态制备基有不同的量子态制备基标识，每个量子态制备基中的量子态对应相应的量子位标识，所述量子态制备基标识可以是一个编号。例如：量子态制备基{|0>,|1>}的编号为1，其中量子态|0>对应的量子位标识为1.1，量子态|1>对应的量子位标识为1.2；量子态制备基{|+>,|->}的编号为2，其中量子态|+>对应的量子位标识为2.1，量子态|2>对应的量子位标识为2.2，以此类推。

[0298] 需要说明的是，所述量子态制备基编号可以定期依据某类算法在客户端和服务端进行同步重编。比如x代表量子态当前编号，y代表下一次请求时的量子态编号，那么y可以以x为基数推导出来，推导规则可以是y＝2x；或y＝2+x等等客户端和服务端协商的规则。从而避免所述量子态库被盗或被破解后，导致伪造服务端对所述客户端发起欺骗行为。在本申请提供的一个实施例中，所述从量子态库中选择至少一种量子态制备基采用随机选择的方式，以保证每一次认证选择的量子态制备基均不相同，实现所述第一动态交互验证信息的动态可变性，从而避免所述第一动态交互验证信息被伪造或复制。

[0299] 具体实施时，客户端从量子态库中随机选择一种或一种以上的量子态制备基，将量子态制备基的编号及以此编号发送的量子比特串长度ι作为第一动态交互验证信息，例如：{量子态制备基标识1，ι_1；量子态制备基标识2，ι_2；……量子态制备基标识n，ι_n}，比如假设客户端随机选择了量子态制备基编号为2、4两种量子态制备基，其长度分别为3,6，那么所述第一动态交互验证信息为{2,3;4,6}。

[0300] 需要说明的是，在上述优选的实施例中，还可以将所述第一量子比特串长度以代码的形式发送，以提高本方法的破译难度，进一步提高安全性，例如，在所述客户端与所述服务端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码，所述服务端在接收到所述第一量子比特串长度代码后，在所述量子串长度数据库中查找对应的第一量子比特串长度，即可用于生成对应的第一量子比特串。

[0301] 步骤S102：将所述第一动态交互验证信息发送至服务端。

[0302] 通过步骤S101，已生成第一动态交互验证信息，接下来，需要将所述第一动态交互验证信息发送至服务端。

[0303] 在本申请提供的一个优选实施例中，所述第一动态交互验证信息包括量子态制备基标识和第一量子比特串长度；

[0304] 所述将所述第一动态交互验证信息发送至服务端的步骤，包括：

[0305] 将所述量子态制备基标识和第一量子比特串长度发送至服务端。

[0306] 考虑到为了避免虚假客户端恶意攻击服务端，或伪造客户端进行认证，或非法用户访问，在本申请提供的一个实施例中，所述第一动态交互验证信息还包括客户端的身份

标识,所述身份标识用于服务端对所述客户端进行初步认证,例如所述客户端的用户识别码和身份证书等。所述服务端在接受到所述身份标识后,根据所述身份标识对所述客户端进行初步认证,若初步认证通过,则继续,否则,判断所述客户端非法,终止认证过程。

[0307] 仍以上述优选的实施例为例,所述将所述第一动态交互验证信息发送至服务端的步骤,包括:

[0308] 将所述量子态制备基标识、第一量子比特串长度及客户端的身份标识发送至服务端,其中,所述客户端的身份标识包括客户端的用户识别码和身份证书。

[0309] 例如,提取的量子态制备基标识、第一量子比特串长度为{2,3;4,6},客户端的用户标识为userid_A,客户端的身份证书为Cer_A,则发送给服务端的第一动态交互验证信息为:{2,3;4,6},userid_A,Cer_A。

[0310] 考虑到数据传输的安全性,在本申请提供的一个实施例中,客户端需要将所述第一动态交互验证信息进行加密后再行发送,同时可以采用https加密传输协议传输。

[0311] 所述将所述第一动态交互验证信息发送至服务端的步骤,包括:

[0312] 将全部或部分所述第一动态交互验证信息采用密钥加密后发送至服务端;

[0313] 仍以上述优选的实施例为例,客户端和服务端在通信之前都有各自的公私钥对和身份证书,或客户端和服务端共享一对对称量子密钥,公私钥对、身份证书及共享的对称量子密钥根据业务需求可以动态变化。在本申请提供的一个实施例中,基于客户端的计算能力考虑,在与服务端通信的时候,采用与服务端的对称量子密钥Key_AB来保证传输的敏感数据安全。

[0314] 在本申请提供的一个具体的实施例中,可以将所述第一动态交互验证信息中的部分信息加密后发送至服务端,例如,将量子态制备基标识和第一量子比特串长度采用对称量子密钥Key_AB进行加密,则发送给服务端的第一动态交互验证信息为:$\{2,3;4,6\}_{Key\_AB}$,userid_A,Cer_A。

[0315] 步骤S103:接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息。

[0316] 通过步骤S102,已将所述第一动态交互验证信息发送至服务端,接下来,接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息。

[0317] 服务端在接收到所述第一动态交互验证信息后,根据所述第一动态交互验证信息生成第二动态交互验证信息,并将所述第二动态交互验证信息发送给客户端进行验证。

[0318] 考虑到数据传输的安全性,在本申请提供的一个实施例中,所述服务端需要将所述动态交互验证信息进行加密后再行发送,同时可以采用https加密传输协议传输。

[0319] 在本申请提供的一个优选实施例中,所述客户端和所述服务端上均预先存储有相同的含有量子态制备基的量子态库,所述量子态制备基用于制备量子比特串或测量量子比特串,每个所述量子态制备基均有对应的量子态制备基标识,所述第一动态交互验证信息包括所述量子态制备基标识;所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基,并通过所述量子态制备基生成第一量子比特串,所述第一量子比特串通过所述量子态制备基发送至客户端,所述客户端采用相同的量子态制备基接收所述第一量子比特串。

[0320] 在本申请提供的一个实施例中,所述第一动态交互验证信息还包括第一量子比特

串长度;所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基,并根据所述第一量子比特串长度通过所述量子态制备基生成的第一量子比特串,所述第一量子比特串通过所述量子态制备基发送至客户端。

[0321] 在本申请提供的一个实施例中,所述客户端与所述服务端上均预先存储有相同的量子串长度数据库,所述第一动态交互验证信息还包括第一量子比特串长度代码;所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在量子态库中查询相应的量子态制备基、根据所述第一量子比特串长度代码在量子串长度数据库中查询相应的第一量子比特串长度,然后根据所述第一量子比特串长度通过所述量子态制备基生成第一量子比特串,所述第一量子比特串通过所述量子态制备基发送至客户端。

[0322] 在本申请提供的一个实施例中,所述第二动态交互验证信息还包括将所述第一量子比特串进行十进制转换后获得的十进制第一量子比特串。所述服务端在生成所述第一量子比特串后,还采用十进制转换方法将所述第一量子比特串转换为十进制第一量子比特串,并采用对称量子密钥加密后传输至所述客户端。所述接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息,还包括:接收所述服务端发送的根据所述第一动态交互验证信息生成的十进制第一量子比特串。

[0323] 在本申请提供的一个实施例中,所述第二动态交互验证信息是经过加密后发送的,因此,所述接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息的步骤,包括:

[0324] 接收所述服务端发送的至少部分信息已加密的根据所述第一动态交互验证信息生成的第二动态交互验证信息;

[0325] 采用与所述服务端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0326] 其中,所述解密密钥与所述服务端加密使用的密钥互为对称量子密钥,或互为公私密钥。

