基于正交乘积态的多方量子秘密共享协议

陈云 李璇冰 李帅†

(宁夏大学信息工程学院, 银川 750021)

(2025 年 3 月 27 日收到; 2025 年 6 月 27 日收到修改稿)

量子秘密共享是一种通过使用量子力学的基本原理, 实现在多个参与者之间安全分配和重建秘密信息的密码学协议. 本文提出了一种可验证的多方量子秘密共享协议, 该协议中存在一个具有验证能力的秘密分发者和多个接收方. 在协议执行过程中, 秘密分发者会通过设定的编码规则将欲共享的信息用对应的正交乘积态表示, 并将量子态进行分割发送给各个接收方, 只有各接收方共同合作才能最终恢复初始秘密信息. 同时, 考虑到在协议过程中可能存在参与者人数变化的情况, 加入了人员动态变化操作. 通过对协议的安全性分析, 证明了该协议可以抵抗常见的内部和外部攻击. 我们希望该思想能够对量子秘密共享的进一步研究产生积极的影响.

关键词: 量子秘密共享, 可验证的, 正交乘积态, 动态变化

PACS: 03.65.Aa, 03.67.Ac, 03.67.Dd **DOI:** 10.7498/aps.74.20250394

CSTR: 32037.14.aps.74.20250394

1 引 言

随着数字化进程的深入演进, 信息安全已成为现代数字文明存续的核心基石. 以公钥密码体系[1]和对称密钥机制[2–4]为代表的传统加密技术虽然构筑了现代信息安全的基础架构, 但其依赖的安全基石正遭受量子计算的严峻挑战. 特别是 Shor 算法[5]对整数分解问题的有效求解, 以及 Grover 算法[6]在搜索加速方面的突破, 使得依托数学难题复杂度的经典密码体系面临被量子算力瓦解的实质性威胁. 在此背景下, 量子密码学这种依赖于量子叠加态、不可克隆定理等物理定律的新型密码范式, 展现出突破传统安全框架的理论优势, 为后量子时代的保密通信提供了革命性的技术方案. 之后, 该领域涌现出量子密钥分发 (quantum key distribution, QKD)[7,8]、受控量子隐形传态[9–11]、量子安全直接通信 (quantum secure direct communication, QSDC)[12,13] 等重要突破, 这些技术方案均可在量子网络架构中实现. 其独特优势在于: 通过将安全性锚定于量子力学基本原理, 从根本上规避了量子计算攻击的威胁. 其中, 基于量子特性的秘密共享协议设计已成为量子密码学研究的重点方向之一.

量子秘密共享 (quantum secret sharing, QSS) 作为经典秘密共享的量子化延伸[14–16], 是构建分布式量子安全体系的关键基础性协议. 该协议通过量子态制备与测量技术, 将原始秘密信息编码为量子叠加态或纠缠态资源, 并基于多方协同的量子操作实现秘密的分布式存储与授权重构. 其核心机制可解构为两个阶段: 首先通过量子态分割编码将秘密信息分解为若干量子份额 (quantum shares), 分发给网络中的参与者; 仅当授权子集 (如满足预设门限条件的参与者群组) 通过量子态联合操作完成解码时, 原始信息才能实现确定性重构. 相较于经典密码学方案, QSS 不仅通过量子不可克隆定理保障了信息传输的物理安全性, 更利用量子态测量的扰动特性实现了对信息泄露与篡改行为的主动防御, 这一特性使其成为量子安全多方计算领

