(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116684093 A
(43)申请公布日 2023.09.01

(21)申请号 202310960937.2

(22)申请日 2023.08.02

(71)申请人 中电信量子科技有限公司
地址 230088 安徽省合肥市高新区创新产业园一期A3-812

(72)发明人 罗俊

(74)专利代理机构 合肥市浩智运专利代理事务所(普通合伙) 34124
专利代理师 闫客

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/12(2006.01)
H04L 9/40(2022.01)
H04L 9/32(2006.01)

权利要求书6页 说明书21页 附图6页

(54)发明名称

身份认证与密钥交换方法及系统

(57)摘要

本发明公开一种身份认证与密钥交换方法及系统,方法包括接收通信发起方发送的第一验证信息,并在第一验证信息验证通过后查询得到第一QKD节点的信息和第二QKD节点的信息;向第一QKD节点发送第一身份验证请求,以使第一QKD节点在验证第一身份验证请求通过后,在第一QKD节点和第二QKD节点生成会话密钥;接收第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息,并转发至第二QKD节点;在第二QKD节点存在与所述会话密钥的标识对应的会话密钥时,接收第二QKD节点发送的会话密钥的标识并将会话密钥的标识转发至通信发起方以使通信发起方携带会话密钥的标识向第一QKD节点申请会话密钥。

CN 116684093 A

1.一种身份认证与密钥交换方法,其特征在于,应用于身份提供方,所述方法包括:

接收通信发起方发送的第一验证信息,并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息;

向所述第一QKD节点发送第一身份验证请求,以使所述第一QKD节点在验证所述第一身份验证请求通过后,通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成,并在所述第一QKD节点和所述第二QKD节点生成会话密钥;

接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息,并转发至所述第二QKD节点;

在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时,接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

2.如权利要求1所述的身份认证与密钥交换方法,其特征在于,所述接收通信发起方发送的第一验证信息,并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息,包括:

接收通信发起方发送的预验证信息,所述预验证信息携带信息包括通信发起方标识、通信响应方标识和主密钥$K_{T_I}[i]$,所述主密钥为所述通信发起方和所述第一QKD节点预先共享;

将当前时间戳T_S返回至所述通信发起方;

接收所述通信发起方发送的第一验证信息,所述第一验证信息携带信息包括时间戳T_S和哈希值$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$,其中,$IP_I$为通信发起方IP地址、$IP_S$为身份提供方IP地址、$ID_I$为通信发起方标识、$ID_R$为通信响应方标识、$T_S$为时间戳,$h\{\ \}$表示哈希值计算,$\|$为拼接字符串,用于将字节串进行拼接;

验证时间戳T_S和$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$通过后,根据所述通信发起方标识和所述通信响应方标识查询得到所述第一QKD节点的信息和所述第二QKD节点的信息。

3.如权利要求1所述的身份认证与密钥交换方法,其特征在于,所述向所述第一QKD节点发送第一身份验证请求,包括:

利用自身产生的随机数N_S、与所述第一QKD节点预先共享的密钥K_{T_S}、主密钥$K_{T_I}[i]$以及所述第一QKD节点的信息和所述第二QKD节点的信息,生成所述第一身份验证请求;

向所述第一QKD节点发送所述第一身份验证请求,以使所述第一QKD节点采用密钥K_{T_S}验证所述第一QKD节点、所述第二QKD节点及所述身份提供方的真实性,以及采用主密钥$K_{T_I}[i]$验证所述通信发起方和所述通信响应方的真实性。

4.如权利要求1所述的身份认证与密钥交换方法,其特征在于,所述接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息,并转发至所述第二QKD节点,包括:

接收所述第一QKD节点发送的密钥分发会话消息,所述密钥分发会话消息采用密钥K_{T_S}和主密钥$K_{T_I}[i]$进行带密钥杂凑运算得到,且所述密钥分发会话消息携带有所述会话密钥、该会话密钥的标识ID_S及所述第一QKD节点产生的随机数N_T,其中所述密钥K_{T_S}为所述身份提供方与所述第一QKD节点预先共享,所述主密钥$K_{T_I}[i]$为所述通信发起方与所述第一

QKD节点预先共享，i表示主密钥的序号；

采用所述密钥K_{T_S}验证所述密钥分发会话消息通过后，将所述标识ID_S和会话信息采用密钥K_{A_S}进行带密钥的杂凑运算得到加密消息并将所述加密消息转发至所述第二QKD节点，所述密钥K_{A_S}为所述身份提供方与所述第二QKD节点预先共享。

5.如权利要求1所述的身份认证与密钥交换方法，其特征在于，所述在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时，接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥，包括：

接收所述第二QKD节点发送的标识加密信息，所述标识加密信息为所述第二QKD节点采用密钥K_{A_S}验证存在与所述会话密钥的标识对应的会话密钥后，采用主密钥$K_{A_R}[j]$对会话密钥的标识ID_S计算带密杂凑值得到，且所述标识加密信息携带有所述第二QKD节点产生的随机数N_A，所述密钥K_{A_S}为所述身份提供方与所述第二QKD节点预先共享，所述主密钥$K_{A_R}[j]$为所述通信响应方与所述第二QKD节点预先共享，j表示主密钥的序号；

采用密钥K_{A_S}验证所述标识加密信息通过后向所述通信发起方转发携带有所述会话密钥的标识的信息，以使所述通信发起方采用主密钥$K_{T_I}[i]$验证后得到所述会话密钥的标识并携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

6.一种身份认证与密钥交换方法，其特征在于，应用于通信发起方，所述方法包括：

向身份提供方发送第一验证信息，以使所述身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

接收所述身份提供方发送的携带有会话密钥的标识的信息，所述会话密钥为基于所述第一QKD节点和所述第二QKD节点之间的密钥分发信道，在所述第一QKD节点和所述第二QKD节点生成；

携带所述会话密钥的标识向所述第一QKD节点申请会话密钥；

生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥。

7.如权利要求6所述的身份认证与密钥交换方法，其特征在于，所述向身份提供方发送第一验证信息，以使所述身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息，包括：

采用主密钥$K_{T_I}[i]$对通信发送方标识、通信响应方标识进行带密钥的杂凑运算后附带主密钥$K_{T_I}[i]$序号一起发送至所述身份提供方；

接收所述身份提供方返回的当前时间戳T_S；

生成所述第一验证信息并发送至所述身份提供方，所述第一验证信息携带信息包括时间戳T_S和哈希值$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$，其中，$IP_I$为通信发起方IP地址、$IP_S$为身份提供方IP地址、$ID_I$为通信发起方标识、$ID_R$为通信响应方标识、$T_S$为时间戳，$h\{\ \}$表示哈希值计算，$\|$为拼接字符串，用于将字节串进行拼接。

8.如权利要求6所述的身份认证与密钥交换方法，其特征在于，所述接收所述身份提供方发送的携带有会话密钥的标识的信息，包括：

接收所述身份提供方发送的携带有会话密钥的标识的信息，并采用主密钥$K_{T_I}[i]$进行带密钥杂凑运算验证得到会话信息和会话密钥的标识，其中所述主密钥$K_{T_I}[i]$为所述通信发起方与所述第一QKD节点预先共享。

9.如权利要求6所述的身份认证与密钥交换方法，其特征在于，所述携带所述会话密钥的标识向所述第一QKD节点申请会话密钥，包括：

向所述第一QKD节点发送会话密钥申请信息，所述会话密钥申请信息携带信息包括会话密钥的标识、主密钥$K_{T_I}[i]$及所述通信发起方产生的随机数N_I；

接收所述第一QKD节点发送的第一保护信息，所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥、所述会话密钥的标识及所述随机数N_I进行加密保护得到；

采用主密钥$K_{T_I}[i]$对所述第一保护信息进行解密并验证得到所述会话密钥。

10.如权利要求9所述的身份认证与密钥交换方法，其特征在于，在所述采用主密钥$K_{T_I}[i]$对所述第一保护信息进行解密并验证得到所述会话密钥之后，所述方法还包括：

标记主密钥$K_{T_I}[i]$无效，并令$i=i+1$。

11.如权利要求6所述的身份认证与密钥交换方法，其特征在于，所述生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥，包括：

生成并向所述通信响应方发送加密通信请求报文以使所述通信响应方在使用主密钥$K_{A_R}[j]$验证加密通信请求报文通过后携带所述会话密钥的标识向所述第二QKD节点申请所述会话密钥，其中所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$、所述通信发起方产生的随机数N_I`、基于所述会话密钥衍生的密钥K_2和所述会话密钥的标识，所述主密钥$K_{A_R}[j]$为所述通信响应方与所述第二QKD节点预先共享。

12.如权利要求11所述的身份认证与密钥交换方法，其特征在于，所述基于所述会话密钥衍生的密钥K_2的公式表示为：

$$K_1 = H(h(K_{I\_R}))\{ID_s \| ID_I \| ID_R \| N_I` \| N_R`\}$$

$$K_2 = H(h(K_1))\{ID_s \| ID_I \| ID_R \| N_I` \| N_R` \| 0\}$$

式中，K_{I_R}为会话密钥，ID_s为身份提供方标识，ID_I为通信发起方标识，ID_R为通信响应方标识，N_I`为所述通信发起方产生的随机数，$N_R$`为所述通信响应方产生的随机数，$h()$为哈希计算，$H()$为带密钥的密码杂凑计算，$\|$表示字节串拼接。

13.一种身份认证与密钥交换方法，其特征在于，应用与通信响应方，所述方法包括：

接收通信发起方发送的加密通信请求报文，所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$和会话密钥的标识，所述主密钥$K_{A_R}[j]$为通信响应方与第二QKD节点预先共享；

使用主密钥$K_{A_R}[j]$验证所述加密通信请求报文通过后，向所述第二QKD节点发送会话密钥请求信息，所述会话密钥请求信息携带所述会话密钥的标识，所述第二QKD节点生成有所述会话密钥；

接收所述第二QKD节点返回的第二保护信息，所述第二保护信息为所述第二QKD节点使用主密钥$K_{A_R}[j]$加密所述会话密钥和所述会话密钥的标识得到；

采用主密钥$K_{A_R}[j]$对所述第二保护信息进行解密获得所述会话密钥，并向所述通信发

起方发送加密通信响应报文。

14.如权利要求13所述的身份认证与密钥交换方法，其特征在于，所述加密通信响应报文中携带有基于所述会话密钥衍生的密钥K_2，公式表示为：

$K_1 = H(h(K_{I\_R}))\{ID_S \| ID_I \| ID_R \| N_I` \| N_R`\}$

$K_2 = H(h(K_1))\{ID_S \| ID_I \| ID_R \| N_I` \| N_R` \| 0\}$

式中，K_{I_R}为会话密钥，ID_S为身份提供方标识，ID_I为通信发起方标识，ID_R为通信响应方标识，$N_I`$为所述通信发起方产生的随机数，$N_R`$为所述通信响应方产生的随机数，$h()$为哈希计算，$H()$为带密钥的密码杂凑计算，$\|$表示字节串拼接。

15.一种身份认证与密钥交换方法，其特征在于，应用于第一QKD节点，所述方法包括：

接收身份提供方发送的第一身份验证请求，并在验证通过后基于与通第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在第一QKD节点和第二QKD节点生成会话密钥，第一QKD节点与通信发起方连接，第二QKD节点与通信响应方连接；

生成携带有会话密钥的标识的密钥分发会话消息并发送至所述身份提供方，以使所述身份提供方将会话密钥的标识及会话信息发送至第二QKD节点；

在通信发起方获取到所述身份提供方分发送的所述会话密钥的标识后，接收所述通信发起方发送的会话密钥请求信息；

向所述通信发起方发送第一保护信息，所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥和所述会话密钥的标识进行加密保护得到。

16.如权利要求15所述的身份认证与密钥交换方法，其特征在于，所述生成携带有会话密钥的标识的密钥分发会话消息并发送至所述身份提供方，包括：

将所述会话密钥的标识分别采用密钥K_{T_S}和主密钥$K_{T_I}[i]$进行带密钥杂凑运算得到，其中，所述密钥K_{T_S}为所述身份提供方与所述第一QKD节点预先共享，所述主密钥$K_{T_I}[i]$为所述通信发起方与所述第一QKD节点预先共享，i表示主密钥的序号。

17.如权利要求15所述的身份认证与密钥交换方法，其特征在于，所述向所述通信发起方发送第一保护信息，包括：

使用主密钥$K_{T_I}[i]$加密所述会话密钥；

使用主密钥$K_{T_I}[i]$进行带密钥的杂凑运算对所述会话密钥的标识、所述会话密钥进行完整性保护，得到所述第一保护信息。

18.如权利要求15所述的身份认证与密钥交换方法，其特征在于，在所述向所述通信发起方发送第一保护信息之后，所述方法还包括：

标记主密钥$K_{T_I}[i]$无效，并删除采用所述会话密钥的标识进行表示的会话。

19.如权利要求15所述的身份认证与密钥交换方法，其特征在于，在所述接收身份提供方发送的第一身份验证请求之前，所述方法还包括：

为域内的通信节点使用量子随机数产生密钥池，所述密钥池中的主密钥采用ID号顺序标引。

20.一种身份提供端，其特征在于，包括：

验证信息接收模块，用于接收通信发起方发送的第一验证信息，并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二

