(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 109525385 B
(45)授权公告日 2022.04.08

(21)申请号 201811408557.3
(22)申请日 2018.11.23
(65)同一申请的已公布的文献号
申请公布号 CN 109525385 A
(43)申请公布日 2019.03.26
(73)专利权人 全链通有限公司
地址 100191 北京市海淀区知春路学院国际大厦1108室
(72)发明人 路成业 王凌 王童
(74)专利代理机构 济南信达专利事务所有限公司 37100
代理人 李世喆
(51)Int.Cl.
H04L 9/00(2022.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/40(2022.01)

审查员 张长梅

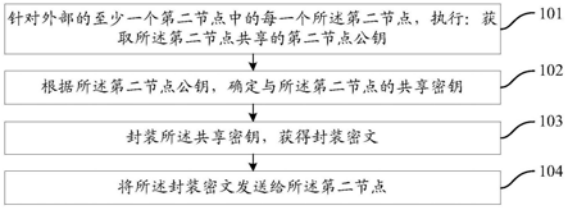
权利要求书6页 说明书15页 附图3页

(54)发明名称

一种共享密钥的封装方法、第一节点和第二节点

(57)摘要

本发明提供了一种共享密钥的封装方法、第一节点和第二节点，应用于第一节点的方法，包括：针对外部的至少一个第二节点中的每一个所述第二节点，执行：获取所述第二节点共享的第二节点公钥；根据所述第二节点公钥，确定与所述第二节点的共享密钥；封装所述共享密钥，获得封装密文；将所述封装密文发送给所述第二节点。本方案能够抵抗量子计算机的攻击。



CN 109525385 B

1.一种共享密钥的封装方法,其特征在于,应用于第一节点,包括:

针对外部的至少一个第二节点中的每一个所述第二节点,执行:

获取所述第二节点共享的第二节点公钥;

根据所述第二节点公钥,确定与所述第二节点的共享密钥;

封装所述共享密钥,获得封装密文;

将所述封装密文发送给所述第二节点;

所述根据所述第二节点公钥,确定与所述第二节点的共享密钥,包括:

根据以下第一式子,确定所述第二节点公钥对应的共享函数:

第一式子:$v(x)=u(x)s(x)+e_1(x)\in R_q$

其中,v(x)表征所述共享函数,u(x)表征所述第二节点公钥,s(x)表征预设的随机函数,$e_1(x)$表征预设的误差函数,R_q表征由奇素数q构成的实数域,其中,$s(x)\in \mathcal{R}R_q,\ e_1(x)\leftarrow \mathcal{R}\chi;$

确定所述共享函数的信号向量,并确定所述信号向量的舍入结果;

根据预设的划分规则,从所述舍入结果中划分出与所述第二节点的共享密钥;

在所述根据预设的划分规则,从所述舍入结果中划分出与所述第二节点的共享密钥之后,在所述封装所述共享密钥,获得封装密文之前,进一步包括:

根据以下第二式子,确定与所述舍入结果和所述共享密钥对应的验证密钥:

第二式子:$\lfloor v(x)\rceil_2 = K\|y$

其中,$\lfloor v(x)\rceil_2$表征所述舍入结果,K表征所述共享密钥,y表征所述验证密钥,其中,y等于剩余的n-l比特,n表征所述舍入结果的第一比特长度,l表征所述共享密钥的第二比特长度;

根据单向哈希函数$H:\{0,1\}^*\rightarrow R_q$,确定所述验证密钥的第一哈希函数;

根据成对独立的哈希函数$h:\{0,1\}^*\rightarrow\{0,1\}^l$,确定所述验证密钥的第二哈希函数;

根据所述第一哈希函数,确定加密函数;

则,

所述封装所述共享密钥,获得封装密文,包括:

根据以下第三式子,获得封装密文:

第三式子:C

$$=\left(c_0=H(y),c_1=\langle v(x)\rangle_2\in(R_2)^n,c_2=\ s(x)\cdot F+e_2(x)\right.$$

$$\left.\in\left(R_q\right)^{2m},c_3=MAC_{h(y)}(c_1,c_2)\right)$$

其中,C表征所述封装密文,H(y)表征所述第一哈希函数,$\langle v(x)\rangle_2$表征所述信号向量,n表征预设的密文指数,F表征所述加密函数,$e_2(x)$表征预设的向量函数,m表征正整数,h(y)表征所述第二哈希函数,其中,$MAC_{h(y)}(c_1,c_2)$表征由所述第二哈希函数对所述(c_1,c_2)运算获得的消息验证码,$c_1=\langle v(x)\rangle_2\in(R_2)^n$,$c_2=s(x)\cdot F+e_2(x)\in(R_q)^{2m}$,其中,

$$e_2(x)=\left(e_{2,1}(x)\leftarrow\mathcal{R}\chi,e_{2,2}(x)\leftarrow\mathcal{R}\chi\right)\in\left(R_q\right)^{2m}。$$

2.根据权利要求1所述的共享密钥的封装方法,其特征在于,

所述根据所述第一哈希函数，确定加密函数，包括：

根据以下第四式子，确定加密函数：

第四式子：$F=\left(\bar{a}(x),\bar{b}(x)+H(y)\bar{c}(x)\right)\in\left(R_q\right)^{2m}$

其中，F表征所述加密函数，$\bar{a}(x)$表征预设的第一系统函数，$\bar{b}(x)$表征预设的第二系统函数，H(y)表征所述第一哈希函数，$\bar{c}(x)$表征预设的第三系统函数；其中，所述第一系统函数、所述第二系统函数和所述第三系统函数分别为m维的多项式列向量。

3.一种共享密钥的封装方法，其特征在于，应用于第二节点，包括：

确定第二节点公钥；

确定所述第二节点公钥对应的第二节点私钥；

将所述第二节点公钥共享给外部的至少一个第一节点；

针对每一个所述第一节点，接收所述第一节点根据共享的所述第二节点公钥发送的封装密文；

利用所述第二节点私钥对所述封装密文进行解封装，获得与所述第一节点的共享密钥；

其中，所述利用所述第二节点私钥对所述封装密文进行解封装，获得与所述第一节点的共享密钥，包括：

根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封装密文中的第一哈希函数，确定所述封装密文中的加密函数；

根据以下第五式子，确定多项式向量：

第五式子：$\bar{e}_2(x)=\left(e_{2,1}(x),e_{2,2}(x),\ldots,e_{2,m}(x)\right)\in R^m$

其中，$\bar{e}_2(x)$表征所述多项式向量，每个分量多项式$e_{2,i}(x)$是系数选择{-1,0,1}的n-1次多项式，m表征正整数；

确定所述封装密文中的信号向量对应的共享函数；

根据以下第六式子，确定任意解：

第六式子：$\bar{a}(x)\cdot w(x)=v(x)-\left(\bar{b}(x)+H(y)\bar{c}(x)\right)\bar{e}_2(x)$

其中，$\bar{a}(x)$表征所述第一系统函数、w(x)表征所述第六式子的任意解，v(x)表征所述共享函数，$\bar{b}(x)$表征所述第二系统函数，H(y)表征所述封装密文中的第一哈希函数，$\bar{c}(x)$表征所述第三系统函数，$\bar{e}_2(x)$表征所述多项式向量；

令$w(x)=(w_1(x),w_2(x),\ldots,w_m(x))\in R^m$，利用所述第二节点私钥S抽样分布$D_{\Lambda^{\perp}(\bar{a}(x))+w_i,s}$上的短向量$e_{1,i}(x)\leftarrow x\ (1\leqslant i\leqslant m)$；

根据以下第七式子，确定小尺寸的解：

第七式子：$\bar{e}_1(x)=\left(e_{1,1}(x),e_{1,2}(x),\ldots,e_{1,m}(x)\right)\in R^m$；

其中，$\bar{e}_1(x)$表征所述小尺寸的解，$e_{1,1}(x),e_{1,2}(x),\ldots,e_{1,m}(x)$表征所述短向量；

根据所述小尺寸的解和所述多项式向量，确定解封函数；

根据所述解封函数和所述信号向量，确定与所述第一节点的共享密钥；

其中，所述根据所述小尺寸的解和所述多项式向量，确定解封函数，包括：

根据以下第八式子，确定解封函数：

第八式子：$v_1(x) = c_1 \cdot \left(\bar{e}_1(x), \bar{e}_2(x)\right)^T$

其中，所述$v_1(x)$表征所述解封函数，c_1表征所述第一哈希函数，$\bar{e}_1(x)$表征所述小尺寸的解，$\bar{e}_2(x)$表征所述多项式向量；

其中，

所述根据所述解封函数和所述信号向量，确定与所述第一节点的共享密钥，包括：

根据以下第九式子，确定与所述第一节点的共享密钥：

第九式子：$rec(v_1(x), \langle v(x) \rangle_2) = K||y$

其中，所述$v_1(x)$表征所述解封函数，$\langle v(x) \rangle_2$表征所述信号向量，K表征解封密钥，y表征获得的验证密钥；

根据单向哈希函数$H:\{0,1\}^* \rightarrow R_q$，确定所述验证密钥的第三哈希函数；

根据成对独立的哈希函数$h:\{0,1\}^* \rightarrow \{0,1\}^l$，确定所述验证密钥的第四哈希函数；

确定所述封装密文中的所述第一哈希函数，是否与所述第三哈希函数相同；

如果是，确定所述封装密文中的第二哈希函数，是否与所述第四哈希函数相同；

如果是，将所述解封密钥作为与所述第一节点的共享密钥。

4.根据权利要求3所述的共享密钥的封装方法，其特征在于，

所述根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封装密文中的第一哈希函数，确定所述封装密文中的加密函数，包括：