[0327] 仍以上述具体的优选实施例为例,服务端在通过对所述客户端的初步认证后,根据所述用户标识查找相应的对称量子密钥Key_AB,对$\{2,3;4,6\}_{Key_AB}$进行解密获得{2,3;4,6},查询量子态制备基标识2代表的量子态制备基a,利用所述量子态制备基a生成长度为3的比特串q1;以及查询量子态制备基标识4代表的量子态制备基b,利用所述量子态制备基b生成长度为6的比特串q2;由q1和q2共同组成第一量子比特串,由于所述第一量子比特串为量子态,因此,采用相应的量子态制备基发送至客户端。此外,服务端采用十进制转换方法将每个所述比特串转换成十进制比特串,比如将q1转换成十进制Q1,将q2转换成Q2,由Q1和Q2共同组成十进制第一量子比特串,然后采用对称量子密钥Key_AB加密后,将$\{Q1,Q2\}_{Key_AB}$传输至客户端,所述客户端在接收到所述$\{Q1,Q2\}_{Key_AB}$后,对其进行解密,获得十进制第一量子比特串Q1、Q2。

[0328] 步骤S104:根据所述第二动态交互验证信息判断所述服务端是否合法,以及根据所述第二动态交互验证信息生成第三动态交互验证信息。

[0329] 通过步骤S103,已接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息,接下来,需要根据所述第二动态交互验证信息判断所述服务端是否合法,以及根据所述第二动态交互验证信息生成第三动态交互验证信息。

[0330] 在本申请提供的一个实施例中,客户端和所述服务端上均预先存储有相应的或相

同的信息处理方法，所述客户端根据所述信息处理方法对动态交互验证信息的处理结果与所述服务端对所述动态交互验证信息的处理结果是相应的或相同的。基于上述设置，客户端生成第一动态交互验证信息后发送给服务端，由所述服务端根据所述第一动态交互验证信息按照预定的信息处理方法处理后生成第二动态交互验证信息，所述客户端在收到所述第二动态交互验证信息后，可采用相应的信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果是否符合预期或根据处理结果与所述第一动态交互验证信息的相关性判断所述服务端是否合法；也可以采用相应或相同的信息处理方法对所述第一动态交互验证信息进行处理，根据处理结果是否符合预期或根据处理结果与所述第二动态交互验证信息的相关性判断所述服务端是否合法。

[0331] 容易理解的是，上述实施例的本质在于，所述客户端将指定信息发送给所述服务端，所述服务端根据所述指定信息按照预定的处理方法处理生成验证信息后发送给所述客户端，所述客户端根据处理结果是否符合预期或根据所述验证信息与所述指定信息的关联性判断所述服务端的合法性。本申请并不限定所述指定信息、所述验证信息以及所述处理方法的具体形式，只要通过上述本质方法实现客户端对服务端的认证，均在本申请的保护范围之内，此处不再赘述。

[0332] 在本申请提供的一个实施例中，所述客户端和所述服务端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述客户端和所述服务端上均具有相应或相同的信息处理方法标识；

[0333] 所述动态交互验证信息中包含有信息处理方法标识；

[0334] 所述根据预先存储的信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果判断所述服务端是否合法的步骤，包括：

[0335] 根据所述第一动态交互验证信息中的信息处理方法标识查询对应的预先存储的信息处理方法；

[0336] 根据所述信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果是否符合预期判断所述服务端是否合法。

[0337] 在本申请提供的一个优选实施例中，客户端和所述服务端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识，所述第一动态交互验证信息包括所述量子态制备基标识；

[0338] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基，并通过所述量子态制备基生成第一量子比特串；

[0339] 所述根据所述第二动态交互验证信息判断所述服务端是否合法的步骤，包括：

[0340] 采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量，获得比特值测量结果；

[0341] 根据所述比特值测量结果是否符合预期判断所述服务端是否合法。

[0342] 容易理解的是，其中，所述量子态制备基标识对应的量子态制备基，对客户端来说是测量服务端发过来的第一量子比特串的测量基，对服务端来说，是发给客户端的第一量子比特串的量子态制备基。

[0343] 根据本申请提供的上述方法，所述第一量子比特串是基于所述客户端发送的量子

态制备基标识生成的，鉴于量子比特串具有不可克隆性和测试塌缩性，通过对所述第一量子比特串进行测量，根据所述比特值测量结果是否符合预期可以有效判断所述服务端是否合法，实现客户端对服务端的认证，同时，采用量子比特串作为动态验证信息，可以有效避免动态验证信息泄露，进而抵御中间人的攻击和伪造服务器发起的欺骗行为。

[0344] 考虑到对量子态本身具备的不确定性，对所述第一量子比特串的测量是基于概率判断所述比特值测量结果是否符合预期，为了进一步增加对所述服务端认证的准确性，在本申请提供的一个实施例中，所述第一动态交互验证信息还包括第一量子比特串长度；所述第二动态交互验证信息还包括将所述第一量子比特串进行十进制转换后获得的十进制第一量子比特串；

[0345] 所述根据所述第二动态交互验证信息判断所述服务端是否合法的步骤，包括：

[0346] 采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量，获得比特值测量结果；

[0347] 将所述十进制第一量子比特串按照十进制转换方法转换为转换后的第一量子比特串；

[0348] 测量所述第一量子比特串的长度，获得比特串长度测量结果；

[0349] 根据所述比特值测量结果是否符合预期和所述比特串长度测量结果是否符合预期判断所述服务端是否合法。

[0350] 其中，针对对所述第一量子比特串的测量，在本申请提供的一个实施例中，所述客户端与所述服务端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码，此种情况下，所述采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量的步骤，包括：

[0351] 在量子态库中查找与所述量子态制备基标识对应的量子态制备基；

[0352] 随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量。

[0353] 在上述实施例中，考虑到量子比特串在传输过程中由于光衰减会导致一定的误码率，判断所述比特值测量结果是否符合预期，可以是通过所述第一量子比特串的误码率是否符合预期进行判定，比如判断所述第一量子比特串的误码率是否低于预设的误码率阈值，例如预设的误码率阈值为6％，检测到的所述第一量子比特串的误码率为5％，则判断所述第一量子比特串的误码率符合预期，即所述比特值测量结果符合预期；此外，还可以通过正确率以及其他多个维度的判断方式判断所述比特值测量结果是否符合预期，此处不再赘述，其均在本申请的保护范围之内。

[0354] 在本申请提供的一个实施例中，判断所述比特串长度测量结果是否符合预期，可以是通过将所述比特串长度测量结果与所述第一量子比特串长度进行比较，因为所述第一量子比特串是根据所述第一量子比特串长度生成的，因此所述比特串长度测量结果不应大于所述第一量子比特串长度，同时考虑到光衰减的影响，所述比特串长度测量结果与所述第一量子比特串长度的差应该不超过预定的阈值，若不符合上述判定条件，则认为所述比特串长度测量结果不符合预期。

[0355] 在本申请提供的一个实施例中，所述根据所述第二动态交互验证信息生成第三动态交互验证信息的步骤，包括：

[0356] 将所述比特值测量结果及测量时使用的量子态的量子位标识作为第三动态交互

验证信息。

[0357] 这样，所述服务端可以采用所述量子位标识对应的量子态制备基的量子态对所述第一量子比特串进行测量，将服务端的比特值测量结果与客户端发送的比特值测量结果进行比对，若符合预设的判断条件，则可判断所述客户端合法，认证通过。