QKD节点的信息；

验证请求发送模块，用于向所述第一QKD节点发送第一身份验证请求，以使所述第一QKD节点在验证所述第一身份验证请求通过后，通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在所述第一QKD节点和所述第二QKD节点生成会话密钥；

密钥分发会话消息接收模块，用于接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息，并转发至所述第二QKD节点；

标识接收模块，用于在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时，接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

21.一种通信发起终端，其特征在于，包括：

验证信息发送模块，用于向身份提供方发送第一验证信息，以使所述身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

标识信息接收模块，用于接收所述身份提供方发送的携带有会话密钥的标识的信息，所述会话密钥为基于所述第一QKD节点和所述第二QKD节点之间的密钥分发信道，在所述第一QKD节点和所述第二QKD节点生成；

第一会话密钥申请模块，用于携带所述会话密钥的标识向所述第一QKD节点申请会话密钥；

报文生成模块，用于生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥。

22.一种通信响应终端，其特征在于，包括：

报文接收模块，用于接收通信发起方发送的加密通信请求报文，所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$和会话密钥的标识，所述主密钥$K_{A_R}[j]$为通信响应方与第二QKD节点预先共享；

第一会话密钥申请模块，用于使用主密钥$K_{A_R}[j]$验证所述加密通信请求报文通过后，向所述第二QKD节点发送会话密钥请求信息，所述会话密钥请求信息携带所述会话密钥的标识，所述第二QKD节点生成有所述会话密钥；

保护信息接收模块，用于接收所述第二QKD节点返回的第二保护信息，所述第二保护信息为所述第二QKD节点使用主密钥$K_{A_R}[j]$加密所述会话密钥和所述会话密钥的标识得到；

响应报文发送模块，用于采用主密钥$K_{A_R}[j]$对所述第二保护信息进行解密获得所述会话密钥，并向所述通信发起方发送加密通信响应报文。

23.一种第一QKD节点，其特征在于，包括：

验证请求接收模块，用于接收身份提供方发送的第一身份验证请求，并在验证通过后基于与通第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在第一QKD节点和第二QKD节点生成会话密钥，第一QKD节点与通信发起方连接，第二QKD节点与通信响应方连接；

密钥分发会话消息生成模块，用于生成携带有会话密钥的标识的密钥分发会话消息并

发送至所述身份提供方，以使所述身份提供方将会话密钥的标识及会话信息发送至第二QKD节点；

密钥请求接收模块，用于在通信发起方获取到所述身份提供方分发送的所述会话密钥的标识后，接收所述通信发起方发送的会话密钥请求信息；

保护信息发送模块，用于向所述通信发起方发送第一保护信息，所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥和所述会话密钥的标识进行加密保护得到。

24.一种身份认证与密钥交换系统，其特征在于，所述系统包括通信发起方、通信响应方、身份提供方以及量子密钥分发网络，所述量子密钥分发网络中包括若干QKD节点，所述通信发起方与第一QKD节点连接，所述通信响应方与第二QKD节点连接，所述第一QKD节点和所述第二QKD节点均与所述身份提供方连接，所述通信发起方与所述通信响应方连接；

通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在所述第一QKD节点和所述第二QKD节点生成会话密钥；

所述身份提供方，用于根据所述通信发起方的标识和所述通信响应方的标识查找其所属安全域及所属QKD节点；

所述通信发起方，用于从所述第一QKD节点获取所述会话密钥，并采用所述会话密钥向所述通信响应方建立加密通信；

所述通信响应方，用于从所述第二QKD节点获取所述会话密钥，并采用所述会话密钥和所述通信发起方建立加密通信。

身份认证与密钥交换方法及系统

技术领域

[0001] 本发明涉及密码应用技术领域,具体涉及一种身份认证与密钥交换方法及系统。

背景技术

[0002] 典型的身份认证与密钥交换协议(Authentication and Key Agreement,AKA),在对称密码体制下有Kerberos,Keberos是为TCP/IP网络系统设计的可信的第三方认证协议;在基于公钥基础设施(Public Key Infrastructure,PKI)的非对称密码体制下有互联网密钥交换协议(Internet Key Exchange,IKE)和传输层安全协议(Transport Layer Security,TLS)等。这些身份认证与密钥协商协议(Authentication and Key Agreement,AKA)存在以下不足:

(1)整个Kerberos协议体系的安全性是基于预共享密钥这一长期有效的静态密钥的不可泄漏,而静态密钥的使用时间越长,被猜测或窃取的可能性越大,由此带来密钥管理的复杂性,跨域的密钥共享尤为困难。

[0003] (2)基于PKI的安全协议体系,私钥作为一种长期有效的静态密钥,随着使用频度的提高是有可能泄露的,而且随着量子计算技术的发展,通过公钥推算私钥在计算上将变得可行。虽然后量子密码算法(Post-Quantum Cryptography,PQC)在TLS等安全协议上的应用极大的缓解了量子计算的威胁,但目前PQC算法的实用化还存在不小的问题。此外,如果进行归属于不同CA证书系统的跨域访问,则需要通过层级结构的CA证书链或者数字证书的交叉认证来实现,复杂度相对高,效率相对较低,而且容易引入新的攻击面。

[0004] 在相关技术中,公布号为CN113612610A的专利申请文献中要求密钥交换服务器生成会话密钥,再通过与发起方和接收方的密钥验证使得通信双方的会话密钥得到安全协商。公布号为CN113630248A的专利申请文献中要求通信发起方主动生成会话密钥,再通过与接收方和服务器的密钥验证使得通信双方的会话密钥得到安全协商。这两种会话密钥协商方案中所有加密密钥和签名密钥均由密钥交换服务器统一管理,能够快速对密钥的使用情况进行响应。但这两件专利申请文献中所记载的密钥交换服务器实际上为密钥管理中心,通信双方的密钥通过该密钥交换服务器进行协商和交换,实质与经典的密钥分发相同。

发明内容

[0005] 本发明所要解决的技术问题在于如何确保风险较大的跨域密钥传输的安全性。

[0006] 本发明通过以下技术手段解决上述技术问题的:

第一方面,本发明提出了一种身份认证与密钥交换方法,应用于身份提供方,所述方法包括:

接收通信发起方发送的第一验证信息,并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息;

向所述第一QKD节点发送第一身份验证请求,以使所述第一QKD节点在验证所述第一身份验证请求通过后,通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发

起会话密钥的生成，并在所述第一QKD节点和所述第二QKD节点生成会话密钥；

接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息，并转发至所述第二QKD节点；

在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时，接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

[0007] 第二方面，本发明提出了一种身份认证与密钥交换方法，应用于通信发起方，所述方法包括：

向身份提供方发送第一验证信息，以使所述身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

接收所述身份提供方发送的携带有会话密钥的标识的信息，所述会话密钥为基于所述第一QKD节点和所述第二QKD节点之间的密钥分发信道，在所述第一QKD节点和所述第二QKD节点生成；

携带所述会话密钥的标识向所述第一QKD节点申请会话密钥；

生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥。

[0008] 第三方面，本发明提出了一种身份认证与密钥交换方法，应用与通信响应方，所述方法包括：

接收通信发起方发送的加密通信请求报文，所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$和会话密钥的标识，所述主密钥$K_{A_R}[j]$为通信响应方与第二QKD节点预先共享；

使用主密钥$K_{A_R}[j]$验证所述加密通信请求报文通过后，向所述第二QKD节点发送会话密钥请求信息，所述会话密钥请求信息携带所述会话密钥的标识，所述第二QKD节点生成有所述会话密钥；

接收所述第二QKD节点返回的第二保护信息，所述第二保护信息为所述第二QKD节点使用主密钥$K_{A_R}[j]$加密所述会话密钥和所述会话密钥的标识得到；

采用主密钥$K_{A_R}[j]$对所述第二保护信息进行解密获得所述会话密钥，并向所述通信发起方发送加密通信响应报文。

[0009] 第四方面，本发明提出了一种身份认证与密钥交换方法，应用于第一QKD节点，所述方法包括：

接收身份提供方发送的第一身份验证请求，并在验证通过后基于与通第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在第一QKD节点和第二QKD节点生成会话密钥，第一QKD节点与通信发起方连接，第二QKD节点与通信响应方连接；

生成携带有会话密钥的标识的密钥分发会话消息并发送至所述身份提供方，以使所述身份提供方将会话密钥的标识及会话信息发送至第二QKD节点；

在通信发起方获取到所述身份提供方分发送的所述会话密钥的标识后，接收所述通信发起方发送的会话密钥请求信息；

向所述通信发起方发送第一保护信息，所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥和所述会话密钥的标识进行加密保护得到。

[0010] 第五方面，本发明提出了一种身份提供端，包括：

验证信息接收模块，用于接收通信发起方发送的第一验证信息，并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

验证请求发送模块，用于向所述第一QKD节点发送第一身份验证请求，以使所述第一QKD节点在验证所述第一身份验证请求通过后，通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在所述第一QKD节点和所述第二QKD节点生成会话密钥；

密钥分发会话消息接收模块，用于接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息，并转发至所述第二QKD节点；

标识接收模块，用于在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时，接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

[0011] 第六方面，本发明提出了一种通信发起终端，包括：

验证信息发送模块，用于向身份提供方发送第一验证信息，以使所述身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

标识信息接收模块，用于接收所述身份提供方发送的携带有会话密钥的标识的信息，所述会话密钥为基于所述第一QKD节点和所述第二QKD节点之间的密钥分发信道，在所述第一QKD节点和所述第二QKD节点生成；

第一会话密钥申请模块，用于携带所述会话密钥的标识向所述第一QKD节点申请会话密钥；

报文生成模块，用于生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥。

[0012] 第七方面，本发明提出了一种通信响应终端，包括：

报文接收模块，用于接收通信发起方发送的加密通信请求报文，所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$和会话密钥的标识，所述主密钥$K_{A_R}[j]$为通信响应方与第二QKD节点预先共享；

第一会话密钥申请模块，用于使用主密钥$K_{A_R}[j]$验证所述加密通信请求报文通过后，向所述第二QKD节点发送会话密钥请求信息，所述会话密钥请求信息携带所述会话密钥的标识，所述第二QKD节点生成有所述会话密钥；

保护信息接收模块，用于接收所述第二QKD节点返回的第二保护信息，所述第二保护信息为所述第二QKD节点使用主密钥$K_{A_R}[j]$加密所述会话密钥和所述会话密钥的标识得到；

响应报文发送模块，用于采用主密钥$K_{A_R}[j]$对所述第二保护信息进行解密获得所

述会话密钥,并向所述通信发起方发送加密通信响应报文。

[0013] 第八方面,本发明提出了一种第一QKD节点,包括:

验证请求接收模块,用于接收身份提供方发送的第一身份验证请求,并在验证通过后基于与通第二QKD节点之间的密钥分发信道发起会话密钥的生成,并在第一QKD节点和第二QKD节点生成会话密钥,第一QKD节点与通信发起方连接,第二QKD节点与通信响应方连接;

密钥分发会话消息生成模块,用于生成携带有会话密钥的标识的密钥分发会话消息并发送至所述身份提供方,以使所述身份提供方将会话密钥的标识及会话信息发送至第二QKD节点;

密钥请求接收模块,用于在通信发起方获取到所述身份提供方分发送的所述会话密钥的标识后,接收所述通信发起方发送的会话密钥请求信息;

保护信息发送模块,用于向所述通信发起方发送第一保护信息,所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥和所述会话密钥的标识进行加密保护得到。

[0014] 第九方面,本发明提出了一种身份认证与密钥交换系统,所述系统包括通信发起方、通信响应方、身份提供方以及量子密钥分发网络,所述量子密钥分发网络中包括若干QKD节点,所述通信发起方与第一QKD节点连接,所述通信响应方与第二QKD节点连接,所述第一QKD节点和所述第二QKD节点均与所述身份提供方连接,所述通信发起方与所述通信响应方连接;

通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成,并在所述第一QKD节点和所述第二QKD节点生成会话密钥;

所述身份提供方,用于根据所述通信发起方的标识和所述通信响应方的标识查找其所属安全域及所属QKD节点;

所述通信发起方,用于从所述第一QKD节点获取所述会话密钥,并采用所述会话密钥向所述通信响应方建立加密通信;

所述通信响应方,用于从所述第二QKD节点获取所述会话密钥,并采用所述会话密钥和所述通信发起方建立加密通信。

[0015] 本发明的优点在于:

