基于非局域性正交乘积态的动态量子秘密共享方案

宋秀丽*①②　　李　闯①
①(重庆邮电大学计算机科学与技术学院　重庆　400065)
②(重庆邮电大学网络空间安全与信息法学院　重庆　400065)

摘　要：当前的量子秘密共享(QSS)存在资源制备开销较大、安全性不强的问题，该文提出一种基于正交乘积态的可验证量子秘密共享方案弥补上述不足，且多方成员能动态地加入或退出秘密共享。该方案将正交乘积态的粒子分成两个序列，第1个序列在多个参与者之间传输，前一个参与者对其执行嵌入份额值的酉算子后传输给下一个参与者，直到全部份额聚合完成；对于另一个序列，只有最后一个参与者(验证者)对接收到的粒子执行Oracle算子。然后，验证者对两个序列中的粒子对执行全局测量，得到秘密值的平方剩余。最后，借鉴Rabin密码中密文与明文之间非单一映射的思想，验证者联合Alice验证测量结果的正确性，并从测量结果确定出秘密值。安全性分析表明，该方案能抵抗常见的外部攻击和内部攻击，且验证过程具有强安全性；由于非局域性正交乘积态以两个序列分开传输，因此增强了秘密重构过程的安全性。性能分析表明，该方案使用正交乘积态作为信息载体，量子资源开销较小，且将正交乘积基的维度从低维拓展到d维，参与者人数能动态地增加和减少，使得方案具有更好的灵活性和通用性。

关键词：量子秘密共享；正交乘积态；动态加入或退出；Rabin密码
中图分类号：TN918; TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2024)03-1109-10
DOI: 10.11999/JEIT230193

Dynamic Quantum Secret Sharing Scheme Based on Nonlocal Orthogonal Product States

SONG Xiuli①②　　LI Chuang①
①(*College of Computer Science and Technology*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*)
②(*College of Cyber Security and Information Law*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*)

Abstract: Current Quantum Secret Sharing(QSS) has the drawbacks of high consumption of resource preparation and the security is not stronger. To overcome the above drawbacks, a verifiable quantum secret sharing scheme based on orthogonal product states is proposed, where multiple participants can dynamically join or leave the secret sharing. In the proposed scheme, the particle pairs of product states are divided into two sequences, the first sequence is transmitted among participants, and the previous participant performs the unitary operator to aggregate the shares on it and then transmits it to the next participant; for the other sequence, the last participant(verifier) performs the Oracle operator on the received particles. Afterward, the verifier uses global measurements on the particle pairs to obtain the quadratic residues of the secrets. Finally, learning from the idea of non-single mapping between ciphertext and plaintext in Rabin cipher, the verifier jointly with Alice verifies the correctness of the measurement results and identifies the secrets from the results. Security analysis shows that the proposed scheme can resist common external and internal attacks, and that

收稿日期：2023-03-28；改回日期：2023-06-18；网络出版：2023-06-26
*通信作者：　宋秀丽　songxl@cqupt.edu.cn
基金项目：国家自然科学基金(62376047)，河南省网络密码技术重点实验室(LNCT2022-A15)，重庆邮电大学博士启动基金(A2020211)，重庆自然科学基金(CSTB2023NSCQ-MSX1093)
Foundation Items: The National Natural Science Foundation of China (62376047), Henan Key Laboratory of Network Cryptography Technology (LNCT2022-A15), Doctor Initiation Found Project of Chongqing University of Posts and Telecommunications (A2020211), The Natural Science Foundation of Chongqing (CSTB2023NSCQ-MSX1093)

the verification process is strongly secure. Since the nonlocal orthogonal product states are transmitted separately in two sequences, the security of the secret reconstruction process is enhanced. Performance analysis shows that the proposed scheme has low quantum resource consumption using orthogonal product state as information carriers，and extends the dimension of orthogonal product basis from low dimension to d dimension, and the number of participants can be dynamically increased or decreased, so it provides better flexibility and generality.

Key words: Quantum Secret Sharing(QSS); Orthogonal product state; Dynamic join or leave; Rabin cipher

1 引言

量子秘密共享(Quantum Secret Sharing, QSS)是量子密码学的一个重要研究子领域，它将1个量子(经典)秘密分成多个份额，并将其分配给多个参与者，每个参与者拥有1个份额，只有多个参与者相互协作才能正确恢复出原始的秘密值。1999年，Hillery等人[1]发现对Greenberger-Horne-Zeilinger态的粒子执行测量，所得的结果具有关联性，基于这一性质，他们提出了首个QSS方案。此后，纠缠态测量结果的关联性引起了学者的广泛关注，一些基于纠缠态的QSS方案相继出现[1-4]，例如Karlsson等人[2]基于二粒子纠缠态的测量关联性提出了QSS方案，并讨论了如何抵抗外部攻击者的窃听攻击或参与者的内部攻击。

上述QSS方案都是基于纠缠态的非局域性设计的，后来一些学者基于经典通信和局域测量(Local Operations and Classical Communications, LOCC)将正交乘积基(Orthogonal Product Basis, OPB)中量子态完全区分开，提出了许多基于LOCC的正交乘积态QSS方案[5-7]，这些方案避免了量子态纠缠的开销。除了基于LOCC的正交乘积态可作为量子资源态之外，Bennett等人[8]构建的非局域性正交乘积基量子态也可以作为量子资源态，其只有全局测量才能被区分。2002年，Walgate等人[9]对文献[8]中构建的9个正交乘积态给出了简单的局域不可区分的证明。之后一些学者研究了一般的非局域性正交乘积基的构造及其证明[10,11]，例如，2021年，Xu等人[11]给出高维非局域性OPB的最小化构造，并证明了$C^d \otimes C^d$系统中至少有$2d-4$个正交乘积态是不能被局域区分的。目前，非局域性OPB量子态已经应用于量子秘密共享和量子签名等领域[12,13]。其中，2022年，Fu等人[13]基于非局域性OPB态提出了一种多方QSS方案，该方案的量子网络中，每个节点都拥有1个OPB态序列，用于共享秘密值，导致其量子资源开销较大。

上述QSS方案中参与者人数是固定的，有一个参与者缺席将导致秘密共享不能成功，动态量子秘密共享[14-18]能有效解决这一问题。2013年，Hsu等人[14]基于Bell态纠缠交换提出了一个动态QSS方案，可以在不改变秘密的情况下，实现参与者加入或退出。Wang等人[15]指出文献[14]中两个不诚实参与者使用Bell态替换攻击能窃取到分发者的秘密。2018年，Du等人[16]提出了可动态更新秘密和参与者份额的QSS方案，但是文献[17]指出该方案也不能抵抗合谋攻击。为了增强动态QSS方案的安全性，Li等人[18]提出了基于Bell态的动态QSS方案，该方案不仅能抵抗合谋攻击，并且考虑了参与者欺骗攻击的问题。

在基于非局域性OPB态的QSS方案中，当参与者人数增加时，量子资源开销较大；现有大多数动态QSS方案中使用纠缠态共享秘密，量子资源制备的难度较大，并且这些方案的安全性有待提升，鉴于以上两种QSS方案的局限性，本文以非局域性正交乘积态作为量子资源态，提出了一种多方参与者可动态加入或退出的量子秘密共享方案。与其他相似的QSS方案相比，提出的方案具有以下优势：

(1) 非局域性OPB态作为量子资源态，不仅量子资源开销较低，而且其非局域性在量子信息传输中拥有较好的安全性；

(2) 根据平方和定理将秘密进行分发和重构，可实现参与者人数的增加与减少，有较好的灵活性；

(3) 依据Rabin密码思想设计验证机制，测量结果验证过程具有强安全性。

2 预备知识

2.1 平方和定理

在整数域$\mathbb{Z}_p$中，p是一个无平方因子数，对于任意整数$r \in \mathbb{Z}_p$，它可以表示成$n \geq 2$个整数$\{r_1, r_2, \cdots, r_n\} \in \mathbb{Z}_p^n$的平方数之和[19]

$$r^2 = {r_1}^2 + {r_2}^2 + \cdots + r_n^2 (\bmod p) \tag{1}$$

2.2 d维酉算子

定义1(d维Pauli算子) 在d维量子空间中，通用的Pauli算子定义为$U(t) = \sum_{k=0}^{d-1} |t \oplus k\rangle\langle k|$，其中$t \in \{0, 1, \cdots, d-1\}$，$\oplus$是模$d$加法。