[0358] 仍以上述优选的具体实施例为例，客户端获得所述服务端利用量子态制备基发送的量子比特串q1、q2，以及利用对称量子密钥发送的十进制第一量子比特串Q1、Q2后，分别随机选择所述量子态制备基标识2、4对应的量子态制备基中的量子态对所述量子比特串q1、q2进行测量(此随机表示同一组正交态的两个量子态随机选其中一个，比如，对于量子态制备基标识为2的量子态制备基：{|0>,|1>}，在随机选择制备基过程中，随机选择的量子态可能是|0>，也可能是|1>，为了进行区分，可以对量子态做量子位标识，比如量子态|0>的量子位标识为2.1，量子态|1>的量子位标识为2.2，)，例如随机选择量子位标识为2.1的量子态和量子位标识为4.2的量子态分别对q1和q2进行测量，可以获得比特值测量结果为m，根据所述比特值测量结果m是符合预设的阈值条件判断所述比特值测量结果是否符合预期；同时，将所述十进制第一量子比特串Q1、Q2按照十进制转换方法转换为第一量子比特串q1、q2，通过测量获得所述第一量子比特串q1、q2的比特串长度测量结果，根据q1、q2的长度与所述第一动态交互验证信息中的第一量子比特串长度3、6的差异判断所述比特串长度测量结果是否符合预期；最后，根据所述比特值测量结果m是否符合预期和所述比特串长度测量结果是否符合预期即可判断所述服务端是否合法。之后，再将所述比特值测量结果m和测量时使用的量子态的量子位标识2.1、4.2发送给服务端，服务端即可利用所述量子位标识2.1、4.2对应的量子态对服务端的第一量子比特串q1、q2进行测量，获得第二量子比特值测量结果n，将服务端的所述第二量子比特值测量结果n和客户端的比特值测量结果m进行比对，根据其差异是否符合预期即可判断所述客户端是否通过认证。

[0359] 需要说明的是，上述实施例中仅以q1、q2进行举例说明，本申请并不限制所述量子比特串的数量和长度，以及具体的测量方法、长度判断方法和比对方法，任何能够实现本发明构思的具体实施方式，均在本申请的保护范围之内。

[0360] 在上述实施例中，采用所述比特值测量结果及测量时使用的量子态的量子位标识作为第三动态交互验证信息，供所述服务端进行测量、比对，完成对所述客户端的认证，除上述方式以外，服务端对客户端的认证，也可以采用上述客户端对服务端认证的方式，例如，在本申请提供的一个实施例中，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的代码及第二量子比特串长度；

[0361] 所述根据所述第二动态交互验证信息生成第三动态交互验证信息的步骤，包括：

[0362] 在量子态库中查询与所述服务端选择的量子态制备基的代码相对应的量子态制备基；

[0363] 根据所述第二量子比特串长度，通过所述量子态制备基生成第二量子比特串；

[0364] 生成包含所述第二量子比特串的第三动态交互验证信息。

[0365] 其中，所述第二量子比特串采用所述量子态制备基发送至服务端。

[0366] 这样，服务端再采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果，根据所述比特值测量结果是否符合预期即可判断所述客户端是否通过认证。

[0367] 在本申请提供的一个实施例中，所述根据所述第二动态交互验证信息生成第三动态交互验证信息的步骤，还包括：将所述第二量子比特串按照十进制转换方法进行转换，获得十进制第二量子比特串；

[0368] 所述生成包含所述第二量子比特串的第三动态交互验证信息的步骤，包括：

[0369] 生成包含所述第二量子比特串和所述十进制第二量子比特串的第三动态交互验证信息。

[0370] 其中，所述第二量子比特串采用所述量子态制备基发送至服务端，所述十进制第二量子比特串采用对称量子密钥加密后发送至服务端。

[0371] 这样，服务端再采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果，根据所述第二量子比特值测量结果是否符合预设的阈值条件判断所述第二量子比特值测量结果是否符合预期，以及测量所述第二量子比特串的长度，获得第二量子比特串长度测量结果，根据所述第二量子比特串长度测量结果与所述第二量子比特串长度的差值是否符合预设的条件判断所述第二量子比特串长度测量结果是否符合预期，根据所述比特值测量结果是否符合预期和所述比特串长度测量结果是否符合预期即可判断所述客户端是否通过认证。

[0372] 由于上述服务端对客户端的认证方法与前述客户端对服务端的认证方法类似，相关之处请参照前文所述，此处不再赘述。需要说明的是，本申请并不限制所述认证的具体方式，只要符合本申请发明构思的实施方式，均在本申请的保护范围之内。

[0373] 步骤S104：若合法，则将所述第三动态交互验证信息发送至服务端，以由所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0374] 通过步骤S105，已根据所述第二动态交互验证信息判断所述服务端是否合法，以及根据所述第二动态交互验证信息生成第三动态交互验证信息，若合法，则将所述第三动态交互验证信息发送至服务端，以由所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0375] 考虑到数据传输的安全性，在本申请提供的一个实施例中，所述客户端需要将所述第三动态交互验证信息的部分或全部进行加密后再行发送，同时可以采用https加密传输协议传输。所述若合法，则将所述第三动态交互验证信息发送至服务端的步骤，包括：

[0376] 若合法，则将全部或部分所述第三动态交互验证信息采用密钥加密后发送至服务端。

[0377] 仍以上述优选的具体实施例为例，所述客户端在认证所述服务端合法后，将所述比特值测量结果m和测量时使用的量子态的量子位标识2.1、4.2一起采用对称量子密钥Key_AB加密后发送给服务端，例如发送信息为：{比特值测量结果m，量子位标识2.1、量子位标识4.2}$_{Key\_AB}$。

[0378] 至此，通过步骤S101至步骤S105，完成了用于客户端的认证流程。服务端即可根据所述第三动态交互验证信息判断所述客户端是否通过认证。相较于传统的动态口令认证，本方法通过客户端与服务端的交互通信，实现了客户端与服务端的交互认证，可以防范假冒的服务器欺骗合法用户，同时，由于客户端和服务端均动态的利用对方的验证信息制作本方验证信息，再发给对方进行验证，因此，可以抵御中间人攻击，且可防御小数攻击，将所述验证信息采用量子态处理后，可以进一步提高验证信息传输及存储的安全性。

[0379] 在上述的实施例中，提供了一种用于客户端的认证方法，与之相对应的，本申请还提供一种用于客户端的认证装置。请参看图2，其为本申请提供的一种用于客户端的认证装置实施例的示意图。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。

[0380] 本实施例提供的一种用于客户端的认证装置，包括：第一动态交互验证信息生成单元101，用于生成第一动态交互验证信息；第一动态交互验证信息发送单元102，用于将所述第一动态交互验证信息发送至服务端；第二动态交互验证信息接收单元103，用于接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息；第二动态交互验证信息验证单元104，用于根据所述第二动态交互验证信息判断所述服务端是否合法，以及根据所述第二动态交互验证信息生成第三动态交互验证信息；第三动态交互验证信息发送单元105，用于若合法，则将所述第三动态交互验证信息发送至服务端，以供所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0381] 可选的，客户端和所述服务端上均预先存储有相应的或相同的信息处理方法，所述客户端根据所述信息处理方法对动态交互验证信息的处理结果与所述服务端对所述动态交互验证信息的处理结果是相应的或相同的；

[0382] 所述第二动态交互验证信息验证单元104包括：

[0383] 处理判断子单元，用于根据预先存储的信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果判断所述服务端是否合法。

[0384] 可选的，所述客户端和所述服务端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述客户端和所述服务端上均具有相应或相同的信息处理方法标识；

[0385] 所述动态交互验证信息中包含有信息处理方法标识；

[0386] 所述处理判断子单元，包括：

[0387] 处理方法查询子单元，用于根据所述第一动态交互验证信息中的信息处理方法标识查询对应的预先存储的信息处理方法；

[0388] 处理方法处理子单元，用于根据所述信息处理方法对所述第二动态交互验证信息进行处理，根据处理结果判断所述服务端是否合法。

[0389] 可选的，所述信息处理方法标识在所述客户端与所述服务端之间同步且定时变更。

[0390] 可选的，客户端和所述服务端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识，所述第一动态交互验证信息包括所述量子态制备基标识；

[0391] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基，并通过所述量子态制备基生成第一量子比特串；

[0392] 所述第二动态交互验证信息验证单元104包括：

[0393] 第一量子测量子单元，用于采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量，获得比特值测量结果；