根据以下第四式子，确定所述封装密文中的加密函数：

第四式子：$F = \left(\bar{a}(x), \bar{b}(x) + H(y)\bar{c}(x)\right) \in \left(R_q\right)^{2m}$

其中，F表征所述加密函数，$\bar{a}(x)$表征预设的第一系统函数，$\bar{b}(x)$表征预设的第二系统函数，H(y)表征所述第一哈希函数，$\bar{c}(x)$表征预设的第三系统函数；其中，所述第一系统函数、所述第二系统函数和所述第三系统函数分别为m维的多项式列向量。

5.根据权利要求3至4中任一所述的共享密钥的封装方法，其特征在于，

所述确定第二节点公钥，包括：

根据以下第十式子，确定第二节点公钥：

第十式子：$u(x) \in \{Z_q[x]/(x^{2k}+1)\}$

其中，u(x)表征所述第二节点公钥，Z_q表征由奇素数q构成的整数域，x表征预设的第一系统参数，k属于正整数；

和/或，

所述确定所述第二节点公钥对应的第二节点私钥，包括：

根据以下第十一式子，确定所述第二节点公钥对应的第二节点私钥：

第十一式子：$S=\begin{pmatrix}A & BC\\ I_\sigma & D\end{pmatrix}\in R^{m\times m}$

其中，S表征所述第二节点私钥，A表征预设的第一矩阵元素，B表征预设的第二矩阵元素，C表征预设的第三矩阵元素，I_σ表征阶为预设的第三系统参数σ的第四矩阵元素，D表征预设的第五矩阵元素，R表征实数集，m表征正整数，其中，$A\in R^{(m-\sigma)\times\sigma}$，$B\in R^{(m-\sigma)\times(m-\sigma)}$，$C=\begin{pmatrix}I_{m-r-\sigma} & (y_{i,j})\\ 0 & I_r\end{pmatrix}\in R^{(m-\sigma)\times(m-\sigma)}$，$D=[0|-2I_r|2(z_{i,j})]\in R^{\sigma\times(m-\sigma)}$，其中，$I_{m-r-\sigma}$表征阶为m-r-σ的第一单位矩阵，$y_{i,j}$表征阶为(i,j)的第六矩阵元素，$I_r$表征阶为预设的第四系统参数r的第二单位矩阵，$z_{i,j}$表征阶为(i,j)的第七矩阵元素。

6.一种第一节点，其特征在于，包括：

第一节点获取单元，用于针对外部的至少一个第二节点中的每一个所述第二节点，执行：获取所述第二节点共享的第二节点公钥；

第一节点确定单元，用于根据所述第一节点获取单元获取的所述第二节点公钥，确定与所述第二节点的共享密钥；

第一节点封装单元，用于封装所述第一节点确定单元确定的所述共享密钥，获得封装密文；

第一节点发送单元，用于将所述第一节点封装单元封装的所述封装密文发送给所述第二节点；

所述根据所述第二节点公钥，确定与所述第二节点的共享密钥，包括：

根据以下第一式子，确定所述第二节点公钥对应的共享函数：

第一式子：$v(x)=u(x)s(x)+e_1(x)\in R_q$

其中，v(x)表征所述共享函数，u(x)表征所述第二节点公钥，s(x)表征预设的随机函数，$e_1(x)$表征预设的误差函数，R_q表征由奇素数q构成的实数域，其中，$s(x)\in\mathcal{R}R_q,\ e_1(x)\leftarrow\mathcal{R}\chi;$

确定所述共享函数的信号向量，并确定所述信号向量的舍入结果；

根据预设的划分规则，从所述舍入结果中划分出与所述第二节点的共享密钥；

在所述根据预设的划分规则，从所述舍入结果中划分出与所述第二节点的共享密钥之后，在所述封装所述共享密钥，获得封装密文之前，进一步包括：

根据以下第二式子，确定与所述舍入结果和所述共享密钥对应的验证密钥：

第二式子：$\lfloor v(x)\rceil_2=K\|y$

其中，$\lfloor v(x)\rceil_2$表征所述舍入结果，K表征所述共享密钥，y表征所述验证密钥，其中，y等于剩余的n-l比特，n表征所述舍入结果的第一比特长度，l表征所述共享密钥的第二比特长度；

根据单向哈希函数$H:\{0,1\}^*\rightarrow R_q$，确定所述验证密钥的第一哈希函数；

根据成对独立的哈希函数$h:\{0,1\}^*\rightarrow\{0,1\}^l$，确定所述验证密钥的第二哈希函数；

根据所述第一哈希函数，确定加密函数；

则，

所述封装所述共享密钥，获得封装密文，包括：

根据以下第三式子，获得封装密文：

第三式子：C

$$= \left(c_0 = H(y), c_1 = \langle v(x) \rangle_2 \in (R_2)^n, c_2 = s(x) \cdot F + e_2(x) \right.$$

$$\left. \in (R_q)^{2m}, c_3 = MAC_{h(y)}(c_1, c_2) \right)$$

其中，C表征所述封装密文，H(y)表征所述第一哈希函数，$\langle v(x) \rangle_2$表征所述信号向量，n表征预设的密文指数，F表征所述加密函数，$e_2(x)$表征预设的向量函数，m表征正整数，h(y)表征所述第二哈希函数，其中，$MAC_{h(y)}(c_1, c_2)$表征由所述第二哈希函数对所述(c_1, c_2)运算获得的消息验证码，$c_1 = \langle v(x) \rangle_2 \in (R_2)^n$，$c_2 = s(x) \cdot F + e_2(x) \in (R_q)^{2m}$，其中，

$e_2(x) = \left(e_{2,1}(x) \leftarrow \mathcal{R}\chi, e_{2,2}(x) \leftarrow \mathcal{R}\chi \right) \in (R_q)^{2m}$。

7.一种第二节点，其特征在于，包括：

第二节点确定单元，用于确定第二节点公钥；确定所述第二节点公钥对应的第二节点私钥；

第二节点共享单元，用于将所述第二节点确定单元确定的所述第二节点公钥共享给外部的至少一个第一节点；

第二节点接收单元，用于针对每一个所述第一节点，接收所述第一节点根据所述第二节点共享单元共享的所述第二节点公钥发送的封装密文；

第二节点解封单元，用于利用所述第二节点确定单元确定的所述第二节点私钥对所述第二节点接收单元接收的所述封装密文进行解封装，获得与所述第一节点的共享密钥；

所述利用所述第二节点私钥对所述封装密文进行解封装，获得与所述第一节点的共享密钥，包括：

根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封装密文中的第一哈希函数，确定所述封装密文中的加密函数；

根据以下第五式子，确定多项式向量：

第五式子：$\bar{e}_2(x) = \left(e_{2,1}(x), e_{2,2}(x), \ldots, e_{2,m}(x) \right) \in R^m$

其中，$\bar{e}_2(x)$表征所述多项式向量，每个分量多项式$e_{2,i}(x)$是系数选择{-1,0,1}的n-1次多项式，m表征正整数；

确定所述封装密文中的信号向量对应的共享函数；

根据以下第六式子，确定任意解：

第六式子：$\bar{a}(x) \cdot w(x) = v(x) - \left(\bar{b}(x) + H(y)\bar{c}(x) \right) \bar{e}_2(x)$

其中，$\bar{a}(x)$表征所述第一系统函数、w(x)表征所述第六式子的任意解，v(x)表征所述共享函数，$\bar{b}(x)$表征所述第二系统函数，H(y)表征所述封装密文中的第一哈希函数，$\bar{c}(x)$表征所述第三系统函数，$\bar{e}_2(x)$表征所述多项式向量；

令$w(x) = (w_1(x), w_2(x), \ldots, w_m(x)) \in R^m$，利用所述第二节点私钥S抽样分布$D_{\Lambda^{\perp}(\bar{a}(x))+w_i,s}$

上的短向量$e_{1,i}(x)\leftarrow x(1\leqslant i\leqslant m)$；

根据以下第七式子，确定小尺寸的解：

第七式子：$\bar{e}_1(x)=\left(e_{1,1}(x),e_{1,2}(x),\ldots,e_{1,m}(x)\right)\in R^m$；

其中，$\bar{e}_1(x)$表征所述小尺寸的解，$e_{1,1}(x)$，$e_{1,2}(x)$，...，$e_{1,m}(x)$表征所述短向量；

根据所述小尺寸的解和所述多项式向量，确定解封函数；

根据所述解封函数和所述信号向量，确定与所述第一节点的共享密钥；

其中，所述根据所述小尺寸的解和所述多项式向量，确定解封函数，包括：

根据以下第八式子，确定解封函数：

第八式子：$v_1(x)=c_1\cdot\left(\bar{e}_1(x),\bar{e}_2(x)\right)^T$

其中，所述$v_1(x)$表征所述解封函数，c_1表征所述第一哈希函数，$\bar{e}_1(x)$表征所述小尺寸的解，$\bar{e}_2(x)$表征所述多项式向量；

其中，

所述根据所述解封函数和所述信号向量，确定与所述第一节点的共享密钥，包括：

根据以下第九式子，确定与所述第一节点的共享密钥：

第九式子：$rec(v_1(x),\langle v(x)\rangle_2)=K||y$

其中，所述$v_1(x)$表征所述解封函数，$\langle v(x)\rangle_2$表征所述信号向量，K表征解封密钥，y表征获得的验证密钥；

根据单向哈希函数$H:\{0,1\}^*\rightarrow R_q$，确定所述验证密钥的第三哈希函数；

根据成对独立的哈希函数$h:\{0,1\}^*\rightarrow\{0,1\}^l$，确定所述验证密钥的第四哈希函数；

确定所述封装密文中的所述第一哈希函数，是否与所述第三哈希函数相同；

如果是，确定所述封装密文中的第二哈希函数，是否与所述第四哈希函数相同；

如果是，将所述解封密钥作为与所述第一节点的共享密钥。

一种共享密钥的封装方法、第一节点和第二节点

技术领域

[0001] 本发明涉及计算机技术领域，特别涉及一种共享密钥的封装方法、第一节点和第二节点。

背景技术

[0002] 随着量子计算机的出现，传统公钥密码的安全性将受到严峻的挑战，它将对通信双方的通信安全性造成极大威胁。

[0003] 针对量子计算机的攻击，在密码学界，有学者提出使用量子密钥分发(Quantum Key Distribution，QKD)技术实现通信双方建立共享密钥。