† 通信作者. E-mail: lis@nxu.edu.cn

域的核心支撑技术. 该领域具有里程碑意义的研究始于 Hillery 等[17] 于 1999 年提出的首个 QSS 协议. 该协议利用三粒子 GHZ 态 (Greenberger-Horne-Zeilinger 态) 的量子纠缠特性, 将秘密量子信息分割为两个关联份额, 通过设计“非完全重构”机制确保任何单一参与者均无法独立提取有效信息, 仅在所有参与者协作时方可实现秘密的完整恢复. Karlsson 等[18] 在此基础上取得重要突破, 他们基于双粒子 Bell 态构建的新型协议不仅验证了多粒子纠缠态在秘密分割中的普适性, 更创新性地提出了基于纠缠交换的量子比特转移机制, 成功将基础方案拓展至 m-out-of-n 门限型协议, 提高了协议的灵活性. Xiao 等[19] 为了解决多方之间秘密共享的局限性, 在 2004 年将 Hillery 的协议进行了推广, 实现了任意多方之间的秘密共享, 并且根据 n–1 个参与方的测量结果所形成的字符串的奇偶性给出了共享秘密信息的显式表达式. 2007 年, Yang 等[20] 提出了一种在 $3\otimes 3$ Hilbert 空间中具有正交乘积态的高效量子秘密共享协议, 正交产物状态的粒子形成两个粒子序列, 一个序列被发送给 Bob, 另一个序列在重新排列粒子顺序后被发送给 Charlie. 在 Alice 的帮助下, Bob 和 Charlie 进行了相应的局部测量, 以获得准备好的正交乘积状态的信息. Wang 等[21] 在 2008 年提出了一种基于单光子和局部酉运算的经典消息多方量子秘密共享方案, 在该方案中, 窃听检查只执行两次, 一个光子可以生成一个比特的经典秘密消息; 此外, 只需要发送者和其中一个代理来存储光子. Wang 等[22] 在 2009 年提出了一种利用偏振化调制的双重纠缠光子对的量子秘密共享方案, 通过调节光子的极化, 对有关初始状态的秘密信息进行编码, 并与不同的成员共享光子实现秘密共享过程.

传统静态 QSS 协议受限于其静态架构设计, 难以适应网络参与者的动态变化需求. 当有参与者加入或退出协议时, 秘密分发者往往需要废弃现有量子资源并重新初始化整个协议流程, 这不仅造成量子资源浪费, 更显著提高了系统运维成本. 因此, 构建具有动态拓扑适应能力的量子秘密共享 (dynamic QSS, DQSS) 机制, 成为提升量子秘密共享协议可扩展性的关键研究方向. 该领域的理论奠基可追溯至 Jia 等[23] 的开创性工作, 其通过构建新型星团纠缠态, 首次实现了在不完全重构共享资源的前提下, 使动态调整后的代理组能够通过协同操作恢复原始秘密. 同期, Hsu 等[24] 基于 EPR (Einstein-Podolsky-Rosen) 纠缠对设计了具有纠缠交换特性的协议框架, 二者共同奠定了 DQSS 技术的理论基础与实现范式. 随后, 许多 DQSS 协议相继问世. 2018 年, Du 等[25] 提出了 Bell 状态的两粒子变换并设计了 (n, n) 阈值的新型 DQSS 协议, 具有动态参数更新的功能. 2020 年, Yang 等[26] 利用 Bell 态与 GHZ 态测量特性的协同效应, 设计了免除光子生成与局域幺正变换的轻量化方案, 仅需 X 基测量即可完成密钥影子提取. 2021 年, Hu 等[27] 通过引入高维量子系统与粒子循环传输技术, 结合局域幺正操作实现了多粒子 GHZ 态的高效制备与共享. 2024 年, Tian 等[28] 采用了 Bell 态与简化的本地幺正操作相结合, 使动态变化的多方之间的秘密可以安全的共享. 同年, Lin 等[29] 创新性地整合纠缠交换与 Bell 测量技术, 开发出支持测量前后双阶段动态调整的协议架构, 实现了代理节点的弹性增删与实时更新.

在当前量子技术发展中, 纠缠态制备技术因受限于较短的量子相干时间和较低的态保真度, 使得依赖纠缠资源的 QSS 协议难以实现实际应用. 为降低协议对纠缠资源的依赖性, 科研人员开始转向研究基于正交乘积态的新型密码学体系. 尽管这类量子态不具备量子纠缠特性, 但其展现的局部操作不可分辨性为密码协议设计提供了全新思路. 值得注意的是, Yu 等[30] 在 2015 年成功构建了一组正交乘积态, 该态集合在局部操作与经典通信 (local operations and classical communication, LOCC) 框架下无法被完美区分. 相较于传统纠缠态, 这类不可分辨的正交乘积 (locally indistinguishable orthogonal product, LIOP) 态不仅具有更易制备的物理优势, 还通过全局量子关联特性突破了局域操作的局限性. 基于 LIOP 态的特殊性质, 其在量子密码领域展现出重要应用潜力. 早在 2001 年, Guo 等[31] 便开创性地将正交乘积态应用于 QKD 协议设计. 随后在 2007 年, Yang 等[20] 基于此类态构建了 QSS 方案. 随着研究的深入, 相关应用场景持续扩展: Jiang 等[32] 于 2019 年开发了基于正交乘积态的量子投票协议, 并在 2020 年进一步拓展其应用范围, 实现了基于 LIOP 态的可信第三方电子支付协议[33]. 这些突破性研究标志着正交乘积态正在成为量子密码学领域的重要基础资源.