[0394] 第一量子判断子单元，用于根据所述比特值测量结果是否符合预期判断所述服务端是否合法。

[0395] 可选的，所述第一动态交互验证信息生成单元101包括：

[0396] 第一制备基选择子单元，用于从量子态库中选择至少一种量子态制备基；

[0397] 第一标识提取子单元，用于提取所述量子态制备基的量子态制备基标识；

[0398] 第一验证信息生成子单元，用于生成包含所述量子态制备基标识的第一动态交互验证信息。

[0399] 可选的，所述从量子态库中选择至少一种量子态制备基采用随机选择的方式，每一次认证选择的量子态制备基均不相同。

[0400] 可选的，所述第一动态交互验证信息还包括第一量子比特串长度；

[0401] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在服务端查询相应的量子态制备基，并根据所述第一量子比特串长度通过所述量子态制备基生成的第一量子比特串，所述第一量子比特串通过所述量子态制备基发送至客户端。

[0402] 可选的，所述第二动态交互验证信息还包括将所述第一量子比特串进行十进制转换后获得的十进制第一量子比特串；

[0403] 所述第二动态交互验证信息验证单元104包括：

[0404] 第二量子测量子单元，用于采用与所述量子态制备基标识对应的量子态制备基对所述第一量子比特串的比特值进行测量，获得比特值测量结果；

[0405] 第二转换子单元，用于将所述十进制第一量子比特串按照十进制转换方法转换为转换后的第一量子比特串；

[0406] 第二长度测量子单元，用于测量所述第一量子比特串的长度，获得比特串长度测量结果；

[0407] 第二判断子单元，用于根据所述比特值测量结果是否符合预期和所述比特串长度测量结果是否符合预期判断所述服务端是否合法。

[0408] 可选的，所述客户端与所述服务端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码；

[0409] 所述第二动态交互验证信息包括所述服务端根据所述量子态制备基标识在量子态库中查询相应的量子态制备基、根据所述第一量子比特串长度代码在量子串长度数据库中查询相应的第一量子比特串长度，然后根据所述第一量子比特串长度通过所述量子态制备基生成第一量子比特串，所述第一量子比特串通过所述量子态制备基发送至客户端。

[0410] 可选的，所述第一量子测量子单元包括：

[0411] 第一量子查询子单元，用于在量子态库中查找与所述量子态制备基标识对应的量子态制备基；

[0412] 第一随机测量子单元，用于随机选择所述量子态制备基的量子态对所述第一量子比特串的比特值进行测量。

[0413] 可选的，所述第二动态交互验证信息验证单元104包括：

[0414] 第三动态验证信息生成子单元，用于将所述比特值测量结果及测量时使用的量子态的量子位标识作为第三动态交互验证信息。

[0415] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基标识及第二量子比特串长度；

[0416] 所述第二动态交互验证信息验证单元104包括：

[0417] 第二量子查询子单元，用于在量子态库中查询与所述服务端选择的量子态制备基标识相对应的量子态制备基；

[0418] 第二量子制备子单元，用于根据所述第二量子比特串长度，通过所述量子态制备基生成第二量子比特串；

[0419] 第三信息生成子单元，用于生成包含所述第二量子比特串的第三动态交互验证信息。

[0420] 可选的，所述第二动态交互验证信息验证单元104还包括：

[0421] 十进制转换子单元，用于将所述第二量子比特串按照十进制转换方法进行转换，获得十进制第二量子比特串；

[0422] 所述第三信息生成子单元包括：

[0423] 十进制第三信息生成子单元，用于生成包含所述第二量子比特串和所述十进制第二量子比特串的第三动态交互验证信息。

[0424] 可选的，所述第三动态交互验证信息发送单元105包括：

[0425] 第三动态交互验证信息量子发送子单元，用于若合法，则将所述第二量子比特串采用所述量子态制备基发送至服务端。

[0426] 可选的，所述客户端的量子态库与所述服务端的量子态库同步且按照预定的规则定时变更。

[0427] 可选的，所述第一动态交互验证信息包括客户端的身份标识，所述身份标识用于服务端对所述客户端进行初步认证。

[0428] 可选的，所述客户端的身份标识包括客户端的用户识别码和身份证书。

[0429] 可选的，所述第一动态交互验证信息发送单元102包括：

[0430] 第一动态交互验证信息加密子单元，用于将全部或部分所述第一动态交互验证信息采用密钥加密后发送至服务端；

[0431] 所述第三动态交互验证信息发送单元105包括：

[0432] 第三动态交互验证信息加密子单元，用于若合法，则将全部或部分所述第三动态交互验证信息采用密钥加密后发送至服务端。

[0433] 可选的，所述密钥与所述服务端解密使用的密钥互为对称量子密钥，或互为公私密钥。

[0434] 可选的，所述第二动态交互验证信息接收单元103包括：

[0435] 加密第二动态交互验证信息接收子单元，用于接收所述服务端发送的至少部分信息已加密的根据所述第一动态交互验证信息生成的第二动态交互验证信息；

[0436] 第二动态交互验证信息解密子单元，用于采用与所述服务端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0437] 可选的，所述解密密钥与所述服务端加密使用的密钥互为对称量子密钥，或互为公私密钥。

[0438] 以上，为本申请提供的一种用于客户端的认证装置的实施例。

[0439] 本申请还提供一种用于服务端的认证方法，请参考图3，其为本申请提供的一种用于服务端的认证方法实施例的流程图，本方法的执行主体为服务端，该方法是与前述用于客户端的认证方法配合实施的，部分内容不再赘述，请参照上述用于客户端的认证方法实

施例进行理解，所述方法包括如下步骤：

[0440] 步骤S201：接收客户端发送的第一动态交互验证信息。

[0441] 本步骤，首先，接收客户端发送的第一动态交互验证信息。

[0442] 其中，所述第一动态交互验证信息由客户端生成，用于服务端在接收到所述第一动态交互验证信息后，根据所述第一动态交互验证信息生成第二动态交互验证信息，如此，客户端在接收到所述服务端发送的第二动态交互验证信息后，根据所述第二动态交互验证信息与所述第一动态交互验证信息的关联性，即可识别所述服务端是否合法，实现客户端对服务端的认证，有效抵御假冒服务器和中间人攻击。

[0443] 为了提高信息传输的安全性，在本申请提供的一个实施例中，所述接收客户端发送的第一动态交互验证信息的步骤，包括：

[0444] 接收客户端发送的至少部分信息已加密的第一动态交互验证信息；

[0445] 采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0446] 其中，所述解密密钥与所述客户端加密使用的密钥互为对称量子密钥，或互为公私密钥。

[0447] 考虑到为了避免虚假客户端恶意攻击服务端，或伪造客户端进行认证，或非法用户访问，在本申请提供的一个实施例中，在接收客户端发送的第一动态交互验证信息的同时，还需要接收所述客户端的身份标识以进行初步认证，所述客户端的身份标识包括客户端的用户识别码和身份证书，若判断所述客户端的身份标识非法，则终止认证过程。

[0448] 步骤S202：根据所述第一动态交互验证信息生成第二动态交互验证信息。

[0449] 通过步骤S201，已接收客户端发送的第一动态交互验证信息，接下来根据所述第一动态交互验证信息生成第二动态交互验证信息。

[0450] 在本申请提供的一个实施例中，服务端和所述客户端上均预先存储有相应的或相同的信息处理方法，所述服务端根据所述信息处理方法对动态交互验证信息的处理结果与所述客户端对所述动态交互验证信息的处理结果是相应的或相同的；

[0451] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0452] 采用所述信息处理方法对所述第一动态交互验证信息进行处理，生成第二动态交互验证信息。

[0453] 在本申请提供的一个实施例中，所述服务端和所述客户端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述服务端和所述客户端上均具有相应或相同的信息处理方法标识；

[0454] 所述动态交互验证信息中包含有信息处理方法标识；

[0455] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0456] 根据所述第一动态交互验证信息中的信息处理方法标识查找对应的信息处理方法；