(1)本发明提出的身份认证与密钥交换方法应用于属于不同安全域的设备或应用之间的加密通信,身份提供方仅提供通信节点和QKD节点的对应关系,会话密钥由不同QKD节点直接向所属通信节点分发,通过采用具备无条件物理安全特性的量子密钥分配(Quantum Key Distribution,QKD)信道进行不同安全域之间的加密通信会话密钥的传输和同步,是基于真正意义上的量子密钥分发QKD实现的,确保了风险较大的跨域密钥传输的安全性。

[0016] (2)整个协议交互过程采用对称密钥进行带密钥的杂凑计算和对称加解密计算来进行身份认证,满足信息传输机密性、完整性、不可追踪和前向/后向保密等安全属性,并且在通信效率与计算开销方面相较于身份认证与密钥交换协议AKA等其他的协议具备一定的优势。

[0017] (3)采用大容量安全介质承载的具备“一次一密”和“用完即毁”使用特点的预共享主密钥进行加密通信会话密钥在同一安全域内部的分发保护,具备前后向安全性。

[0018] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0019] 图1是本发明一实施例提出的一种身份认证与密钥交换方法的流程示意图；
图2是本发明一实施例提出的一种身份认证与密钥交换方法的流程示意图；
图3是本发明一实施例提出的一种身份认证与密钥交换方法的流程示意图；
图4是本发明一实施例提出的一种身份认证与密钥交换方法的流程示意图；
图5是本发明一实施例提出的一种身份提供端的结构示意图；
图6是本发明一实施例提出的一种通信发起终端的结构示意图；
图7是本发明一实施例提出的一种通信响应终端的结构示意图；
图8是本发明一实施例提出的一种第一QKD节点的结构示意图；
图9是本发明一实施例提出的一种身份认证与密钥交换系统的结构示意图；
图10是本发明一实施例提出的一种身份认证与密钥交换系统的工作流程图。

具体实施方式

[0020] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0021] 实施例1

如图1所示，本发明第一实施例公开了一种身份认证与密钥交换方法，应用于身份提供方，所述方法包括以下步骤：

S101、接收通信发起方发送的第一验证信息，并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

S102、向所述第一QKD节点发送第一身份验证请求，以使所述第一QKD节点在验证所述第一身份验证请求通过后，通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在所述第一QKD节点和所述第二QKD节点生成会话密钥；

S103、接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息，并转发至所述第二QKD节点；

S104、在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时，接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

[0022] 本实施例通过采用具备无条件物理安全特性的量子密钥分配信道进行不同安全域之间的加密通信会话密钥的传输，确保了风险较大的跨域密钥传输的安全性。

[0023] 在一实施例中，所述步骤S101：接收通信发起方发送的第一验证信息，并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息，具体包括以下步骤：

S111、接收通信发起方发送的预验证信息，所述预验证信息携带信息包括通信发

起方标识、通信响应方标识和主密钥$K_{T_I}[i]$，所述主密钥为所述通信发起方和所述第一QKD节点预先共享；

具体地，通信发起方I将自己的标识ID_I和通信响应方R的标识ID_R发给身份提供方S，通信发起方I从自身的大容量安全介质中按序选择有效的且和第一QKD节点T共享的预主密钥$K_{T_I}[i]$对通信双方标识信息及主密钥序号i进行带密钥的杂凑运算后附带主密钥序号i一起发给身份提供方S，表示形式为：

$$I \rightarrow S: \{ID_S \| ID_I \| ID_R \| i \| H(K_{T\_I}[i])\{ID_I \| ID_R \| i\}\}$$

式中：$I \rightarrow S$表示通信发起方I向身份提供方S发送消息，ID_S为身份提供方的标识，$H(K_{T_I}[i])\{ID_I \| ID_R \| i\}$表示对$\{ID_I \| ID_R \| i\}$进行带主密钥$K_{T_I}[i]$的杂凑运算，$\|$表示将字节串进行拼接。

[0024] S112、将当前时间戳T_S返回至所述通信发起方，表示形式为：

$$S \rightarrow I: \{T_S\}$$

式中，$S \rightarrow I$表示身份提供方S向通信发起方I发送消息。

[0025] S113、接收所述通信发起方发送的第一验证信息，所述第一验证信息携带信息包括时间戳T_S和哈希值$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$，其中，$IP_I$为通信发起方IP地址、$IP_S$为身份提供方IP地址、$ID_I$为通信发起方标识、$ID_R$为通信响应方标识、$T_S$为时间戳，$h\{\ \}$表示哈希值计算，$\|$为拼接字符串，用于将字节串进行拼接；

具体地，通信发起方I计算$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$，将该计算结果与时间戳一起发给身份提供方$S$，表示形式为：

$$I \rightarrow S: \{ID_S \| ID_I \| ID_R \| i \| T_S \| h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\} \| H(K_{T\_I}[i])\{ID_I \| ID_R \| i\}\}$$

式中，$I \rightarrow S$表示通信发起方I向身份提供方S发送消息，IP_I表示通信发起方IP地址，IP_S表示身份提供方IP地址，$\|$为拼接字符串，$h\{\}$表示哈希计算，$H()$表示带密钥的密码杂凑计算。

[0026] S114、验证时间戳T_S和$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$通过后，根据所述通信发起方标识和所述通信响应方标识查询得到所述第一QKD节点的信息和所述第二QKD节点的信息。

[0027] 具体地，身份提供方S验证时间戳T_S在当前时间窗口范围内，计算并验证$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$，通过后根据$ID_I$和$ID_R$查询自身数据库得到通信发起方和通信响应方对应的第一QKD节点T的标识信息ID_T和第二QKD节点A的标识信息ID_A，并向第一QKD节点T进行发起方身份验证。

[0028] 需要说明的是，本实施例为各通信节点即通信发起方和通信响应方分别配备一个大容量安全介质，具有2M字节以上的密钥存储空间，以密钥长度为128比特位的AES或SM4算法为参照，可存储10万条以上的密钥。利用各安全域的QKD节点为域内的每个通信节点使用量子随机数产生容量不小于10万条密钥的密钥池(密钥池中的主密钥由32比特位以上的ID号顺序索引)，将密钥池拷贝到各通信节点的大容量安全介质中存储并将安全介质分发给通信节点使用。所有的QKD节点和通信节点均在身份提供方S(也可称为IDP)注册并登记从属关系。

[0029] 在一实施例中，所述步骤S102：向所述第一QKD节点发送第一身份验证请求，包括以下步骤：

S121、利用自身产生的随机数N_S、与所述第一QKD节点预先共享的密钥K_{T_S}、主密钥$K_{T_I}[i]$以及所述第一QKD节点的信息和所述第二QKD节点的信息，生成所述第一身份验证请求；

具体地，身份提供方S向第一QKD节点T进行发起方身份验证，生成的第一身份验证请求的表示形式为：

$$S\rightarrow T:\{ID_S\|ID_T\|ID_A\|ID_I\|ID_R\|i\|N_S\|H(K_{T\_I}[i])\{ID_I\|ID_R\|i\}\|H(K_{T\_S})\{ID_S\|ID_T\|ID_A\|ID_I\|ID_R\|N_S\}\}$$

式中，$S\rightarrow T$表示身份提供方S向第一QKD节点T发送消息，N_S为身份提供方S产生的随机数。

[0030] S122、向所述第一QKD节点发送所述第一身份验证请求，以使所述第一QKD节点采用密钥K_{T_S}验证所述第一QKD节点、所述第二QKD节点及所述身份提供方的真实性，以及采用主密钥$K_{T_I}[i]$验证所述通信发起方和所述通信响应方的真实性。

[0031] 具体地，第一QKD节点T采用密钥K_{T_S}验证身份提供方S的身份及第一QKD节点的标识ID_T和第二QKD节点的标识ID_A的真实性，确认主密钥$K_{T_I}[i]$的有效性并采用$K_{T_I}[i]$验证通信发起者的身份ID_I和通信响应方的身份ID_R的真实性，验证通过后基于和第一QKD节点和第二QKD节点之间的QKD密钥分发信道发起会话密钥的生成和同步传输，同时QKD信道两端生成相应的会话密钥ID-ID_s，第一QKD节点T使用会话密钥的标识ID_s标识该次密钥分发会话$(ID_s:K_{I_R},ID_I,ID_R)$，K_{I_R}为会话密钥。

[0032] 在一实施例中，所述步骤S103：所述接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息，并转发至所述第二QKD节点，包括以下步骤：

S131、接收所述第一QKD节点发送的密钥分发会话消息，所述密钥分发会话消息采用密钥K_{T_S}和主密钥$K_{T_I}[i]$进行带密钥杂凑运算得到，且所述密钥分发会话消息携带有所述会话密钥、该会话密钥的标识ID_s及所述第一QKD节点产生的随机数N_T，其中所述密钥K_{T_S}为所述身份提供方与所述第一QKD节点预先共享，所述主密钥$K_{T_I}[i]$为所述通信发起方与所述第一QKD节点预先共享，i表示主密钥的序号；

具体地，第一QKD节点将会话标识ID_s分别用K_{T_S}和$K_{T_I}[i]$进行带密钥杂凑运算并新产生随机数N_T发给身份提供方S，表示形式为：

$$T\rightarrow S:\{ID_S\|ID_T\|ID_I\|ID_R\|ID_s\|i\|N_T\|N_S\|H(K_{T\_I}[i])\{ID_s\|ID_T\|ID_I\|ID_R\|i\|N_T\}\|H(K_{T\_S})\{ID_S\|ID_T\|ID_I\|N_S\|N_T\}\}$$

式中，$T\rightarrow S$表示第一QKD节点T向身份提供方S发送消息，N_T为所述第一QKD节点产生的随机数。

[0033] S132、采用所述密钥K_{T_S}验证所述密钥分发会话消息通过后，将所述标识ID_s和会话信息采用密钥K_{A_S}进行带密钥的杂凑运算得到加密消息并将所述加密消息转发至所述第二QKD节点，所述密钥K_{A_S}为所述身份提供方与所述第二QKD节点预先共享。

[0034] 具体地，身份提供方S采用密钥K_{T_S}验证消息后，将会话标识ID_s和会话信息采用密钥K_{A_S}进行带密钥杂凑运算并发给第二QKD节点A，表示形式为：

$$S\rightarrow A:\{ID_A\|ID_S\|ID_T\|ID_R\|ID_I\|ID_s\|N_S`\|H(K_{A\_S})\{ID_A\|ID_S\|ID_T\|ID_R\|ID_I\|ID_s\|N_S`\}\}$$

式中，$S\rightarrow A$表示身份提供方S向第二QKD节点发送消息，$N_S`$为身份提供方产生的随机数。

[0035] 这里会话信息指的是会话参与方的标识：ID_A、ID_T、ID_R、ID_I。

[0036] 在一实施例中，所述步骤S104：在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时，接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥，包括以下步骤：

S141、接收所述第二QKD节点发送的标识加密信息，所述标识加密信息为所述第二QKD节点采用密钥K_{A_S}验证存在与所述会话密钥的标识对应的会话密钥后，采用主密钥$K_{A_R}[j]$对会话密钥的标识ID_s计算带密杂凑值得到，且所述标识加密信息携带有所述第二QKD节点产生的随机数N_A，所述密钥K_{A_S}为所述身份提供方与所述第二QKD节点预先共享，所述主密钥$K_{A_R}[j]$为所述通信响应方与所述第二QKD节点预先共享，j表示主密钥的序号；

具体地，第二QKD节点A采用密钥K_{A_S}验证并确认存在ID_s所标识的会话密钥时，使用ID_s标识该次密钥分发会话（ID_s:K_{I_R},ID_I,ID_R），并从密钥池中按序选择和通信响应方共享的有效预主密钥$K_{A_R}[j]$，j为主密钥序号，对会话标识ID_s计算带密钥杂凑值并新产生随机数N_A后发送给身份提供方S，表示形式为：

$$A\rightarrow S:\{ID_S\|ID_A\|ID_T\|ID_I\|ID_R\|j\|ID_s\|N_A\|N_S`\|H(K_{A\_S})\{ID_S\|ID_A\|ID_R\|N_A\|N_S`\}\|H(K_{A\_R}[j])\{ID_s\|ID_A\|ID_R\|ID_I\|j\|N_A\}\}$$

式中，$A\rightarrow S$表示第二QKD节点向身份提供方S发送消息，N_A为第二QKD节点产生的随机数。

[0037] S142、采用密钥K_{A_S}验证所述标识加密信息通过后向所述通信发起方转发携带有所述会话密钥的标识的信息，以使所述通信发起方采用主密钥$K_{T_I}[i]$验证后得到所述会话密钥的标识并携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