定义2(d维拉格朗日酉算子) 由定义1可知，所有的通用酉算子集合$\{\boldsymbol{U}(0), \boldsymbol{U}(1), \cdots, \boldsymbol{U}(d-1)\}$构

成了一个有限循环矩阵群。以此循环矩阵群为基础，可构造一个如式(2)所示的拉格朗日酉算子[20]

$$\boldsymbol{M}(\theta)=\sum_{j,k=0}^{n-1}\frac{\prod\limits_{k\neq j}(\mathrm{e}^{i\theta}-\omega^k)}{\prod\limits_{k\neq j}(\omega^j-\omega^k)}\boldsymbol{U}(j) \tag{2}$$

其中$\omega=\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}$。酉算子$\boldsymbol{U}(t)$与$\boldsymbol{M}(\theta)$满足如式(3)的交换和结合性质

$$\begin{aligned}\boldsymbol{U}(t)\boldsymbol{M}(\theta)&=\boldsymbol{M}(\theta)\boldsymbol{U}(t)\\&=\sum_{j,k=0}^{n-1}\frac{\prod\limits_{k\neq j}(\mathrm{e}^{\mathrm{i}\theta}-\omega^k)}{\prod\limits_{k\neq j}(\omega^j-\omega^k)}\boldsymbol{U}(j\oplus t)\end{aligned} \tag{3}$$

定义3(d维F变换及逆变换$\boldsymbol{F}^\dagger$)　d维(d是奇数)希尔伯特空间中，定义F变换为

$$\boldsymbol{F}=\frac{1}{\sqrt{2}}\sum_{k=0}^{d-1}(|k\rangle\langle k|+|k\oplus 1\rangle\langle k|) \tag{4}$$

将其作用在$|k\rangle(k\in\{0,1,\cdots,d-1\})$上，$|k\rangle$演变成$\frac{1}{\sqrt{2}}(|k\rangle+|k\oplus 1\rangle)$。并且，$F$变换的逆变换$F^\dagger$定义为

$$\boldsymbol{F}^\dagger=\frac{1}{\sqrt{2}}\left(\sum_{j=0}^{d-1}\sum_{k=0}^{d-1}\mathrm{e}^{\pi j}|k\oplus j\rangle\langle k|\right) \tag{5}$$

将$F^\dagger$算子作用量子态$\frac{1}{\sqrt{2}}(|k\rangle+|k\oplus 1\rangle)$，其演变为$F^\dagger\left(\frac{1}{\sqrt{2}}(|k\rangle+|k\oplus 1\rangle)\right)=|k\rangle$，其中$k\in\{0,1,\cdots,d-1\}$。

2.3　d维正交乘积态

在$C^d\otimes C^d$(d为奇数)系统中，最小化不可局域区分的正交乘积基[11]包含$2d-4$个元素，它们表示为

$$\begin{aligned}&\varPsi^\pm=\begin{cases}|\psi_0^\pm\rangle=|0\rangle_1|0\pm 1\rangle_2\\|\psi_1^\pm\rangle=|d-1\rangle_1|1\pm 2\rangle_2\\\quad\vdots\\|\psi_{d-2}^\pm\rangle=|d-1\rangle_1|(d-2)\pm(d-1)\rangle_2\end{cases}\\&\varPhi^\pm=\begin{cases}|\phi_0^\pm\rangle=|0\pm 1\rangle_1|d-1\rangle_2\\|\phi_1^\pm\rangle=|1\pm 2\rangle_1|0\rangle_2\\\quad\vdots\\|\phi_{d-2}^\pm\rangle=|(d-2)\pm(d-1)\rangle_1|0\rangle_2\end{cases}\end{aligned} \tag{6}$$

其中$|j\pm(j+1)\rangle=\frac{1}{\sqrt{2}}(|j\rangle\pm|j+1\rangle)$。特别的，将酉变换$\boldsymbol{U}(k)\otimes\boldsymbol{O}^k,k\in\{0,1,\cdots,d-2\}$作用在量子态$|\phi_0^\pm\rangle$上，演变过程如式(7)，其中，如果$k=1(\mathrm{mod}2)$，酉算子$\boldsymbol{O}^k=\boldsymbol{U}(1)$；如果$k=0(\mathrm{mod}2)$，$\boldsymbol{O}^k$为单位门$\boldsymbol{I}$

$$\boldsymbol{U}(k)\otimes\boldsymbol{O}^k|\phi_0^\pm\rangle=|\phi_k^\pm\rangle \tag{7}$$

3　基于非局域性正交乘积态的动态量子秘密共享方案

作为秘密序列的分发者，Alice在参与者集合$B=\{\mathrm{Bob}_1,\mathrm{Bob}_2,\cdots,\mathrm{Bob}_l\}$中分发秘密值，且她从集合$B$中选取任意一个参与者$\mathrm{Bob}_l$作为半可信的验证者，$\mathrm{Bob}_l$的职责是联合Alice对测量结果进行验证。本文所提方案主体上包括份额分发阶段、粒子制备阶段、秘密重构阶段和测量结果验证4个阶段。如果有其他参与者想要加入或退出秘密共享方案，则执行后续的参与者加入与退出过程。

3.1　份额分发阶段

Alice选择一个合适的有限域GF(d)，其中d是两个素数d_1,d_2的乘积。Alice生成一个秘密值序列$T=\{T_1,T_2,\cdots,T_n\}$，其中$\{T_j\in\mathrm{GF}(d)|j=1,2,\cdots,n\}$。以序列$T$为基础，Alice根据等式(1)构建$l\times n$矩阵

$$\boldsymbol{M}=\begin{pmatrix}m_{1,1}&m_{1,2}&\cdots&m_{1,n}\\\vdots&\vdots&\ddots&\vdots\\m_{l,1}&m_{l,2}&\cdots&m_{l,n}\end{pmatrix} \tag{8}$$

其中$\{{T_j}^2=\sum_{i=1}^{l}m_{i,j}^2(\mathrm{mod}d)|j=1,2,\cdots,n\}$。然后，Alice将式(8)中矩阵的行向量$\boldsymbol{m}_i=(m_{i,1},m_{i,2},\cdots,m_{i,n})$，$i=1,2,\cdots,l$，作为每一个对应参与者$\mathrm{Bob}_i$的隐私份额向量，通过量子安全信道发送给他。再次，Alice根据序列T计算向量$\boldsymbol{E}=(E_j={T_j}^2(\mathrm{mod}2)|j=1,2,\cdots,n)$，并计算序列$A=\{A_j=\sum_{i=1}^{l}m_{i,j}(\mathrm{mod}2d)|j=1,2,\cdots,n\}$，她将向量$\boldsymbol{E}$和序列$A$保留，将参数$d_1,d_2$在参与者集合$B$之间公开。

参与者$\mathrm{Bob}_i(i=1,2,\cdots,l)$收到份额向量后，他们与Alice共同协商一个随机数$b\in\mathbb{Z}_n$用于向量移位。

3.2　粒子制备阶段

步骤1　Alice从集合$\{\phi_0^+,\phi_0^-,\psi_0^+\}$中随机选取$n$个粒子对，将这些粒子对的第1个粒子组成信息粒子序列$P_S=\{|p_1\rangle_S,|p_2\rangle_S,\cdots,|p_n\rangle_S\}$，第2个粒子组成信息粒子序列$Q_S=\{|q_1\rangle_S,|q_2\rangle_S,\cdots,|q_n\rangle_S\}$，然后根据序列$A=\{A_1,A_2,\cdots,A_n\}$，对序列$P_S$中粒子$|p_j\rangle_S$($j$=1, 2, ⋯, n)执行酉算子$\boldsymbol{M}(\omega_j)$得到$|p_j\rangle_0$=$\boldsymbol{M}(\omega_j)|p_j\rangle_S$，参数$\omega_j=\pi(2d-A_{j'})/d$, $j'=1+((j+b-1)\mathrm{mod}n)$，对应于图1的步骤①。随后，Alice从集合$\{\varPsi^\pm,\varPhi^\pm\}$中任意选取$v$个粒子对作为诱骗粒子插入到序列$P_0=\{|p_1\rangle_0,|p_2\rangle_0,\cdots,|p_n\rangle_0\}$得到新的序列$\bar{P}_0$，当Alice记录序列$\bar{P}_0$中诱骗粒子的位置和初始态之后，她将序列$\bar{P}_0$发送给参与者$\mathrm{Bob}_1$。