[0457] 采用所述信息处理方法对所述第一动态交互验证信息进行处理，生成第二动态交互验证信息。

[0458] 在本申请提供的一个实施例中，所述信息处理方法标识在所述服务端与所述客户端之间同步且定时变更。

[0459] 在本申请提供的一个优选的实施例中，服务端和所述客户端上均预先存储有相同

的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识；

[0460] 所述第一动态交互验证信息包括所述客户端选择的至少一种量子态制备基的量子态制备基标识；

[0461] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0462] 根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0463] 采用所述量子态制备基生成第一量子比特串；

[0464] 生成包含所述第一量子比特串的第二动态交互验证信息。

[0465] 在本申请提供的一个优选的实施例中，服务端和所述客户端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识；所述第一动态交互验证信息还包括第一量子比特串长度；

[0466] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0467] 根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0468] 根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

[0469] 将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

[0470] 生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

[0471] 作为上述实施方式的变更，在本申请提供的一个的实施例中，所述服务端与所述客户端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码；

[0472] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0473] 根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；以及

[0474] 根据所述第一量子比特串长度代码在所述量子串长度数据库中查找相应的第一量子比特串长度；

[0475] 根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

[0476] 将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

[0477] 生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

[0478] 在本申请提供的一个的实施例中，所述服务端的量子态库与所述客户端的量子态库同步且按照预定的规则定时变更。

[0479] 步骤S203：将所述第二动态交互验证信息发送至所述客户端。

[0480] 通过步骤S202，已根据所述第一动态交互验证信息生成第二动态交互验证信息，接下来，将所述第二动态交互验证信息发送至所述客户端，

[0481] 为了保证信息传输的安全性，在本申请提供的一个实施例中，所述将所述第二动态交互验证信息发送至所述客户端的步骤，包括：

[0482] 将全部或部分所述第二动态交互验证信息采用密钥加密后发送至服务端。

[0483] 其中，所述密钥与所述客户端解密使用的密钥互为对称量子密钥，或互为公私密钥。

[0484] 在本申请提供的一个实施例中，服务端和所述客户端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识；

[0485] 所述第一动态交互验证信息包括所述客户端选择的至少一种量子态制备基的量子态制备基标识；

[0486] 所述根据所述第一动态交互验证信息生成第二动态交互验证信息的步骤，包括：

[0487] 根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0488] 采用所述量子态制备基生成第一量子比特串；

[0489] 生成包含所述第一量子比特串的第二动态交互验证信息；

[0490] 所述将所述第二动态交互验证信息发送至所述客户端的步骤，包括：

[0491] 将所述第一量子比特串采用所述量子态制备基发送至所述客户端。

[0492] 步骤S204：接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息。

[0493] 通过步骤S203，将所述第二动态交互验证信息发送至所述客户端，接下来，接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息。

[0494] 客户端在接收到所述第二动态交互验证信息后，会根据所述第二动态交互验证信息判断所述服务端是否合法，以及根据所述第二动态交互验证信息生成第三动态交互验证信息。在判断所述服务端为合法时，将所述第三动态交互验证信息发送给服务端进行认证，由所述服务端判断所述客户端是否通过认证。

[0495] 在本申请提供的一个实施例中，所述第三动态交互验证信息包括所述客户端测量所述第二动态交互验证信息时采用的量子态的量子位标识以及比特值测量结果。

[0496] 在本申请提供的一个实施例中，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0497] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串。

[0498] 为了提高信息传输的安全性，在本申请提供的一个实施例中，所述接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息的步骤，包括：

[0499] 接收所述客户端发送的至少部分信息已加密的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

[0500] 采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0501] 其中，所述解密密钥与所述客户端加密使用的密钥互为对称量子密钥，或互为公私密钥。

[0502] 步骤S205：根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0503] 通过步骤S204，已接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息，接下来，根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0504] 在本申请提供的一个实施例中，服务端和所述客户端上均预先存储有相应的或相同的信息处理方法，所述服务端根据所述信息处理方法对动态交互验证信息的处理结果与所述客户端对所述动态交互验证信息的处理结果是相应的或相同的；

[0505] 所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

[0506] 采用与所述客户端相应的或相同的信息处理方法对所述第三动态交互验证信息进行处理，根据处理结果是否符合预期判断所述客户端是否通过认证。

[0507] 在本申请提供的一个实施例中，所述信息处理方法标识在所述服务端与所述客户端之间同步且定时变更。

[0508] 在本申请提供的一个实施例中，所述第三动态交互验证信息包括所述客户端测量所述第二动态交互验证信息时采用的量子态的量子位标识以及比特值测量结果；

[0509] 所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

[0510] 采用所述量子位标识对应的量子态测量所述第一量子比特串的比特值，获得服务端比特值测量结果；

[0511] 比较所述比特值测量结果与所述服务端比特值测量结果，根据比较结果是否符合预设的判断条件判断所述客户端是否通过认证。

[0512] 在本申请提供的一个实施例中，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0513] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串；

[0514] 所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

[0515] 采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

[0516] 根据所述第二量子比特值测量结果是否符合预期判断所述客户端是否通过认证。

[0517] 在本申请提供的一个实施例中，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0518] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串，以及将所述第二量子比特串进行十进制转换获得的十进制第二量子比特串；

[0519] 所述根据所述第三动态交互验证信息判断所述客户端是否通过认证的步骤，包括：

[0520] 采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

[0521] 将所述十进制第二量子比特串按照十进制转换方法转换为转换后的第二量子比特串；

[0522] 测量所述第二量子比特串的长度，获得第二量子比特串长度测量结果；

[0523] 根据所述第二量子比特值测量结果是否符合预期和所述第二量子比特串长度测量结果是否符合预期判断所述服务端是否通过认证。

[0524] 在本申请提供的一个实施例中，所述服务端的量子态库与所述客户端的量子态库同步且按照预定的规则定时变更。

[0525] 至此，通过步骤S201至步骤S205，完成了用于服务端的认证流程。

[0526] 在上述的实施例中，提供了一种用于服务端的认证方法，与之相对应的，本申请还提供一种用于服务端的认证装置。请参看图4，其为本申请提供的一种用于服务端的认证装置实施例的示意图。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。

[0527] 本实施例的一种用于客户端的认证装置，包括：第一动态交互验证信息接收单元201，用于接收客户端发送的第一动态交互验证信息；第二动态交互验证信息生成单元202，用于根据所述第一动态交互验证信息生成第二动态交互验证信息；第二动态交互验证信息发送单元203，用于将所述第二动态交互验证信息发送至所述客户端；第二动态交互验证信息发送单元204，用于接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息；第三动态交互验证信息判断单元205，用于根据所述第三动态交互验证信息判断所述客户端是否通过认证。

[0528] 可选的，服务端和所述客户端上均预先存储有相应的或相同的信息处理方法，所述服务端根据所述信息处理方法对动态交互验证信息的处理结果与所述客户端对所述动态交互验证信息的处理结果是相应的或相同的；

[0529] 所述第三动态交互验证信息判断单元205包括：

[0530] 第三动态交互验证信息处理子单元，用于采用与所述客户端相应的或相同的信息处理方法对所述第三动态交互验证信息进行处理，根据处理结果是否符合预期判断所述客户端是否通过认证。

[0531] 可选的，所述服务端和所述客户端上均预先存储有多组相应的或相同的信息处理方法，且每组所述信息处理方法在所述服务端和所述客户端上均具有相应或相同的信息处理方法标识；

[0532] 所述动态交互验证信息中包含有信息处理方法标识；

[0533] 所述第二动态交互验证信息生成单元202包括：

[0534] 处理方法查询子单元，用于根据所述第一动态交互验证信息中的信息处理方法标识查找对应的信息处理方法；

[0535] 第一信息处理子单元，用于采用所述信息处理方法对所述第一动态交互验证信息进行处理，生成第二动态交互验证信息。

[0536] 可选的，所述信息处理方法标识在所述服务端与所述客户端之间同步且定时变更。

[0537] 可选的，服务端和所述客户端上均预先存储有相同的含有量子态制备基的量子态库，所述量子态制备基用于制备量子比特串或测量量子比特串，每个所述量子态制备基均有对应的量子态制备基标识；