[0038] 具体地，身份提供方S采用密钥K_{A_S}验证消息后，将相关信息转发给通信发起方I，表示形式为：

$S\rightarrow I$：

$$\{ID_I\|ID_S\|ID_s\|ID_R\|i\|j\|N_T\|N_A\|H(K_{T\_I}[i])\{ID_s\|ID_T\|ID_I\|ID_R\|i\|N_T\}\|H(K_{A\_R}[j])\{ID_s\|ID_A\|ID_R\|ID_I\|j\|N_A\}\}$$

$S\rightarrow I$表示身份提供方S向通信发起方I发送消息，以使通信发起方I使用主密钥$K_{T_I}[i]$进行带密钥杂凑运算验证并保存会话信息，携带会话标识向第一QKD节点T申请会话密钥。

[0039] 需要说明的是，整个协议交互过程采用对称密钥进行带密钥的杂凑计算和对称加解密计算来进行身份认证，满足信息传输机密性、完整性、不可追踪和前向/后向保密等安全属性，并且在通信效率与计算开销方面相较于身份认证与密钥交换协议AKA等其他的协议具备一定的优势。

[0040] 实施例2

如图2所示，本发明第二实施例公开了一种身份认证与密钥交换方法，应用于通信发起方，所述方法包括以下步骤：

S201、向身份提供方发送第一验证信息，以使所述身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

S202、接收所述身份提供方发送的携带有会话密钥的标识的信息，所述会话密钥为基于所述第一QKD节点和所述第二QKD节点之间的密钥分发信道，在所述第一QKD节点和所述第二QKD节点生成；

S203、携带所述会话密钥的标识向所述第一QKD节点申请会话密钥；

S204、生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥。

[0041] 本实施例在身份认证与密钥交换协议中，采用具备无条件物理安全特性的量子密钥分配信道进行不同安全域之间的加密通信会话密钥的传输，确保了风险较大的跨域密钥传输的安全性。

[0042] 在一实施例中，所述步骤S201：向身份提供方发送第一验证信息，以使所述身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息，包括以下步骤：

S211、采用主密钥$K_{T_I}[i]$对通信发送方标识、通信响应方标识进行带密钥的杂凑运算后附带主密钥$K_{T_I}[i]$序号一起发送至所述身份提供方，表示形式为：

$$I\rightarrow S:\{ID_S\|ID_I\|ID_R\|i\|H(K_{T\_I}[i])\{ID_I\|ID_R\|i\}\}$$

式中：$I\rightarrow S$表示通信发起方I向身份提供方S发送消息，ID_S为身份提供方的标识，$H(K_{T_I}[i])\{ID_I\|ID_R\|i\}$表示对$\{ID_I\|ID_R\|i\}$进行带主密钥$K_{T_I}[i]$的杂凑运算，$\|$表示字节串拼接。

[0043] S212、接收所述身份提供方返回的当前时间戳T_S；

S213、生成所述第一验证信息并发送至所述身份提供方，所述第一验证信息携带信息包括时间戳T_S和哈希值$h\{IP_I\|IP_S\|ID_I\|ID_R\|T_S\}$，其中，$IP_I$为通信发起方IP地址、$IP_S$为身份提供方IP地址、$ID_I$为通信发起方标识、$ID_R$为通信响应方标识、$T_S$为时间戳，$h\{\ \}$表示哈希值计算，$\|$为拼接字符串，用于将字节串进行拼接。

[0044] 具体地，通信发起方I计算$h\{IP_I\|IP_S\|ID_I\|ID_R\|T_S\}$，将该计算结果与时间戳一起发给身份提供方$S$，表示形式为：

$$I\rightarrow S:\{ID_S\|ID_I\|ID_R\|i\|T_S\|h\{IP_I\|IP_S\|ID_I\|ID_R\|T_S\}\|H(K_{T\_I}[i])\{ID_I\|ID_R\|i\}\}$$

式中，$I\rightarrow S$表示通信发起方I向身份提供方S发送消息，IP_I表示通信发起方IP地址，IP_S表示身份提供方IP地址，$\|$表示字节串拼接，$h\{\}$表示哈希计算，$H()$表示带密钥的密码杂凑计算。

[0045] 在一实施例中，所述步骤S202：接收所述身份提供方发送的携带有会话密钥的标识的信息，包括：

接收所述身份提供方发送的携带有会话密钥的标识的信息，并采用主密钥$K_{T_I}[i]$进行带密钥杂凑运算验证得到会话信息和会话密钥的标识，其中所述主密钥$K_{T_I}[i]$为所述通信发起方与所述第一QKD节点预先共享。

[0046] 具体地，所述携带有会话密钥的标识的信息的表示形式为：

$S\rightarrow I$:

$\{ID_I \| ID_S \| ID_s \| ID_R \| i \| j \| N_T \| N_A \| H(K_{T\_I}[i])\{ID_s \| ID_T \| ID_I \| ID_R \| i \| N_T\} \| H(K_{A\_R}[j])\{ID_s \| ID_A \| ID_R \| ID_I \| j \| N_A\}\}$

式中,N_A为第二QKD节点产生的随机数。

[0047] 所述通信发起方使用主密钥$K_{T_I}[i]$进行带密钥杂凑运算验证并保存会话信息和会话标识。

[0048] 在一实施例中,所述步骤S203:携带所述会话密钥的标识向所述第一QKD节点申请会话密钥,具体包括以下步骤:

S231、向所述第一QKD节点发送会话密钥申请信息,所述会话密钥申请信息携带信息包括会话密钥的标识、主密钥$K_{T_I}[i]$及所述通信发起方产生的随机数N_I;

具体地,所述通信发起方携带会话标识向第一QKD节点T申请会话密钥,表示形式为:

$I\rightarrow T$:$\{ID_T \| ID_I \| ID_s \| i \| N_I \| N_T \| H(K_{T\_I}[i])\{ID_s \| i \| N_I \| N_T\}\}$

其中,N_I为通信发起方新产生的随机数,N_T为第一QKD节点产生的随机数。

[0049] S232、接收所述第一QKD节点发送的第一保护信息,所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥、所述会话密钥的标识及所述随机数N_I进行加密保护得到;

具体地,第一QKD节点T使用主密钥$K_{T_I}[i]$加密会话密钥,然后使用主密钥$K_{T_I}[i]$进行带密钥杂凑运算对会话标识、会话密钥和随机数N_T进行完整性保护,发给通信发起方I,之后第一QKD节点T标记主密钥$K_{T_I}[i]$为无效并删除ID_s标识的会话,第一保护信息表示形式为:

$T\rightarrow I$:$\{ID_I \| ID_T \| ID_s \| i \| N_I \| E(K_{T\_I}[i])\{K_{I\_R}\} \| H(K_{T\_I}[i])\{ID_s \| i \| N_I \| E(K_{T\_I}[i])\{K_{I\_R}\}\}\}$

其中,$T\rightarrow I$表示第一QKD节点T向通信发起方I发送消息,K_{I_R}为会话密钥。

[0050] S233、采用主密钥$K_{T_I}[i]$对所述第一保护信息进行解密并验证得到所述会话密钥。

[0051] 具体地,通信发起方I使用主密钥$K_{T_I}[i]$解密并验证会话密钥K_{I_R},之后通信发起方I标记主密钥$K_{T_I}[i]$为无效并使$i=i+1$。

[0052] 需要说明的是,本实施例为各通信节点即通信发起方和通信响应方分别配备一个大容量安全介质。利用各安全域的QKD节点为域内的每个通信节点使用量子随机数产生密钥池(密钥池中的主密钥由32比特位以上的ID号顺序索引),将密钥池拷贝到各通信节点的大容量安全介质中存储并将安全介质分发给通信节点使用。

[0053] 本实施例采用大容量安全介质承载的具备“一次一密”和“用完即毁”使用特点的预共享主密钥进行加密通信会话密钥在同一安全域内部的分发保护,具备前后向安全性。

[0054] 在一实施例中,所述步骤S204:所述生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥,具体包括:

生成并向所述通信响应方发送加密通信请求报文以使所述通信响应方在使用主密钥$K_{A_R}[j]$验证加密通信请求报文通过后携带所述会话密钥的标识向所述第二QKD节点申

请所述会话密钥，其中所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$、所述通信发起方产生的随机数$N_I`$、基于所述会话密钥衍生的密钥K_2和所述会话密钥的标识，所述主密钥$K_{A_R}[j]$为所述通信响应方与所述第二QKD节点预先共享。

[0055] 具体地，通信发起方I向通信响应方R发送加密通信请求报文，表示形式为：

$I \rightarrow R$：

$\{ID_R \| ID_I \| ID_s \| j \| N_A \| N_I` \| H(K_2)\{ID_I \| ID_R \| N_I`\} \| H(K_{A\_R}[j])\{ID_s \| ID_A \| ID_R \| ID_I \| j \| N_A\}\}$

其中，$I \rightarrow R$表示通信发起方I向通信响应方R发送消息，$N_I`$为通信发起方新产生随机数，K_2为基于会话密钥进行密钥衍生得到的密钥。

[0056] 在一实施例中，所述基于所述会话密钥衍生的密钥K_2的公式表示为：

$K_1=H(h(K_{I\_R}))\{ID_s \| ID_I \| ID_R \| N_I` \| N_R`\}$

$K_2=H(h(K_1))\{ID_s \| ID_I \| ID_R \| N_I` \| N_R` \| 0\}$

式中，K_{I_R}为会话密钥，ID_s为身份提供方标识，ID_I为通信发起方标识，ID_R为通信响应方标识，$N_I`$为所述通信发起方产生的随机数，$N_R`$为所述通信响应方产生的随机数，$h()$为哈希计算，$H()$为带密钥的密码杂凑计算，P表示字节串拼接。

[0057] 本实施例整个协议交互过程采用对称密钥进行带密钥的杂凑计算和对称加解密计算来进行身份认证，满足信息传输机密性、完整性、不可追踪和前向/后向保密等安全属性，并且在通信效率与计算开销方面相较于身份认证与密钥交换协议AKA等其他的协议具备一定的优势。

[0058] 实施例3

如图3所示，本发明第三实施例提出了一种身份认证与密钥交换方法，应用与通信响应方，所述方法包括以下步骤：

S301、接收通信发起方发送的加密通信请求报文，所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$和会话密钥的标识，所述主密钥$K_{A_R}[j]$为通信响应方与第二QKD节点预先共享；

S302、使用主密钥$K_{A_R}[j]$验证所述加密通信请求报文通过后，向所述第二QKD节点发送会话密钥请求信息，所述会话密钥请求信息携带所述会话密钥的标识，所述第二QKD节点生成有所述会话密钥；

S303、接收所述第二QKD节点返回的第二保护信息，所述第二保护信息为所述第二QKD节点使用主密钥$K_{A_R}[j]$加密所述会话密钥和所述会话密钥的标识得到；

S304、采用主密钥$K_{A_R}[j]$对所述第二保护信息进行解密获得所述会话密钥，并向所述通信发起方发送加密通信响应报文。

[0059] 本实施例在身份认证与密钥交换协议中，采用具备无条件物理安全特性的量子密钥分配信道进行不同安全域之间的加密通信会话密钥的传输，确保了风险较大的跨域密钥传输的安全性。

[0060] 具体地，通信响应方R在接收到通信发起方发送的加密通信请求报文后，确认主密钥$K_{A_R}[j]$有效性并使用$K_{A_R}[j]$计算杂凑验证会话信息，携带会话标识向响应方QKD节点A申

请会话密钥：

$R\rightarrow A:\{ID_A\|ID_R\|ID_s\|j\|N_A\|N_R\|H(K_{A\_R}[j])\{ID_s\|ID_A\|ID_R\|ID_I\|j\|N_A\}\}$

其中，N_R为通信响应方新产生的随机数。

[0061] 第二QKD节点A使用主密钥$K_{A_R}[j]$加密会话密钥，然后进行带密钥杂凑运算对会话标识、会话密钥和随机数N_A进行完整性保护生成第二保护信息，发给通信响应方R，之后第二QKD节点A标记$K_{A_R}[j]$为无效并使$j=j+1$并删除ID_s标识的会话，第二保护信息表示形式为：

$A\rightarrow R:\{ID_R\|ID_A\|ID_s\|j\|N_R\|E(K_{A\_R}[j])\{K_{I\_R}\}\|H(K_{A\_R}[j])\{ID_s\|j\|N_R\|E(K_{A\_R}[j])\{K_{I\_R}\}\}\}$

通信响应方R使用主密钥$K_{A_R}[j]$解密获得会话密钥K_{I_R}后，计算并验证$H(h(K_{I_R}))\{ID_I\|ID_R\|N_I`\}$之后，向通信发起方$I$发送加密通信响应报文，表示形式为：

$R\rightarrow I:\{ID_I\|ID_R\|ID_s\|N_R`\|H(K_2)\{ID_I\|ID_R\|ID_s\|N_I`\|N_R`\}\}$

