软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(12):4804–4815 [doi: 10.13328/j.cnki.jos.006379]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于 Cluster 态的可验证多方量子密钥协商方案*

芦殿军[1,2], 李志慧[1], 闫晨红[1], 刘 璐[1]

[1](陕西师范大学 数学与统计学院, 陕西 西安 710119)

[2](青海师范大学 数学与统计学院, 青海 西宁 810008)

通信作者: 李志慧, E-mail: lizhihui@snnu.edu.cn

摘 要: 基于四量子比特 Cluster 态, 提出一种可验证多方量子密钥协商方案. 方案允许每次由两个参与者利用自己的子密钥分别在每个四量子比特 Cluster 态的两个粒子上执行 X 运算, 并对转换后的 Cluster 态执行延迟测量, 这保证了每个参与者对协商密钥的贡献相等. 提出的方案使用相互无偏基粒子作为诱饵粒子, 并且利用对称二元多项式的一对函数值对这些诱饵粒子执行酉运算, 不仅可以进行窃听检验, 而且还能进行参与者之间的身份验证. 本方案适用于任意大于 2 的参与者人数. 安全性分析表明, 提出的方案能够抵抗外部攻击及参与者攻击. 与现有的多方密钥协商方案相比, 该方案不仅在诱饵粒子的使用上有优势, 同时具有较高的量子比特效率.

关键词: 量子密钥协商; 四量子比特 Cluster 态; 多方; 可验证

中图法分类号: TP309

中文引用格式: 芦殿军, 李志慧, 闫晨红, 刘璐. 基于 Cluster 态的可验证多方量子密钥协商方案. 软件学报, 2022, 33(12): 4804–4815. http://www.jos.org.cn/1000-9825/6379.htm

英文引用格式: Lu DJ, Li ZH, Yan CH, Liu L. Verifiable Multi-party Quantum Key Agreement with Cluster State. Ruan Jian Xue Bao/Journal of Software, 2022, 33(12): 4804–4815 (in Chinese). http://www.jos.org.cn/1000-9825/6379.htm

Verifiable Multi-party Quantum Key Agreement with Cluster State

LU Dian-Jun[1,2], LI Zhi-Hui[1], YAN Chen-Hong[1], LIU Lu[1]

[1](School of Mathematics and Statistics, Shaanxi Normal University, Xi'an 710119, China)

[2](School of Mathematics and Statistics, Qinghai Normal University, Xining 810008, China)

Abstract: This study proposes a verifiable multi-party quantum key agreement protocol which based on X operation and four-qubit cluster states. The protocol allows two participants to perform X operations on two particles of each four-qubit cluster states using their own key at a time, and to perform delay measurements on the converted cluster state, which ensures that each participant contributes equally to the agreement key. The proposed protocol uses mutually unbiased bases particles as decoy particles and performs unitary operations on these decoy particles using a pair of function values of symmetric binary polynomial, which can not only perform eavesdropping checks, but also achieved the identity authentication between participants. The scheme can be applied to any situation with more than 2 participants. The security analysis shows that the proposed protocol can resist external attacks and participant attacks. Compared with the existing multi-party QKA, the proposed protocol not only has advantages in the use of decoy particles, but also has high quantum bit efficiency.

Key words: quantum key agreement; four-qubit Cluster states; multi-party; verifiable

自从 Bennett 和 Brassard[1]于 1984 年提出量子密钥分配协议以来, 量子密码学开始蓬勃发展. 量子密钥协商(quantum key agreement, QKA), 由于其在量子密码学中的重要作用, 已经引起越来越多的关注[2−5]. 第 1 种 QKA 协议是由 Zhou[6]于 2004 年提出的, 该方案基于量子隐形传态技术. 随后, Tsai[7]指出: Zhou 的协议中, 一方完全可以单独确定共享密钥, 而不被检测到, 所以它无法抵抗参与者攻击. 2010 年, Chong 等人[8]首次提出

* 基金项目: 国家自然科学基金(11671244, 12071271)
收稿时间: 2021-01-10; 修改时间: 2021-03-06, 2021-04-21; 采用时间: 2021-05-19

了基于 BB84 的两方 QKA 协议, 该协议采用了酉运算和延迟测量技术. 之后, 文献[9,10]提出了几种新的两方 QKA 协议, 它们分别采用最大纠缠态、Bell 态和 Bell 测量等方法. 但这些 QKA 协议并不完美, 因为它们只适用于两方参与者的情况. 直到 2013 年, Shi 等人[11]提出一种具有 Bell 态和 Bell 测量的多方 QKA 协议. 不幸的是, 文献[12]证明了 Shi 等人的协议不能抵抗参与者的攻击, 并提出了一种具有单粒子的安全多方 QKA 协议.

近年来, 多量子比特态[13,14]逐渐成为研究热点, 特别是具有 GHZ 态和 W 态属性的 Cluster 态. 2001 年, Briegel[15]和 Raussendorf[16]首次介绍了在纠缠粒子数大于 3 时, Cluster 态的一些有趣性质. 例如, Cluster 态是最大连接的, 比 GHZ 态更难被局部操作破坏, 表现出更好的持久性等. 2014 年, 文献[17]提出一种基于四粒子 Cluster 态的两方 QKA 协议, 该方案的两个参与者使用酉运算联合建立共享密钥, 保证了他们对协商密钥的贡献相等. 2015 年, 文献[18]提出一种改进的 QKA 协议, 以抵抗参与者攻击和外部攻击. 然而,文献[17,18]提出的方案实施起来有些复杂, 例如需要进行双向量子通信. 2019 年, 文献[19]提出一种简化的基于四量子比特 Cluster 态的 QKA 协议, 编码的四量子比特 Cluster 态通过顺序重排操作的手段, 可以避免进行双向量子通信. 文献[19]还分析了协议的可扩展性, 提出一种基于四量子比特 Cluster 态的三方 QKA 协议. 同年, 文献[20]提出一种多方量子密钥协商协议, 该协议充分利用四量子比特 Cluster 态作为量子资源, 并执行 X 运算以生成共享密钥. 然而, 文献[20]的方案只适合于参与者人数为奇数的情形. 2020 年, 文献[21]提出一种具有非最大纠缠四量子比特 Cluster 态的多方量子密钥协商方案. 在该方案中, 每个参与者编码 Cluster 态中的第 2 个和第 4 个粒子, 以确保共享密钥由所有参与者确定. 然而, 文献[19,20]的方案均没有考虑参与者之间的身份验证.

本文在文献[20]的基础上, 基于 X 运算和四量子比特 Cluster 态, 提出了一种可验证多方量子密钥协商方案(verifiable multi-party quantum key agreement, VM-QKA). 方案允许每个参与者在四量子比特 Cluster 态的两个粒子上执行 X 运算, 并对转换后的 Cluster 态执行延迟测量, 这保证了每个参与者对协商密钥的贡献相等. 16 个四量子比特 Cluster 态构成一个完整的正交基, 其中每一个态都可以携带四比特的密钥信息. 安全性分析表明, 本文的协议能抵抗参与者攻击和外部攻击. 此外, 该协议还具有较高的量子比特的效率. 与原始方案比较, 本文的方案有以下优点:

(1) 使用相互无偏基粒子作为诱饵粒子, 防止在传送过程中被外部敌手窃听, 且接收方无须询问测量基;

(2) 具有对参与者身份验证的功能. 利用对称二元多项式的一对函数值作为酉变换的参数, 利用该酉变换作用在诱饵粒子上, 进行参与者之间的身份验证;

(3) 方案适用于任意大于 2 的参与者人数.

本文第 1 节介绍 X 运算、四量子比特 Cluster 态及相互无偏基的相关概念. 第 2 节介绍提出的 VM-QKA 协议的详细过程. 第 3 节给出两个实例. 第 4 节–第 6 节分别进行正确性、可验证性及安全性分析. 第 7 节将提出的方案与其他多方 QKA 协议进行对比分析. 最后, 本文在第 8 节给出一个简短的结论.