本文提出了一种实用的新的基于正交乘积态的可验证的多方 QSS 协议. 在协议准备阶段, 秘密拥有者会将秘密信息编码为正交乘积态, 同时, 他

会将初始状态中的粒子位置打乱, 在对各个量子态进行线性变换后将这些量子态发送给所有的参与者. 协议信息传输过程中, 当参与者接收到其他参与者发送的量子序列信息后, 会与发送方进行协商检查是否在传输过程中存在窃听, 如果存在窃听攻击就会终止协议. 只有所有的参与者一起协作, 在协议中诚实地传输量子态序列, 才可以恢复秘密. 在每个传输阶段, 最后一个接收方会与秘密拥有者对自己接收到的完整量子序列进行验证, 只有在通过秘密拥有者的验证之后, 协议才能继续执行. 协议使用 QKD 进行密钥分发, 确保参与者在通信中使用的密钥足够安全. 同时, 考虑到在协议进行过程中可能会存在参与者人数变化的问题, 设计了人员变化的动态方案, 保障协议的灵活性. 由于不可分辨的正交乘积态的性质, 即使攻击者得到了 $n-1$ ($n \geqslant 3$) 个正交乘积态的粒子, 他也无法确定共享的秘密信息.

研究的其余部分组织如下: 在第 2 节中, 我们对协议中将会使用到的正交乘积态进行介绍; 第 3 节提出了一个新的可仲裁的多方 QSS 协议; 第 4 节给出了一个例子来更好地说明我们的协议; 协议的安全性将会在第 5 节进行讨论; 第 6 节对协议进行了仿真模拟, 同时将提出的协议和其他几个 DQSS 协议进行了比较和分析; 最后, 在第 7 节对我们的研究进行简短总结.

2 相关工作

本节将介绍不可分辨正交乘积态的具体形式和属性, 其会在后面的协议过程中使用. 如果一组正交乘积态不能被 LOCC 完美区分, 我们称其为局部不可区分的[34].

协议拟通过使用一组局部不可区分的正交乘积态进行信息的编码工作. 在 $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ 量子体系中, 包含以下 $2n$ 个正交积态 (其中 $n \geqslant 3$):

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}(|0\rangle+|1\rangle)_n,$$

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}|1\rangle_1|1\rangle_2|1\rangle_3\cdots(|0\rangle+|1\rangle)_{n-1}|0\rangle_n,$$

$$\cdots$$

$$|\phi_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_1|0\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}|1\rangle_n,$$

$$|\phi_{n+1}\rangle = \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}(|0\rangle-|1\rangle)_n,$$

$$|\phi_{n+2}\rangle = \frac{1}{\sqrt{2}}|1\rangle_1|1\rangle_2|1\rangle_3\cdots(|0\rangle-|1\rangle)_{n-1}|0\rangle_n,$$

$$\cdots$$

$$|\phi_{2n}\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_1|0\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}|1\rangle_n.$$

这些状态不能完全由 LOCC 来区分. 在文献 [35,36] 中, 正交乘积态被证明了不能完全由 LOCC 区分. 而且, 这些状态具有如下的一些性质.

性质 1 量子系统的状态唯一性判定需满足完备性条件: 仅当所有正交乘积态的关联粒子被完整获取时, 方可对量子序列的精确状态进行确定性重构.

性质 2 正交乘积态具备粒子级传输解耦特征, 即各粒子可在不依赖其他分组协同性的前提下, 通过独立信道实现安全分发与物理传输.