[0538] 所述第一动态交互验证信息包括所述客户端选择的至少一种量子态制备基的量子态制备基标识；

[0539] 所述第二动态交互验证信息生成单元202包括：

[0540] 第一服务端量子查询子单元，用于根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0541] 第一服务端比特串生成子单元，用于采用所述量子态制备基生成第一量子比特

串；

[0542] 第一服务端验证信息生成子单元，用于生成包含所述第一量子比特串的第二动态交互验证信息。

[0543] 可选的，所述第二动态交互验证信息发送单元203包括：

[0544] 第一量子比特串发送子单元，用于将所述第一量子比特串采用所述量子态制备基发送至所述客户端。

[0545] 可选的，所述第一动态交互验证信息还包括第一量子比特串长度；

[0546] 所述第二动态交互验证信息生成单元202包括：

[0547] 第二服务端量子查询子单元，用于根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0548] 第二服务端比特串生成子单元，用于根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

[0549] 第二十进制转换子单元，用于将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

[0550] 第二服务端验证信息生成子单元，用于生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

[0551] 可选的，所述服务端与所述客户端上均预先存储有相同的量子串长度数据库，所述第一动态交互验证信息还包括第一量子比特串长度代码；

[0552] 所述第二动态交互验证信息生成单元202包括：

[0553] 第三服务端量子查询子单元，根据所述量子态制备基标识在量子态库中查找相应的量子态制备基；

[0554] 第三服务端长度查询子单元，根据所述第一量子比特串长度代码在所述量子串长度数据库中查找相应的第一量子比特串长度；

[0555] 第三服务端比特串生成子单元，用于根据所述第一量子比特串长度采用所述量子态制备基生成第一量子比特串；

[0556] 第三十进制转换子单元，用于将所述第一量子比特串按照十进制转换方法转换为十进制第一量子比特串；

[0557] 第三服务端验证信息生成子单元，用于生成包含所述第一量子比特串和所述十进制第一量子比特串的第二动态交互验证信息。

[0558] 可选的，所述第三动态交互验证信息包括所述客户端测量所述第二动态交互验证信息时采用的量子态的量子位标识以及比特值测量结果；

[0559] 所述第三动态交互验证信息判断单元205包括：

[0560] 服务端第一量子串测量子单元，用于采用所述量子位标识对应的量子态测量所述第一量子比特串的比特值，获得服务端比特值测量结果；

[0561] 服务端测量比较子单元，用于比较所述比特值测量结果与所述服务端比特值测量结果，根据比较结果是否符合预设的判断条件判断所述客户端是否通过认证。

[0562] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0563] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备

基标识及第二量子比特串长度生成的第二量子比特串；

[0564] 所述第三动态交互验证信息判断单元205包括：

[0565] 第一服务端比特串测量子单元，用于采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

[0566] 第一服务端测量判断子单元，用于根据所述第二量子比特值测量结果是否符合预期判断所述客户端是否通过认证。

[0567] 可选的，所述第二动态交互验证信息还包括所述服务端选择的量子态制备基的量子态制备基标识及第二量子比特串长度；

[0568] 所述第三动态交互验证信息包括所述客户端根据所述服务端选择的量子态制备基标识及第二量子比特串长度生成的第二量子比特串，以及将所述第二量子比特串进行十进制转换获得的十进制第二量子比特串；

[0569] 所述第三动态交互验证信息判断单元205包括：

[0570] 第二服务端比特串测量子单元，用于采用所述服务端选择的量子态制备基对所述第二量子比特串的比特值进行测量，获得第二量子比特值测量结果；

[0571] 第二服务端十进制转换子单元，用于将所述十进制第二量子比特串按照十进制转换方法转换为转换后的第二量子比特串；

[0572] 第二服务端长度判断子单元，用于测量所述第二量子比特串的长度，获得第二量子比特串长度测量结果；

[0573] 第二服务端测量判断子单元，用于根据所述第二量子比特值测量结果是否符合预期和所述第二量子比特串长度测量结果是否符合预期判断所述服务端是否通过认证。

[0574] 可选的，所述服务端的量子态库与所述客户端的量子态库同步且按照预定的规则定时变更。

[0575] 可选的，所述第一动态交互验证信息包括客户端的身份标识；

[0576] 所述第二动态交互验证信息生成单元202包括：

[0577] 初步认证子单元，用于根据所述客户端的身份标识对所述客户端进行初步认证；

[0578] 第二动态交互验证信息生成子单元，用于若初步认证通过，则根据所述第一动态交互验证信息生成第二动态交互验证信息。

[0579] 可选的，所述客户端的身份标识包括客户端的用户识别码和身份证书。

[0580] 可选的，所述第二动态交互验证信息发送单元203包括：

[0581] 加密第二动态交互验证信息发送子单元，用于将全部或部分所述第二动态交互验证信息采用密钥加密后发送至服务端。

[0582] 可选的，所述密钥与所述客户端解密使用的密钥互为对称量子密钥，或互为公私密钥。

[0583] 可选的，所述第一动态交互验证信息接收单元201包括：

[0584] 加密第一动态交互验证信息接收子单元，用于接收客户端发送的至少部分信息已加密的第一动态交互验证信息；

[0585] 第一动态交互验证信息解密子单元，用于采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密；

[0586] 所述第二动态交互验证信息发送单元204包括：

[0587] 加密第三动态交互验证信息接收子单元，用于接收所述客户端发送的至少部分信息已加密的根据所述第二动态交互验证信息生成的第三动态交互验证信息；

[0588] 第三动态交互验证信息解密子单元，用于采用与所述客户端加密使用的密钥相对应的解密密钥对加密部分信息进行解密。

[0589] 可选的，所述解密密钥与所述客户端加密使用的密钥互为对称量子密钥，或互为公私密钥。

[0590] 以上，为本申请提供的一种用于服务端的认证装置的实施例。

[0591] 本申请还提供一种用于客户端的认证终端设备，包括：

[0592] 中央处理器；

[0593] 输入输出单元；

[0594] 存储器；

[0595] 所述存储器中存储有本申请提供的用于客户端的认证方法；并在启动后能够根据上述方法运行。

[0596] 由于本用于客户端的认证终端设备使用上述用于客户端的认证方法，相关之处请参见上述用于客户端的认证方法的实施例说明，此处不再赘述。

[0597] 本申请还提供一种用于服务端的认证终端设备，包括：

[0598] 中央处理器；

[0599] 输入输出单元；

[0600] 存储器；

[0601] 所述存储器中存储有本申请提供的用于服务端的认证方法；并在启动后能够根据上述方法运行。

[0602] 由于本用于服务端的认证终端设备使用上述用于服务端的认证方法，相关之处请参见上述用于服务端的认证方法的实施例说明，此处不再赘述。

[0603] 本申请还提供了一种用于用户认证的系统，包括客户端和服务端，所述客户端配置有本申请提供的用于客户端的认证装置，所述服务端配置有本申请提供的用于服务端的认证装置。

[0604] 由于本系统的客户端配置有本申请提供的用于客户端的认证装置，服务端配置有本申请提供的用于服务端的认证装置，因此相关之处请参见上述用于客户端的认证装置的实施例说明以及用于服务端的认证装置的实施例说明，此处不再赘述。