3.3　秘密重构阶段

步骤2　Bob_1收到序列$\bar{P}_0$后，Alice告知Bob_1在$\bar{P}_0$中诱骗粒子对的位置和初始态，Bob_1根据收到

的位置信息，使用OPB基测量每对诱骗粒子。然后，Bob_1将得到的测量结果与Alice告知的初始态进行比较。如果错误率高于阈值(一般选取2%～8%)，将会放弃本轮操作，开始新一轮协议；否则Bob_1恢复出序列P_0并执行步骤3。

步骤3 Bob_1使用份额向量$\boldsymbol{m}_1$中的元素$m_{1,j}$ $(j=1,2,\cdots,n)$分别对相应的粒子$|p_j\rangle_0$执行酉算子$\boldsymbol{U}(m_{1,j}^2)$得到$\boldsymbol{U}(m_{1,j}^2)|p_j\rangle_0$，然后根据$\boldsymbol{m}_1$的第$j'$个元素$m_{1,j'}$计算$\theta_{1,j}=\pi m_{1,j'}/d$，$j'=1+((b+j-1)\bmod n)$。接着，$\mathrm{Bob}_1$对$\boldsymbol{U}(m_{1,j}^2)|p_j\rangle_0$执行拉格朗日酉算子$\boldsymbol{M}(\theta_{1,j})$，得到$|p_j\rangle_1=\boldsymbol{M}(\theta_{1,j})\boldsymbol{U}(m_{1,j}^2)|p_j\rangle_0$，对应于图1的步骤②。当$P_0$中的所有粒子变换完毕，得到序列$P_1=\{|p_1\rangle_1,|p_2\rangle_1,\cdots,|p_n\rangle_1\}$。

最后，Bob_1从集合$\{\varPsi^\pm,\varPhi^\pm\}$中随机选择$v$对诱骗粒子，将诱骗粒子插入到序列$P_1$中得到一个新的序列$\bar{P}_1$，并将其发送给下一个参与者$\mathrm{Bob}_2$。

步骤4 参与者Bob_2收到序列$\bar{P}_1$之后，执行类似于Bob_1的步骤2和3。恢复出序列P_1之后，Bob_2首先使用隐私份额向量$\boldsymbol{m}_2$中的每一个元素$m_{2,j}(j=1,2,\cdots,n)$分别对相应的粒子$|p_j\rangle_1$执行$\boldsymbol{U}(m_{2,j}^2)$得到$\boldsymbol{U}(m_{2,j}^2)|p_j\rangle_1$，然后根据$\boldsymbol{m}_2$中元素$m_{2,j'}$计算角度$\theta_{2,j}=\pi m_{2,j'}/d$，其中$j'=1+((b+j-1)\bmod n)$，再次对$\boldsymbol{U}(m_{2,j}^2)|p_j\rangle_0$执行拉格朗日酉算子$M(\theta_{2,j})$，得到$|p_j\rangle_2=\boldsymbol{M}(\theta_{2,j})\boldsymbol{U}(m_{2,j}^2)|p_j\rangle_1$，对应于图1的步骤③。当序列$P_1$中所有粒子变换完毕，得到序列$P_2=\{|p_1\rangle_2,|p_2\rangle_2,\cdots,|p_n\rangle_2\}$。

最后，Bob_2以诱骗粒子的传输模式将序列P_2发送给参与者Bob_3。其他参与者$\mathrm{Bob}_i(i=3,4,\cdots,l)$执行类似于$\mathrm{Bob}_2$的操作步骤，直到最后一个参与者$\mathrm{Bob}_l$执行完酉变换得到序列$P_l$，对应图1的步骤④。

步骤5 当所有参与者执行完自己的操作步骤之后，Alice将序列Q_S和向量$\boldsymbol{E}$以诱骗粒子的模式发送给参与者Bob_l，并且告知Bob_l粒子对$|p_j,q_j\rangle_S$ $(j=1,2,\cdots,n)$的制备时初态。Bob_l根据向量$\boldsymbol{E}$中元素$E_j(j=1,2,\cdots,n)$对Q_S中粒子$|q_j\rangle_S$执行Oracle算子O^{E_j}得到$O^{E_j}|q_j\rangle_S$(如果$E_j=1$，则O^{E_j}为酉算子$\boldsymbol{U}(1)$；如果$E_j=0$，则$\boldsymbol{O}^{E_j}$为单位门$\boldsymbol{I}$)，将这个过程记为$\boldsymbol{O}$变换，对应于图1的步骤⑤。当序列Q_S中的$\boldsymbol{n}$个粒子执行完毕，得到一个新的序列$Q_l=\{|q_1\rangle_l,|q_2\rangle_l,\cdots,|q_n\rangle_l\}$。

步骤6 当Alice选取的粒子对$|p_j,q_j\rangle_S(j\in\{1,2,\cdots,n\})$为$|\psi_0^+\rangle$时，$\mathrm{Bob}_l$对$|p_j,q_j\rangle_l$执行$(\boldsymbol{F}\otimes\boldsymbol{F}^\dagger\boldsymbol{U}(d-1))$变换得到$|p_j,q_j\rangle_l'$；当Alice选取的粒子对属于$\{|\phi_0^+\rangle,|\phi_0^-\rangle\}$时，$\mathrm{Bob}_l$对$|p_j,q_j\rangle_l$不执行任何变换。当所有粒子对变换完成，$\mathrm{Bob}_l$得到新的粒子对序列$\{P',Q'\}=\{|p_1,q_1\rangle_l',|p_2,q_2\rangle_l',\cdots,|p_n,q_n\rangle_l'\}$时，将该过程记为$\boldsymbol{F}$变换。

步骤7 Bob_l使用OPB基对序列$\{P',Q'\}$中的$\boldsymbol{n}$个粒子对执行测量操作，其中每个粒子对的量子态是集合$\{|\phi_0^\pm\rangle|\phi_1^\pm\rangle,\cdots,|\phi_{d-2}^\pm\rangle\}$中的一个元素，对应于图1的步骤⑥。量子态集合$\{|\phi_0^\pm\rangle|\phi_1^\pm\rangle,\cdots,|\phi_{d-2}^\pm\rangle\}$与经典整数集合$\{0,1,\cdots,d-2\}$之间的编码关系为：$\{|\phi_0^\pm\rangle\to 0;|\phi_0^\pm\rangle\to 1;\cdots;|\phi_{d-2}^\pm\rangle\to(d-2)\}$。那么，$\mathrm{Bob}_l$根据每个粒子对的量子态得到对应的整数，记为$\{R_1,R_2,\cdots,R_n\}$。

3.4 测量结果验证阶段

步骤8 针对测量结果$R_j(j=1,2,\cdots,n)$，如果它不是GF(d)中的平方剩余数，那么Bob_l认为被测量的粒子对是不合法的，本次秘密共享协议中存在不诚实的参与者，放弃本次协议；否则对于合法