性质 3 正交乘积态体系具有操作局部化属性: 对任意单粒子的量子态实施测量或变换时, 其操作效应仅局限于目标粒子本身, 而不会引发其他粒子的量子态坍缩或关联性改变.

在量子编码方案设计中, 选定一组正交乘积态后, 需依据其结构特性建立对应的二进制编码规则. 具体而言, 二进制编码位数 m 的确定需满足关系式 $m = \lfloor \log_2 n \rfloor + 1$, 其中 n 表示每个量子态包含的粒子数量. 例如, 当每个正交乘积态由 3 个粒子构成时 (此时正交乘积态总数为 6), 编码位数应设定为 2 bit, 对应 $2^2 = 4$ 种可能的编码结果. 剩余的 2 个正交乘积态可作为诱饵态, 用于后续量子通信中的窃听检测. 若强行采用 3 bit 编码 (需覆盖 8 种结果), 则 6 个正交乘积态无法完整表达所有编码组合, 导致信息丢失. 因此, 编码规则的设计需严格确保正交乘积态的总数至少覆盖 2^m 种编码需求, 超出部分则可通过预设为诱饵态来增强协议的安全性.

3 可仲裁的多方 QSS 协议

3.1 具体协议内容

协议以 3 个接收方为例进行介绍, 操作流程如图 1 所示, 红色标注的量子序列对应保留的序列, 蓝色标注的对应待发送的序列. 该协议涉及两方参与者, 其中一方 A 为秘密分发者, 另一方 B_i , B_{i+1} , B_{i+2} 为秘密接收者. A 会将所拥有的秘密序列分块并打乱分别发送给接收方 B_i , B_{i+1} , B_{i+2} , 只有