[0004] 但是，该技术需要通信双方建立量子信道，由于目前还无法有效地实现，从而无法抵抗量子计算机的攻击。

发明内容

[0005] 本发明实施例提供了一种共享密钥的封装方法、第一节点和第二节点，能够抵抗量子计算机的攻击。

[0006] 第一方面，本发明实施例提供了一种共享密钥的封装方法，应用于第一节点，包括：

[0007] 针对外部的至少一个第二节点中的每一个所述第二节点，执行：

[0008] 获取所述第二节点共享的第二节点公钥；

[0009] 根据所述第二节点公钥，确定与所述第二节点的共享密钥；

[0010] 封装所述共享密钥，获得封装密文；

[0011] 将所述封装密文发送给所述第二节点。

[0012] 优选地，

[0013] 所述根据所述第二节点公钥，确定与所述第二节点的共享密钥，包括：

[0014] 根据以下第一式子，确定所述第二节点公钥对应的共享函数：

[0015] 第一式子：$v(x)=u(x)s(x)+e_1(x)\in R_q$

[0016] 其中，v(x)表征所述共享函数，u(x)表征所述第二节点公钥，s(x)表征预设的随机函数，$e_1(x)$表征预设的误差函数，R_q表征由奇素数q构成的实数域，其中，$s(x)\in\mathcal{R}R_q$，$e_1(x)\leftarrow\mathcal{R}\chi$；

[0017] 确定所述共享函数的信号向量，并确定所述信号向量的舍入结果；

[0018] 根据预设的划分规则，从所述舍入结果中划分出与所述第二节点的共享密钥。

[0019] 优选地，

[0020] 在所述根据预设的划分规则，从所述舍入结果中划分出与所述第二节点的共享密钥之后，在所述封装所述共享密钥，获得封装密文之前，进一步包括：

[0021] 根据以下第二式子，确定与所述舍入结果和所述共享密钥对应的验证密钥：

[0022] 第二式子：$\lfloor v(x)\rceil_2=K\|y$

[0023] 其中，$\lfloor v(x) \rceil_2$表征所述舍入结果，K表征所述共享密钥，y表征所述验证密钥，其中，y＝n-l，n表征所述舍入结果的第一比特长度，l表征所述共享密钥的第二比特长度；

[0024] 根据单向哈希函数H：$\{0,1\}^* \rightarrow R_q$，确定所述验证密钥的第一哈希函数；

[0025] 根据成对独立的哈希函数h：$\{0,1\}^* \rightarrow \{0,1\}^l$，确定所述验证密钥的第二哈希函数；

[0026] 根据所述第一哈希函数，确定加密函数；

[0027] 则，

[0028] 所述封装所述共享密钥，获得封装密文，包括：

[0029] 根据以下第三式子，获得封装密文：

[0030] 第三式子：C

[0031] ＝(c_0＝H(y)，c_1＝$\langle v(x) \rangle_2 \in (R_2)^n$，$c_2$＝s(x)·F+$e_2$(x)

[0032] $\in (R_q)^{2m}$，c_3＝$MAC_{h(y)}$(c_1，c_2))

[0033] 其中，C表征所述封装密文，H(y)表征所述第一哈希函数，$\langle v(x) \rangle_2$表征所述信号向量，n表征预设的密文指数，F表征所述加密函数，e_2(x)表征预设的向量函数，m表征正整数，h(y)表征所述第二哈希函数，其中，$MAC_{h(y)}$(c_1，c_2)表征由所述第二哈希函数对所述(c_1，c_2)运算获得的消息验证码，c_1＝$\langle v(x) \rangle_2 \in (R_2)^n$，$c_2$＝s(x)·F+$e_2(x)\in (R_q)^{2m}$，其中，

$$e_2(x) = \left(e_{2,1}(x) \leftarrow \mathcal{R}\chi, e_{2,2}(x) \leftarrow \mathcal{R}\chi\right) \in \left(R_q\right)^{2m}。$$

[0034] 优选地，

[0035] 所述根据所述第一哈希函数，确定加密函数，包括：

[0036] 根据以下第四式子，确定加密函数：

[0037] 第四式子：$F = \left(\bar{a}(x), \bar{b}(x) + H(y)\bar{c}(x)\right) \in \left(R_q\right)^{2m}$

[0038] 其中，F表征所述加密函数，$\bar{a}(x)$表征预设的第一系统函数，$\bar{b}(x)$表征预设的第二系统函数，H(y)表征所述第一哈希函数，$\bar{c}(x)$表征预设的第三系统函数；其中，所述第一系统函数、所述第二系统函数和所述第三系统函数分别为m维的多项式列向量。

[0039] 第二方面，本发明实施例提供了一种共享密钥的封装方法，应用于第二节点，包括：

[0040] 确定第二节点公钥；

[0041] 确定所述第二节点公钥对应的第二节点私钥；

[0042] 将所述第二节点公钥共享给外部的至少一个第一节点；

[0043] 针对每一个所述第一节点，接收所述第一节点根据共享的所述第二节点公钥发送的封装密文；

[0044] 利用所述第二节点私钥对所述封装密文进行解封装，获得与所述第一节点的共享密钥。

[0045] 优选地，

[0046] 所述利用所述第二节点私钥对所述封装密文进行解封装，获得与所述第一节点的共享密钥，包括：

[0047] 根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封

装密文中的第一哈希函数，确定所述封装密文中的加密函数；

[0048] 根据以下第五式子，确定多项式向量：

[0049] 第五式子：$\bar{e}_2(x)=\left(e_{2,1}(x),e_{2,2}(x),\ldots,e_{2,m}(x)\right)\in R^m$

[0050] 其中，$\bar{e}_2(x)$表征所述多项式向量，每个分量多项式$e_{2,i}(x)$是系数选择{-1,0,1}的n-1次多项式，m表征正整数；

[0051] 确定所述封装密文中的信号向量对应的共享函数；

[0052] 根据以下第六式子，确定任意解：

[0053] 第六式子：$\bar{a}(x)\cdot w(x)=v(x)-\left(\bar{b}(x)+H(y)\bar{c}(x)\right)\bar{e}_2(x)$

[0054] 其中，$\bar{a}(x)$表征所述第一系统函数、w(x)表征所述第六式子的任意解，v(x)表征所述共享函数，$\bar{b}(x)$表征所述第二系统函数，H(y)表征所述封装密文中的第一哈希函数，$\bar{c}(x)$表征所述第三系统函数，$\bar{e}_2(x)$表征所述多项式向量；

[0055] 令$w(x)=(w_1(x),w_2(x),\ldots,w_m(x))\in R^m$，利用所述第二节点私钥S抽样分布$D_{\Lambda^{\perp}(\bar{a}(x))+w_i,s}$上的短向量$e_{1,i}(x)\leftarrow x(1\leqslant i\leqslant m)$；

[0056] 根据以下第七式子，确定小尺寸的解：

[0057] 第七式子：$\bar{e}_1(x)=\left(e_{1,1}(x),e_{1,2}(x),\ldots,e_{1,m}(x)\right)\in R^m;$

[0058] 其中，$\bar{e}_1(x)$表征所述小尺寸的解，$e_{1,1}(x),e_{1,2}(x),\ldots,e_{1,m}(x)$表征所述短向量；

[0059] 根据所述小尺寸的解和所述多项式向量，确定解封函数；

[0060] 根据所述解封函数和所述信号向量，确定与所述第一节点的共享密钥。

[0061] 优选地，

[0062] 所述根据所述小尺寸的解和所述多项式向量，确定解封函数，包括：

[0063] 根据以下第八式子，确定解封函数：

[0064] 第八式子：$v_1(x)=c_1\cdot\left(\bar{e}_1(x),\bar{e}_2(x)\right)^T$

[0065] 其中，所述$v_1(x)$表征所述解封函数，c_1表征所述第一哈希函数，$\bar{e}_1(x)$表征所述小尺寸的解，$\bar{e}_2(x)$表征所述多项式向量。

[0066] 优选地，

[0067] 所述根据所述解封函数和所述信号向量，确定与所述第一节点的共享密钥，包括：

[0068] 根据以下第九式子，确定与所述第一节点的共享密钥：

[0069] 第九式子：$rec(v_1(x),\langle v(x)\rangle_2)=K||y$

[0070] 其中，所述$v_1(x)$表征所述解封函数，$\langle v(x)\rangle_2$表征所述信号向量，K表征解封密钥，y表征获得的验证密钥；

[0071] 根据单向哈希函数$H:\{0,1\}^*\rightarrow R_q$，确定所述验证密钥的第三哈希函数；

[0072] 根据成对独立的哈希函数$h:\{0,1\}^*\rightarrow\{0,1\}^l$，确定所述验证密钥的第四哈希函数；

[0073] 确定所述封装密文中的所述第一哈希函数，是否与所述第三哈希函数相同；

[0074] 如果是，确定所述封装密文中的所述第二哈希函数，是否与所述第四哈希函数相同；

[0075] 如果是，将所述解封密钥作为与所述第一节点的共享密钥。

[0076] 优选地，

[0077] 所述根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封装密文中的第一哈希函数，确定所述封装密文中的加密函数，包括：