其中，$N_R`$为通信响应方新产生随机数，$N_I`$为通信发送方产生的随机数，K_2为基于会话密钥进行密钥衍生得到的密钥。

[0062] 在一实施例中，S通信发起方I和通信响应方R基于会话密钥K_{I_R}进行密钥衍生，按照具体加密通信协议的需求得到各数据流向的对称加密密钥、MAC密钥、初始化向量等，本实施例不涉及具体的加密通信协议和密码算法。密钥衍生过程为：

$K_1=H(h(K_{I\_R}))\{ID_s\|ID_I\|ID_R\|N_I`\|N_R`\}$

$K_2=H(h(K_1))\{ID_s\|ID_I\|ID_R\|N_I`\|N_R`\|0\}$

$K_3=H(h(K_1))\{ID_s\|ID_I\|ID_R\|N_I`\|N_R`\|1\}$。

[0063] 实施例4

如图4所示，本发明第四实施例提出了一种身份认证与密钥交换方法，应用于第一QKD节点，所述方法包括以下步骤：

S401、接收身份提供方发送的第一身份验证请求，并在验证通过后基于与通第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在第一QKD节点和第二QKD节点生成会话密钥，第一QKD节点与通信发起方连接，第二QKD节点与通信响应方连接；

S402、生成携带有会话密钥的标识的密钥分发会话消息并发送至所述身份提供方，以使所述身份提供方将会话密钥的标识及会话信息发送至第二QKD节点；

S403、在通信发起方获取到所述身份提供方分发送的所述会话密钥的标识后，接收所述通信发起方发送的会话密钥请求信息；

S404、向所述通信发起方发送第一保护信息，所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥和所述会话密钥的标识进行加密保护得到。

[0064] 本实施例采用具备无条件物理安全特性的量子密钥分配信道进行不同安全域之间的加密通信会话密钥的传输，确保了风险较大的跨域密钥传输的安全性。

[0065] 在一实施例中，所述步骤S402：所述生成携带有会话密钥的标识的密钥分发会话消息并发送至所述身份提供方，包括：

将所述会话密钥的标识分别采用密钥K_{T_S}和主密钥$K_{T_I}[i]$进行带密钥杂凑运算得到，其中，所述密钥K_{T_S}为所述身份提供方与所述第一QKD节点预先共享，所述主密钥$K_{T_I}[i]$

为所述通信发起方与所述第一QKD节点预先共享，i表示主密钥的序号。

[0066] 具体地，第一QKD节点将会话标识分别用密钥K_{T_S}和$K_{T_I}[i]$进行带密钥杂凑运算并新产生随机数N_T发给身份提供方S，表示形式为：

$T\rightarrow S$：

$\{ID_S \| ID_T \| ID_I \| ID_R \| ID_s \| i \| N_T \| N_S \| H(K_{T\_I}[i])\{ID_s \| ID_T \| ID_I \| ID_R \| i \| N_T\} \| H(K_{T\_S})\{ID_S \| ID_T \| ID_I \| N_S \| N_T\}\}$

身份提供方S采用K_{T_S}验证消息后，将会话标识和会话信息采用K_{A_S}进行带密钥杂凑运算并发给第二QKD节点A，表示形式为：

$S\rightarrow A$：$\{ID_A \| ID_S \| ID_T \| ID_R \| ID_I \| ID_s \| N_S` \| H(K_{A\_S})\{ID_A \| ID_S \| ID_T \| ID_R \| ID_I \| ID_s \| N_S`\}\}$

第二QKD节点A采用K_{A_S}验证并确认存在ID_s所标识的会话密钥，使用ID_s标识该次密钥分发会话（ID_s:K_{I_R},ID_I,ID_R），从密钥池中按序选择和通信响应方共享的有效预主密钥$K_{A_R}[j]$对会话标识计算带密钥杂凑值并新产生随机数N_A后发送给身份提供方S，表示形式为：

$A\rightarrow S$：$\{ID_S \| ID_A \| ID_T \| ID_I \| ID_R \| j \| ID_s \| N_A \| N_S` \| H(K_{A\_S})\{ID_S \| ID_A \| ID_R \| N_A \| N_S`\} \| H(K_{A\_R}[j])\{ID_s \| ID_A \| ID_R \| ID_I \| j \| N_A\}\}$

身份提供方S采用K_{A_S}验证消息后，将相关信息转发给通信发起方I，表示形式为：

$S\rightarrow I$：

$\{ID_I \| ID_S \| ID_s \| ID_R \| i \| j \| N_T \| N_A \| H(K_{T\_I}[i])\{ID_s \| ID_T \| ID_I \| ID_R \| i \| N_T\} \| H(K_{A\_R}[j])\{ID_s \| ID_A \| ID_R \| ID_I \| j \| N_A\}\}$

通信发起方I使用$K_{T_I}[i]$进行带密钥杂凑运算验证并保存会话信息，携带会话标识向发起方QKD节点T申请会话密钥，其中N_I为通信发起方新产生随机数，表示形式为：

$I\rightarrow T$：$\{ID_T \| ID_I \| ID_s \| i \| N_I \| N_T \| H(K_{T\_I}[i])\{ID_s \| i \| N_I \| N_T\}\}$。

[0067] 在一实施例中，第一QKD节点T使用$K_{T_I}[i]$加密会话密钥，然后使用$K_{T_I}[i]$进行带密钥杂凑运算对会话标识、会话密钥和随机数N_T进行完整性保护，得到第一保护信息发给通信发起方I，第一保护信息表示形式为：

$T\rightarrow I$：$\{ID_I \| ID_T \| ID_s \| i \| N_I \| E(K_{T\_I}[i])\{K_{I\_R}\} \| H(K_{T\_I}[i])\{ID_s \| i \| N_I \| E(K_{T\_I}[i])\{K_{I\_R}\}\}\}$。

[0068] 在一实施例中，在所述向所述通信发起方发送第一保护信息之后，所述方法还包括：

标记主密钥$K_{T_I}[i]$无效，并删除采用所述会话密钥的标识进行表示的会话。

[0069] 在一实施例中，在所述接收身份提供方发送的第一身份验证请求之前，所述方法还包括：

为域内的通信节点使用量子随机数产生密钥池，所述密钥池中的主密钥采用ID号顺序标引。

[0070] 实施例5

如图5所示，本发明第一实施例还提出了一种身份提供端，包括：

验证信息接收模块11，用于接收通信发起方发送的第一验证信息，并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

验证请求发送模块12，用于向所述第一QKD节点发送第一身份验证请求，以使所述第一QKD节点在验证所述第一身份验证请求通过后，通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在所述第一QKD节点和所述第二QKD节点生成会话密钥；

密钥分发会话消息接收模块13，用于接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息，并转发至所述第二QKD节点；

标识接收模块14，用于在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时，接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

[0071] 在一实施例中，所述验证信息接收模块11，用于：

接收通信发起方发送的预验证信息，所述预验证信息携带信息包括通信发起方标识、通信响应方标识和主密钥$K_{T_I}[i]$，所述主密钥为所述通信发起方和所述第一QKD节点预先共享；

将当前时间戳T_S返回至所述通信发起方；

接收所述通信发起方发送的第一验证信息，所述第一验证信息携带信息包括时间戳T_S和哈希值$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$，其中，$IP_I$为通信发起方IP地址、$IP_S$为身份提供方IP地址、$ID_I$为通信发起方标识、$ID_R$为通信响应方标识、$T_S$为时间戳，$h\{\ \}$表示哈希值计算，$\|$为拼接字符串，用于将字节串进行拼接；

验证时间戳T_S和$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$通过后，根据所述通信发起方标识和所述通信响应方标识查询得到所述第一QKD节点的信息和所述第二QKD节点的信息。

[0072] 在一实施例中，所述验证请求发送模块12，用于：

利用自身产生的随机数N_S、与所述第一QKD节点预先共享的密钥K_{T_S}、主密钥$K_{T_I}[i]$以及所述第一QKD节点的信息和所述第二QKD节点的信息，生成所述第一身份验证请求；

向所述第一QKD节点发送所述第一身份验证请求，以使所述第一QKD节点采用密钥K_{T_S}验证所述第一QKD节点、所述第二QKD节点及所述身份提供方的真实性，以及采用主密钥$K_{T_I}[i]$验证所述通信发起方和所述通信响应方的真实性。

[0073] 在一实施例中，所述密钥分发会话消息接收模块13，用于：

接收所述第一QKD节点发送的密钥分发会话消息，所述密钥分发会话消息采用密钥K_{T_S}和主密钥$K_{T_I}[i]$进行带密钥杂凑运算得到，且所述密钥分发会话消息携带有所述会话密钥、该会话密钥的标识ID_S及所述第一QKD节点产生的随机数N_T，其中所述密钥K_{T_S}为所述身份提供方与所述第一QKD节点预先共享，所述主密钥$K_{T_I}[i]$为所述通信发起方与所述第一QKD节点预先共享，i表示主密钥的序号；

采用所述密钥K_{T_S}验证所述密钥分发会话消息通过后，将所述标识ID_S和会话信息(参与方标识：ID_A、ID_T、ID_R、ID_I)采用密钥K_{A_S}进行带密钥的杂凑运算得到加密消息并将所

述加密消息转发至所述第二QKD节点，所述密钥K_{A_S}为所述身份提供方与所述第二QKD节点预先共享。

[0074] 在一实施例中，所述标识接收模块14，用于：

接收所述第二QKD节点发送的标识加密信息，所述标识加密信息为所述第二QKD节点采用密钥K_{A_S}验证存在与所述会话密钥的标识对应的会话密钥后，采用主密钥$K_{A_R}[j]$对会话密钥的标识ID_S计算带密杂凑值得到，且所述标识加密信息携带有所述第二QKD节点产生的随机数N_A，所述密钥K_{A_S}为所述身份提供方与所述第二QKD节点预先共享，所述主密钥$K_{A_R}[j]$为所述通信响应方与所述第二QKD节点预先共享，j表示主密钥的序号；

采用密钥K_{A_S}验证所述标识加密信息通过后向所述通信发起方转发携带有所述会话密钥的标识的信息，以使所述通信发起方采用主密钥$K_{T_I}[i]$验证后得到所述会话密钥的标识并携带所述会话密钥的标识向所述第一QKD节点申请会话密钥。

[0075] 需要说明的是，本发明所述身份提供端的其他实施例或具有实现方法可参照上述方法实施例1，此处不再赘余。

[0076] 实施例6

如图6所示，本发明第六实施例公开了一种通信发起终端，包括：

验证信息发送模块21，用于向身份提供方发送第一验证信息，以使所述身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息；

标识信息接收模块22，用于接收所述身份提供方发送的携带有会话密钥的标识的信息，所述会话密钥为基于所述第一QKD节点和所述第二QKD节点之间的密钥分发信道，在所述第一QKD节点和所述第二QKD节点生成；

第一会话密钥申请模块23，用于携带所述会话密钥的标识向所述第一QKD节点申请会话密钥；

报文生成模块24，用于生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥。

[0077] 在一实施例中，所述验证信息发送模块21，用于：

采用主密钥$K_{T_I}[i]$对通信发送方标识、通信响应方标识进行带密钥的杂凑运算后附带主密钥$K_{T_I}[i]$序号一起发送至所述身份提供方；

接收所述身份提供方返回的当前时间戳T_S；

生成所述第一验证信息并发送至所述身份提供方，所述第一验证信息携带信息包括时间戳T_S和哈希值$h\{IP_I \| IP_S \| ID_I \| ID_R \| T_S\}$，其中，$IP_I$为通信发起方IP地址、$IP_S$为身份提供方IP地址、$ID_I$为通信发起方标识、$ID_R$为通信响应方标识、$T_S$为时间戳，$h\{\ \}$表示哈希值计算，$\|$为拼接字符串，用于将字节串进行拼接。

[0078] 在一实施例中，所述标识信息接收模块22，用于：

接收所述身份提供方发送的携带有会话密钥的标识的信息，并采用主密钥$K_{T_I}[i]$进行带密钥杂凑运算验证得到会话信息和会话密钥的标识，其中所述主密钥$K_{T_I}[i]$为所述通信发起方与所述第一QKD节点预先共享。

[0079] 在一实施例中，所述第一会话密钥申请模块23，用于：

向所述第一QKD节点发送会话密钥申请信息，所述会话密钥申请信息携带信息包括会话密钥的标识、主密钥$K_{T_I}[i]$及所述通信发起方产生的随机数N_I；

接收所述第一QKD节点发送的第一保护信息，所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥、所述会话密钥的标识及所述随机数N_I进行加密保护得到；