1 预备知识

1.1 X运算与四量子比特Cluster态

本文使用四量子比特 Cluster 态作为量子资源, 即:

$$|C\rangle=(1/2)(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle)_{1234}.$$

假设 Alice 和 Bob 随机地生成他们的子密钥:

$$K_A=(K_A^{(1)},K_A^{(2)},...,K_A^{(m)}),\ K_B=(K_B^{(1)},K_B^{(2)},...,K_B^{(m)}).$$

这里, $K_A^{(j)},K_B^{(j)}\in\{00,01,10,11\}$, j=1,2,…,m. Alice 根据 K_A 在 Cluster 态$|C\rangle$的粒子 1 和粒子 2 上执行 X 运算, 其中, $X=|0\rangle\langle 1|+|1\rangle\langle 0|$. 运算的规则是: 如果 K_A 的第 1 个比特是 0(1), 粒子 1 被单独留下(翻转); 如果 K_A 的第 2 个比特是 0(1), 则粒子 2 被单独留下(翻转). Bob 根据 K_B 在粒子 3 和粒子 4 上执行 X 运算. 运算的规则是: 如果 K_B 的第 1 个比特是 0(1), 粒子 3 被单独留下(翻转); 如果 K_B 的第 2 个比特是 0(1), 则粒子 4 被单独留下(翻转). 通过对 Cluster 态$|C\rangle$上的粒子根据子密钥 K_A, K_B 执行 X 运算后, 可以得到以下 16 种 Cluster 态中的一种:

表 1 16 种 Cluster 态

$\|C_1\rangle=(1/2)(\|0000\rangle+\|0011\rangle+\|1100\rangle+\|1111\rangle)_{1234}$	$\|C_9\rangle=(1/2)(\|1000\rangle+\|1011\rangle+\|0100\rangle+\|0111\rangle)_{1234}$
$\|C_2\rangle=(1/2)(\|0001\rangle+\|0010\rangle+\|1101\rangle+\|1110\rangle)_{1234}$	$\|C_{10}\rangle=(1/2)(\|1001\rangle+\|1010\rangle+\|0101\rangle+\|0110\rangle)_{1234}$
$\|C_3\rangle=(1/2)(\|0010\rangle+\|0001\rangle+\|1110\rangle+\|1101\rangle)_{1234}$	$\|C_{11}\rangle=(1/2)(\|1010\rangle+\|1001\rangle+\|0110\rangle+\|0101\rangle)_{1234}$
$\|C_4\rangle=(1/2)(\|0011\rangle+\|0000\rangle+\|1111\rangle+\|1100\rangle)_{1234}$	$\|C_{12}\rangle=(1/2)(\|1011\rangle+\|1000\rangle+\|0111\rangle+\|0100\rangle)_{1234}$
$\|C_5\rangle=(1/2)(\|0100\rangle+\|0111\rangle+\|1000\rangle+\|1011\rangle)_{1234}$	$\|C_{13}\rangle=(1/2)(\|1100\rangle+\|1111\rangle+\|0000\rangle+\|0011\rangle)_{1234}$
$\|C_6\rangle=(1/2)(\|0101\rangle+\|0110\rangle+\|1001\rangle+\|1010\rangle)_{1234}$	$\|C_{14}\rangle=(1/2)(\|1101\rangle+\|1110\rangle+\|0001\rangle+\|0010\rangle)_{1234}$
$\|C_7\rangle=(1/2)(\|0110\rangle+\|0101\rangle+\|1010\rangle+\|1001\rangle)_{1234}$	$\|C_{15}\rangle=(1/2)(\|1110\rangle+\|1101\rangle+\|0010\rangle+\|0001\rangle)_{1234}$
$\|C_8\rangle=(1/2)(\|0111\rangle+\|0100\rangle+\|1011\rangle+\|1000\rangle)_{1234}$	$\|C_{16}\rangle=(1/2)(\|1111\rangle+\|1100\rangle+\|0011\rangle+\|0000\rangle)_{1234}$

表 1 中, C 的下标表示 Cluster 态的序号, 每个态后的下标 1234 表示 Cluster 态的 4 个粒子. 子密钥 K_A, K_B 的不同取值 $K_A^{(j)}$, $K_B^{(j)}$ ($j=1,2,...,m$) 与 Cluster 终态之间的对应关系见表 2 所示.

表 2 密钥的不同取值与转换后的 Cluster 终态之间的关系

终态	$K_A^{(j)}$	$K_B^{(j)}$	终态	$K_A^{(j)}$	$K_B^{(j)}$	终态	$K_A^{(j)}$	$K_B^{(j)}$	终态	$K_A^{(j)}$	$K_B^{(j)}$
$\|C_1\rangle$	(00)	(00)	$\|C_5\rangle$	(01)	(00)	$\|C_9\rangle$	(10)	(00)	$\|C_{13}\rangle$	(11)	(00)
$\|C_2\rangle$	(00)	(01)	$\|C_6\rangle$	(01)	(01)	$\|C_{10}\rangle$	(10)	(01)	$\|C_{14}\rangle$	(11)	(01)
$\|C_3\rangle$	(00)	(10)	$\|C_7\rangle$	(01)	(10)	$\|C_{11}\rangle$	(10)	(10)	$\|C_{15}\rangle$	(11)	(10)
$\|C_4\rangle$	(00)	(11)	$\|C_8\rangle$	(01)	(11)	$\|C_{12}\rangle$	(10)	(11)	$\|C_{16}\rangle$	(11)	(11)

在表 2 中, 每一个终态表示根据两个子密钥中 $K_A^{(j)}$ 和 $K_B^{(j)}$ 对初态执行 X 运算后的结果, 即 $K_A^{(j)}$, $K_B^{(j)}$ 的不同取值对应着终态$|C_k\rangle$, 其中, $k\in\{1,2,\ldots,16\}$, $j=1,2,\ldots,m$.

1.2 相互无偏基

定义 1[22,23]. 假设 $A_1=\{|\phi_i\rangle\}_{i=1}^q$ 和 $A_2=\{|\psi_i\rangle\}_{i=1}^q$ 是空间 C^q 中的两个标准正交基. 如果他们满足关系式: $|\langle\phi_i|\psi_j\rangle|=\frac{1}{\sqrt{q}}$, 那么称它们是相互无偏的.

若空间 C^q 中标准正交基的集合$\{A_1,A_2,\ldots,A_m\}$中每一对基都是无偏的, 则称此集合为无偏基集. 文献[21,22]中已经给出: 当量子系统维数 q 是奇素数时, 至多能够找出 q+1 组相互无偏基. 特别地, 将计算基表示为$\{|k\rangle|k\in D\}$, 其中, $D=\{0,1,\ldots,q-1\}$. 为了一致性, 本节中限制 q 为奇素数. 除了计算基之外, 剩余的 q 组相互无偏基可以表示为:

$$|\varphi_l^{(j)}\rangle=\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{k(l+jk)}|k\rangle.$$

其中, $\omega=e^{2\pi i/q}$, $j\in D$ 表示无偏基的序号, $l\in D$ 列举在给定无偏基中向量的序号. 对于 $j\neq j'$, 这些无偏基满足关系式:

$$|\langle\phi_l^{(j)}|\phi_{l'}^{(j')}\rangle|=\frac{1}{\sqrt{q}}.$$

设 $X_q=\sum_{n=0}^{q-1}\omega^n|n\rangle\langle n|$, 则有:

$$X_q^x|\varphi_l^{(j)}\rangle=X_q^x\left(\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{k(l+jk)}|k\rangle\right)=\frac{1}{\sqrt{q}}\left(\sum_{n=0}^{q-1}\omega^{xn}|n\rangle\langle n|\right)\left(\sum_{k=0}^{q-1}\omega^{k(l+jk)}|k\rangle\right)=\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{k(l+x)+jk}|k\rangle=|\varphi_{l+x}^{(j)}\rangle.$$

为了方便表达, 我们用 U_x 表示酉算子 X_q^x, 于是, $U_x|\varphi_l^{(j)}\rangle=|\varphi_{l+x}^{(j)}\rangle$. 特别地, $U_l|\varphi_0^{(0)}\rangle=|\varphi_l^{(0)}\rangle$.

2 提出的 VM-QKA 协议

在提出的 VM-QKA 方案中, 参与者包括可信的分发者 Alice、n 个参与者$\{P_1,P_2,\ldots,P_n\}$和一些内部或外部敌手. 由于该方案为多方协议, 我们假设 $n\geqslant3$ 且所有这些参与者都有无限的计算能力. 在 n 个参与者中, 使用公开身份信息 x_i(i=1,2,…,n)的成员被认为是诚实的. 假设分发者和每个参与者之间存在一个安全的经典信

道, 从而使份额多项式可以安全地分发给参与者. 参与者收到的份额多项式可以作为酉运算的一部分, 作用到相互无偏基粒子上, 以执行参与者的身份验证及对窃听者进行检验. 参与者 $P_i(i=1,2,\ldots,n)$之间均存在量子通信信道. 本协议中, 参与者之间的通信模型如图 1 所示.