[0078] 根据以下第四式子，确定所述封装密文中的加密函数：

[0079] 第四式子：$F=\left(\bar{a}(x),\bar{b}(x)+H(y)\bar{c}(x)\right)\in\left(R_q\right)^{2m}$

[0080] 其中，F表征所述加密函数，$\bar{a}(x)$表征预设的第一系统函数，$\bar{b}(x)$表征预设的第二系统函数，H(y)表征所述第一哈希函数，$\bar{c}(x)$表征预设的第三系统函数；其中，所述第一系统函数、所述第二系统函数和所述第三系统函数分别为m维的多项式列向量。

[0081] 优选地，

[0082] 所述确定第二节点公钥，包括：

[0083] 根据以下第十式子，确定第二节点公钥：

[0084] 第十式子：$u(x)\in\{Z_q[x]/(x^{2k}+1)\}$

[0085] 其中，u(x)表征所述第二节点公钥，Z_q表征由奇素数q构成的整数域，x表征预设的第一系统参数，k属于正整数。

[0086] 优选地，

[0087] 所述确定所述第二节点公钥对应的第二节点私钥，包括：

[0088] 根据以下第十一式子，确定所述第二节点公钥对应的第二节点私钥：

[0089] 第十一式子：$S=\begin{pmatrix}A & BC\\ I_\sigma & D\end{pmatrix}\in R^{m\times m}$

[0090] 其中，S表征所述第二节点私钥，A表征预设的第一矩阵元素，B表征预设的第二矩阵元素，C表征预设的第三矩阵元素，I_σ表征阶为预设的第三系统参数σ的第四矩阵元素，D表征预设的第五矩阵元素，R表征实数集，m表征正整数，其中，$A\in R^{(m-\sigma)\times\sigma}$，$B\in R^{(m-\sigma)\times(m-\sigma)}$，$C=\begin{pmatrix}I_{m-r-\sigma} & (y_{i,j})\\ 0 & I_r\end{pmatrix}\in R^{(m-\sigma)\times(m-\sigma)}$，$D=[0|-2I_r|2(z_{i,j})]\in R^{\sigma\times(m-\sigma)}$，其中，$I_{m-r-\sigma}$表征阶为m-r-σ的第一单位矩阵，$y_{i,j}$表征阶为(i,j)的第六矩阵元素，$I_r$表征阶为预设的第四系统参数r的第二单位矩阵，$z_{i,j}$表征阶为(i,j)的第七矩阵元素。

[0091] 第三发明，本发明实施例提供了一种第一节点，包括：

[0092] 第一节点获取单元，用于针对外部的至少一个第二节点中的每一个所述第二节点，执行：获取所述第二节点共享的第二节点公钥；

[0093] 第一节点确定单元，用于根据所述第一节点获取单元获取的所述第二节点公钥，确定与所述第二节点的共享密钥；

[0094] 第一节点封装单元，用于封装所述第一节点确定单元确定的所述共享密钥，获得封装密文；

[0095] 第一节点发送单元，用于将所述第一节点封装单元封装的所述封装密文发送给所

述第二节点。

[0096] 第四方面，本发明实施例提供了一种第二节点，包括：

[0097] 第二节点确定单元，用于确定第二节点公钥；确定所述第二节点公钥对应的第二节点私钥；

[0098] 第二节点共享单元，用于将所述第二节点确定单元确定的所述第二节点公钥共享给外部的至少一个第一节点；

[0099] 第二节点接收单元，用于针对每一个所述第一节点，接收所述第一节点根据所述第二节点共享单元共享的所述第二节点公钥发送的封装密文；

[0100] 第二节点解封单元，用于利用所述第二节点确定单元确定的所述第二节点私钥对所述第二节点接收单元接收的所述封装密文进行解封装，获得与所述第一节点的共享密钥。

[0101] 本发明一实施例提供了一种共享密钥的封装方法，在应用于第一节点的方法中，第一节点针对外部的每一个第二节点，在与该第二节点进行交互之前，需要先获取该第二节点共享的第二节点公钥，再利用该第二节点公钥确定在与其交互时所使用的共享密钥，对共享密钥进行封装处理，获得封装密文，最后将该封装密文发送给该第二节点，以使该第二节点通过封装密文获取交互时使用的共享密钥，抵抗量子计算机的攻击的目的，提高共享密钥传输过程中的安全性。

附图说明

[0102] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0103] 图1是本发明一实施例提供的一种共享密钥的封装方法的流程图；

[0104] 图2是本发明一实施例提供的另一种共享密钥的封装方法的流程图；

[0105] 图3是本发明一实施例提供的又一种共享密钥的封装方法的流程图；

[0106] 图4是本发明一实施例提供的一种第一节点的结构示意图；

[0107] 图5是本发明一实施例提供的一种第二节点的结构示意图。

具体实施方式

[0108] 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中的附图，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做出创造性劳动的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。

[0109] 如图1所示，本发明实施例提供了一种共享密钥的封装方法，应用于第一节点，包括：

[0110] 步骤101：针对外部的至少一个第二节点中的每一个所述第二节点，执行：获取所述第二节点共享的第二节点公钥；

[0111] 步骤102：根据所述第二节点公钥，确定与所述第二节点的共享密钥；

[0112] 步骤103:封装所述共享密钥,获得封装密文;

[0113] 步骤104:将所述封装密文发送给所述第二节点。

[0114] 本发明一实施例提供了一种共享密钥的封装方法,在应用于第一节点的方法中,针对外部的每一个第二节点,在与该第二节点进行交互之前,需要先获取该第二节点共享的第二节点公钥,再利用该第二节点公钥确定在与其交互时所使用的共享密钥,对共享密钥进行封装处理,获得封装密文,最后将该封装密文发送给该第二节点,以使该第二节点通过封装密文获取交互时使用的共享密钥,抵抗量子计算机的攻击的目的,提高共享密钥传输过程中的安全性。

[0115] 在本发明一实施例中,所述根据所述第二节点公钥,确定与所述第二节点的共享密钥,包括:

[0116] 根据以下第一式子,确定所述第二节点公钥对应的共享函数:

[0117] 第一式子:$v(x)=u(x)s(x)+e_1(x)\in R_q$

[0118] 其中,v(x)表征所述共享函数,u(x)表征所述第二节点公钥,s(x)表征预设的随机函数,$e_1(x)$表征预设的误差函数,R_q表征由奇素数q构成的实数域,其中,$s(x)\in \mathcal{R}R_q,\ e_1(x)\leftarrow \mathcal{R}\chi$;

[0119] 确定所述共享函数的信号向量,并确定所述信号向量的舍入结果;

[0120] 根据预设的划分规则,从所述舍入结果中划分出与所述第二节点的共享密钥。

[0121] 在本发明实施例中,在确定与第二节点交互时所使用的共享密钥之前,需要,先随机选择$s(x)\in \mathcal{R}R_q$,将$s(x)\in \mathcal{R}R_q$作为预设的随机函数,再抽样误差向量$e_1(x)\leftarrow \mathcal{R}\chi$,利用获取的第二节点公钥,通过上述第一式子计算共享函数v(x),确定v(x)的信号向量,即二进制信号,对所述信号向量进行模2运算,获得舍入结果,最后根据预设的划分规则,即可从该舍入结果中确定交互时所使用的出共享密钥。

[0122] 在本发明一实施例中,在所述根据预设的划分规则,从所述舍入结果中划分出与所述第二节点的共享密钥之后,在所述封装所述共享密钥,获得封装密文之前,进一步包括:

[0123] 根据以下第二式子,确定与所述舍入结果和所述共享密钥对应的验证密钥:

[0124] 第二式子:$\lfloor v(x)\rceil_2 = K\|y$

[0125] 其中,$\lfloor v(x)\rceil_2$表征所述舍入结果,K表征所述共享密钥,y表征所述验证密钥,其中,y=n-l,n表征所述舍入结果的第一比特长度,l表征所述共享密钥的第二比特长度;

[0126] 根据单向哈希函数H:$\{0,1\}^*\rightarrow R_q$,确定所述验证密钥的第一哈希函数;

[0127] 根据成对独立的哈希函数h:$\{0,1\}^*\rightarrow\{0,1\}^l$,确定所述验证密钥的第二哈希函数;

[0128] 根据所述第一哈希函数,确定加密函数;

[0129] 则,

[0130] 所述封装所述共享密钥,获得封装密文,包括:

[0131] 根据以下第三式子,获得封装密文:

[0132] 第三式子:C

[0133] $=(c_0=H(y),c_1=\langle v(x)\rangle_2\in(R_2)^n,c_2=s(x)\cdot F+e_2(x)$

[0134] $\in(R_q)^{2m},c_3=MAC_{h(y)}(c_1,c_2))$

[0135] 其中，C表征所述封装密文，H(y)表征所述第一哈希函数，$\langle v(x)\rangle_2$表征所述信号向量，n表征预设的密文指数，F表征所述加密函数，$e_2(x)$表征预设的向量函数，m表征正整数，h(y)表征所述第二哈希函数，其中，$MAC_{h(y)}(c_1,c_2)$表征由所述第二哈希函数对所述(c_1,c_2)运算获得的消息验证码，$c_1=\langle v(x)\rangle_2\in(R_2)^n$，$c_2=s(x)\cdot F+e_2(x)\in(R_q)^{2m}$，其中，

$$e_2(x)=\left(e_{2,1}(x)\leftarrow\mathcal{R}\chi,e_{2,2}(x)\leftarrow\mathcal{R}\chi\right)\in\left(R_q\right)^{2m}。$$