采用主密钥$K_{T_I}[i]$对所述第一保护信息进行解密并验证得到所述会话密钥。

[0080] 在一实施例中，在所述采用主密钥$K_{T_I}[i]$对所述第一保护信息进行解密并验证得到所述会话密钥之后，所述方法还包括：

标记主密钥$K_{T_I}[i]$无效，并令$i=i+1$。

[0081] 在一实施例中，所述报文生成模块24，用于：

生成并向所述通信响应方发送加密通信请求报文以使所述通信响应方在使用主密钥$K_{A_R}[j]$验证加密通信请求报文通过后携带所述会话密钥的标识向所述第二QKD节点申请所述会话密钥，其中所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$、所述通信发起方产生的随机数N_I`、基于所述会话密钥衍生的密钥K_2和所述会话密钥的标识，所述主密钥$K_{A_R}[j]$为所述通信响应方与所述第二QKD节点预先共享。

[0082] 在一实施例中，所述基于所述会话密钥衍生的密钥K_2的公式表示为：

$$K_1=H(h(K_{I\_R}))\{ID_s\|ID_I\|ID_R\|N_I`\|N_R`\}$$

$$K_2=H(h(K_1))\{ID_s\|ID_I\|ID_R\|N_I`\|N_R`\|0\}$$

式中，K_{I_R}为会话密钥，ID_s为身份提供方标识，ID_I为通信发起方标识，ID_R为通信响应方标识，N_I`为所述通信发起方产生的随机数，$N_R$`为所述通信响应方产生的随机数，$h()$为哈希计算，$H()$为带密钥的密码杂凑计算，$\|$表示字节串拼接。

[0083] 需要说明的是，本发明所述身份提供端的其他实施例或具有实现方法可参照上述方法实施例2，此处不再赘余。

[0084] 实施例7

如图7所示，本发明第七实施例公开了一种通信响应终端，包括：

报文接收模块31，用于接收通信发起方发送的加密通信请求报文，所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$和会话密钥的标识，所述主密钥$K_{A_R}[j]$为通信响应方与第二QKD节点预先共享；

第一会话密钥申请模块32，用于使用主密钥$K_{A_R}[j]$验证所述加密通信请求报文通过后，向所述第二QKD节点发送会话密钥请求信息，所述会话密钥请求信息携带所述会话密钥的标识，所述第二QKD节点生成有所述会话密钥；

保护信息接收模块33，用于接收所述第二QKD节点返回的第二保护信息，所述第二保护信息为所述第二QKD节点使用主密钥$K_{A_R}[j]$加密所述会话密钥和所述会话密钥的标识得到；

响应报文发送模块34，用于采用主密钥$K_{A_R}[j]$对所述第二保护信息进行解密获得所述会话密钥，并向所述通信发起方发送加密通信响应报文。

[0085] 在一实施例中，所述加密通信响应报文中携带有基于所述会话密钥衍生的密钥K_2，公式表示为：

$K_1=H(h(K_{I\_R}))\{ID_s\|ID_I\|ID_R\|N_I`\|N_R`\}$

$K_2=H(h(K_1))\{ID_s\|ID_I\|ID_R\|N_I`\|N_R`\|0\}$

式中，K_{I_R}为会话密钥，ID_s为身份提供方标识，ID_I为通信发起方标识，ID_R为通信响应方标识，$N_I`$为所述通信发起方产生的随机数，$N_R`$为所述通信响应方产生的随机数，$h()$为哈希计算，$H()$为带密钥的密码杂凑计算，$\|$表示字节串拼接。

[0086] 需要说明的是，本发明所述身份提供端的其他实施例或具有实现方法可参照上述方法实施例3，此处不再赘余。

[0087] 实施例8

如图8所示，本发明第八实施例公开了一种第一QKD节点，包括：

验证请求接收模块41，用于接收身份提供方发送的第一身份验证请求，并在验证通过后基于与通第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在第一QKD节点和第二QKD节点生成会话密钥，第一QKD节点与通信发起方连接，第二QKD节点与通信响应方连接；

密钥分发会话消息生成模块42，用于生成携带有会话密钥的标识的密钥分发会话消息并发送至所述身份提供方，以使所述身份提供方将会话密钥的标识及会话信息发送至第二QKD节点；

密钥请求接收模块43，用于在通信发起方获取到所述身份提供方分发送的所述会话密钥的标识后，接收所述通信发起方发送的会话密钥请求信息；

保护信息发送模块44，用于向所述通信发起方发送第一保护信息，所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥和所述会话密钥的标识进行加密保护得到。

[0088] 在一实施例中，所述密钥分发会话消息生成模块42，用于：

将所述会话密钥的标识分别采用密钥K_{T_S}和主密钥$K_{T_I}[i]$进行带密钥杂凑运算得到，其中，所述密钥K_{T_S}为所述身份提供方与所述第一QKD节点预先共享，所述主密钥$K_{T_I}[i]$为所述通信发起方与所述第一QKD节点预先共享，i表示主密钥的序号。

[0089] 在一实施例中，所述保护信息发送模块44，用于：

使用主密钥$K_{T_I}[i]$加密所述会话密钥；

使用主密钥$K_{T_I}[i]$进行带密钥的杂凑运算对所述会话密钥的标识、所述会话密钥进行完整性保护，得到所述第一保护信息。

[0090] 在一实施例中，在所述向所述通信发起方发送第一保护信息之后，所述方法还包括：

标记主密钥$K_{T_I}[i]$无效，并删除采用所述会话密钥的标识进行表示的会话。

[0091] 在一实施例中，在所述接收身份提供方发送的第一身份验证请求之前，所述方法还包括：

为域内的通信节点使用量子随机数产生密钥池，所述密钥池中的主密钥采用ID号顺序标引。

[0092] 需要说明的是，本发明所述身份提供端的其他实施例或具有实现方法可参照上述方法实施例4，此处不再赘余。

[0093] 实施例9

如图9所示，本发明第九实施例公开了一种身份认证与密钥交换系统，所述系统包括通信发起方1、通信响应方2、身份提供方3以及量子密钥分发网络4，所述量子密钥分发网络中包括若干QKD节点，所述通信发起方1与第一QKD节点连接，所述通信响应方2与第二QKD节点连接，所述第一QKD节点和所述第二QKD节点均与所述身份提供方3连接，所述通信发起方1与所述通信响应方2连接；

通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在所述第一QKD节点和所述第二QKD节点生成会话密钥；

所述身份提供方3，用于根据所述通信发起方1的标识或所述通信响应方2的标识查找其所属安全域及所属QKD节点；

所述通信发起方1，用于从所述第一QKD节点获取所述会话密钥，并采用所述会话密钥向所述通信响应方建立加密通信；

所述通信响应方2，用于从所述第二QKD节点获取所述会话密钥，并采用所述会话密钥和所述通信发起方建立加密通信。

[0094] 具体地，通信发起方为用于发起加密通信的用户终端或者对发起侧用户数据进行加解密处理的加密代理或者加密网关，从第一QKD节点获取会话密钥，向通信响应方进行密钥确认后采用会话密钥和响应方建立加密通信。

[0095] 通信响应方为接受加密通信的用户终端或者对接受侧用户数据进行加解密处理的加密代理或者加密网关，从第二QKD节点获取会话密钥，回复发起方的密钥确认消息并采用会话密钥和发起方建立加密通信。

[0096] QKD节点包括发起方QKD节点和响应方QKD节点以及连接两个节点的量子通信链路构成一条QKD密钥分发信道，该信道被认为是满足无条件物理安全特性的。QKD节点负责域内的密钥分发以及域间的密钥传输，在QKD密钥分发信道上传输域间会话密钥被认为是安全的，QKD节点和其域内的通信节点之间的密钥分发通过预共享的主密钥进行保护。QKD节点为域内所有通信节点分别维护一个主密钥池，并通过大容量安全介质将主密钥池拷贝到通信节点内部，QKD节点和通信节点之间的通信采用随机选择的主密钥进行保护。

[0097] 身份提供方用于根据发起方或响应方的ID(可以是IP地址、域名、电话号码、其他名字空间等)查找其所属安全域及QKD节点。所有的QKD节点和通信节点均应在IDP注册并登记从属关系。通信发起方或响应方从IDP获取通信对端所属QKD节点信息之后即根据该信息从本域QKD节点获取域间会话密钥。

[0098] 量子密钥分发网络包含QKD节点和量子网络链路控制中心，实现量子密钥生成、量子密钥中继、量子密钥提供等服务；量子网络链路控制中心可按照QKD节点ID建立节点间的量子密钥分发及中继链路。

[0099] 具体地，如图10所示，本实施例提出的一种身份认证与密钥交换系统的工作流程为：

(1)初始化阶段，为各通信节点配备一个大容量安全介质，具有2M字节以上的密钥存储空间，以密钥长度为128比特位的AES或SM4算法为参照，可存储10万条以上的密钥。各安全域的QKD节点为域内的每个通信节点使用量子随机数产生容量不小于10万条密钥的密钥池(密钥池中的密钥由32比特位以上的ID号顺序索引)，将密钥池拷贝到各通信节点的大容量安全介质中存储并将安全介质分发给通信节点使用。所有的QKD节点和通信节点均在

IDP注册并登记从属关系。

[0100] (2)通信发起方I将自己的标识和通信响应方R的标识发给身份提供方S,I从自己的大容量安全介质中按序选择有效的和发起方QKD节点T共享的预主密钥$K_{T_I}[i]$对双方标识信息及主密钥序号i进行带密钥的杂凑运算后附带主密钥序号i一起发给S:

$$I\rightarrow S:\{ID_S\|ID_I\|ID_R\|i\|H(K_{T\_I}[i])\{ID_I\|ID_R\|i\}\}。$$

[0101] (3)身份提供方S将当前时间戳发回给通信发起方I:

$$S\rightarrow I:\{T_S\}。$$

[0102] (4)通信发起方I计算$h\{IP_I\|IP_S\|ID_I\|ID_R\|T_S\}$,将该计算结果与时间戳一起发给身份提供方$S$:

$$I\rightarrow S:\{ID_S\|ID_I\|ID_R\|i\|T_S\|h\{IP_I\|IP_S\|ID_I\|ID_R\|T_S\}\|H(K_{T\_I}[i])\{ID_I\|ID_R\|i\}\}。$$

[0103] (5)身份提供方S验证时间戳在当前时间窗口范围内,计算并验证$h\{IP_I\|IP_S\|ID_I\|ID_R\|T_S\}$,通过后根据$ID_I$和$ID_R$查询自身数据库得到发起方和响应方对应QKD节点信息ID_T和ID_A,并向发起者QKD节点T进行发起方身份验证:

$$S\rightarrow T:$$

$$\{ID_S\|ID_T\|ID_A\|ID_I\|ID_R\|i\|N_S\|H(K_{T\_I}[i])\{ID_I\|ID_R\|i\}\|H(K_{T\_S})\{ID_S\|ID_T\|ID_A\|ID_I\|ID_R\|N_S\}\}。$$

[0104] (6)第一QKD节点T采用K_{T_S}验证身份提供方的身份及ID_T和ID_A的真实性,确认主密钥$K_{T_I}[i]$的有效性并采用$K_{T_I}[i]$验证通信发起者的身份及ID_I和ID_R的真实性,然后通过和响应者QKD节点A之间的QKD密钥分发信道发起会话密钥的生成和同步传输,同时QKD信道两端生成相应的会话密钥ID-ID_s,发起方QKD节点T使用ID_s标识该次密钥分发会话(ID_s:K_{I_R},ID_I,ID_R);

第一QKD节点将会话标识分别用K_{T_S}和$K_{T_I}[i]$进行带密钥杂凑运算并新产生随机数N_T发给身份提供方S:

$$T\rightarrow S:$$

$$\{ID_S\|ID_T\|ID_I\|ID_R\|ID_s\|i\|N_T\|N_S\|H(K_{T\_I}[i])\{ID_s\|ID_T\|ID_I\|ID_R\|i\|N_T\}\|H(K_{T\_S})\{ID_S\|ID_T\|ID_I\|N_S\|N_T\}\}。$$

[0105] (7)身份提供方S采用K_{T_S}验证消息后,将会话标识和会话信息采用K_{A_S}进行带密钥杂凑运算并发给响应方QKD节点A:

$$S\rightarrow A:\{ID_A\|ID_S\|ID_T\|ID_R\|ID_I\|ID_s\|N_S`\|H(K_{A\_S})\{ID_A\|ID_S\|ID_T\|ID_R\|ID_I\|ID_s\|N_S`\}\}。$$

[0106] (8)第二QKD节点A采用K_{A_S}验证并确认存在ID_s所标识的会话密钥,使用ID_s标识该次密钥分发会话(ID_s:K_{I_R},ID_I,ID_R),从密钥池中按序选择和通信响应方共享的有效预主密钥$K_{A_R}[j]$对会话标识计算带密钥杂凑值并新产生随机数N_A后发送给身份提供方S:

$$A\rightarrow S:\{ID_S\|ID_A\|ID_T\|ID_I\|ID_R\|j\|ID_s\|N_A\|N_S`\|H(K_{A\_S})\{ID_S\|ID_A\|ID_R\|N_A\|N_S`\}PH(K_{A\_R}[j])\{ID_s\|ID_A\|ID_R\|ID_I\|j\|N_A\}\}。$$