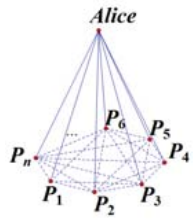


图 1 本协议中参与者之间的通信模型示意图

2.1 初始化阶段

Alice 选择一个 $k-1$ 次对称二元多项式:

$$F(x,y)=a_{00}+a_{10}x+a_{01}y+a_{11}xy+a_{20}x^2+a_{02}y^2+a_{21}x^2y+a_{12}xy^2+a_{22}x^2y^2+\ldots+a_{k-1,k-1}x^{k-1}y^{k-1} \bmod q.$$

其中, $a_{ij}\in F_q$, $i,j=\{0,1,\ldots,k-1\}$, $a_{ij}=a_{ji}$, q 是一个素数. 假设每个参与者的身份信息 x_i 是公开的, Alice 计算 n 个份额多项式 $f_i(y)=F(x_i,y)$, 并将份额多项式 $f_i(y)$通过安全信道发送给参与者 $P_i(i=1,2,\ldots,n)$. 参与者 P_i 可以根据其他成员的身份信息计算 $f_i(x_j)=F(x_i,x_j)$, 其中, $x_i\in F_q$, $x_j\in F_q$. P_i 通过计算可以得到的信息如表 3 所示. 每个参与者 P_i 生成一个随机的 $2m$ 比特的串作为他的子密钥: $K_i=(K_i^{(1)},K_i^{(2)},\ldots,K_i^{(m)})$, 这里, $K_i^{(j)}\in\{00,01,10,11\}$, $i=1,2,\ldots,n$, $j=1,2,\ldots,m$.

每个参与者 P_i 准备足够多的 q-维相互无偏基诱饵粒子: $|\varphi\rangle=|\phi_0^{(0)}\rangle=\frac{1}{\sqrt{q}}\sum_{i=0}^{q-1}|i\rangle$.

表 3 P_i 通过计算得到的信息

P_1	P_2	…	P_n
$f_1(x_2)=F(x_1,x_2)$	$f_2(x_1)=F(x_2,x_1)$	…	$f_n(x_1)=F(x_n,x_1)$
$f_1(x_3)=F(x_1,x_3)$	$f_2(x_3)=F(x_2,x_3)$	…	$f_n(x_2)=F(x_n,x_2)$
…	…	…	…
$f_1(x_n)=F(x_1,x_n)$	$f_2(x_n)=F(x_2,x_n)$	…	$f_n(x_{n-1})=F(x_n,x_{n-1})$

2.2 密钥协商阶段

在密钥协商阶段, 需要由 n 个参与者发起 n 轮协商. 为方便起见, 在这里只演示第 i 轮密钥协商过程, 其他 $n-1$ 轮以此类推. 第 i 轮密钥协商过程是由参与者 P_i 发起的, 可以形成参与者之间的对应关系, 如图 2 所示.

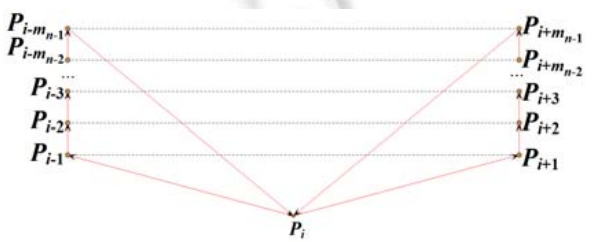


图 2 在第 i 轮中参与者之间的对应关系示意图

在图 2 中, $m_{n-2}=\lceil(n-2)/2\rceil$, $m_{n-1}=\lceil(n-1)/2\rceil$(注记: 方案中所有的下标均执行模 n 运算, 若 n 为偶数, 则令 $P_{i-\lceil(n-1)/2\rceil}=P_+$, 对应的密钥为 $K_+=(00,00,\ldots,00)$):

(1) 参与者 P_i 准备一个有序的 m 个四量子比特 Cluster 初始态$|C_1\rangle$的序列 $(Q_1^1,Q_2^1,Q_3^1,Q_4^1),(Q_1^2,Q_2^2,Q_3^2,Q_4^2),\ldots,(Q_1^m,Q_2^m,Q_3^m,Q_4^m)$, 并从每个四量子比特 Cluster 态中提取第 k 个粒子来组成子序列 $S_{k,i}^i$. 这里,

i=1,2,…,n, k=1,2,3,4. 也就是说, $S^i_{1,i}=(Q^1_1,Q^2_1,...,Q^m_1)$, $S^i_{2,i}=(Q^1_2,Q^2_2,...,Q^m_2)$, $S^i_{3,i}=(Q^1_3,Q^2_3,...,Q^m_3)$, $S^i_{4,i}=(Q^1_4,Q^2_4,...,Q^m_4)$. 这里, Q 的下标表示一个 Cluster 态下的 4 个不同粒子, Q 的上标表示第 k 个粒子在纠缠态序列 $S^j_{k,i}$ 中的位置. S 的下标中, 第 1 个数字还是表示一个 Cluster 态下的 4 个不同粒子, 第 2 个数字表示第 i 轮密钥协商, S 的上标用于标识参与者的序号. 然后, P_i 选择足够的诱饵粒子 $|\phi\rangle_{i,i-1}=U_{F(x_i,x_{i-1})}|\varphi^{(0)}_0\rangle=|\varphi^{(0)}_{F(x_i,x_{i-1})}\rangle$及 $|\phi\rangle_{i,i+1}=U_{F(x_i,x_{i+1})}|\varphi^{(0)}_0\rangle=|\varphi^{(0)}_{F(x_i,x_{i+1})}\rangle$, 并且随机地将诱饵粒子$|\phi\rangle_{i,i-1}$ 插入到 $S^i_{1,i}$, $S^i_{2,i}$ 中形成 $S^{i*}_{1,i}$, $S^{i*}_{2,i}$, 将诱饵粒子$|\phi\rangle_{i,i+1}$ 插入到 $S^i_{3,i}$, $S^i_{4,i}$ 中形成 $S^{i*}_{3,i}$, $S^{i*}_{4,i}$. 最后, P_i 分别发送序列 $S^{i*}_{1,i}$, $S^{i*}_{2,i}$ 给 P_{i-1} 并且发送序列 $S^{i*}_{3,i}$, $S^{i*}_{4,i}$ 给 P_{i+1};

(2) 在确认了 $P_{i-1}(P_{i+1})$已经接收到序列 $S^{i*}_{1,i}$和$S^{i*}_{2,i}$($S^{i*}_{3,i}$和$S^{i*}_{4,i}$) 以后, P_i 公布诱饵粒子的位置. 然后, $P_{i-1}(P_{i+1})$对诱饵粒子做酉运算 $|\phi\rangle_{i-1,i}=U_{-F(x_{i-1},x_i)}|\phi\rangle_{i,i-1}$($|\phi\rangle_{i+1,i}=U_{-F(x_{i+1},x_i)}|\phi\rangle_{i,i+1}$), 使用测量基 $\{|\varphi^{(0)}_l\rangle|l\in q\}$ 测量诱饵粒子, 如果 $|\phi\rangle_{i-1,i}\neq|\varphi^{(0)}_0\rangle$($|\phi\rangle_{i+1,i}\neq|\varphi^{(0)}_0\rangle$), 则说明 P_i 的身份认证不能通过或者该粒子被窃听了, 即发生了错误. 最后, $P_{i-1}(P_{i+1})$根据对诱饵粒子的测量结果计算错误率: 如果错误率小于预先给定的值, 他们将执行下一步; 否则, 他们将抛弃这个协议;

(3) $P_{i-1}(P_{i+1})$首先剔除掉诱饵粒子, 恢复序列 $S^i_{1,i}$和$S^i_{2,i}$($S^i_{3,i}$和$S^i_{4,i}$). 然后, $P_{i-1}(P_{i+1})$根据 $K^{(j)}_{i-1}(K^{(j)}_{i+1})$($j$=1,2,…, m)在 $S^i_{1,i}$ 上的第 j 个和 $S^i_{2,i}$ 上的第 j 个粒子($S^i_{3,i}$ 上的第 j 个和 $S^i_{4,i}$ 上的第 j 个粒子)执行 X 运算, 他可以获得序列 $S^{i-1}_{1,i}$和$S^{i-1}_{2,i}$($S^{i+1}_{3,i}$和$S^{i+1}_{4,i}$). 这个规则被描述如下: 如果 $K^{(j)}_{i-1}$ 的第 1 个比特是 0(1), 则 $S^{i-1}_{1,i}$ 的第 j 个粒子被单独留下(翻转); 如果 $K^{(j)}_{i-1}$ 的第 2 个比特是 0(1), 则 $S^{i-1}_{2,i}$ 的第 j 个粒子被单独留下(翻转); 如果 $K^{(j)}_{i+1}$ 的第 1 个比特是 0(1), 则 $S^{i+1}_{3,i}$ 的第 j 个粒子被单独留下(翻转); 如果 $K^{(j)}_{i+1}$ 的第 2 个比特是 0(1), 则 $S^{i+1}_{4,i}$ 的第 j 个粒子被单独留下(翻转);