[0136] 在本发明实施例中，通过定义模2舍入函数$\lfloor\cdot\rceil_2:Z_q\rightarrow Z_2$表达式为$\lfloor x\rceil_2=\left\lfloor\frac{2}{q}\cdot x\right\rceil$，根据预设的划分规则，将$\lfloor v(x)\rceil_2$分成两部分$\lfloor v(x)\rceil_2=K\|y$，其中，K是要传输的共享密钥，K的大小是根据设计需求随机选择，用1比特表示K的大小，y表示剩余的n-1比特，即验证密钥，再通过单向哈希函数和成对独立的哈希函数确定验证密钥分别对应的第一哈希函数和第二哈希函数。再通过确定加密函数，即可通过上述第三式子，根据第一哈希函数、信号向量、加密函数、预设的向量函数、第二哈希函数，以及第一哈希函数和信号向量的消息认证码，获得封装密文。

[0137] 其中，$c_2=s(x)\cdot F+e_2(x)\in(R_q)^{2m}$中的运算按照多项式乘法定义进行计算。$e_2(x)=\left(e_{2,1}(x)\leftarrow\mathcal{R}\chi,e_{2,2}(x)\leftarrow\mathcal{R}\chi\right)\in\left(R_q\right)^{2m}$的两部分从离散高斯分布中随机抽取。

[0138] 在本发明一实施例中，所述根据所述第一哈希函数，确定加密函数，包括：

[0139] 根据以下第四式子，确定加密函数：

[0140] 第四式子：$F=\left(\bar{a}(x),\bar{b}(x)+H(y)\bar{c}(x)\right)\in\left(R_q\right)^{2m}$

[0141] 其中，F表征所述加密函数，$\bar{a}(x)$表征预设的第一系统函数，$\bar{b}(x)$表征预设的第二系统函数，H(y)表征所述第一哈希函数，$\bar{c}(x)$表征预设的第三系统函数；其中，所述第一系统函数、所述第二系统函数和所述第三系统函数分别为m维的多项式列向量。

[0142] 在本发明实施例中，通过预先设置m维的多项式向量第一系统函数、第二系统函数和第三系统函数，再根据上述第四式子和第一哈希函数，即可确定一个2m维的多项式向量，即加密函数。

[0143] 可以理解的是，m维的第一系统函数，如：

[0144] $\bar{a}(x)=\left(a_1(x),a_2(x),\ldots,a_m(x)\right)^m\in\left(R_q\right)^m$，即每一个第一系统函数分量为一个系数在$Z_q$上的n-1次多项式$a_i(x)\in R_q$，i=1,2,...,m。

[0145] 同样地，m维的第二系统函数，如：

[0146] $\bar{b}(x)=\left(b_1(x),b_2(x),\ldots,b_m(x)\right)^m\in\left(R_q\right)^m$，即每一个第二系统函数分量为一个系数在$Z_q$上的n-1次多项式$b_i(x)\in R_q$，i=1,2,...,m。

[0147] 同样地，m维的第二系统函数，如：

[0148] $\bar{c}(x)=\left(c_1(x),c_2(x),\ldots,c_m(x)\right)^m\in\left(R_q\right)^m$，即每一个第三系统函数分量为一个系数在$Z_q$上的n-1次多项式$c_i(x)\in R_q$，i=1,2,...,m。

[0149] 将$\bar{a}(x)$简写为$\bar{a}$，将$a_i(x)$简写为a_i。定义R_q上的两种乘法运算：

[0150] 1) $\bar{a}b = (a_1 b, a_2 b, \ldots, a_m b) \in (R_q)^m, \bar{a} \in (R_q)^m$，$b \in R_q$；

[0151] 2) $\bar{a} \otimes \bar{b} = \sum_{i=1}^{m} a_i b_i \in R_q, \bar{a} \in (R_q)^m$，$b \in (R_q)^m$。

[0152] 如图2所示，本发明实施例提供了一种共享密钥的封装方法，应用于第二节点，包括：

[0153] 步骤201：确定第二节点公钥；

[0154] 步骤202：确定所述第二节点公钥对应的第二节点私钥；

[0155] 步骤203：将所述第二节点公钥共享给外部的至少一个第一节点；

[0156] 步骤204：针对每一个所述第一节点，接收所述第一节点根据共享的所述第二节点公钥发送的封装密文；

[0157] 步骤205：利用所述第二节点私钥对所述封装密文进行解封装，获得与所述第一节点的共享密钥。

[0158] 本发明一实施例提供了一种共享密钥的封装方法，在应用于第二节点的方法中，第二节点在与外部的每一个第一节点交互之前，需要先确定自身的第二节点公钥和对应的第二节点私钥，共享第二节点公钥，以使外部的各个第一节点利用该第二节点公钥封装交互时所使用的共享密钥，在接收到任一第一节点发来的封装密文时，利用确定的第二节点私钥可以对该封装密文进行解封，即可得到与发来封装密文的第一节点交互时所使用的共享密钥，从而实现抵抗量子计算机的攻击的目的，提高共享密钥传输的安全性。

[0159] 在本发明一实施例中，所述利用所述第二节点私钥对所述封装密文进行解封装，获得与所述第一节点的共享密钥，包括：

[0160] 根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封装密文中的第一哈希函数，确定所述封装密文中的加密函数；

[0161] 根据以下第五式子，确定多项式向量：

[0162] 第五式子：$\bar{e}_2(x) = \left(e_{2,1}(x), e_{2,2}(x), \ldots, e_{2,m}(x)\right) \in R^m$

[0163] 其中，$\bar{e}_2(x)$表征所述多项式向量，每个分量多项式$e_{2,i}(x)$是系数选择{-1,0,1}的n-1次多项式，m表征正整数；

[0164] 确定所述封装密文中的信号向量对应的共享函数；

[0165] 根据以下第六式子，确定任意解：

[0166] 第六式子：$\bar{a}(x) \cdot w(x) = v(x) - \left(\bar{b}(x) + H(y)\bar{c}(x)\right)\bar{e}_2(x)$

[0167] 其中，$\bar{a}(x)$表征所述第一系统函数、$w(x)$表征所述第六式子的任意解，$v(x)$表征所述共享函数，$\bar{b}(x)$表征所述第二系统函数，$H(y)$表征所述封装密文中的第一哈希函数，$\bar{c}(x)$表征所述第三系统函数，$\bar{e}_2(x)$表征所述多项式向量；

[0168] 令$w(x) = (w_1(x), w_2(x), \ldots, w_m(x)) \in R^m$，利用所述第二节点私钥S抽样分布$D_{\Lambda^{\perp}(\bar{a}(x))+w_i, s}$上的短向量$e_{1,i}(x) \leftarrow x$ $(1 \leqslant i \leqslant m)$；

[0169] 根据以下第七式子，确定小尺寸的解：

[0170] 第七式子：$\bar{e}_1(x)=\left(e_{1,1}(x),e_{1,2}(x),\ldots,e_{1,m}(x)\right)\in R^m$；

[0171] 其中，$\bar{e}_1(x)$表征所述小尺寸的解，$e_{1,1}(x)$，$e_{1,2}(x)$，...，$e_{1,m}(x)$表征所述短向量；

[0172] 根据所述小尺寸的解和所述多项式向量，确定解封函数；

[0173] 根据所述解封函数和所述信号向量，确定与所述第一节点的共享密钥。

[0174] 在本发明实施例中，在利用第二节点私钥解封封装密文确定密钥时，需要先确定加密函数、多项式向量和共享函数，其中，加密函数可以根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封装密文中的第一哈希函数确定，多项式向量可以根据上述第五式子确定，而共享函数可以根据封装密文中的信号向量确定(如根据封装密文中的信号向量$\langle v(x)\rangle_2$，确定其对应的共享函数$v(x)$)，再用线性代数的方法将加密函数、多项式向量、共享函数、预设的第一系统函数、预设的第二系统函数和预设的第三系统函数，代入上述第六式子即可获得该式子的任意解$w(x)$，令$w(x)=(w_1(x),w_2(x),\ldots,w_m(x))\in R^m$，然后用密钥S抽样分布$D_{\Lambda^{\perp}(\bar{a}(x))+w_i,s}$上的短向量$e_{1,i}(x)\leftarrow x(1\leqslant i\leqslant m)$，它满足后用密钥$\|\bar{e_1}(x)\|\leq\sqrt{mn}=\beta\sqrt{m/\log_2 n}$和$\bar{a}(x)t(x)=v(x)-\left(\bar{b}(x)+H(y)\bar{c}(x)\right)\cdot\bar{e_2}(x)$，这里调用离散高斯分布采用算法。再通过确定的解封函数和信号向量即可确定共享密钥。

[0175] 在本发明一实施例中，所述根据所述小尺寸的解和所述多项式向量，确定解封函数，包括：

[0176] 根据以下第八式子，确定解封函数：

[0177] 第八式子：$v_1(x)=c_1\cdot\left(\bar{e}_1(x),\bar{e}_2(x)\right)^T$

[0178] 其中，所述$v_1(x)$表征所述解封函数，c_1表征所述第一哈希函数，$\bar{e}_1(x)$表征所述小尺寸的解，$\bar{e}_2(x)$表征所述多项式向量。