[0605] 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。

[0606] 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。

[0607] 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。

[0608] 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。

[0609] 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。

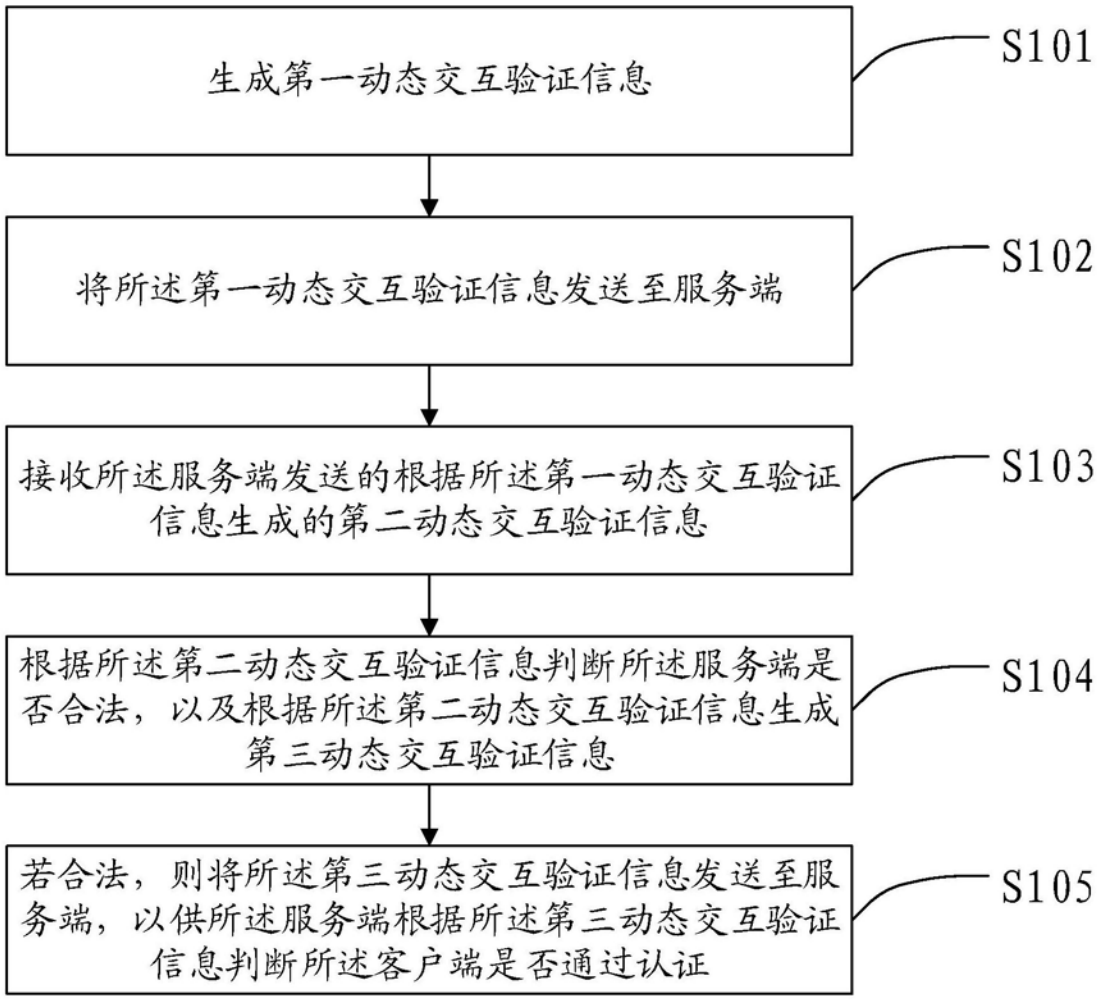

生成第一动态交互验证信息
S101
将所述第一动态交互验证信息发送至服务端
S102
接收所述服务端发送的根据所述第一动态交互验证信息生成的第二动态交互验证信息
S103
根据所述第二动态交互验证信息判断所述服务端是否合法，以及根据所述第二动态交互验证信息生成第三动态交互验证信息
S104
若合法，则将所述第三动态交互验证信息发送至服务端，以供所述服务端根据所述第三动态交互验证信息判断所述客户端是否通过认证
S105

图1

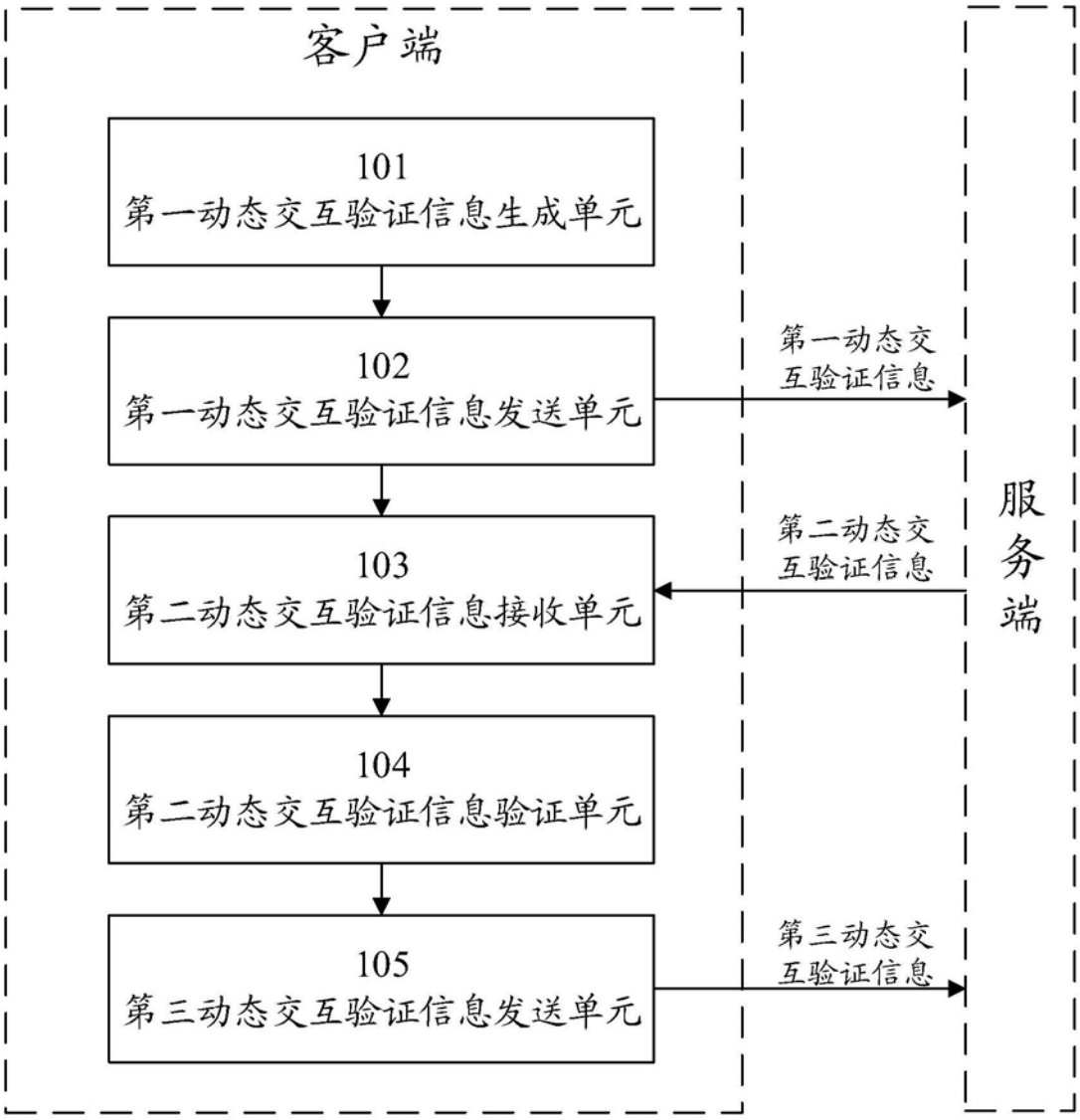

客户端
101
第一动态交互验证信息生成单元
102
第一动态交互验证信息发送单元
103
第二动态交互验证信息接收单元
104
第二动态交互验证信息验证单元
105
第三动态交互验证信息发送单元
第一动态交互验证信息
第二动态交互验证信息
第三动态交互验证信息
服务端