(4) $P_{i-1}(P_{i+1})$随机地选择足够的诱饵粒子 $|\phi\rangle_{i-1,i-2}=U_{F(x_{i-1},x_{i-2})}|\varphi^{(0)}_0\rangle=|\varphi^{(0)}_{F(x_{i-1},x_{i-2})}\rangle$及 $|\phi\rangle_{i+1,i+2}=U_{F(x_{i+1},x_{i+2})}|\phi^{(0)}_0\rangle=|\varphi^{(0)}_{F(x_{i+1},x_{i+2})}\rangle$, 并且随机地将诱饵粒子$|\phi\rangle_{i-1,i-2}$($|\phi\rangle_{i+1,i+2}$)插入到序列 $S^{i-1}_{1,i}$和$S^{i-1}_{2,i}$($S^{i+1}_{3,i}$和$S^{i+1}_{4,i}$) 中, 获得序列 $S^{i-1*}_{1,i}$和$S^{i-1*}_{2,i}$($S^{i+1*}_{3,i}$和$S^{i+1*}_{4,i}$). 最后, $P_{i-1}(P_{i+1})$向 $P_{i-2}(P_{i+2})$发送序列 $S^{i-1*}_{1,i}$和$S^{i-1*}_{2,i}$($S^{i+1*}_{3,i}$和$S^{i+1*}_{4,i}$);

(5) 参与者 P_{i-2},P_{i+2},…,$P_{i-\lceil(n-1)/2\rceil}$,$P_{i+\lceil(n-1)/2\rceil}$执行相应的身份认证及窃听检查, 并且做与第(3)步、第(4)步中的 P_{i-1} 和 P_{i+1} 所作相同的 X 运算. 他们完成过程, 直到 $P_{i-\lceil n-1\rceil/2}(P_{i+\lceil n-1\rceil/2})$发送序列 $S^{(i-\lceil n-1\rceil/2)*}_{1,i}$, $S^{(i-\lceil n-1\rceil/2)*}_{2,i}$($S^{(i+\lceil n-1\rceil/2)*}_{3,i}$, $S^{(i+\lceil n-1\rceil/2)*}_{4,i}$) 给 P_i;

(6) 在 P_i 公布他已经从 $P_{i-\lceil n-1\rceil/2}(P_{i+\lceil n-1\rceil/2})$接收了序列 $S^{(i-\lceil n-1\rceil/2)*}_{1,i}$, $S^{(i-\lceil n-1\rceil/2)*}_{2,i}$($S^{(i+\lceil n-1\rceil/2)*}_{3,i}$, $S^{(i+\lceil n-1\rceil/2)*}_{4,i}$) 以后, $P_{i-\lceil n-1\rceil/2}(P_{i+\lceil n-1\rceil/2})$公布诱饵粒子的位置. P_i 对诱饵粒子做酉运算 $|\phi\rangle_{i,i-\lceil(n-1)/2\rceil}=U_{-F(x_i,x_{i-\lceil(n-1)/2\rceil})}|\phi\rangle_{i-\lceil(n-1)/2\rceil,i}$($|\phi\rangle_{i,i+\lceil(n-1)/2\rceil}=U_{-F(x_i,x_{i+\lceil(n-1)/2\rceil})}|\phi\rangle_{i+\lceil(n-1)/2\rceil,i}$), 使用测量基 $\{|\varphi^{(0)}_l\rangle|l\in q\}$ 测量诱饵粒子, 如果 $|\phi\rangle_{i,i-\lceil(n-1)/2\rceil}\neq|\varphi^{(0)}_0\rangle$($|\phi\rangle_{i,i+\lceil(n-1)/2\rceil}\neq|\varphi^{(0)}_0\rangle$), 则说明 $P_{i-\lceil n-1\rceil/2}(P_{i+\lceil n-1\rceil/2})$的身份验证不能通过或者该粒子被窃听了, 即发生了错误. 最后, P_i 根据对诱饵粒子的测量结果计算错误率: 如果错误率小于预先给定的值, 他们将执行下一步; 否则, 他们将抛弃这个协议;

(7) 参与者 P_i 首先剔除掉诱饵粒子, 恢复序列 $S^{(i-\lceil n-1\rceil/2)}_{1,i}$, $S^{(i-\lceil n-1\rceil/2)}_{2,i}$($S^{(i+\lceil n-1\rceil/2)}_{3,i}$, $S^{(i+\lceil n-1\rceil/2)}_{4,i}$), 利用 Cluster 基对它们进行测量, 以提取相应的密钥并获得最终的共享密钥:

$$K=K_i\oplus K_{i-1}\oplus\ldots\oplus K_{i-\lceil(n-1)/2\rceil}\oplus K_{i+\lceil(n-1)/2\rceil}\oplus\ldots\oplus K_{i+1}.$$

P_i 计算并公布 $H_i=h(K)$, 其中, $h(\cdot)$是一个公开的 Hash 函数;

(8) 当 P_j(j=1,2,…,i–1,i+1,…,n)执行同样的运算得到 H_j 后, 与 H_i 进行对比: 若两者相同, 则继续执行密钥协商, 直到全部参与者均获得协商密钥为止; 若有任意一对不相等, 则说明有不诚实参与者, 进程

中断.

3 举 例

3.1 例1

设 n=8, m=5, 参与者生成随机的 2m 比特的串, 如表 4 所示:

表 4 参与者生成的密钥比特

参与者	密钥	参与者	密钥	参与者	密钥
P_1	K_1=(01,11,11,10,00)	P_4	K_1=(01,11,11,10,10)	P_7	K_7=(00,00,11,11,10)
P_2	K_2=(10,10,11,00,10)	P_5	K_5=(11,10,01,01,11)	P_8	K_8=(10,10,01,01,11)
P_3	K_3=(11,00,01,01,10)	P_6	K_6=(01,01,10,10,11)	P_+	K_+=(00,00,00,00,00)

预期的协商密钥为: $K=K_1\oplus K_2\oplus\ldots\oplus K_8\oplus K_+$=(01,11,11,00,11). 令 i=3, 下面只演示第 3 轮密钥协商过程. 此时, 算法的执行顺序如图 3 所示:

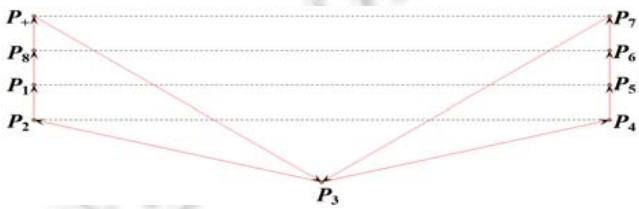


图 3 在第 3 轮中, 参与者之间的对应关系示意图

P_3 准备 5 个四量子比特 Cluster 态$|C_1\rangle$, 并从每个四量子比特 Cluster 态中提取第 k 个粒子(k=1,2,3,4)来组成子序列 $S^3_{1,3},S^3_{2,3},S^3_{3,3},S^3_{4,3}$. 由于$|C_1\rangle$对应的密钥比特为(0000), 所以子序列中没有携带任何密钥信息. 用 $C_{3,0}$ 表示这 5 个四量子比特 Cluster 态组成的集合, 类似地, 后面的态集合分别为 $C_{3,1},\ldots,C_{3,4}$, 所有参与者及四量子比特 Cluster 态集合的对应关系如图 4 所示.

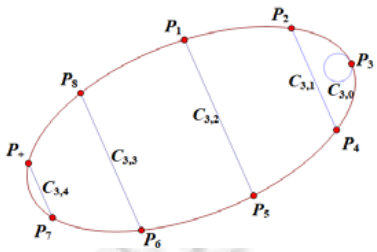


图 4 第 3 轮参与者及 Cluster 态集合的对应关系示意图

当 P_2(P_4)根据 $K_2^{(j)}$($K_4^{(j)}$)(j=1,2,...,5) 在 $S^3_{1,3}$ 上的第 j 个和 $S^3_{2,3}$ 上的第 j 个($S^3_{3,3}$ 上的第 j 个和 $S^3_{4,3}$ 上的第 j 个)粒子上执行 X 运算后, 5 个 Cluster 态变为$|C_{10}\rangle$, $|C_{12}\rangle$, $|C_{16}\rangle$, $|C_3\rangle$, $|C_{11}\rangle$. 对应的密钥为: (1001), (1011), (1111), (0010), (1010), 子序列变为 $S^2_{1,3},S^2_{2,3},S^4_{3,3},S^4_{4,3}$. 于是, 由 P_3, P_2, P_4 共同产生的态集合 $C_{3,1}$ 上有 5 个四量子比特 Cluster 态, 分别在每个态的第 1 个、第 2 个粒子上携带了 K_2 的信息, 在每个态的第 3 个、第 4 个粒子上携带了 K_4 的信息.