[0179] 在本发明实施例中，利用确定的第一哈希函数、小尺寸的解和多项式列向量，通过上述第八式子，即可确定解封函数。

[0180] 在本发明一实施例中，所述根据所述解封函数和所述信号向量，确定与所述第一节点的共享密钥，包括：

[0181] 根据以下第九式子，确定与所述第一节点的共享密钥：

[0182] 第九式子：$rec(v_1(x),\langle v(x)\rangle_2)=K||y$

[0183] 其中，所述$v_1(x)$表征所述解封函数，$\langle v(x)\rangle_2$表征所述信号向量，K表征解封密钥，y表征获得的验证密钥；

[0184] 根据单向哈希函数$H:\{0,1\}^*\rightarrow R_q$，确定所述验证密钥的第三哈希函数；

[0185] 根据成对独立的哈希函数$h:\{0,1\}^*\rightarrow\{0,1\}^l$，确定所述验证密钥的第四哈希函数；

[0186] 确定所述封装密文中的所述第一哈希函数，是否与所述第三哈希函数相同；

[0187] 如果是，确定所述封装密文中的所述第二哈希函数，是否与所述第四哈希函数相同；

[0188] 如果是，将所述解封密钥作为与所述第一节点的共享密钥。

[0189] 在本发明实施例中，通过确定的解封函数和封装密文中的信号向量，确定调和函数$rec(v_1(x),\langle v(x)\rangle_2)=K||y$，进而确定解封密钥和验证密钥，通过计算验证密钥的第三哈希函数和第四哈希函数，再将第三哈希函数与封装密文中的第一哈希函数比对，将第四哈希函数与封装密文中的第二哈希函数进行比对，以验证第三哈希函数和第四哈希函数是否正确，如果均正确，则可确定解封密钥即为与第一节点交互时所使用的共享密钥。

[0190] 在本发明一实施例中，所述根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封装密文中的第一哈希函数，确定所述封装密文中的加密函数，包括：

[0191] 根据以下第四式子，确定所述封装密文中的加密函数：

[0192] 第四式子：$F=\left(\bar{a}(x),\bar{b}(x)+H(y)\bar{c}(x)\right)\in\left(R_q\right)^{2m}$

[0193] 其中，F表征所述加密函数，$\bar{a}(x)$表征预设的第一系统函数，$\bar{b}(x)$表征预设的第二系统函数，H(y)表征所述第一哈希函数，$\bar{c}(x)$表征预设的第三系统函数；其中，所述第一系统函数、所述第二系统函数和所述第三系统函数分别为m维的多项式列向量。

[0194] 在本发明实施例中，通过预先设置m维的多项式向量第一系统函数、第二系统函数和第三系统函数，再根据上述第四式子和第一哈希函数，即可确定一个2m维的多项式向量，即加密函数。

[0195] 在本发明一实施例中，所述确定第二节点公钥，包括：

[0196] 根据以下第十式子，确定第二节点公钥：

[0197] 第十式子：$u(x)\in\{Z_q[x]/(x^{2k}+1)\}$

[0198] 其中，u(x)表征所述第二节点公钥，Z_q表征由奇素数q构成的整数域，x表征预设的第一系统参数，k属于正整数。

[0199] 在本发明实施例中，$(x^{2k}+1)$即等于f(x)，是一个次数为2k的分圆多项式，设q为满足f(x)在有限域Z_q上只有n个线性因式。设$R=Z[X]/(f(x))$，$R_q=Z_q[X]/(f(x))$，即可确定第二节点公钥，其中，$u(x)\in R_q$。

[0200] 在本发明一实施例中，所述确定所述第二节点公钥对应的第二节点私钥，包括：

[0201] 根据以下第十一式子，确定所述第二节点公钥对应的第二节点私钥：

[0202] 第十一式子：$S=\begin{pmatrix}A & BC\\ I_\sigma & D\end{pmatrix}\in R^{m\times m}$

[0203] 其中，S表征所述第二节点私钥，A表征预设的第一矩阵元素，B表征预设的第二矩阵元素，C表征预设的第三矩阵元素，I_σ表征阶为预设的第三系统参数σ的第四矩阵元素，D表征预设的第五矩阵元素，R表征实数集，m表征正整数，其中，$A\in R^{(m-\sigma)\times\sigma}$，$B\in R^{(m-\sigma)\times(m-\sigma)}$，$C=\begin{pmatrix}I_{m-r-\sigma} & (y_{i,j})\\ 0 & I_r\end{pmatrix}\in R^{(m-\sigma)\times(m-\sigma)}$，$D=[0|-2I_r|2(z_{i,j})]\in R^{\sigma\times(m-\sigma)}$，其中，$I_{m-r-\sigma}$表征阶为m-r-σ的第一单位矩阵，$y_{i,j}$表征阶为(i,j)的第六矩阵元素，$I_r$表征阶为预设的第四系统参数r的第二单位矩阵，$z_{i,j}$表征阶为(i,j)的第七矩阵元素。

[0204] 在本发明实施例中，私钥S是一个m×m的矩阵，矩阵元素属于R，其尺寸为：

$\|S\| = Ef(f,2)\sqrt{9r+\sigma}\sqrt{n} = Ef(f,2)\sqrt{2}kr^{1/2}n^{3/2}$,其中Ef(f,2)＝max{||g mod f||/g|g∈Z[X]\{0}}且deg(g)≤2(deg(f)-1)。

[0205] 综上可见,本发明提供的一种共享密钥的封装方法,采用后量子密钥封装方案在通信双方建立共享密钥,通过共享密钥实现通信双方交互抵抗量子计算机的攻击的目的。

[0206] 如图3所示,下面以新入节点X和原始节点Y为例,对本发明实施例提供的一种共享密钥的封装方法进行说明,具体可以包括以下步骤:

[0207] 步骤301:新入节点X确定新入节点公钥和对应的新入节点私钥。

[0208] 具体地,新入节点X在与原始节点Y交互之前,需要先确定自身的新入节点公钥和对应的新入节点私钥,以使通过新入节点公钥与原始节点Y交互。

[0209] 步骤302:新入节点X将新入节点公钥共享给原始节点Y。

[0210] 具体地,新入节点X通过将新入节点公钥共享给原始节点Y,以使原始节点Y利用新入节点公钥确定双方通信时的共享密钥,利用该共享密钥加密交互信息,以抵抗量子计算机的攻击。

[0211] 步骤303:原始节点Y获取新入节点X共享的新入节点公钥。

[0212] 步骤304:原始节点Y根据新入节点公钥,确定与新入节点X的共享密钥。

[0213] 具体地,原始节点Y在获取到新入节点公钥时,需要利用新入节点公钥确定共享密钥,以使该共享密钥与新入节点X相对应。

[0214] 步骤305:原始节点Y封装共享密钥,获得封装密文。

[0215] 步骤306:原始节点Y将封装密文发送给新入节点X。

[0216] 具体地,原始节点Y在确定与新入节点X对应的共享密钥后,不是直接将共享密钥发送给新入节点X,而是需要先对共享密钥进行封装,以抵抗量子计算机的攻击,提高共享密钥传输的安全性,再将共享密钥封装后获得的封装密文发送给新入节点X,以使其通过封装密文,获得共享密钥。

[0217] 步骤307:新入节点X接收原始节点Y根据共享的新入节点公钥发送的封装密文。

[0218] 步骤308:新入节点X利用原始节点Y私钥对封装密文进行解封装,获得与第一节点的共享密钥。

[0219] 如图4所示,本发明实施例提供了一种第一节点,包括:

[0220] 第一节点获取单元401,用于针对外部的至少一个第二节点中的每一个所述第二节点,执行:获取所述第二节点共享的第二节点公钥;

[0221] 第一节点确定单元402,用于根据所述第一节点获取单元401获取的所述第二节点公钥,确定与所述第二节点的共享密钥;

[0222] 第一节点封装单元403,用于封装所述第一节点确定单元402确定的所述共享密钥,获得封装密文;

[0223] 第一节点发送单元404,用于将所述第一节点封装单元403封装的所述封装密文发送给所述第二节点。

[0224] 在本发明实施例中,针对外部的每一个第二节点,在与该第二节点进行交互之前,需要先通过第一节点获取单元获取该第二节点共享的第二节点公钥,再通过第一节点确定单元利用该第二节点公钥确定在第二节点其交互时所使用的共享密钥,通过第一节点封装单元对共享密钥进行封装处理,获得封装密文,最后通过第一节点发送单元将该封装密文

发送给该第二节点，以使该第二节点通过封装密文获取交互时使用的共享密钥，抵抗量子计算机的攻击的目的，提高共享密钥传输过程中的安全性。

[0225] 在本发明一实施例中，所述第一节点确定单元，用于根据第一式子，确定所述第二节点公钥对应的共享函数；确定所述共享函数的信号向量，并确定所述信号向量的舍入结果；根据预设的划分规则，从所述舍入结果中划分出与所述第二节点的共享密钥；其中，所述第一式子为：

[0226] 第一式子：$v(x)=u(x)s(x)+e_1(x)\in R_q$

[0227] 其中，$v(x)$表征所述共享函数，$u(x)$表征所述第二节点公钥，$s(x)$表征预设的随机函数，$e_1(x)$表征预设的误差函数，R_q表征由奇素数q构成的实数域，其中，

$s(x)\in \mathcal{R}R_q,\ e_1(x)\leftarrow \mathcal{R}\chi$。

[0228] 在本发明一实施例中，所述第一节点确定单元，进一步用于根据第二式子，确定与所述舍入结果和所述共享密钥对应的验证密钥；根据单向哈希函数$H:\{0,1\}^*\rightarrow R_q$，确定所述验证密钥的第一哈希函数；根据成对独立的哈希函数$h:\{0,1\}^*\rightarrow\{0,1\}^l$，确定所述验证密钥的第二哈希函数；根据所述第一哈希函数，确定加密函数；其中，所述第二式子为：