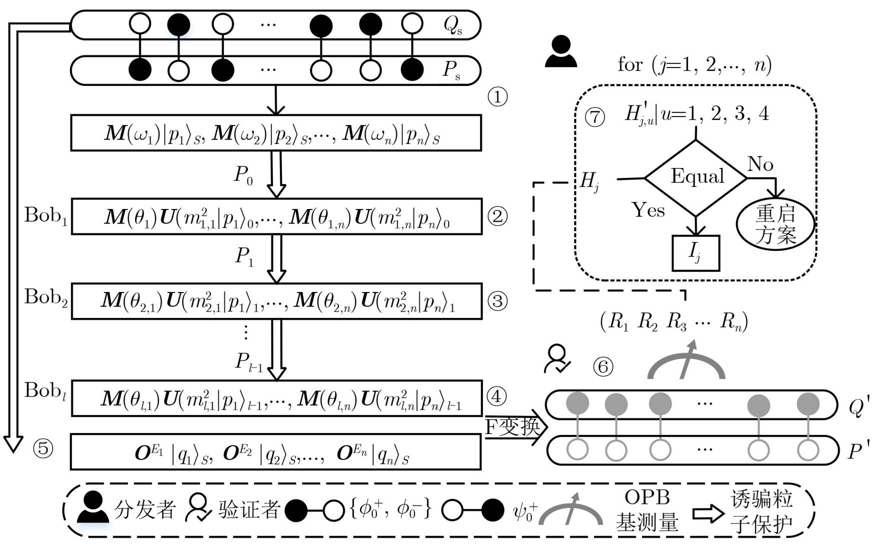

图 1 方案主体流程图

的测量结果R_j，Bob_l根据$\{r^2\equiv R_j(\mathrm{mod}d_1), r^2\equiv R_j(\mathrm{mod}d_2)\}$计算出4个平方根$r_{j,1},r_{j,2},r_{j,3},r_{j,4}$。然后，$\mathrm{Bob}_l$从平方根之中随机选取一个元素$r_{j,\tau}$ $(\tau\in\{1,2,3,4\})$，并使用安全单向函数H计算哈希值$H_j=H(\mathrm{ID}_l||r_{j,\tau}\times m_{l,j})$，$\mathrm{ID}_l$是$\mathrm{Bob}_l$的公开身份信息。最后，$\mathrm{Bob}_l$通过经典安全信道将$\{H_j|j=1,2,\cdots,n\}$发送给Alice。

步骤9　Alice收到Bob_l的$\{H_j|j=1,2,\cdots,n\}$后，根据Bob_l的份额向量中元素$m_{l,j}$和ID_l，以及T_j^2的平方根向量$\boldsymbol{t}_j=(t_{j,1},t_{j,2},t_{j,3},t_{j,4})$($T_j$在$\boldsymbol{t}_j$中序号为$I_j\in\{1,2,3,4\}$)，分别计算$\{H'_{j,u}=H(\mathrm{ID}_l||t_{j,u}\times m_{l.j})|u=1,2,3,4\}$，并将它们与$H_j$分别进行比对，如果有一个$H'_{j,u}(u\in\{1,2,3,4\})$与$H_j$相等，则认为测量结果$R_j$验证成功；反之，则告知$\mathrm{Bob}_l$本次秘密共享中存在不诚实的参与者，放弃本次协议。直到所有测量结果R_j被验证成功后，Alice将$T_j(j=1,2,\cdots,n)$在$\boldsymbol{t}_j$中的序号I_j作为标识信息通过经典安全信道发送给Bob_l，此时Bob_l确定R_j的平方根r_{j,I_j}为秘密值T_j，最后将秘密序列T在参与者之间共享。对应图1的步骤⑦。

3.5 参与者加入与退出过程

如果有其他t位参与者$\mathrm{Bob}_{l+1}, \mathrm{Bob}_{l+2}, \cdots, \mathrm{Bob}_{l+t}$想要加入到秘密共享过程之中，同时有一位参与者$\mathrm{Bob}_k(k\in\{1,2,\cdots,l\})$想要退出秘密共享过程，则他们执行以下操作：

参与者Bob_k根据份额向量$\boldsymbol{m}_k=(m_{k,1},m_{k,2},\cdots,m_{k,n})$重新计算一个新的$t\times n$矩阵

$$\boldsymbol{Y}=\begin{pmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,n}\\ \vdots & \vdots & \ddots & \vdots\\ y_{t,1} & y_{t,2} & \cdots & y_{t,n}\end{pmatrix}\tag{9}$$

其中，$m_{k,j}^2=\sum_{i=1}^{t}y_{i,j}^2(\mathrm{mod}d), j=1,2,\cdots,n$。然后，$\mathrm{Bob}_k$计算$a_j=\sum_{i=1}^{t}y_{i,j}-m_{k,j}(\mathrm{mod}2d)$并公布给Alice，Alice计算新的$A'_j=A_j+a_j$替换原有的参数$A_j$，并保留$A'_j$。此时，$\mathrm{Bob}_k$得到$t$个行向量$\{\boldsymbol{y}_1,\boldsymbol{y}_2,\cdots,\boldsymbol{y}_t\}$，并且将行向量$\boldsymbol{y}_i(i=1,2,\cdots,t)$通过量子安全信道分别分发给对应的参与者$\mathrm{Bob}_{l+i}$作为他的隐私份额向量，此时$\mathrm{Bob}_k$退出秘密共享，参与者$\mathrm{Bob}_{l+1}, \mathrm{Bob}_{l+2}, \cdots, \mathrm{Bob}_{l+t}$替换他加入到参与者集合$B$之中。剩下的步骤类似于参与者$\{\mathrm{Bob}_1, \mathrm{Bob}_2, \cdots, \mathrm{Bob}_l\}$所执行的操作。

4　正确性证明

定理1　若粒子对的初态为$|\psi_0^+\rangle$，先对其执行$\boldsymbol{U}(k)\otimes\boldsymbol{O}^k$, $k\in\{0,1,\cdots,d-2\}$变换，然后再执行变换$(\boldsymbol{F}\otimes\boldsymbol{F}^\dagger\boldsymbol{U}(d-1))$得到量子态$|\phi_k^+\rangle$。

证明　对于初态$|\psi_0^+\rangle=|0\rangle\otimes|0+1\rangle$，对其执行$\boldsymbol{U}(k)\otimes\boldsymbol{O}^k$变换，其中，若$k=1(\mathrm{mod}2)$，则酉算子$\boldsymbol{O}^k$为$\boldsymbol{U}(1)$，$|\psi_0^+\rangle$演变为$|\psi_0^+\rangle'=(|k\rangle\otimes|1+2\rangle)$；若$k=0(\mathrm{mod}2)$，则$\boldsymbol{O}^k$为单位门$\boldsymbol{I}$，$|\psi_0^+\rangle$演变为$(|k\rangle\otimes|0+1\rangle)$。然后，对$|\psi_0^+\rangle'$执行$(\boldsymbol{F}\otimes\boldsymbol{F}^\dagger\boldsymbol{U}(d-1))$变换将演变为

$$\begin{aligned}|\psi_0^+\rangle''&=(\boldsymbol{F}\otimes\boldsymbol{F}^\dagger\boldsymbol{U}(d-1))|\psi_0^+\rangle'\\&=\begin{cases}|k+(k+1)\rangle\otimes|0\rangle, & k=1(\mathrm{mod}2)\\ |k+(k+1)\rangle\otimes|d-1\rangle, & k=0(\mathrm{mod}2)\end{cases}\end{aligned}\tag{10}$$

此时，量子态$|\psi_0^+\rangle''$对应于式(6)中OPB集合的$|\phi_k^+\rangle$。

引理1　在份额重构阶段，如果参与者Bob_i $(i=1,2,\cdots,l)$对序列P_0中每一个粒子$|p_j\rangle_0(j=1,2,\cdots,n)$依次执行酉算子$\boldsymbol{M}(\theta_{i,j})\boldsymbol{U}(m_{i,j}^2)$，当所有参与者执行完毕，$\mathrm{Bob}_l$对序列$Q_S$中粒子$|q_j\rangle_S$执行$\boldsymbol{O}^{E_j}$变换，得到$|p_j,q_j\rangle_l$。$\mathrm{Bob}_l$对粒子对$|p_j,q_j\rangle_l$执行F变换后，$\mathrm{Bob}_l$使用OPB基测量序列$\{P',Q'\}$得到测量结果$\{R_1,R_2,\cdots,R_n\}$。当所有测量结果通过验证后，所有参与者能共享正确的秘密值序列$T=\{T_1,T_2,\cdots,T_n\}$。