当 P_1(P_5)根据 $K_1^{(j)}$($K_5^{(j)}$)(j=1,2,...,5) 在 $S^2_{1,3}$ 上的第 j 个和 $S^2_{2,3}$ 上的第 j 个($S^4_{3,3}$ 上的第 j 个和 $S^4_{4,3}$ 上的第 j 个)粒子上执行 X 运算后, 5 个 Cluster 态变为$|C_{15}\rangle$, $|C_6\rangle$, $|C_3\rangle$, $|C_{12}\rangle$, $|C_{10}\rangle$. 对应的密钥为: (1110), (0101), (0010), (1011), (1001), 子序列变为 $S^1_{1,3},S^1_{2,3},S^5_{3,3},S^5_{4,3}$. 于是, 由 P_3, P_2, P_1, P_4, P_5 共同产生的态集合 $C_{3,2}$ 上有 5 个四量子比特 Cluster 态, 分别在每个态的第 1 个、第 2 个粒子上携带了 K_2, K_1 的信息, 在每个态的第 3 个、第 4 个粒

子上携带了 K_4, K_5 的信息.

当 $P_8(P_6)$根据 $K_8^{(j)}(K_6^{(j)})(j=1,2,...,5)$ 在 $S_{1,3}^1$ 上的第 j 个和 $S_{2,3}^1$ 上的第 j 个($S_{3,3}^5$ 上的第 j 个和 $S_{4,3}^5$ 上的第 j 个)粒子上执行 X 运算后, 5 个 Cluster 态变为$|C_8\rangle$, $|C_{13}\rangle$, $|C_5\rangle$, $|C_{14}\rangle$, $|C_7\rangle$. 对应的密钥为: (0111), (1100), (0100), (1101), (0110), 子序列变为 $S_{1,3}^8, S_{2,3}^8, S_{3,3}^6, S_{4,3}^6$.

当 $P_+(P_7)$根据 $K_+^{(j)}(K_7^{(j)})(j=1,2,...,5)$ 在 $S_{1,3}^8$ 上的第 j 个和 $S_{2,3}^8$ 上的第 j 个($S_{3,3}^6$ 上的第 j 个和 $S_{4,3}^6$ 上的第 j 个)粒子上执行 X 运算后, 5 个 Cluster 态变为$|C_8\rangle$, $|C_{13}\rangle$, $|C_8\rangle$, $|C_{15}\rangle$, $|C_5\rangle$. 对应的密钥为: (0111), (1100), (0111), (1110), (0100), 子序列变为 $S_{1,3}^+, S_{2,3}^+, S_{3,3}^7, S_{4,3}^7$.

最后, 当 P_3 根据测量提取的密钥(0111), (1100), (0111), (1110), (0100)及自己的密钥(11,00,01,01,10), 运算后得协商密钥为(01,11,11,00,11), 恰好是预期的协商密钥(表 5).

表 5 Cluster 态-序列-密钥对应表

步骤	第0步		第1步		第2步		第3步		第4步	
	态	密钥	态	密钥	态	密钥	态	密钥	态	密钥
Cluster态的变化过程	$\|C_1\rangle$	(0000)	$\|C_{10}\rangle$	(1001)	$\|C_{15}\rangle$	(1110)	$\|C_8\rangle$	(0111)	$\|C_8\rangle$	(0111)
	$\|C_1\rangle$	(0000)	$\|C_{12}\rangle$	(1011)	$\|C_6\rangle$	(0101)	$\|C_{13}\rangle$	(1100)	$\|C_{13}\rangle$	(1100)
	$\|C_1\rangle$	(0000)	$\|C_{16}\rangle$	(1111)	$\|C_3\rangle$	(0010)	$\|C_5\rangle$	(0100)	$\|C_8\rangle$	(0111)
	$\|C_1\rangle$	(0000)	$\|C_3\rangle$	(0010)	$\|C_{12}\rangle$	(1011)	$\|C_{14}\rangle$	(1101)	$\|C_{15}\rangle$	(1110)
	$\|C_1\rangle$	(0000)	$\|C_{11}\rangle$	(1010)	$\|C_{10}\rangle$	(1001)	$\|C_7\rangle$	(0110)	$\|C_5\rangle$	(0100)
对应的序列	$S_{1,3}^3, S_{2,3}^3, S_{3,3}^3, S_{4,3}^3$		$S_{1,3}^2, S_{2,3}^2, S_{3,3}^4, S_{4,3}^4$		$S_{1,3}^1, S_{2,3}^1, S_{3,3}^5, S_{4,3}^5$		$S_{1,3}^8, S_{2,3}^8, S_{3,3}^6, S_{4,3}^6$		$S_{1,3}^+, S_{2,3}^+, S_{3,3}^7, S_{4,3}^7$	
对应的密钥			P_2: (10,10,11,00,10) P_4: (01,11,11,10,10)		P_1: (01,11,11,10,00) P_5: (11,10,01,01,11)		P_8: (10,10,01,01,11) P_6: (01,01,10,10,11)		P_+: (00,00,00,00,00) P_7: (00,00,11,11,10)	

3.2 例2

接例 1, Alice 选择一个 4 次对称二元多项式 $F(x,y)=11+7x+4x^2+21x^3+18x^4+7y+9xy+5x^2y+10x^3y+13x^4y+4y^2+5xy^2+6x^2y^2+14x^3y^2+19x^4y^2+21y^3+10xy^3+14x^2y^3+22x^3y^3+2x^4y^3+18y^4+13xy^4+19x^2y^4+2x^3y^4+19x^4y^4 \bmod 23$. 假设 P_i 的身份信息为 $i(i=1,2,...,8)$, 且 P_+的身份信息为 9, 则 Alice 可为参与者提供如表 6 所示的份额多项式序列:

表 6 Alice 为 P_i 提供的份额多项式

P_i	份额多项式	P_i	份额多项式	P_i	份额多项式
P_1	$f_1(y)=15+21y+2y^2+0y^3+2y^4$	P_4	$f_4(y)=6+20y+15y^2+20y^3+7y^4$	P_7	$f_7(y)=8+21y+16y^2+15y^3+11y^4$
P_2	$f_2(y)=14+11y+17y^2+6y^3+3y^4$	P_5	$f_5(y)=14+7y+4y^2+5y^3+10y^4$	P_8	$f_8(y)=2+2y+21y^2+6y^3+8y^4$
P_3	$f_3(y)=0+22y+12y^2+13y^3+4y^4$	P_6	$f_6(y)=1+21y+22y^2+17y^3+7y^4$	P_+	$f_+(y)=14+18y+22y^2+22y^3+3y^4$

以例 1 中图 3 的顺序为例, 各参与者的身份验证过程如下所示:

(1) P_3 查询 $P_2(P_4)$的身份信息 2(身份信息 4)后, 根据自己的份额多项式 $f_3(y)=0+22y+12y^2+13y^3+4y^4$ 计算 $f_3(2)=7$, $f_3(4)=20$, 于是, P_3 制备足够的诱饵粒子 $|\phi\rangle_{3,2}=U_7|\varphi_0^{(0)}\rangle=|\varphi_7^{(0)}\rangle$及$|\phi\rangle_{3,4}=U_{20}|\varphi_0^{(0)}\rangle=|\varphi_{20}^{(0)}\rangle$, 并且随机地将诱饵粒子$|\phi\rangle_{3,2}$ 插入到 $S_{1,3}^3$, $S_{2,3}^3$ 中形成 $S_{1,3}^{3*}$, $S_{2,3}^{3*}$, 将诱饵粒子$|\phi\rangle_{3,4}$ 插入到 $S_{3,3}^3$, $S_{4,3}^3$ 中形成 $S_{3,3}^{3*}$, $S_{4,3}^{3*}$. 最后, P_3 分别发送序列 $S_{1,3}^{3*}$, $S_{2,3}^{3*}$给 P_2, 并且发送序列 $S_{3,3}^{3*}$, $S_{4,3}^{3*}$给 P_4;

(2) 在确认了 $P_2(P_4)$已经接收到序列 $S_{1,3}^{3*}$, $S_{2,3}^{3*}(S_{3,3}^{3*}$, $S_{4,3}^{3*})$ 以后, P_3 公布诱饵粒子的位置. P_2 根据 P_3 的身份信息及自己的份额多项式 $f_2(y)=14+11y+17y^2+6y^3+3y^4$ 计算 $f_2(3)=7$, P_4 根据 P_3 的身份信息及份额多项式 $f_4(y)=6+20y+15y^2+20y^3+7y^4$ 计算 $f_4(3)=20$. 然后, $P_2(P_4)$对诱饵粒子做酉运算$|\phi\rangle_{2,3}=U_{-7}|\phi\rangle_{3,2}=|\varphi_0^{(0)}\rangle$ $(|\phi\rangle_{4,3}=U_{-20}U_{20}|\varphi_0^{(0)}\rangle=|\varphi_0^{(0)}\rangle)$, 使用测量基 $\{|\varphi_l^{(0)}\rangle|l\in q\}$ 测量诱饵粒子, 如果$|\phi\rangle_{2,3}\neq|\varphi_0^{(0)}\rangle(|\phi\rangle_{4,3}\neq|\varphi_0^{(0)})$, 则说明 P_3 的身份验证不能通过或者该粒子被窃听了, 即发生了错误. 最后, $P_2(P_4)$根据对诱饵粒子的测量结果计算错误率: 如果错误率小于预先给定的值, 他们将执行下一步; 否则, 他们将抛弃这个协议;