[0229] 第二式子：$\lfloor v(x)\rceil_2 = K\|y$

[0230] 其中，$\lfloor v(x)\rceil_2$表征所述舍入结果，K表征所述共享密钥，y表征所述验证密钥，其中，$y=n-l$，n表征所述舍入结果的第一比特长度，l表征所述共享密钥的第二比特长度；

[0231] 所述第一节点封装单元，用于根据以下第三式子，获得封装密文：

[0232] 第三式子：C

[0233] $=(c_0=H(y),c_1=\langle v(x)\rangle_2\in(R_2)^n,c_2=s(x)\cdot F+e_2(x)$

[0234] $\in(R_q)^{2m},c_3=MAC_{h(y)}(c_1,c_2))$

[0235] 其中，C表征所述封装密文，$H(y)$表征所述第一哈希函数，$\langle v(x)\rangle_2$表征所述信号向量，n表征预设的密文指数，F表征所述加密函数，$e_2(x)$表征预设的向量函数，m表征正整数，$h(y)$表征所述第二哈希函数，其中，$MAC_{h(y)}(c_1,c_2)$表征由所述第二哈希函数对所述(c_1,c_2)运算获得的消息验证码，$c_1=\langle v(x)\rangle_2\in(R_2)^n,c_2=s(x)\cdot F+e_2(x)\in(R_q)^{2m}$，其中，

$e_2(x)=\left(e_{2,1}(x)\leftarrow\mathcal{R}\chi,e_{2,2}(x)\leftarrow\mathcal{R}\chi\right)\in\left(R_q\right)^{2m}$。

[0236] 在本发明一实施例中，所述第一节点确定单元，用于根据以下第四式子，确定加密函数：

[0237] 第四式子：$F=\left(\bar{a}(x),\bar{b}(x)+H(y)\bar{c}(x)\right)\in\left(R_q\right)^{2m}$

[0238] 其中，F表征所述加密函数，$\bar{a}(x)$表征预设的第一系统函数，$\bar{b}(x)$表征预设的第二系统函数，$H(y)$表征所述第一哈希函数，$\bar{c}(x)$表征预设的第三系统函数；其中，所述第一系统函数、所述第二系统函数和所述第三系统函数分别为m维的多项式列向量。

[0239] 如图5所示，本发明实施例提供了一种第二节点，包括：

[0240] 第二节点确定单元501，用于确定第二节点公钥；确定所述第二节点公钥对应的第二节点私钥；

[0241] 第二节点共享单元502，用于将所述第二节点确定单元501确定的所述第二节点公钥共享给外部的至少一个第一节点；

[0242] 第二节点接收单元503，用于针对每一个所述第一节点，接收所述第一节点根据所述第二节点共享单元502共享的所述第二节点公钥发送的封装密文；

[0243] 第二节点解封单元504，用于利用所述第二节点确定单元501确定的所述第二节点私钥对所述第二节点接收单元503接收的所述封装密文进行解封装，获得与所述第一节点的共享密钥。

[0244] 在本发明实施例中，在与外部的每一个第一节点交互之前，需要先通过第二节点确定单元确定自身的第二节点公钥和对应的第二节点私钥，再通过第二节点共享单元共享第二节点公钥，以使外部的各个第一节点利用该第二节点公钥封装交互时所使用的共享密钥，在通过第二节点接收单元接收到任一第一节点发来的封装密文时，通过第二节点解封单元利用确定的第二节点私钥可以对该封装密文进行解封，即可得到与发来封装密文的第一节点交互时所使用的共享密钥，从而实现抵抗量子计算机的攻击的目的，提高共享密钥传输的安全性。

[0245] 在本发明一实施例中，所述第二节点解封单元，包括：参数确定子单元、多项式确定子单元、解封确定子单元和密钥确定子单元；

[0246] 所述参数确定子单元，用于根据预设的第一系统函数、预设的第二系统函数、预设的第三系统函数和所述封装密文中的第一哈希函数，确定所述封装密文中的加密函数；根据第五式子，确定多项式向量；确定所述封装密文中的信号向量对应的共享函数；其中，所述第五式子为：

[0247] 第五式子：$\bar{e}_2(x)=\left(e_{2,1}(x),e_{2,2}(x),\ldots,e_{2,m}(x)\right)\in R^m$

[0248] 其中，$\bar{e}_2(x)$表征所述多项式向量，每个分量多项式$e_{2,i}(x)$是系数选择{-1,0,1}的n-1次多项式，m表征正整数；

[0249] 所述解封确定子单元，用于根据第六式子，确定任意解；令$w(x)=(w_1(x),w_2(x),\ldots,w_m(x))\in R^m$，利用所述第二节点私钥S抽样分布$D_{\Lambda^{\perp}(\bar{a}(x))+w_i,s}$上的短向量$e_{1,i}(x)\leftarrow x(1\leqslant i\leqslant m)$；根据第七式子，确定小尺寸的解；根据所述小尺寸的解和所述多项式向量，确定解封函数；

[0250] 其中，所述第六式子为：

[0251] 第六式子：$\bar{a}(x)\cdot w(x)=v(x)-\left(\bar{b}(x)+H(y)\bar{c}(x)\right)\bar{e}_2(x)$

[0252] 其中，$\bar{a}(x)$表征所述参数确定子单元确定的所述第一系统函数、$w(x)$表征所述第六式子的任意解，$v(x)$表征所述参数确定子单元确定的所述共享函数，$\bar{b}(x)$表征所述参数确定子单元确定的所述第二系统函数，$H(y)$表征所述封装密文中的第一哈希函数，$\bar{c}(x)$表征所述参数确定子单元确定的所述第三系统函数，$\bar{e}_2(x)$表征所述参数确定子单元确定的所述多项式向量；

[0253] 所述第七式子为：

[0254] 第七式子：$\bar{e}_1(x)=\left(e_{1,1}(x),e_{1,2}(x),\ldots,e_{1,m}(x)\right)\in R^m$；

[0255] 其中，$\bar{e}_1(x)$表征所述解封确定子单元确定的所述小尺寸的解，$e_{1,1}(x)$，$e_{1,2}(x)$，...，$e_{1,m}(x)$表征所述解封确定子单元抽样的所述短向量。

[0256] 所述密钥确定子单元，用于根据所述解封确定子单元确定的所述解封函数和所述信号向量，确定与所述第一节点的共享密钥。

[0257] 在本发明一实施例中，所述解封确定子单元，用于根据以下第八式子，确定解封函数：

[0258] 第八式子：$v_1(x)=c_1\cdot\left(\bar{e}_1(x),\bar{e}_2(x)\right)^T$

[0259] 其中，所述$v_1(x)$表征所述解封函数，c_1表征所述第一哈希函数，$\bar{e}_1(x)$表征所述小尺寸的解，$\bar{e}_2(x)$表征所述多项式向量。

[0260] 在本发明一实施例中，所述密钥确定子单元，用于根据第九式子，确定与所述第一节点的共享密钥；根据单向哈希函数$H:\{0,1\}^*\rightarrow R_q$，确定所述验证密钥的第三哈希函数；根据成对独立的哈希函数$h:\{0,1\}^*\rightarrow\{0,1\}^1$，确定所述验证密钥的第四哈希函数；确定所述封装密文中的所述第一哈希函数，是否与所述第三哈希函数相同；如果是，确定所述封装密文中的所述第二哈希函数，是否与所述第四哈希函数相同；如果是，将所述解封密钥作为与所述第一节点的共享密钥；其中，所述第九式子为：

[0261] 第九式子：$rec(v_1(x),\langle v(x)\rangle_2)=K||y$

[0262] 其中，所述$v_1(x)$表征所述解封函数，$\langle v(x)\rangle_2$表征所述信号向量，K表征解封密钥，y表征获得的验证密钥。

[0263] 在本发明一实施例中，所述参数确定单元，用于根据以下第四式子，确定所述封装密文中的加密函数：

[0264] 第四式子：$F=\left(\bar{a}(x),\bar{b}(x)+H(y)\bar{c}(x)\right)\in\left(R_q\right)^{2m}$

[0265] 其中，F表征所述加密函数，$\bar{a}(x)$表征预设的第一系统函数，$\bar{b}(x)$表征预设的第二系统函数，$H(y)$表征所述第一哈希函数，$\bar{c}(x)$表征预设的第三系统函数；其中，所述第一系统函数、所述第二系统函数和所述第三系统函数分别为m维的多项式列向量。

[0266] 在本发明一实施例中，所述第二节点确定单元，用于根据以下第十式子，确定第二节点公钥：

[0267] 第十式子：$u(x)\in\{Z_q[x]/(x^{2k}+1)\}$

[0268] 其中，$u(x)$表征所述第二节点公钥，Z_q表征由奇素数q构成的整数域，x表征预设的第一系统参数，k属于正整数。

[0269] 在本发明一实施例中，所述第二节点确定单元，用于根据以下第十一式子，确定所述第二节点公钥对应的第二节点私钥：

[0270] 第十一式子：$S=\begin{pmatrix}A & BC\\ I_\sigma & D\end{pmatrix}\in R^{m\times m}$

[0271] 其中，S表征所述第二节点私钥，A表征预设的第一矩阵元素，B表征预设的第二矩

阵元素，C表征预设的第三矩阵元素，I_{σ}表征阶为预设的第三系统参数σ的第四矩阵元素，D表征预设的第五矩阵元素，R表征实数集，m表征正整数，其中，$A\in R^{(m-\sigma)\times\sigma}$，$B\in R^{(m-\sigma)\times(m-\sigma)}$，$C=\begin{pmatrix} I_{m-r-\sigma} & (y_{i,j}) \\ 0 & I_r \end{pmatrix}\in R^{(m-\sigma)\times(m-\sigma)}$，$D=[0|-2I_r|2(z_{i,j})]\in R^{\sigma\times(m-\sigma)}$，其中，$I_{m-r-\sigma}$表征阶为m-r-σ的第一单位矩阵，$y_{i,j}$表征阶为(i,j)的第六矩阵元素，$I_r$表征阶为预设的第四系统参数r的第二单位矩阵，$z_{i,j}$表征阶为(i,j)的第七矩阵元素。