证明　针对序列P_0中的任意一个粒子$|p_j\rangle_0$ $(j=1,2,\cdots,n)$，如果参与者$\mathrm{Bob}_i(i=1,2,\cdots,l)$对其依次执行酉算子$M(\theta_{i,j})\boldsymbol{U}(m_{i,j}^2)$，当所有参与者执行完毕之后，那么该粒子将演变为

$$\begin{aligned}|p_j\rangle_l=&\boldsymbol{M}(\theta_{l,j})\boldsymbol{U}(m_{l,j}^2)\cdots\boldsymbol{M}(\theta_{2,j})\boldsymbol{U}(m_{2,j}^2)\\&\boldsymbol{M}(\theta_{1,j})\boldsymbol{U}(m_{1,j}^2)|p_j\rangle_0\end{aligned}\tag{11}$$

由式(3)可知，通用酉算子$\boldsymbol{U}$与拉格朗日酉算子$\boldsymbol{M}$满足交换性质，因此式(11)可改写为

$$|p_j\rangle_l=\boldsymbol{U}\left(\sum_{i=1}^{l}m_{i,j}^2\right)\boldsymbol{M}\left(\frac{\pi}{d}\sum_{i=1}^{l}m_{i,j'}\right)|p_j\rangle_0\tag{12}$$

其中，$j'=1+((b+j-1)\mathrm{mod}n)$。由于$|p_j\rangle_0=M(\omega_j)|p_j\rangle_S$，混淆角度$\omega_j=\pi(2d-A_{j'})/d$，其中$A_{j'}=\sum_{i=1}^{l}m_{i,j'}(\mathrm{mod}2d)$，那么式(12)可改写为

$$\begin{aligned}|p_j\rangle_l=&\boldsymbol{U}\left(\sum_{i=1}^{l}m_{i,j}^2\right)\\&\cdot\boldsymbol{M}\left(\frac{\pi}{d}\left(\sum_{i=1}^{l}m_{i,j'}-A_{j'}\right)\right)|p_j\rangle_S\\=&\boldsymbol{U}\left(\sum_{i=1}^{l}m_{i,j}^2\right)|p_j\rangle_S\end{aligned}\tag{13}$$

当Bob_l对序列$\boldsymbol{Q}_S$中的粒子$|q_j\rangle_S(j=(1,2,\cdots,n))$执行$\boldsymbol{O}^{E_j}$操作之后，粒子对$|p_j\rangle_l\otimes|q_j\rangle_S$演变为

$$|p_j\rangle_l\otimes|q_j\rangle_l=\boldsymbol{U}\left(\sum_{i=1}^{l}m_{i,j}^2\right)|p_j\rangle_S\otimes\boldsymbol{O}^{E_j}|q_j\rangle_S\tag{14}$$

由式(1)可知，参与者份额向量中的元素的平方之和等于秘密值平方，即${T_j}^2=\sum_{i=1}^{l} m_{i,j}^2$。由于$E_j=\sum_{i=1}^{l} m_{i,j}^2 (\mathrm{mod}2)$，粒子对$|p_j\rangle_l \otimes |q_j\rangle_l$等于$\boldsymbol{U}(T_j^2)\otimes \boldsymbol{O}^{T_j^2}|p_j,q_j\rangle_S$。在$\boldsymbol{F}$变换中，若Alice制备的粒子对$|p_j,q_j\rangle_S (j\in\{1,2,\cdots,n\})$属于$\{|\phi_0^+\rangle,|\phi_0^-\rangle\}$，由式(7)可知，粒子对$|p_j,q_j\rangle_l$属于$\{|\phi_{T_j^2}^+\rangle,|\phi_{T_j^2}^-\rangle\}$；若粒子对$|p_j,q_j\rangle_S$为$|\psi_0^+\rangle$，由定理1可知，对$|p_j,q_j\rangle_l$执行$(\boldsymbol{F}\otimes\boldsymbol{F}^\dagger \boldsymbol{U}(d-1))$变换后，$|p_j,q_j\rangle_l$演变成$|\phi_{T_j^2}^+\rangle$。当$\mathrm{Bob}_l$对序列$\{P',Q'\}$执行OPB基测量，根据编码规则$|\phi_{T_j^2}^\pm\rangle\to T_j^2$，$\mathrm{Bob}_l$的测量结果为$\{R_j=T_j^2|j=1,2,\cdots,n\}$。在测量结果验证阶段，对于每一个测量结果$R_j(j=1,2,\cdots,n)$，$\mathrm{Bob}_l$根据$r^2\equiv R_j(\mathrm{mod}d)$计算$R_j$的平方根$\boldsymbol{r}_j=(r_{j,1},r_{j,2},r_{j,3},r_{j,4})$，等价于计算$\{r^2\equiv R_j(\mathrm{mod}d_1),r^2\equiv R_j(\mathrm{mod}d_2)\}$，然后随机选取元素$r_{j,\tau}(\tau\in\{1,2,3,4\})$计算$H_j=H(\mathrm{ID}_l||r_{j,\tau}\times m_{l,j})$发送给Alice。由于$R_j=T_j^2$，Alice计算出$T_j^2$的平方根$\boldsymbol{t}_j=(t_{j,1},t_{j,2},t_{j,3},t_{j,4})$与$\boldsymbol{r}_j$相同，其中元素$t_{j,\tau}=r_{j,\tau}$，使得$H'_{j,\tau}=H(\mathrm{ID}_l||t_{j,\tau}\times m_{l,j})$与$\mathrm{Bob}_l$的$H_j$相等，那么Alice认为测量结果$R_j$是正确的。如果$R_1,R_2,\cdots,R_n$都是正确的，那么Alice将每一个秘密$T_j(j=1,2,\cdots,n)$在$\boldsymbol{t}_j$中序号$I_j$作为标识信息发送给$\mathrm{Bob}_l$，然后$\mathrm{Bob}_l$在$\boldsymbol{r}_j$中选取$r_{j,I_j}$作为秘密值$T_j$。最后，$\mathrm{Bob}_l$得到序列$\{T_j=r_{j,I_j}|j=1,2,\cdots,n\}$并将其在所有参与者之间共享。 证毕

5 安全性分析

5.1 抗共享秘密的泄露攻击

在测量结果验证阶段，对于验证者Bob_l的每一个测量结果$R_j(j=1,2,\cdots,n)$，Bob_l从R_j的4个平方根$r_{j,1},r_{j,2},r_{j,3},r_{j,4}$中随机选取元素$r_{j,\tau}(\tau\in\{1,2,3,4\})$，计算$H_j=H(\mathrm{ID}_l||r_{j,\tau}\times m_{l,j})$并通过经典信道将其发送给Alice。假设外部攻击者Eve截获了哈希值H_j，并想从H_j中获取有效信息。如果Eve使用碰撞攻击推测出$\mathrm{ID}_l||r_{j,\tau}\times m_{l,j}$，虽然$\mathrm{ID}_l$是公开信息，但Eve并不知道$\mathrm{Bob}_l$的隐私份额向量$\boldsymbol{m}_l$，且$r_{j,\tau}$对于她而言是未知的，那么Eve从碰撞攻击中不能获取到任何有用的信息。

5.2 抗截获-重放攻击性

假设存在一个攻击者Eve，具有仅仅受限于量子力学原理的强大的计算能力，并且可以截获量子信道的粒子或重放伪造的粒子，并试图从截获的粒子中获得有效的信息。在秘密重构阶段，假设Eve截获了从Alice或$\mathrm{Bob}_i(i\in\{1,2,\cdots,l-1\})$传输给下一个参与者的序列$\bar{P}_i$，并试图传输伪造序列$\bar{P}_i^*$给下一个参与者以逃过Alice或$\mathrm{Bob}_i$对量子信道的窃听检测。因为序列$\bar{P}_i$中包含$v$个诱骗粒子对，且这些诱骗粒子对是局域不可完美区分的，如果Eve想要正确测量出这些诱骗粒子对的量子态，前提是她知道每个诱骗粒子对在$\bar{P}_i$中的位置并且使用正确的OPB基测量，然而Eve对诱骗粒子对的位置是未知的。如果Eve从截获的粒子中随机选择一个粒子，这个粒子是诱骗粒子的概率是$2v/(n+2v)$，从剩下的诱骗粒子中找到与之配对粒子的概率为$1/(2v-1)$，那么这一诱骗粒子对被成功找出的概率为$(\frac{2v}{n+2v})^2\cdot\frac{1}{2v-1}$。对于$v$个诱骗粒子对，那么Eve错误地找出这些诱骗粒子对的概率为$P_\mathrm{e}=1-(\frac{2v}{n+2v})^{2v}\cdot(\prod_{i=1}^{v}2i-1)^{-1}$。若诱骗粒子对数目$v$越来越大，$P_\mathrm{e}$接近于1，Eve使用OPB基测量诱骗粒子引入错误的概率接近于1，那么伪造的序列$\bar{P}_i^*$与原序列$\bar{P}_i$不同的概率接近于1，Bob_{i+1}在3.3节步骤3中能检测到该错误。因此，本方案能抵抗截获-重放攻击。