(3) 同样, P_2 根据 P_1 的身份信息及自己的份额多项式 $f_2(y)=14+11y+17y^2+6y^3+3y^4$ 计算 $f_2(1)=5$, P_4 根据 P_5

的身份信息及份额多项式 $f_4(y)=6+20y+15y^2+20y^3+7y^4$ 计算 $f_4(5)=19$, 他们分别制备诱饵粒子 $|\phi\rangle_{2,1}=U_5|\varphi_0^{(0)}\rangle=|\varphi_5^{(0)}\rangle$及 $|\phi\rangle_{4,5}=U_{19}|\varphi_0^{(0)}\rangle=|\varphi_{19}^{(0)}\rangle$. P_1, P_5 利用份额多项式 $f_1(y)=15+21y+2y^2+0y^3+2y^4$ 和 $f_5(y)=14+7y+4y^2+5y^3+10y^4$ 及 P_2, P_4 的身份信息计算: $f_1(2)=5$, $f_5(4)=19$, 他们的身份验证及窃听检查表达式为: $|\phi\rangle_{1,2}=U_{-5}|\varphi_5^{(0)}\rangle=U_{-5}U_5|\varphi_0^{(0)}\rangle=|\varphi_0^{(0)}\rangle$, $|\phi\rangle_{4,5}=U_{-19}|\phi\rangle_{5,4}=U_{-19}U_{19}|\varphi_0^{(0)}\rangle=|\varphi_0^{(0)}\rangle$. 其他身份验证过程以此类推, 不再赘述.

4 正确性分析

定理 1. 参与者 $P_i(i=1,2,\ldots,n)$按照 VM-QKA 协议执行 w 次后, 四量子比特 Cluster 态集合 $C_{i,w}$ 中携带了 P_{i-1}, $P_{i-2},\ldots,P_{i-w}$ 及 $P_{i+1},P_{i+2},\ldots,P_{i+w}$ 的密钥信息.

证明: 根据协议规则, 由于 P_i 准备的 m 个 Cluster 态均为$|C_1\rangle=(1/2)(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle)_{1234}$, 这 m 个四量子比特 Cluster 态的集合表示为 $C_{i,0}$. P_i 从每个四量子比特 Cluster 态中提取第 k 个粒子来组成子序列 $S_{k,i}^i$. 这里, $i=1,2,\ldots,n$, $k=1,2,3,4$. 注意到, 此时每个 $S_{k,i}^i$ 中携带的密钥信息均为 m 个 0.

当 $P_{i-1}(P_{i+1})$根据 $K_{i-1}^{(j)}(K_{i+1}^{(j)})(j=1,2,...,m)$ 在 $S_{1,i}^i$ 上的第 j 个和 $S_{2,i}^i$ 上的第 j 个($S_{3,i}^i$ 上的第 j 个和 $S_{4,i}^i$ 上的第 j 个粒子)粒子上执行 X 运算后所获得的序列中, $S_{1,i}^{i-1}$和$S_{2,i}^{i-1}$ 上携带了 $K_{i-1}^{(j)}$ 的信息($S_{3,i}^{i+1}$和$S_{4,i}^{i+1}$ 上携带了 $K_{i+1}^{(j)}$ 的信息). 于是, 由 P_i, P_{i-1}, P_{i+1} 共同产生的态集合 $C_{i,1}$ 上有 m 个四量子比特 Cluster 态, 分别在每个态的第 1 个、第 2 个粒子上携带了 K_{i-1} 的信息, 在每个态的第 3 个、第 4 个粒子上携带了 K_{i+1} 的信息, 表示为 $C_{i,1}$~(K_{i-1},K_{i+1}).

当 $P_{i-2}(P_{i+2})$根据 $K_{i-2}^{(j)}(K_{i+2}^{(j)})(j=1,2,...,m)$ 在 $S_{1,i}^{i-1}$ 上的第 j 个和 $S_{2,i}^{i-1}$ 上的第 j 个($S_{3,i}^{i+1}$ 上的第 j 个和 $S_{4,i}^{i+1}$ 上的第 j 个)粒子上执行 X 运算后所获得序列中, $S_{1,i}^{i-2}$和$S_{2,i}^{i-2}$ 上携带了 $K_{i-1}^{(j)}\oplus K_{i-2}^{(j)}$ 的信息($S_{3,i}^{i+2}$和$S_{4,i}^{i+2}$ 携带了 $K_{i+1}^{(j)}\oplus K_{i+2}^{(j)}$ 的信息). 于是, 由 P_i, P_{i-1}, P_{i+1} 及 P_{i-2}, P_{i+2} 共同产生的态集合 $C_{i,2}$ 上有 m 个四量子比特 Cluster 态, 分别在第 j 个态的第 1 个、第 2 个粒子上携带了 $K_{i-1}^{(j)}\oplus K_{i-2}^{(j)}$ 的信息, 在第 j 个态的第 3 个、第 4 个粒子上携带了 $K_{i+1}^{(j)}\oplus K_{i+2}^{(j)}$ 的信息, 表示为 $C_{i,2}$~(K_{i-1},$K_{i+1}\oplus K_{i+1}$,K_{i+2}).

以此类推, 当 $P_{i-w}(P_{i+w})$根据 $K_{i-w}^{(j)}(K_{i+w}^{(j)})(j=1,2,...,m)$ 在 $S_{1,i}^{i-(w-1)}$ 上的第 j 个和 $S_{2,i}^{i-(w-1)}$ 上的第 j 个($S_{3,i}^{i+w-1}$ 上的第 j 个和 $S_{4,i}^{i+w-1}$ 上的第 j 个)粒子上执行 X 运算后所获得的序列中, $S_{1,i}^{i-w}$ 和 $S_{2,i}^{i-w}$ 上携带了 $K_{i-1}^{(j)}\oplus K_{i-2}^{(j)}\oplus\ldots\oplus K_{i-w}^{(j)}$ 的信息($S_{3,i}^{i+w}$ 和 $S_{4,i}^{i+w}$ 携带了 $K_{i+1}^{(j)}\oplus K_{i+2}^{(j)}\oplus\ldots\oplus K_{i+w}^{(j)}$ 的信息). 于是, 由 P_i,$P_{i-1},\ldots,P_{i-w}$ 及 $P_{i+1},\ldots,P_{i+w}$ 共同产生的态集合 $C_{i,w}$ 上有 m 个四量子比特 Cluster 态, 分别在第 j 个态的第 1 个、第 2 个粒子上携带了 $K_{i-1}^{(j)}\oplus K_{i-2}^{(j)}\oplus\ldots\oplus K_{i-w}^{(j)}$ 的信息, 在第 j 个态的第 3 个、第 4 个粒子上携带了 $K_{i+1}^{(j)}\oplus K_{i+2}^{(j)}\oplus\ldots\oplus K_{i+w}^{(j)}$ 的信息, 表示为 $C_{i,w}$~(K_{i-1}, $K_{i+1}\oplus\ldots\oplus K_{i-w}\oplus K_{i+1}$,$K_{i+2}\oplus\ldots\oplus K_{i+w}$). 证毕.

以上参与者及 Cluster 态集合 $C_{i,k}(k=0,1,\ldots,w)$的对应关系如图 5 所示.

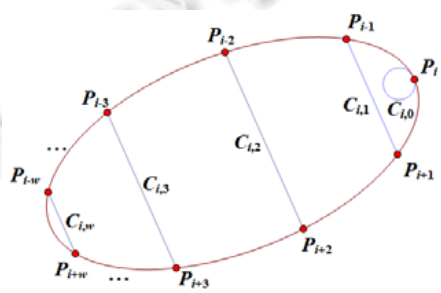


图 5 第 i 轮参与者及 Cluster 态集合的对应关系示意图

由方案的构造方法可知: 无论 n 为奇数还是偶数, 在第 i 轮密钥协商过程中, P_i 总能形成图 2 所示的参与者序列. 由定理 1 可知: 以上过程执行到第$\lceil(n-1)/2\rceil$步时, $C_{i,\lceil(n-1)/2\rceil}$携带了除 K_i 之外的所有参与者的密钥信息,

P_i 只需要将自己的密钥与其他密钥求和, 即可形成协商密钥:

$$K=K_i\oplus K_{i-1}\oplus\ldots\oplus K_{i-\lceil(n-1)/2\rceil}\oplus K_{i+\lceil(n-1)/2\rceil}\oplus\ldots\oplus K_{i+1}.$$

5 可验证性分析

定理 2. 在本方案中, 两个参与者之间可以根据诱饵粒子的测量结果进行身份验证及窃听检查.