[0272] 本发明各个实施例至少具有如下有益效果：

[0273] 1、在本发明实施例中，本发明一实施例提供了一种共享密钥的封装方法，在应用于第一节点的方法中，第一节点针对外部的每一个第二节点，在与该第二节点进行交互之前，需要先获取该第二节点共享的第二节点公钥，再利用该第二节点公钥确定在与其交互时所使用的共享密钥，对共享密钥进行封装处理，获得封装密文，最后将该封装密文发送给该第二节点，以使该第二节点通过封装密文获取交互时使用的共享密钥，抵抗量子计算机的攻击的目的，提高共享密钥传输过程中的安全性。

[0274] 2、在本发明实施例中，本发明一实施例提供了一种共享密钥的封装方法，在应用于第二节点的方法中，第二节点在与外部的每一个第一节点交互之前，需要先确定自身的第二节点公钥和对应的第二节点私钥，共享第二节点公钥，以使外部的各个第一节点利用该第二节点公钥封装交互时所使用的共享密钥，在接收到任一第一节点发来的封装密文时，利用确定的第二节点私钥可以对该封装密文进行解封，即可得到与发来封装密文的第一节点交互时所使用的共享密钥，从而实现抵抗量子计算机的攻击的目的，提高共享密钥传输的安全性。

[0275] 需要说明的是，在本文中，诸如第一和第二之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个〃・・・・〃”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同因素。

[0276] 最后需要说明的是：以上所述仅为本发明的较佳实施例，仅用于说明本发明的技术方案，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所做的任何修改、等同替换、改进等，均包含在本发明的保护范围内。

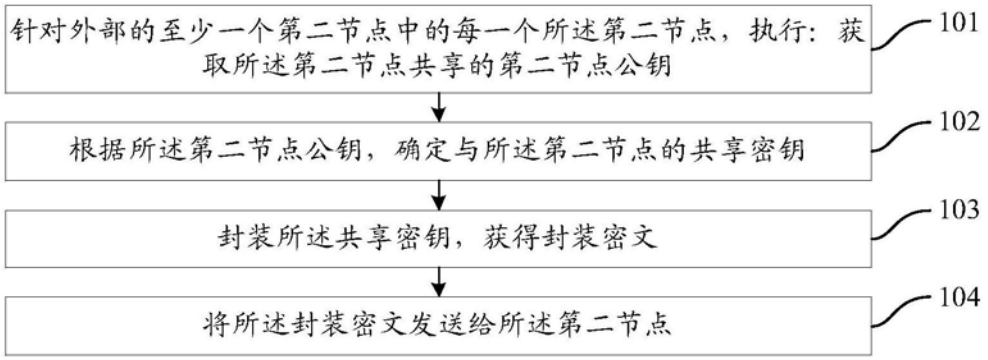

针对外部的至少一个第二节点中的每一个所述第二节点，执行：获取所述第二节点共享的第二节点公钥
101
根据所述第二节点公钥，确定与所述第二节点的共享密钥
102
封装所述共享密钥，获得封装密文
103
将所述封装密文发送给所述第二节点
104

图1

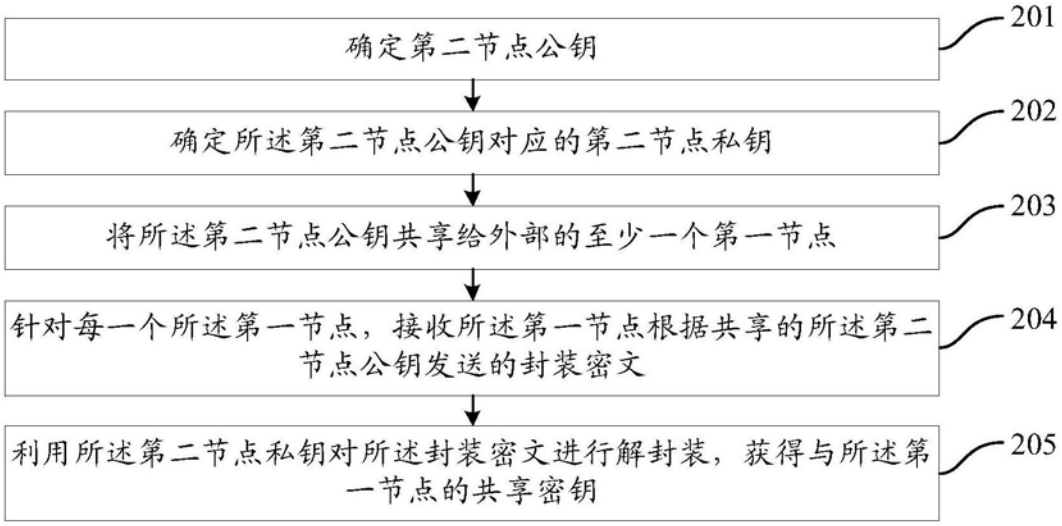

确定第二节点公钥
201
确定所述第二节点公钥对应的第二节点私钥
202
将所述第二节点公钥共享给外部的至少一个第一节点
203
针对每一个所述第一节点，接收所述第一节点根据共享的所述第二节点公钥发送的封装密文
204
利用所述第二节点私钥对所述封装密文进行解封装，获得与所述第一节点的共享密钥
205

图2

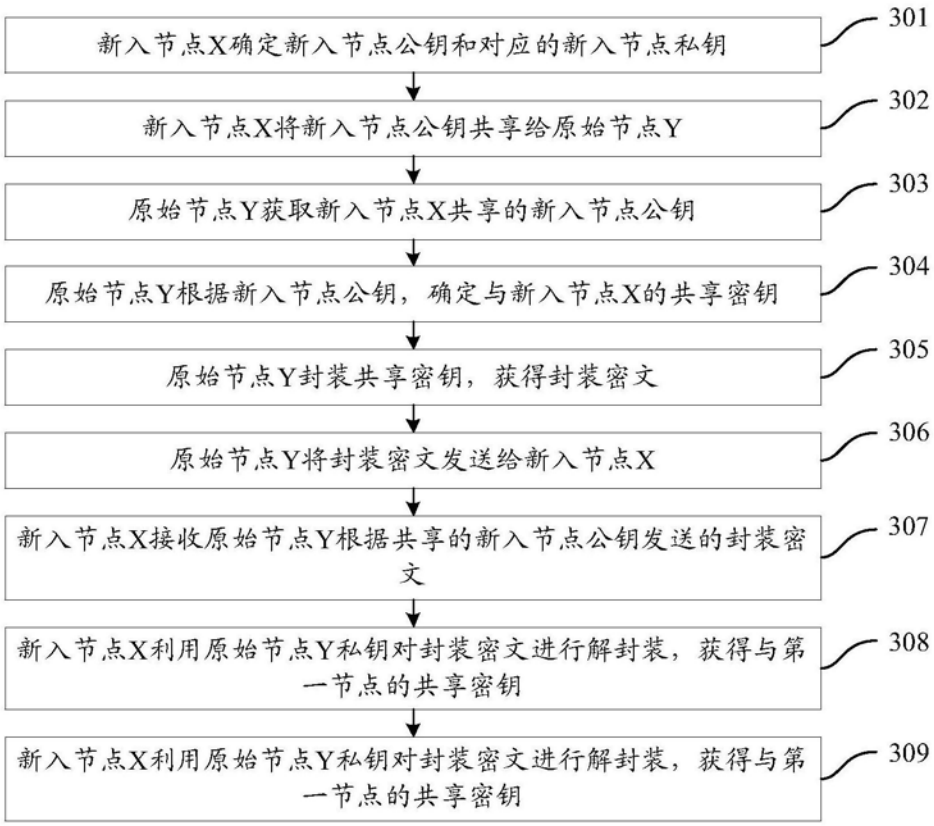

新入节点X确定新入节点公钥和对应的新入节点私钥
301
新入节点X将新入节点公钥共享给原始节点Y
302
原始节点Y获取新入节点X共享的新入节点公钥
303
原始节点Y根据新入节点公钥，确定与新入节点X的共享密钥
304
原始节点Y封装共享密钥，获得封装密文
305
原始节点Y将封装密文发送给新入节点X
306
新入节点X接收原始节点Y根据共享的新入节点公钥发送的封装密文
307
新入节点X利用原始节点Y私钥对封装密文进行解封装，获得与第一节点的共享密钥
308
新入节点X利用原始节点Y私钥对封装密文进行解封装，获得与第一节点的共享密钥
309

图3


第一节点获取单元
401
第一节点确定单元
402
第一节点封装单元
403
第一节点发送单元
404

图4

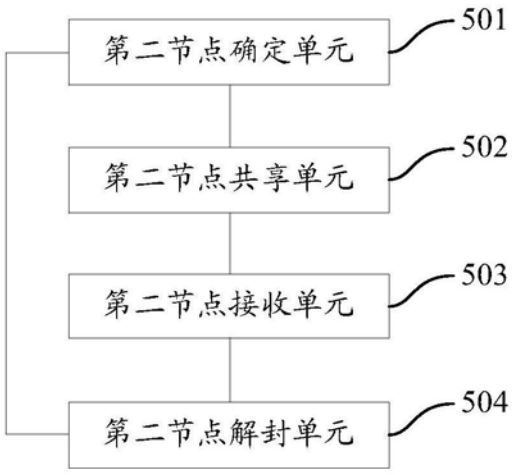


图5