5.3 抗纠缠-测量攻击性

在纠缠-测量攻击中，攻击者Eve截获分发者Alice或参与者Bob_i传输的序列$\bar{P}_i(i=0,1,\cdots,l-1)$中的粒子，执行酉操作$\boldsymbol{U}_\mathrm{E}$将自己制备的附加粒子$|\psi\rangle$与截获的粒子纠缠起来，并试图通过测量附加粒子获取有效信息。为了不失一般性，假设酉操作$\boldsymbol{U}_\mathrm{E}$满足式(15)

$$\boldsymbol{U}_E(|k\rangle|\psi\rangle)=\sum_{m=0}^{d-1}a_{k,m}|m\rangle|E_{k,m}\rangle \tag{15}$$

其中，$k=0,1,\cdots,d-1$；$\{|E_{k,m}\rangle|m=0,1,\cdots,d-1\}$是一组正交基；$\sum_{m=0}^{d-1}|a_{k,m}|^2=1$。序列$\bar{P}_i$中诱骗粒子属于两组正交基：$\{\eta_t^\pm=|t\pm(t+1)\rangle,\eta_{d-1}=|d-1\rangle|t=0,2,\cdots,d-3\}$，$\{\sigma_0=|0\rangle,\sigma_t^\pm=|t\pm(t+1)\rangle|t=1,3,\cdots,d-2\}$，那么以诱骗态$\eta_t^+=|t+(t+1)\rangle$为例，Eve对其执行酉变换$\boldsymbol{U}_\mathrm{E}$将得到

$$\begin{aligned}
&U_E\left(|t+(t+1)\rangle|\psi\rangle\right)\\
&=\frac{1}{\sqrt{2}}\sum_{m=0}^{d-1}|m\rangle(a_{t,m}|E_{t,m}\rangle+a_{t+1,m}|E_{t+1,m}\rangle)\\
&=\frac{1}{2}\left((\eta_0^++\eta_0^-)(a_{t,0}|E_{t,0}\rangle+a_{t+1,0}|E_{t+1,0}\rangle)+\cdots\right.\\
&\quad+(\eta_t^++\eta_t^-)(a_{t,t}|E_{t,t}\rangle+a_{t+1,t}|E_{t+1,t}\rangle)\\
&\quad+(\eta_t^+-\eta_t^-)(a_{t,t+1}|E_{t,t+1}\rangle+a_{t+1,t+1}|E_{t+1,t+1}\rangle)\\
&\quad+\cdots+|d-1\rangle(a_{t,d-1}|E_{t,d-1}\rangle\\
&\quad\left.+a_{t+1,d-1}|E_{t+1,d-1}\rangle)\right)
\end{aligned} \tag{16}$$

因此，Alice或参与者对式(16)中的诱骗粒子执行测量得到η_t^+的概率为$\frac{1}{2}(a_{t,t}^2+a_{t,t+1}^2+a_{t+1,t}^2+a_{t+1,t+1}^2)$。事实上，如果Eve想要避开Alice或参与

者对序列$\bar{P}_i$中粒子的安全检测，诱骗粒子的测量结果应只为η_t^+。当且仅当$(a_{t,t}|E_{t,t}\rangle+a_{t+1,t}|E_{t+1,t}\rangle)=(a_{t+1,t+1}|E_{t+1,t+1}\rangle+a_{t,t+1}|E_{t,t+1}\rangle)$，且$a_{t,t}=0(1)$，$a_{t,t+1}=1(0)$；$a_{t+1,t}=0(1)$，$a_{t+1,t+1}=1(0)$时，该诱骗粒子的测量结果为$\eta_t^+$，此时诱骗粒子和附加粒子组成的复合量子系统为

$$\boldsymbol{U}_{\mathrm{E}}\left(|t+(t+1)\rangle|\psi\rangle\right)=\left(\eta_t^+\otimes(a_{t,t}|E_{t,t}\rangle+a_{t+1,t}|E_{t+1,t}\rangle)\right)\tag{17}$$

由式(17)可知，诱骗粒子与附加粒子并没有发生纠缠，因此当Eve测量附加粒子时，不能获得任何有用的信息。类似的，对于属于正交基$\{\sigma_0=|0\rangle,\sigma_t^+=|t\pm(t+1)\rangle|t=1,3,\cdots,d-2\}$的诱骗粒子，Eve也执行酉操作$\boldsymbol{U}_{\mathrm{E}}$将制备的附加粒子$|\psi\rangle$与此诱骗粒子纠缠起来，如果Eve想要避开窃听检测，根据诱骗粒子只能出现的测量结果，附加粒子与诱骗粒子并不会产生纠缠关系，同理可证明，此时Eve也不能获取任何有用的信息。因此，本方案可以抵抗纠缠-测量攻击。

5.4 抗欺骗攻击性

在秘密重构阶段，假设不诚实参与者Bob_r $(r\in\{1,2,\cdots,l-1\})$在对序列P_{r-1}中粒子$|p_j\rangle_{r-1}$ $(j=1,2,\cdots,n)$执行$\boldsymbol{U}(m_{r,j}^2)$和$M(\theta_{r,j})$的过程中，使用虚假值$\tilde{m}_{r,j}(j\in\{1,2,\cdots,n\})$替换真实的份额值$m_{r,j}$，其他参与者都诚实地执行3.3节步骤4，$\mathrm{Bob}_l$执行完步骤5后，序列$\{Q_l,P_l\}$中第$j$和$k(=1+(j-b-1(\mathrm{mod}n)))$个粒子对演变成

$$|p_j\rangle_l\otimes|q_j\rangle_l=\boldsymbol{U}(\tilde{m}_{r,j}^2-m_{r,j}^2)\boldsymbol{U}(T_j^2)\otimes\boldsymbol{O}^{T_j^2(\mathrm{mod}2)}(|p_j\rangle_S\otimes|q_j\rangle_S)\tag{18}$$

$$|p_k\rangle_l\otimes|q_k\rangle_l=M\left(\frac{\pi}{d}(\tilde{m}_{r,j}-m_{r,j})\right)\boldsymbol{U}(T_k^2)\otimes\boldsymbol{O}^{T_k^2(\mathrm{mod}2)}(|p_k\rangle_S\otimes|q_k\rangle_S)\tag{19}$$

由式(7)和定理1可知，当且仅当$\tilde{m}_{r,j}^2\equiv m_{r,j}^2(\mathrm{mod}2)$时，对$|p_j\rangle_l\otimes|q_j\rangle_l$执行F变换后，得到的量子态$|p_j\rangle'\otimes|q_j\rangle'$属于OPB基，$\mathrm{Bob}_l$的测量结果$R_j{}^*$等于$T_j^2-m_{r,j}^2+\tilde{m}_{r,j}^2$；否则，$|p_j\rangle'\otimes|q_j\rangle'$将不能使用OPB基测量完美区分，测量结果$R_j{}^*$不可确定。对于第$\boldsymbol{k}$个粒子对，酉变换$M(\frac{\pi}{d}(\tilde{m}_{r,j}-m_{r,j}))$将不可避免地引入错误，导致测量结果$R_k{}^*$与$T_k^2$不相等。在测量结果验证阶段，以$R_j{}^*$的验证过程为例，如果$R_j{}^*$不是$\mathrm{GF}(d)$中的平方剩余数，那么$\mathrm{Bob}_l$放弃本轮秘密共享；如果$R_j{}^*$正好是平方剩余数，但由于$R_j{}^*\neq T_j^2$，那么$\mathrm{Bob}_l$计算$R_j^*$的平方根向量$\boldsymbol{r}_j^*$与Alice计算$T_j^2$的平方根向量$\boldsymbol{t}_j$并不相同，则Alice认为测量结果$R_j{}^*$是不正确的。同理，Alice也认为测量结果$R_k^*$不正确。因此，$\mathrm{Bob}_r$使用一个伪造的份额值替换真实的份额值，导致两个测量结果产生错误，本轮秘密共享失败。最终，Bob_r从本次攻击中不会获得任何有用的信息。