证明: 假设 P_i, P_j 是任意两个参与者. 根据算法设计, 假设 P_i 依据自己掌握的份额多项式 $F(x_i,y)$, 利用 P_j 的公开身份信息 x_j, 计算 $F(x_i,x_j)$并制成诱饵粒子 $|\phi\rangle_{i,j}=U_{F(x_i,x_j)}|\varphi_0^{(0)}\rangle=|\varphi_{F(x_i,x_j)}^{(0)}\rangle$, 当 P_j 接收到$|\phi\rangle_{i,j}$后, 根据 P_i 的公开身份信息 x_i, 利用自己掌握的份额多项式 $F(x_j,y)$计算 $F(x_j,x_i)$后, 执行运算 $|\phi\rangle_{j,i}=-U_{F(x_j,x_i)}|\phi\rangle_{i,j}$, 根据对称二元多项式的性质, 可以得出 $F(x_j,x_i)=F(x_i,x_j)$. 于是, $|\phi\rangle_{j,i}=-U_{F(x_j,x_i)}U_{F(x_i,x_j)}|\varphi_0^{(0)}\rangle=|\varphi_0^{(0)}\rangle$. 由此可知: 若没有外部窃听行为, 并且 P_i 也没有作弊, 则 P_j 对诱饵粒子的测量结果应该是 $|\varphi_0^{(0)}\rangle$, 否则可以判断: 要么 P_i 存在身份作弊行为, 要么存在外部窃听行为, 或者两者都存在. 所以, P_j 可以根据对诱饵粒子的测量结果是不是 $|\varphi_0^{(0)}\rangle$ 来验证 P_i 的身份是否作弊.

由定理 2 可知: 在图 2 中的参与者序列中, P_{i-1} 及 P_{i+1} 均可以验证 P_i 的身份是否作弊, P_{i-2} 及 P_{i+2} 可以分别验证 P_{i-1} 及 P_{i+1} 的身份是否作弊. 以此类推, 所有参与者的身份均可以被验证.

6 安全性分析

在所提出的 VM-QKA 方案中, 内部敌手是一个拥有合法身份信息及子密钥的参与者, 他可能单独工作或与其他内部敌手勾结, 以使用虚假的身份信息或子密钥构造非法的协商密钥. 外部敌手是一个攻击者, 她不拥有分发者产生的任何份额多项式, 但她可能试图了解她未经授权访问的秘密. 本文将证明提出的协议是安全的. 攻击有两种, 即外部攻击和参与者攻击.

6.1 外部攻击

6.1.1 测量-重发攻击

如果 Eve 想成功地执行测量-重发攻击, 她需要在窃听检查之前就知道诱饵粒子的位置. 否则, 她的测量将会影响诱饵粒子的态. 由于窃听检查, 参与者能够以概率为 $1-(1/q)^m$ 发现这种攻击(m 是用于检查攻击的诱饵粒子数).

6.1.2 拦截-重发攻击

如果 Eve 执行拦截-重发攻击, 她必须拦截发送的序列并将假序列发送给参与者. 然而, 她不知道诱饵粒子的任何信息, 因此这种攻击可以很容易地被检测到. 发现这种攻击的概率为 $1-1/q^m$, 其中, m 表示诱饵粒子的数目.

6.1.3 纠缠-测量攻击

引理 1. 对于测量基 $|\varphi_g^{(0)}\rangle=\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{kg}|k\rangle$, 其中, $\omega=e^{2\pi i/q}$, 我们有 $\sum_{m=0}^{q-1}|m\rangle=\frac{1}{\sqrt{q}}\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{-mg}|\varphi_g^{(0)}\rangle$.

证明:

$$\begin{aligned}\frac{1}{\sqrt{q}}\sum_{g=0}^{q-1}\omega^{-mg}|\varphi_g^{(0)}\rangle&=\frac{1}{\sqrt{q}}[|\varphi_0^{(0)}\rangle+\omega^{-m}|\varphi_1^{(0)}\rangle+\omega^{-2m}|\varphi_2^{(0)}\rangle+\ldots+\omega^{-m(q-1)}|\varphi_{q-1}^{(0)}\rangle]\\&=\frac{1}{\sqrt{q}}\left[\sum_{k=0}^{q-1}|k\rangle+\omega^{-m}\sum_{k=0}^{q-1}\omega^{k}|k\rangle+\omega^{-2m}\sum_{k=0}^{q-1}\omega^{2k}|k\rangle+\ldots+\omega^{-m(q-1)}\sum_{k=0}^{q-1}\omega^{k(q-1)}|k\rangle\right]\\&=\frac{1}{\sqrt{q}}\left[\sum_{g=0}^{q-1}\omega^{-mg}|0\rangle+\sum_{g=0}^{q-1}\omega^{g(1-m)}|1\rangle+\sum_{g=0}^{q-1}\omega^{g(2-m)}|2\rangle+\ldots+\sum_{g=0}^{q-1}\omega^{g(g-1-m)}|q-1\rangle\right]\end{aligned}$$

$$\frac{1}{\sqrt{q}}\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{-mg}|\varphi_g^{(0)}\rangle=\frac{1}{q}\left[\sum_{m=0}^{q-1}\left(\sum_{g=0}^{q-1}\omega^{-mg}|0\rangle+\sum_{g=0}^{q-1}\omega^{g(1-m)}|1\rangle+\sum_{g=0}^{q-1}\omega^{g(2-m)}|2\rangle+\ldots+\sum_{g=0}^{q-1}\omega^{g(g-1-m)}|q-1\rangle\right)\right]$$

$$=\frac{1}{q}\left[\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{-mg}|0\rangle+\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{g(1-m)}|1\rangle+\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{g(2-m)}|2\rangle+\ldots+\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{g(q-1-m)}|q-1\rangle\right]$$

$$=\frac{1}{q}\left[q|0\rangle+q|1\rangle+\ldots+q|q-1\rangle\right]$$

$$=\sum_{m=0}^{q-1}|m\rangle$$

假设 Eve 制备了一个辅助量子态$|E\rangle$, 执行酉变换 U_E 将辅助量子态纠缠到所传输的粒子上, 通过测量辅助粒子以窃取秘密信息. 考虑对诱饵粒子攻击中所对应的测量基 $|\varphi_l^{(0)}\rangle=\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{kl}|k\rangle$. 通过酉变换 U_E 的作用, 根据引理 1, 可以得到如下表达式:

$$U_E|k\rangle|E\rangle=\sum_{m=0}^{q-1}a_{km}|m\rangle|\varepsilon_{km}\rangle \tag{1}$$

$$\begin{aligned}U_E|\varphi_l^{(0)}\rangle|E\rangle&=U_E\left(\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{kl}|k\rangle\right)|E\rangle\\&=\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{kl}\left(\sum_{m=0}^{q-1}a_{km}|m\rangle|\varepsilon_{km}\rangle\right)\\&=\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\sum_{m=0}^{q-1}\omega^{kl}a_{km}\left(\frac{1}{\sqrt{q}}\sum_{g=0}^{q-1}\omega^{-mg}|\varphi_g^{(0)}\rangle\right)|\varepsilon_{km}\rangle\\&=\frac{1}{q}\sum_{k=0}^{q-1}\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{kl-mg}a_{km}|\varphi_g^{(0)}\rangle|\varepsilon_{km}\rangle\end{aligned} \tag{2}$$

其中: $\omega=e^{2\pi i/q}$, $|E\rangle$表示 Eve 辅助系统的初始态; $|\varepsilon_{km}\rangle(k,m=0,1,\ldots,q-1)$表示由酉变换 U_E 作用之后得到的唯一纯态. 因此, 系数满足条件 $\sum_{m=0}^{q-1}|a_{km}|^2=1,\ k=0,1,...,q-1$. 如果 Eve 没有引入错误, 则算子 U_E 必须满足以下条件:

$$a_{km}=\begin{cases}0, & k\neq m\\1, & k=m\end{cases},\ k,m\in\{0,1,...,q-1\}.$$

因此, 公式(1)和公式(2)式简化为:

$$U_E|k\rangle|E\rangle=a_{kk}|k\rangle|\varepsilon_{kk}\rangle,\ U_E|\varphi_l^{(0)}\rangle|E\rangle=\frac{1}{q}\sum_{k=0}^{q-1}\sum_{g=0}^{q-1}\omega^{k(l-g)}a_{kk}|\varphi_g^{(0)}\rangle|\varepsilon_{kk}\rangle.$$

类似地, Eve 可以得到方程组 $\sum_{k=0}^{q-1}\omega^{k(l-g)}a_{kk}|\varepsilon_{kk}\rangle=0$. 其中, $g\neq l$, $g\in\{0,1,\ldots,q-1\}$. 对于任意 $l\in\{0,1,\ldots,q-1\}$, 可以得到 q 个方程. 通过这 q 个方程, 可以计算得到下式:

$$a_{00}|\varepsilon_{00}\rangle=a_{11}|\varepsilon_{11}\rangle=\ldots=a_{q-1,q-1}|\varepsilon_{q-1,q-1}\rangle.$$

这意味着: 无论采用什么量子态, Eve 只能从辅助粒子中获得同样的信息. 因此, 这种攻击不能在没有被检测到的情况下获得密钥信息.