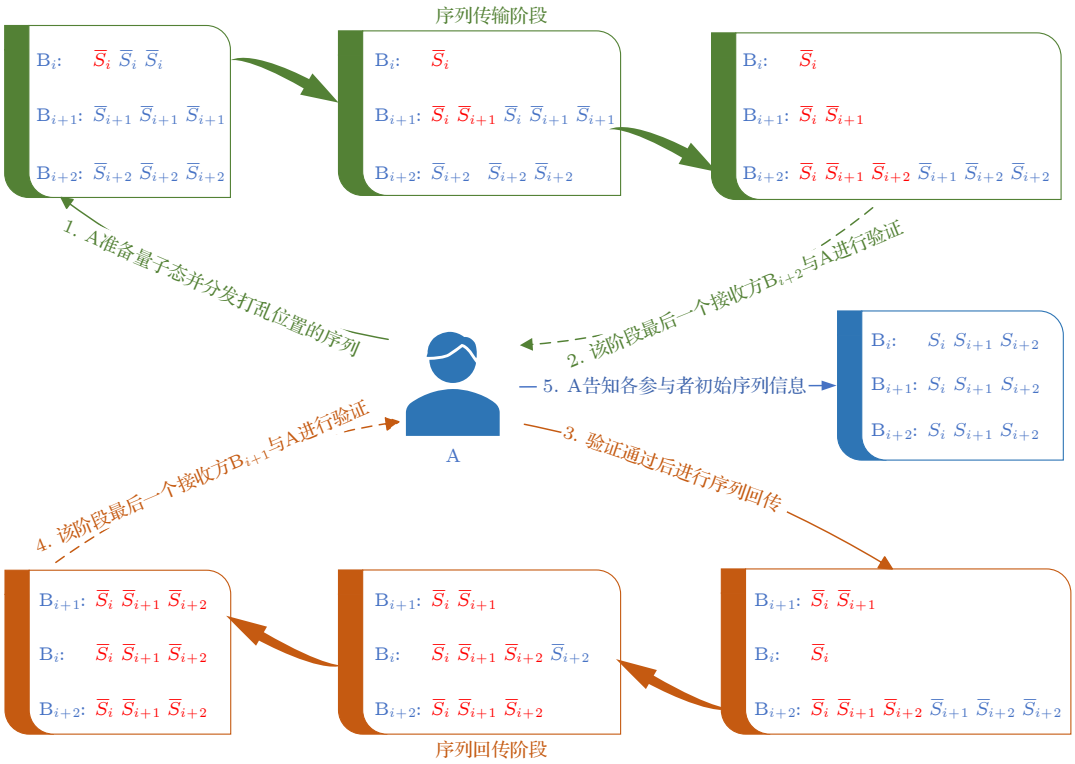

图 1 协议整体流程图. 其中红色标注的量子序列是在传输阶段参与者进行保留的序列, 蓝色标注的量子序列是在传输阶段不同参与者的传输回合中待发送的序列

Fig. 1. The overall flowchart of the protocol. The quantum sequences marked in red are the sequences that the participants retain during the transmission stage, and the quantum sequences marked in blue are the sequences to be sent in the transmission rounds of different participants during the transmission phase.

3 个接收方共同合作, 才能恢复 A 的初始秘密. 同时, 在该协议中 A 会充当一个仲裁者的身份, 用来判断在协议阶段进行的过程中是否有不诚实接收方的情况, 由于协议是基于正交乘积态的, 接收方的人数至少为 3 个人. 对于可扩展的 n 个接收方的 QSS 协议, 只需要在初始阶段准备 n 部正交乘积态并设定相应编码规则, 协议其余过程与我们以三方为例介绍的协议过程相同.

3.1.1 初始化阶段

Step 1) (秘密编码): 秘密分发者 A 将待共享的秘密 M 编码为 n 个分块, 即 $M=m_1\|m_2\|\cdots\|m_n$, 其中每个分块 m_t 从集合 $\{00,01,10,11\}$ 中选取 ($t=1,2,\cdots,n$). 每个分块 m_t 对应一个正交乘积态, 所有可能的正交乘积态表示如下:

$$|\psi_1\rangle=\frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2(|0\rangle+|1\rangle)_3,$$

$$|\psi_2\rangle=\frac{1}{\sqrt{2}}|1\rangle_1(|0\rangle+|1\rangle)_2|0\rangle_3,$$

$$|\psi_3\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_1|0\rangle_2|1\rangle_3,$$

$$|\psi_4\rangle=\frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2(|0\rangle-|1\rangle)_3,$$

$$|\psi_5\rangle=\frac{1}{\sqrt{2}}|1\rangle_1(|0\rangle-|1\rangle)_2|0\rangle_3,$$

$$|\psi_6\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_1|0\rangle_2|1\rangle_3.$$

A 根据以下编码规则 $\{00,01,10,11\}\longmapsto\{|\psi_1\rangle,|\psi_2\rangle,|\psi_3\rangle,|\psi_4\rangle\}$ 将每一个 m_t 编码为对应的量子态 $|\psi_i\rangle$ ($i=1,2,3,4$), 剩余的量子态 $|\psi_5\rangle$ 和 $|\psi_6\rangle$ 可以在序列传输的窃听检测过程中当作诱饵粒子使用.

Step 2) (密钥分发): 在秘密分发者 A 和各个接收方 B_i, B_{i+1}, B_{i+2} 之间, 通过量子密钥分发协议获得共享密钥: A 首先制备量子态, 随机选择一组二进制比特 (0 或 1) 并为每个比特选择一种编码基: 当编码基是基 1 (直线基) 时, 用光子的水平偏振表示比特 0, 垂直偏振表示比特 1; 当编码基是基 2 (对角基) 时, 用光子的 45° 偏振表示比特 0, 135° 偏振表示比特 1. 各接收方 B_i 对接收到的每

个光子随机选择测量基测量. 双方会公开对比使用的基, 保留匹配基对应的比特作为原始密钥. 在验证随机公开部分比特错误率后, 通过纠错和隐私放大生成 n 位密钥 K_{AB_i}, $K_{\mathrm{AB}_{i+1}}$, $K_{\mathrm{AB}_{i+2}}$. 对于各接收方 B_i, B_{i+1}, B_{i+2} 之间, 他们只需通过协商随机生成 n 位随机密钥 $K_{\mathrm{B}_i\mathrm{B}_{i+1}}$, $K_{\mathrm{B}_{i+1}\mathrm{B}_{i+2}}$, $K_{\mathrm{B}_{i+2}\mathrm{B}_i}$, 这个密钥只有他们双方自己知晓.