图2

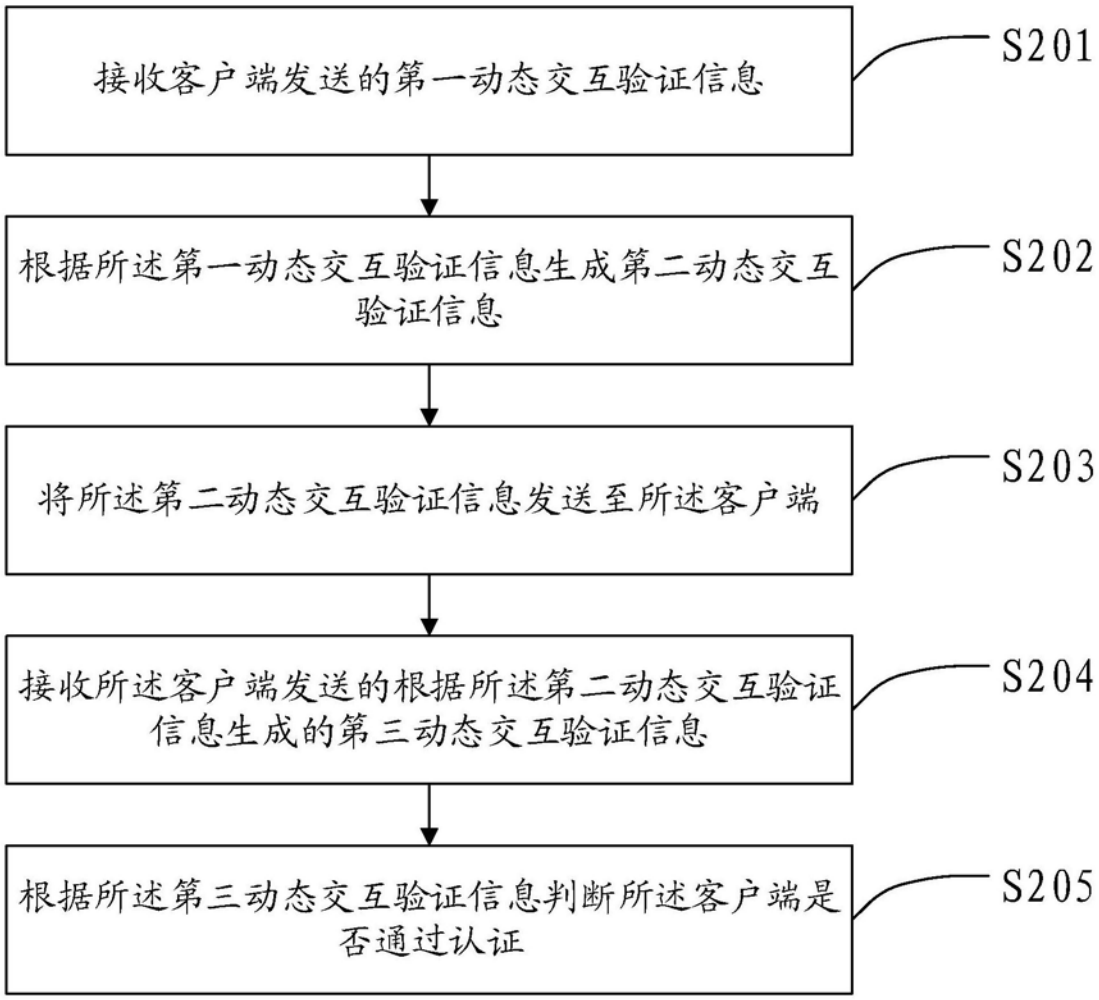

接收客户端发送的第一动态交互验证信息
S201
根据所述第一动态交互验证信息生成第二动态交互验证信息
S202
将所述第二动态交互验证信息发送至所述客户端
S203
接收所述客户端发送的根据所述第二动态交互验证信息生成的第三动态交互验证信息
S204
根据所述第三动态交互验证信息判断所述客户端是否通过认证
S205

图3

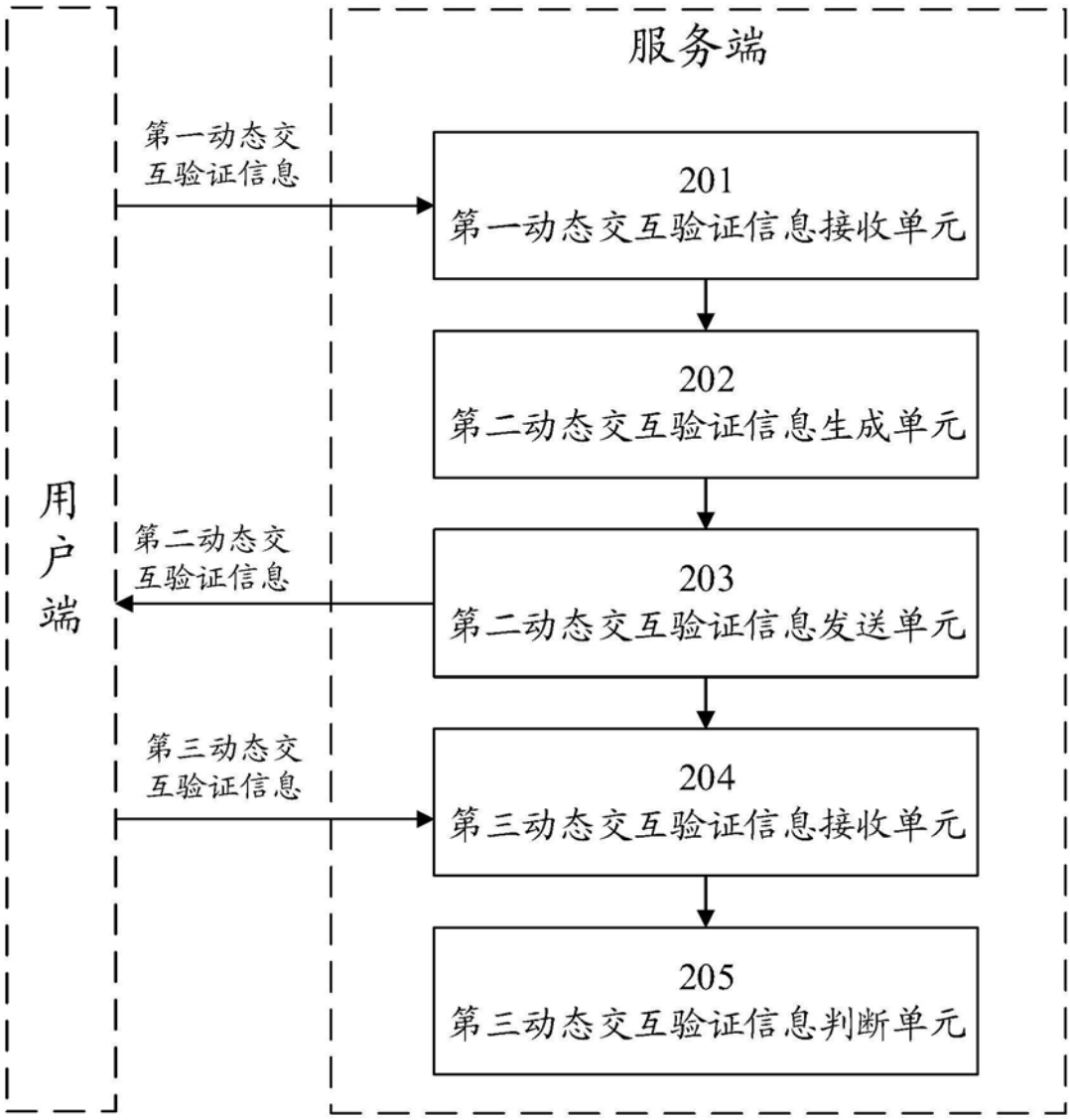

服务端
用户端
第一动态交互验证信息
第二动态交互验证信息
第三动态交互验证信息
201
第一动态交互验证信息接收单元
202
第二动态交互验证信息生成单元
203
第二动态交互验证信息发送单元
204
第三动态交互验证信息接收单元
205
第三动态交互验证信息判断单元

图4