[0107] (9)身份提供方S采用K_{A_S}验证消息后,将相关信息转发给通信发起方I:

$$S\rightarrow I:\{ID_I\|ID_S\|ID_s\|ID_R\|i\|j\|N_T\|N_A\|H(K_{T\_I}[i])\{ID_s\|ID_T\|ID_I\|ID_R\|i\|N_T\}\|H$$

$(K_{A\_R}[j])\{ID_s \| ID_A \| ID_R \| ID_I \| j \| N_A\}\}$。

[0108] (10)通信发起方I使用$K_{T_I}[i]$进行带密钥杂凑运算验证并保存会话信息,携带会话标识向发起方QKD节点T申请会话密钥,其中N_I为通信发起方新产生随机数:

$I \rightarrow T$:$\{ID_T \| ID_I \| ID_s \| i \| N_I \| N_T \| H(K_{T\_I}[i])\{ID_s \| i \| N_I \| N_T\}\}$。

[0109] (11)第一QKD节点T使用$K_{T_I}[i]$加密会话密钥,然后使用$K_{T_I}[i]$进行带密钥杂凑运算对会话标识、会话密钥和随机数N_T进行完整性保护,发给通信发起方I,之后T标记$K_{T_I}[i]$为无效并删除ID_s标识的会话:

$T \rightarrow I$:$\{ID_I \| ID_T \| ID_s \| i \| N_I \| E(K_{T\_I}[i])\{K_{I\_R}\} \| H(K_{T\_I}[i])\{ID_s \| i \| N_I \| E(K_{T\_I}[i])\{K_{I\_R}\}\}\}$。

[0110] (12)通信发起方I使用$K_{T_I}[i]$解密并验证会话密钥K_{I_R},之后I标记$K_{T_I}[i]$为无效并使$i=i+1$,I向通信响应方R发送加密通信请求报文,N_I`为通信发起方新产生随机数,K_2的产生方法见步骤(16):

$I \rightarrow R$:

$\{ID_R \| ID_I \| ID_s \| j \| N_A \| N_I` \| H(K_2)\{ID_I \| ID_R \| N_I`\} \| H(K_{A\_R}[j])\{ID_s \| ID_A \| ID_R \| ID_I \| j \| N_A\}\}$。

[0111] (13)通信响应方R确认预主密钥$K_{A_R}[j]$有效性并使用$K_{A_R}[j]$计算杂凑验证会话信息,携带会话标识向响应方QKD节点A申请会话密钥,其中N_R为通信响应方新产生随机数:

$R \rightarrow A$:$\{ID_A \| ID_R \| ID_s \| j \| N_A \| N_R \| H(K_{A\_R}[j])\{ID_s \| ID_A \| ID_R \| ID_I \| j \| N_A\}\}$。

[0112] (14)第二QKD节点A使用$K_{A_R}[j]$加密会话密钥,然后进行带密钥杂凑运算对会话标识、会话密钥和随机数N_A进行完整性保护,发给通信响应方R,之后A标记$K_{A_R}[j]$为无效并使$j=j+1$并删除ID_s标识的会话:

$A \rightarrow R$:$\{ID_R \| ID_A \| ID_s \| j \| N_R \| E(K_{A\_R}[j])\{K_{I\_R}\} \| H(K_{A\_R}[j])\{ID_s \| j \| N_R \| E(K_{A\_R}[j])\{K_{I\_R}\}\}\}$。

[0113] (15)通信响应方R使用$K_{A_R}[j]$解密获得K_{I_R}后,计算并验证$H(h(K_{I_R}))\{ID_I \| ID_R \| N_I`\}$,之后向通信发起方$I$发送加密通信响应报文,其中$N_R$`为通信响应方新产生随机数,K_2的产生方法见步骤(16):

$R \rightarrow I$:$\{ID_I \| ID_R \| ID_s \| N_R` \| H(K_2)\{ID_I \| ID_R \| ID_s \| N_I` \| N_R`\}\}$。

[0114] (16)通信发起方I和通信响应方R基于会话密钥K_{I_R}进行密钥衍生,按照具体加密通信协议的需求得到各数据流向的对称加密密钥、MAC密钥、初始化向量等,本专利不涉及具体的加密通信协议和密码算法,密钥衍生:

$K_1=H(h(K_{I\_R}))\{ID_s \| ID_I \| ID_R \| N_I` \| N_R`\}$

$K_2=H(h(K_1))\{ID_s \| ID_I \| ID_R \| N_I` \| N_R` \| 0\}$

$K_3=H(h(K_1))\{ID_s \| ID_I \| ID_R \| N_I` \| N_R` \| 1\}$

…

本实施例基于量子密钥分配进行身份认证与密钥交换系统,用于属于不同安全域的设备或应用之间的加密通信,具有的技术优势在于:

(1)采用具备无条件物理安全特性的量子密钥分配信道进行不同安全域之间的加密通信会话密钥的传输,确保了风险较大的跨域密钥传输的安全性;

(2)采用大容量安全介质承载的具备“一次一密”和“用完即毁”使用特点的预共享密钥进行加密通信会话密钥在同一安全域内部的分发保护,具备前后向安全性;

(3)整个协议交互过程采用对称密钥进行带密钥的杂凑计算和对称加解密计算来进行身份认证,计算开销方面相较于身份认证与密钥交换协议AKA等其他的协议具备一定的优势。

[0115] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不一定指的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0116] 此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中,“多个”的含义是至少两个,例如两个,三个等,除非另有明确具体的限定。

[0117] 尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

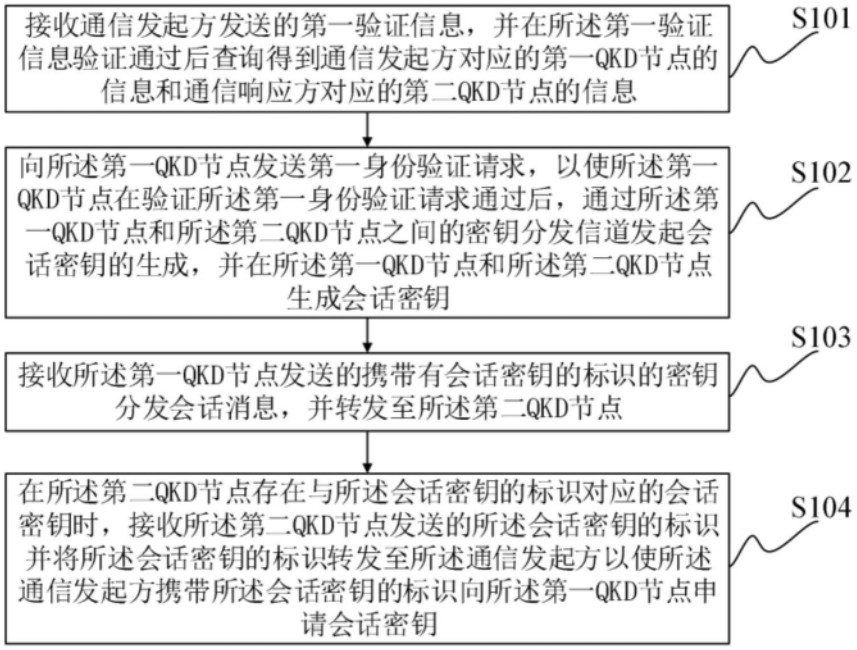
接收通信发起方发送的第一验证信息，并在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息
S101
向所述第一QKD节点发送第一身份验证请求，以使所述第一QKD节点在验证所述第一身份验证请求通过后，通过所述第一QKD节点和所述第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在所述第一QKD节点和所述第二QKD节点生成会话密钥
S102
接收所述第一QKD节点发送的携带有会话密钥的标识的密钥分发会话消息，并转发至所述第二QKD节点
S103
在所述第二QKD节点存在与所述会话密钥的标识对应的会话密钥时，接收所述第二QKD节点发送的所述会话密钥的标识并将所述会话密钥的标识转发至所述通信发起方以使所述通信发起方携带所述会话密钥的标识向所述第一QKD节点申请会话密钥
S104

图1

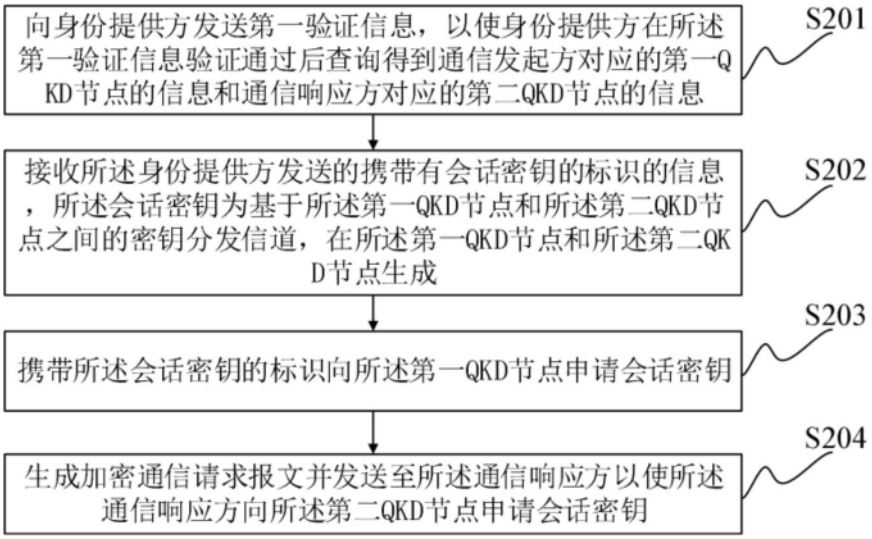
向身份提供方发送第一验证信息，以使身份提供方在所述第一验证信息验证通过后查询得到通信发起方对应的第一QKD节点的信息和通信响应方对应的第二QKD节点的信息
S201
接收所述身份提供方发送的携带有会话密钥的标识的信息，所述会话密钥为基于所述第一QKD节点和所述第二QKD节点之间的密钥分发信道，在所述第一QKD节点和所述第二QKD节点生成
S202
携带所述会话密钥的标识向所述第一QKD节点申请会话密钥
S203
生成加密通信请求报文并发送至所述通信响应方以使所述通信响应方向所述第二QKD节点申请会话密钥
S204

图2

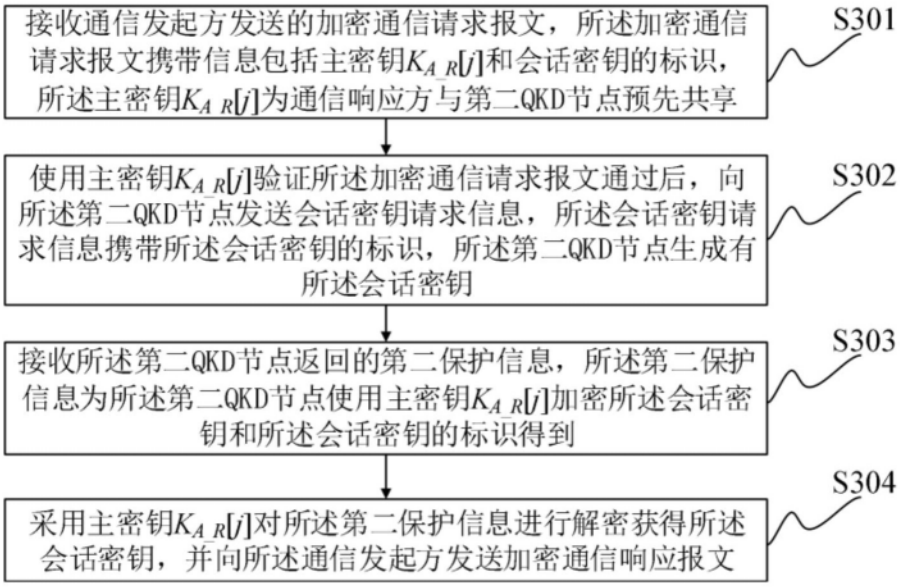
接收通信发起方发送的加密通信请求报文，所述加密通信请求报文携带信息包括主密钥$K_{A_R}[j]$和会话密钥的标识，所述主密钥$K_{A_R}[j]$为通信响应方与第二QKD节点预先共享
S301
使用主密钥$K_{A_R}[j]$验证所述加密通信请求报文通过后，向所述第二QKD节点发送会话密钥请求信息，所述会话密钥请求信息携带所述会话密钥的标识，所述第二QKD节点生成有所述会话密钥
S302
接收所述第二QKD节点返回的第二保护信息，所述第二保护信息为所述第二QKD节点使用主密钥$K_{A_R}[j]$加密所述会话密钥和所述会话密钥的标识得到
S303
采用主密钥$K_{A_R}[j]$对所述第二保护信息进行解密获得所述会话密钥，并向所述通信发起方发送加密通信响应报文
S304