6.2 参与者攻击

一般来说, 由于参与者知道许多有用的信息, 所以参与者攻击构成了最大的威胁. 如果 P_i 首先获得其他参与者的密钥, 他可以按照自己的意愿确定最后的共享密钥. 为了避免这种攻击, 所有参与者在已经完成了窃听检查之后, 对 $S_{1,i}^i$, $S_{2,i}^i$, $S_{3,i}^i$, $S_{4,i}^i$ 的粒子进行 X 运算. 因此, 没有人可以事先得到最终的协商秘钥, 并单独确定它.

此外, P_i必须公布诱饵粒子的正确位置和数目. 如果P_i在窃听监测时公布了错误的诱饵粒子的位置, 一些诱饵粒子会变成编码粒子, 那么这些 Cluster 态的纠缠关系将被破坏. 于是, 参与者的测量结果变得随机, 参与者不能生成相同的协商秘钥.

7 对比分析

对于 VM-QKA 协议, 量子比特效率[24]被定义为 $\eta=\frac{c}{q+b}$, 其中, c 表示最终共享密钥的长度, q 表示使用量子比特的总数, b 表示用于解码消息的经典比特数. 在本文的方案中, 为了生成 $2m$ 比特的共享密钥, 每个参与者必须准备 m 个四量子比特 Cluster 态和 $4m$ 个诱饵粒子. 假设参与者人数为 N, 则本文协议的量子比特效率是 $\eta=\frac{2m}{(4\cdot m+4\cdot m)\cdot N/2}=\frac{1}{2N}$. 接下来, 根据量子资源、可验证性、必要的量子运算、诱饵粒子及量子效率的不同, 将本方案与现存的其他 3 种多方 QKA 协议进行比较, 结果由表 7 所示.

表 7 本协议与几种多方 QKA 协议的比较

QKA协议	QR	可验证性	NQO	DP	QE
文献[2]的协议	GHZ态	无	SQUO+SQM	$\|0\rangle, \|1\rangle, \|+\rangle, \|-\rangle$	$\frac{1}{N(N-1)}$
文献[12]的协议	单粒子	无	SQUO+SQM	$\|+\rangle, \|-\rangle, \|+y\rangle, \|-y\rangle$	$\frac{1}{N(N-1)}$
文献[20]的协议	四粒子cluster态	无	FQOM+SQUO	$\|0\rangle, \|1\rangle, \|+\rangle, \|-\rangle$	$\frac{1}{2N}$
本文的协议	四粒子cluster态	有	FQOM+SQUO	$\|\varphi_i^{(0)}$	$\frac{1}{2N}$

QR: 量子资源, NQO: 必要的量子运算, DP: 诱饵粒子, QE: 量子效率, SQUO: 单量子比特酉运算, SQM: 单量子比特测量, FQOM: 四量子比特正交测量.

8 结 论

本文提出了一种可验证多方量子密钥协商方案. 方案允许每次由两个参与者利用自己的子密钥分别在每个四量子比特 Cluster 态的两个粒子上执行 X 运算, 并对转换后的 Cluster 态执行延迟测量, 保证了每个参与者对协商密钥的贡献相等. 方案适用于任意大于 2 的参与者人数. 通过对方案的正确性和安全性进行分析, 提出的方案能抵抗参与者攻击和外部攻击. 通过对部分多方 QKA 方案进行对比分析, 方案不仅在诱饵粒子的使用上有优势, 而且还实现了参与者的身份验证, 且效率较高. 该方案有待在实际场景中推广应用.

References:

[1] Bennett CH, Brassard G. Public-key distribution and coin tossing. In: Proc. of the IEEE Int'l Conf. on Computers, Systems and Signal Processing. Bangalore, 1984. 175−179.

[2] Xu GB, Wen QY, Gao F, *et al*. Novel multiparty quantum key agreement protocol with GHZ states. Quantum Information Processing, 2014, 13: 2587−2594.

[3] Abulkasim H, Alotaibi A. Improvement on multiparty quantum key agreement with four-qubit symmetric W state. Int'l Journal of Theoretical Physics, 2019, 58(12): 4235−4240.

[4] Li L, Li Z. A verifiable multiparty quantum key agreement based on bivariate polynomial. Information Sciences, 2020, 521: 343−349.

[5] Sun ZW, Yu JP, Wang P. Efficient multi-party quantum key agreement by cluster states. Quantum Information Processing, 2016, 15(1): 373−384.

[6] Zhou N, Zeng G, Xiong J. Quantum key agreement protocol. Electronics Letters, 2004, 40(18): 1149−1150.

[7] Tsai CW, Hwang T. On “quantum key agreement protocol”. Technical Report, 2009.

[8] Chong SK, Hwang T. Quuantm key agreement protocol based on BB84. Optics Communications, 2010, 283(6): 1192−1195.

[9] Chong SK, Tsai CW, Hwang T. Improvement on “quantum key agreement protocol with maximally entangled states”. Int’l Journal of Theoretical Physics, 2011, 50(6): 1793−1802.

[10] Shukla C, Alam N, Pathak A. Protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Information Processing, 2014, 13(11): 2391−2405.

[11] Shi RH, Zhong H. Multi-party quantum key agreement with bell states and bell measurements. Quantum Information Processing, 2013, 12(2): 921−932.

[12] Liu B, Gao F, Huang W, *et al*. Multiparty quantum key agreement with single particles. Quantum Information Processing, 2013, 12(4): 1797−1805.

[13] Cai T, Jiang M, Cao G. Multi-party quantum key agreement with five-qubit brown states. Quantum Information Processing, 2018, 17(5): 103.

[14] He YF, Ma WP. Two-party quantum key agreement with five-particle entangled states. Int’l Journal of Quantum Information, 2017, 15: 1750018.

[15] Briegel HJ, Raussendorf R. Persistent entanglement in arrays of interacting particles. Physical Review Letters, 2001, 86(5): 910−913.

[16] Raussendorf R, Briegel HJ. A one-way quantum computer. Physical Review Letters, 2001, 86(22): 5188−5191.

[17] Shen DS, Ma WP, Wang L. Two-party quantum key agreement with four-qubit cluster states. Quantum Information Processing, 2014, 13: 2313−2324.

[18] He YF, Ma WP. Quantum key agreement protocols with four-qubit cluster states. Quantum Information Processing, 2015, 14: 3483−3498.

[19] Yang YG, Li BR, Kang SY. New quantum key agreement protocols based on cluster states. Quantum Information Processing, 2019, 18(3): 322.

[20] Liu HN, Liang XQ, Jiang DH. Multi-party quantum key agreement with four-qubit cluster states. Quantum Information Processing, 2019, 18(8): 242.

[21] Li TC, Wang X, Jiang M. Quantum key agreement via non-maximally entangled cluster states. Int’l Journal of Theoretical Physics, 2020, 9: 1−16.

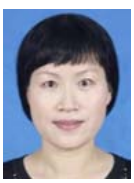
[22] Ivonovic ID. Geometrical description of quantal state determination. Journal of Physics A General Physics, 1981, 14(12): 3241−3245.

[23] Wootters WK, Fields BD. Optimal state-determination by mutually unbiased measurements. Annals of Physics, 1989, 191(2): 363−381.

[24] Cabello A. Quantum key distribution in the Holevo limit. Physical Review Letters, 2000, 85(26 Pt 1): 5635−5638.

芦殿军(1970－), 男, 博士生, 教授, 主要研究领域为量子密码学.

闫晨红(1997－), 女, 硕士生, 主要研究领域为量子密码学.



李志慧(1966－), 女, 博士, 教授, 博士生导师, 主要研究领域为量子密码学.

刘璐(1996－), 女, 硕士生, 主要研究领域为量子密码学.