5.5 抗合谋攻击性

合谋攻击是指存在多个不诚实参与者联合起来想获取其他诚实参与者的份额值，目的是不需要这些诚实参与者参与就能恢复出秘密值。对于合谋攻击，本节考虑以下两种假设。

假设1　$\mathrm{Bob}_{i-1}(i\in\{2,3,\cdots,l-2\})$和$\mathrm{Bob}_{i+1}$的合谋攻击。

由于OPB态的单个粒子在Z基下是不可区分的，因此本节考虑Bob_{i-1}从Z基$\{|u\rangle\}_0^{d-1}$中选取一个伪造序列$W_D=\{|w\rangle_1,|w\rangle_2,\cdots,|w\rangle_n\}$替换原有的序列$P_{i-1}$，并将其发送给$\mathrm{Bob}_i$来实施合谋攻击。$\mathrm{Bob}_i$收到序列$W_D$后，根据份额向量$\boldsymbol{m}_i=(m_{i,1},m_{i,2},\cdots,m_{i,n})$对$|w\rangle_j(j=1,2,\cdots,n)$执行酉变换$\boldsymbol{U}(m_{i,j}^2)$和$\boldsymbol{M}(\theta_{i,j})$得到$|w\rangle_j'$，参数$\theta_{i,j}=\pi m_{i,j'}/d$，$j'=1+((b+j-1)\mathrm{mod}n)$，然后将$|w\rangle_j'$发送给$\mathrm{Bob}_{i+1}$。接着，对于第$j$个粒子$|w\rangle_j'=\boldsymbol{M}(\pi m_{i,j'}/d)\boldsymbol{U}(m_{i,j}^2)|w\rangle_j$，$\mathrm{Bob}_{i+1}$在$\mathrm{GF}(d)$上以相等概率猜测$m_{i,j'}$。如果以$1/\boldsymbol{d}$的概率猜测正确，那么他对$|w\rangle_j'$执行$\boldsymbol{M}(\pi(2d-m_{i,j'})/d)$得到$U(m_{i,j}^2)|w\rangle_j$，并通过$\boldsymbol{Z}$基测量得到$m_{i,j}^2$。由于$m_{i,j}^2$对应4个不同的平方根，那么$\mathrm{Bob}_{i+1}$窃取到$m_{i,j}$的概率为1/4。假设$\mathrm{Bob}_{i+1}$获得份额值$m_{i,j}$，那么他对粒子$|w\rangle_k'(k=1+((j-b-1)\mathrm{mod}n))$执行酉变换$M(-m_{i,j}\pi/d)$，并测量酉变换后的粒子得到$m_{i,k}^2$。$\mathrm{Bob}_{i+1}$从$m_{i,k}^2$正确推测出$m_{i,k}$的概率为1/4。依次类推，$\mathrm{Bob}_{i+1}$测量序列$W'$得到正确结果的概率为$1/(4^{n-1}\cdot d)$。当序列$\boldsymbol{m}_i$的长度$n\geq 6$时，$\mathrm{Bob}_{i+1}$得到错误结果的概率接近于1。因此，$\mathrm{Bob}_{i-1}$与$\mathrm{Bob}_{i+1}$的本次合谋攻击将会失败。

假设2　Bob_1和Bob_l的合谋攻击。

在本方案中，验证者Bob_l是半诚实的，他除了执行预定的方案流程，也可能联合其他参与者发起合谋攻击。如果Bob_1将Alice发来的序列P_0保留，并伪造一个新的序列$\tilde{P}_0$代替P_0在其他参与者之间顺序传输，最后Bob_l将Alice告知的粒子对$|p_j,q_j\rangle_S$ $(j=1,2,\cdots,n)$制备时初态告诉Bob_1，Bob_1可以选择相应的测量基测量序列P_0中粒子，并试图推测出Alice的序列$\boldsymbol{A}$。假设$|p_j\rangle_0=\boldsymbol{M}(\pi(2d-A_{j'})/d)|0\rangle$，$j'=1+((j+b-1)\mathrm{mod}n)$，它可能是量子态集合$\{\rho_t=M(\pi t/d)|0\rangle|t=0,1,\cdots,2d-1\}$中的任意一个，该集合中的元素两两是非正交的，内积$|\langle\rho_t|\rho_{t+1}\rangle|^2=((1-\mathrm{e}^{(2d-1)\pi/d})/((1-\mathrm{e}^{\pi/d})d))^2\neq 0$，那么角度$\pi(2d-A_{j'})/d$不能准确地通过$Z$基测量得到。同理，当$|p_j\rangle_0=\boldsymbol{M}(\pi(2d-A_{j'})/d)|0\pm 1\rangle$时，

西算子$\boldsymbol{M}$的旋转角度也不能准确地被测量出。因此，Bob_1的本次测量将不可避免地引入错误，测量结果A^*与序列A不同。在最差的情况下，可能有其他$l-2$个不诚实参与者配合他合谋，根据A^*推测诚实参与者$\mathrm{Bob}_t(t\in\{2,3,\cdots,l-1\})$的份额向量$\boldsymbol{m}_t$，此时他们也得不到$\boldsymbol{m}_t$的全部信息。因此，本方案可以抵抗该合谋攻击。

5.6 抗光学器件的非理想特性攻击

以上理论安全分析是建立在量子态制备和测量是完美的前提假设，现有的光学器件中存在不满足理论安全的非理想特性。针对实际系统中的弱相干光源引起的光子数分流攻击，本方案使用与信息粒子具有不可区分性的OPB粒子作为诱骗态，这些诱骗态的平均光子数与信息粒子的平均光子数不同，通信双方在对量子信道的安全检测中，通过比较诱骗态的响应比脉冲可以判断是否存在光子数分流攻击。在量子信道中，攻击者Eve可能发起的两种特洛伊木马攻击：不可见光子攻击和延迟光子攻击。针对不可见光子攻击，本方案中每个参与者可以在接收量子态序列之前添加滤波器，只允许接近合法波长的光子通过，这样不可见光子就会被过滤掉。针对延迟光子攻击，本方案中参与者在接收到通过滤波器的粒子序列之后，可以选取部分光子进行多光子率检测，通过观察多光子率是否超出阈值达到检测延迟光子攻击行为的目的。

6 性能分析

本节首先将本文方案与其他OPB态QSS方案(文献[7,13])从信息粒子类型、粒子数量、计算消耗等5个方面进行比较，比较结果如表1所示。为了便于比较，这里规定各方案的属性，l是多方参与者的人数，本方案每次共享1个d进制秘密，文献[7,13]中共享长度为$m=\left\lceil\log_2^d\right\rceil$的二进制秘密序列。

从表1可以得出，文献[7]是基于3维OPB态的两方QSS方案，参与者人数受到正交乘积态中粒子数量限制，在拓展至更高维量子系统以及多个参与者的秘密共享场景下存在较大局限性；文献[13]使用2维多粒子OPB态拓展了参与者的人数，每个参与者都拥有1个OPB态，量子资源开销较大。本方案使用d维OPB态拓展了正交乘积态QSS方案的量子维度，参与者人数可以动态调整，并且降低了参与者人数拓展时产生的量子资源开销，具有更好的灵活性和通用性。

其次，本节将本文方案与其他动态QSS方案(文献[16,18,21])主要从抗截获-重放攻击性、抗纠缠-测量攻击性、抗合谋攻击性等5个方面进行比较和分析，比较结果如表2所示。在表2中，文献[18,21]和提出的方案能抵抗截获-重放攻击；在文献[17]指出，文献[16]中只需要两个参与者就能获取到分发者的秘密，因此不能抵抗合谋攻击；与其他相似方案相比，只有文献[18]和本方案考虑了内部参与者参与欺骗的安全问题，文献[18]中分发者将秘密S的哈希值$H(S)$编码在Bell态粒子中并发送给最后一个参与者，如果存在不诚实参与者Bob_m使用虚假值R'_m代替真实份额值R_m参与秘密重构，最后一个参与者测量粒子得到$u_1=S+(R'_m-R_m)+\sum_{r\in B}\theta_r$和$u_2=H(S)+(R'_m-R_m)+\sum_{r\in B}\theta_r$，并将$u_1$和$u_2$在参与者之间公布，此时$\mathrm{Bob}_m$计算