图3

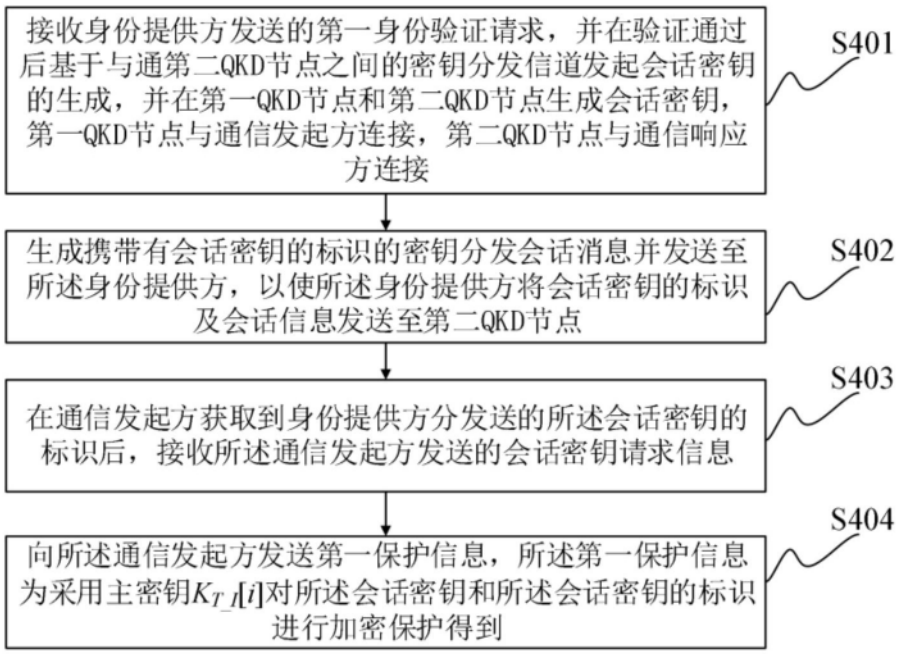
接收身份提供方发送的第一身份验证请求，并在验证通过后基于与通第二QKD节点之间的密钥分发信道发起会话密钥的生成，并在第一QKD节点和第二QKD节点生成会话密钥，第一QKD节点与通信发起方连接，第二QKD节点与通信响应方连接
S401
生成携带有会话密钥的标识的密钥分发会话消息并发送至所述身份提供方，以使所述身份提供方将会话密钥的标识及会话信息发送至第二QKD节点
S402
在通信发起方获取到身份提供方分发送的所述会话密钥的标识后，接收所述通信发起方发送的会话密钥请求信息
S403
向所述通信发起方发送第一保护信息，所述第一保护信息为采用主密钥$K_{T_I}[i]$对所述会话密钥和所述会话密钥的标识进行加密保护得到
S404

图4

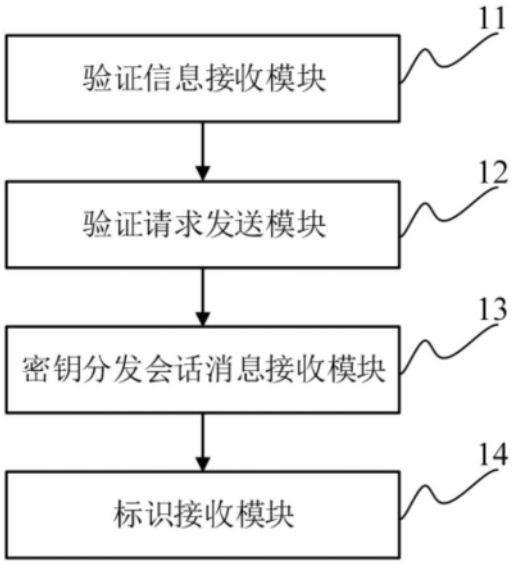
11
验证信息接收模块
12
验证请求发送模块
13
密钥分发会话消息接收模块
14
标识接收模块

图5

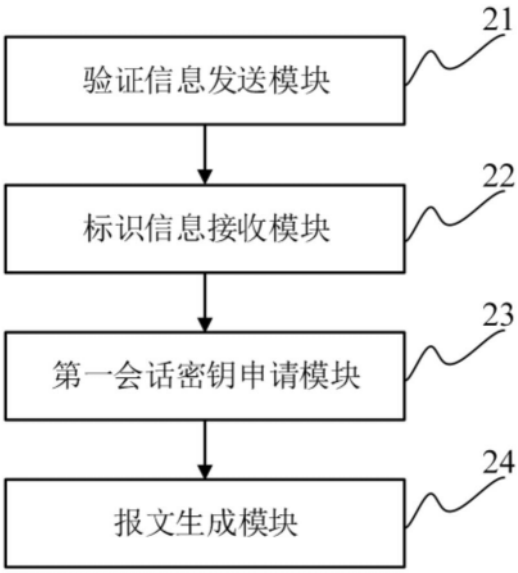
21
验证信息发送模块
22
标识信息接收模块
23
第一会话密钥申请模块
24
报文生成模块

图6

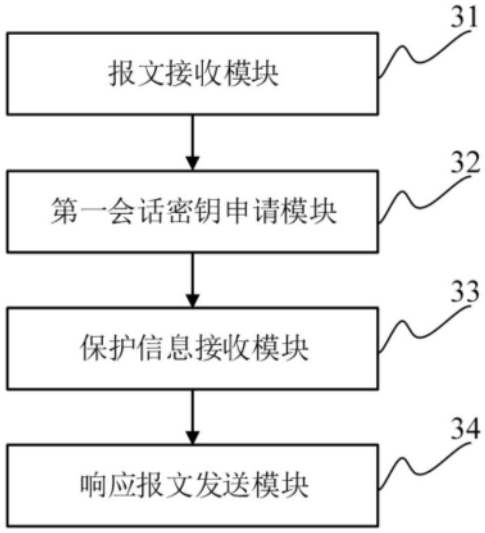
31
报文接收模块
32
第一会话密钥申请模块
33
保护信息接收模块
34
响应报文发送模块

图7

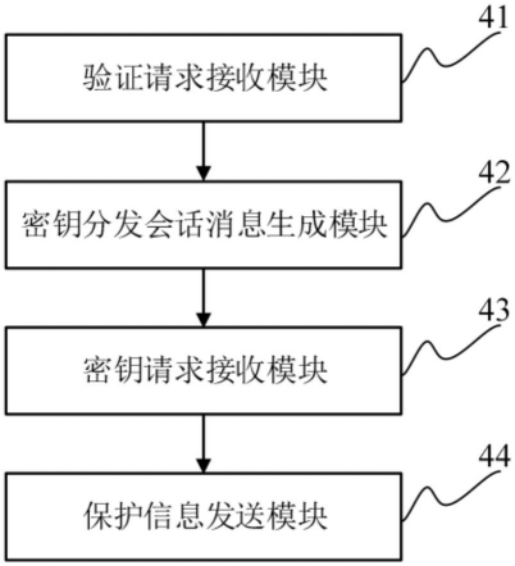
41
验证请求接收模块
42
密钥分发会话消息生成模块
43
密钥请求接收模块
44
保护信息发送模块

图8

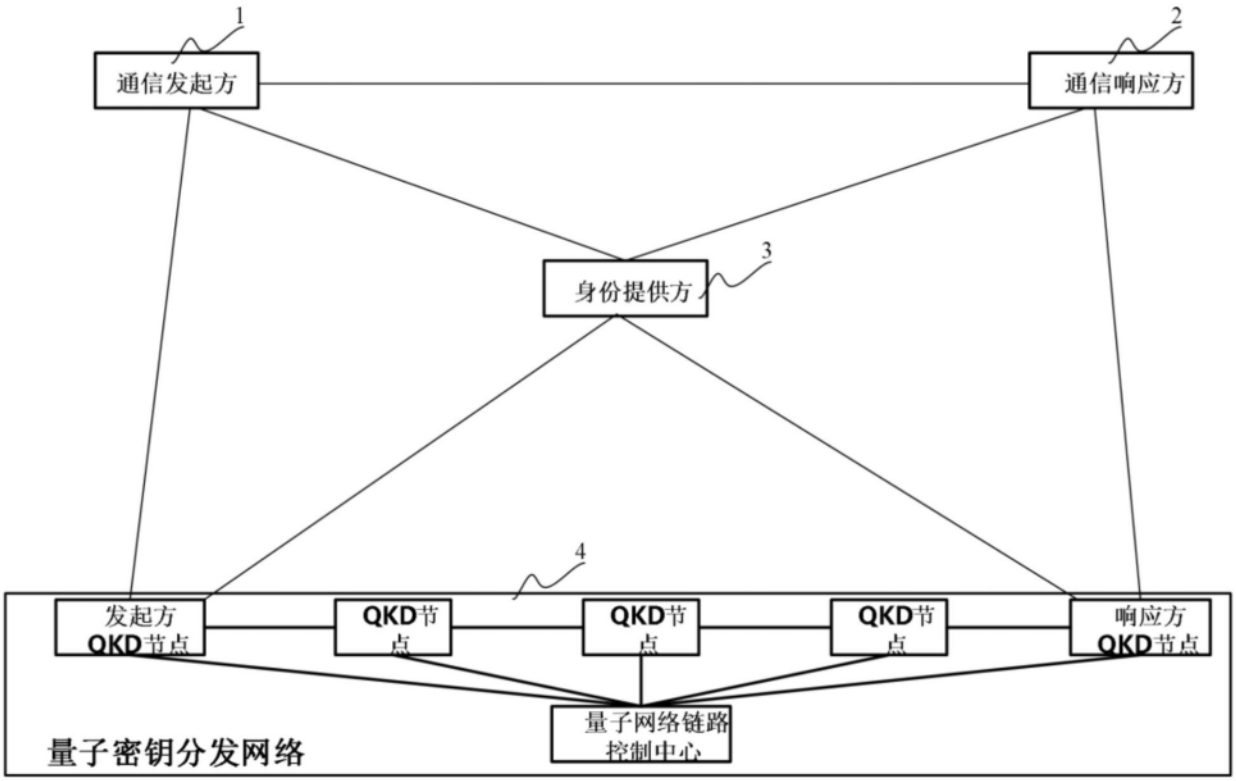
1
通信发起方
2
通信响应方
3
身份提供方
4
发起方
QKD节点
QKD节
点
QKD节
点
QKD节
点
响应方
QKD节点
量子网络链路
控制中心
量子密钥分发网络

图9


初始化阶段，为各通信节点配备一个大容量安全介质，将密钥池拷贝到各通信节点的大容量安全介质中存储并将安全介质分发给通信节点使用。所有的QKD节点和通信节点均在IDP注册并登记从属关系
通信发起方将自己的标识和通信响应方的标识发给身份提供者S，按序选择有效的预主密钥对双方标识信息及主密钥序号进行带密钥的杂凑运算后附带主密钥序号一起发给S
身份提供者S将当前时间戳发回给通信发起方
通信发起方计算身份鉴别值,将该计算结果与时间戳一起发给身份提供者S
身份提供者S验证时间戳在当前时间窗口范围内，计算并验证身份鉴别值， 通过查询自身数据库得到发起方和响应方对应QKD节点信息，并向发起者QKD节点进行发起方身份验证
发起方QKD节点验证身份提供者的身份，确认主密钥的有效性并验证通信发起者的身份，然后通过和响应者QKD节点之间的QKD密钥分发信道发起会话密钥的生成和同步传输，同时QKD信道两端生成相应的会话密钥。发起方ODK节点将会话标识进行带密钥杂凑运算发给身份提供者S
身份提供者S验证消息后，将会话标识和会话信息进行带密钥杂凑运算并发给响应方QKD节点
响应方QKD节点从密钥池中按序选择和通信响应方共享的有效预主密钥，对会话标识计算带密钥杂凑值后发送给身份提供者S
身份提供者S验证消息后，将相关信息转发给通信发起方
通信发起方进行带密钥杂凑运算验证并保存会话信息，携带会话标识向发起方QKD节点申请会话密钥
发起方ODK节点加密会话密钥，进行带密钥杂凑运算对会话标识、会话密钥进行完整性保护，发给通信发起方
通信发起方解密并验证会话密钥，向通信响应方R发送加密通信请求报文
通信响应方R确认预主密钥有效性并计算杂凑验证会话信息，携带会话标识向响应方QKD节点申请会话密钥
响应方OKD节点加密会话密钥,进行带密钥杂凑运算对会话标识、会话密钥进行完整性保护，发给通信响应方
通信响应方解密获得会话密钥后向通信发起方发送加密通信响应报文
通信发起方和通信响应方基于会话密钥进行密钥衍生，按照具体加密通信协议的需求得到各数据流向的对称加密密钥、MAC密钥、初始化向量等

图10