表 1 相似方案的性能比较

属性	文献[7]	文献[13]	本文方案
信息粒子类型	3维OPB态	2维OPB态	d维OPB态
粒子数量	m	$2^{m-1}\cdot l$	$2m$
计算消耗	$m(\mathrm{QFT}+\mathrm{IQFT})/2$	–	$l\cdot\boldsymbol{U}+(l+1)\boldsymbol{M}+\boldsymbol{O}+1/3(\boldsymbol{F}+\boldsymbol{F}^\dagger+\boldsymbol{U})$
参与者人数	两方固定	多方固定	多方动态
测量消耗	m次单粒子测量	l次OPB测量	1次OPB测量

表 2 相似动态QSS方案的安全性比较

安全性	文献[16]	文献[18]	文献[21]	本文方案
抗截获-重放攻击性	–	√	√	√
抗纠缠-测量攻击性	√	√	√	√
抗合谋攻击性	–	√	√	√
抗欺骗攻击	–	√	–	√
抗共享秘密的泄露攻击	–	–	–	√

$u_2-u_1=H(S)-S$，其中$\{H(S),S\}\in \mathrm{GF}(d)$。在安全性不依赖于$d$是大整数的情况下，$\mathrm{Bob}_m$使用穷举攻击能以一定概率推测出秘密值，那么该验证过程会泄露秘密值；本方案在粒子测量阶段得到秘密的平方剩余，由于平方剩余与其平方根是一对多映射，随机选取一个平方根实现对平方剩余的验证，验证过程中不会泄露有效信息，防止了秘密值的泄露。从分析可知，与其他相似方案相比，本方案的安全性能最优。

7　结束语

本文提出基于非局域性正交乘积态的动态量子秘密共享方案。本文使用非局域性OPB态携带信息，并借鉴Rabin密码思想设计验证机制，保证了秘密共享和验证过程具有较好的安全性。相对于现有基于OPB态QSS方案，本方案拓展了量子空间的维度，并且参与者人数动态增减，具有更好的灵活性和通用性；与相似的动态QSS方案相比，本方案具有更好的安全性。下一步工作是使用新的非局域性正交乘积态，进一步降低基于正交乘积态的QSS方案的量子资源开销。

参 考 文 献

[1] HILLERY M, BUŽEK V, and BERTHIAUME A. Quantum secret sharing[J]. *Physical Review A*, 1999, 59(3): 1829–1834. doi: 10.1103/PhysRevA.59.1829.

[2] KARLSSON A, KOASHI M, and IMOTO N. Quantum entanglement for secret sharing and secret splitting[J]. *Physical Review A*, 1999, 59(1): 162–168. doi: 10.1103/PhysRevA.59.162.

[3] 杜宇韬, 鲍皖苏, 李坦. 基于秘密认证的可验证量子秘密共享协议[J]. 电子与信息学报, 2021, 43(1): 212–217. doi: 10.11999/JEIT190901.

DU Yutao, BAO Wansu, and LI Tan. Verifiable quantum secret sharing protocol based on secret authentication[J]. *Journal of Electronics & Information Technology*, 2021, 43(1): 212–217. doi: 10.11999/JEIT190901.

[4] BAI Chenming, ZHANG Sujuan, and LIU Lu. Verifiable quantum secret sharing scheme using d-dimensional GHZ state[J]. *International Journal of Theoretical Physics*, 2021, 60(10): 3993–4005. doi: 10.1007/s10773-021-04955-1.

[5] HSU L Y and LI Cheming. Quantum secret sharing using product states[J]. *Physical Review A*, 2005, 71(2): 022321. doi: 10.1103/PhysRev.A.71.022321.

[6] YANG Yuguang, WEN Qiaoyun, and ZHU Fuchen. An efficient quantum secret sharing protocol with orthogonal product states[J]. *Science in China Series G:Physics, Mechanics and Astronomy*, 2007, 50(3): 331–338. doi: 10.1007/s11433-007-0028-8.

[7] XU Juan and YUAN Jiabing. Improvement and extension of quantum secret sharing using orthogonal product states[J]. *International Journal of Quantum Information*, 2014, 12(1): 1450008. doi: 10.1142/S0219749914500087.

[8] BENNETT C H, DIVINCENZO D P, MOR T, *et al*. Unextendible product bases and bound entanglement[J]. *Physical Review Letters*, 1999, 82(26): 5385–5388. doi: 10.1103/PhysRevLett.82.5385.

[9] WALGATE J and HARDY L. Nonlocality, asymmetry, and distinguishing bipartite states[J]. *Physical Review Letters*, 2002, 89(14): 147901. doi: 10.1103/PhysRevLett.89.147901.

[10] ZHEN Xiaofan, FEI Shaoming, and ZUO Huijuan. Nonlocality without entanglement in general multipartite quantum systems[J]. *Physical Review A*, 2022, 106(6): 062432. doi: 10.1103/PhysRevA.106.062432.

[11] XU Guangbao and JIANG Donghuan. Novel methods to construct nonlocal sets of orthogonal product states in an arbitrary bipartite high-dimensional system[J]. *Quantum Information Processing*, 2021, 20(4): 128. doi: 10.1007/s11128-021-03062-8.

[12] JIANG Donghuan, YUAN Fei, and XU Guangbao. Novel quantum group signature scheme based on orthogonal product states[J]. *Modern Physics Letters B*, 2021, 35(26): 2150418. doi: 10.1142/S0217984921504182.

[13] FU Sijia, ZHANG Kejia, ZHANG Long, *et al*. A new non-entangled quantum secret sharing protocol among different nodes in further quantum networks[J]. *Frontiers in Physics*, 2022, 10: 1021113. doi: 10.3389/fphy.2022.1021113.

[14] HSU J L, CHONG Songkong, HWANG T, *et al*. Dynamic quantum secret sharing[J]. *Quantum Information Processing*, 2013, 12(1): 331–344. doi: 10.1007/s11128-012-0380-0.

[15] WANG Tianying and LI Yanping. Cryptanalysis of dynamic quantum secret sharing[J]. *Quantum Information Processing*, 2013, 12(5): 1991–1997. doi: 10.1007/s11128-012-0508-2.

[16] DU Yutao and BAO Wansu. Dynamic quantum secret sharing protocol based on two-particle transform of Bell states[J]. *Chinese Physics B*, 2018, 27(8): 080304. doi: 10.1088/1674-1056/27/8/080304.

[17] GAO Gan, WEI Changcheng, and WANG Dong. Cryptanalysis and improvement of dynamic quantum secret sharing protocol based on two-particle transform of Bell

states[J]. *Quantum Information Processing*, 2019, 18(6): 186. doi: 10.1007/s11128-019-2301-y.

[18] LI Fulin, CHEN Tingyan, and ZHU Shixin. Dynamic (t, n) threshold quantum secret sharing based on d-dimensional Bell state[J]. *Physica A:Statistical Mechanics and its Applications*, 2022, 606: 128122. doi: 10.1016/j.physa.2022.128122.

[19] SMALL C. A simple proof of the four-squares theorem[J]. *The American Mathematical Monthly*, 1982, 89(1): 59–61. doi: 10.1080/00029890.1982.11995381.

[20] DE VOS A and DE BAERDEMACKER S. From reversible computation to quantum computation by Lagrange interpolation[EB/OL]. http://arXiv.org/abs/1502.00819, 2015.

[21] YANG Chunwei and TSAI C W. Efficient and secure dynamic quantum secret sharing protocol based on bell states[J]. *Quantum Information Processing*, 2020, 19(5): 162. doi: 10.1007/s11128-020-02662-0.

宋秀丽：女，博士，副教授，研究方向为量子密码学、量子保密通信、云计算安全和车联网安全.

李　闯：男，硕士生，研究方向为量子密码学.

责任编辑：余　蓉