Step 3) (生成量子序列): A 依次从每个编码后的量子态中提取第 i 个粒子, 生成对应的量子序列 S_i ($i=1,2,3$). 对于每种序列 S_i, A 会根据参与者数量, 共准备 3 份供后续协议使用.

Step 4) (发送量子序列): 对于每一种序列 S_i, A 首先打乱其中粒子的初始位置重新排列, 得到 $\overline{S_i}$, 并记录各粒子的初始位置. 然后通过使用 Hadamard 算子对 $\overline{S_i}$ 进行线性变换得到 $\widetilde{S}_i$, 即:

$$\widetilde{S}_i = \boldsymbol{H}^{K_{\mathrm{AB}_i}}\overline{S}_i,$$

其中 $i=0,1,2$,

$$\boldsymbol{H} \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

当 $K_{\mathrm{AB}_i}=0$ 时, $\boldsymbol{H}^{K_{\mathrm{AB}_i}}=I$, 当 $K_{\mathrm{AB}_i}=1$ 时, $\boldsymbol{H}^{K_{\mathrm{AB}_i}}=\boldsymbol{H}$. 完成线性变换操作后, A 随机选择诱饵粒子插入到序列 $\widetilde{S}_i$ 的随机位置得到 $\widetilde{S}'_i$. 最后, A 将每一种序列 $\widetilde{S}'_i$ 发送给对应的接收方 B_i, 每个接收方都会收到三个同种量子序列 $\widetilde{S}'_i$, 即 B_i 会接收到序列 $\widetilde{S}'_i\widetilde{S}'_i\widetilde{S}'_i$, B_{i+1} 会接收到序列 $\widetilde{S}'_{i+1}\widetilde{S}'_{i+1}\widetilde{S}'_{i+1}$, B_{i+2} 会接收到序列 $\widetilde{S}'_{i+2}\widetilde{S}'_{i+2}\widetilde{S}'_{i+2}$.

Step 5) (窃听检测): 在 B_i 收到序列 $\widetilde{S}'_i$ 后, A 告诉 B_i 诱饵粒子的测量基和具体位置, B_i 用相应的测量基测量每个诱饵粒子, 以检查窃听. 如果错误概率在一定阈值内, B_i 恢复量子序列 $\widetilde{S}_i$, 并执行线性变换 $H^{K_{\mathrm{AB}_i}}$ 得到 $\overline{S}_i = H^{K_{\mathrm{AB}_i}}\widetilde{S}_i$; 否则将终止该协议.

3.1.2 秘密揭示阶段

Step 6) (量子序列传输): 在 B_i 恢复量子序列 $\overline{S}_i$ 后, 首先 B_i 会保留一个序列 $\overline{S}_i$, 将剩余的其他量子序列 $\overline{S}_i$ 通过使用和 B_{i+1} 的共享密钥 $K_{\mathrm{B}_i\mathrm{B}_{i+1}}$ 进行线性变换 $\widehat{S}_i = H^{K_{\mathrm{B}_i\mathrm{B}_{i+1}}}\overline{S}_i$, 然后随机插入诱饵粒子到序列得到 $\widehat{S}''_i$, 将 $\widehat{S}''_i$ 发送给下一个接收者 B_{i+1}. 在 B_{i+1} 接收到 B_i 发送的量子序列后, 首先会进行窃听检测, 如果满足阈值, 则恢复序列 $\widehat{S}_i$, 并进行线性变换得到 $\overline{S}_i = H^{K_{\mathrm{B}_i\mathrm{B}_{i+1}}}\widehat{S}_i$; 否则, 终止该协议. 在 B_{i+1} 接收到 B_i 的量子序列 $\overline{S}_i$ 后, 他会保留一个接收到的序列 $\overline{S}_i$, 并将剩余接收的序列通过相同的线性变换操作后发送给下一个接收方 B_{i+2}. 接着, B_{i+1} 会保留自己的一个量子序列 $\overline{S}_{i+1}$, 并将剩余的其他序列 $\overline{S}_{i+1}$ 通过相同的变换操作后也发送给下一个接收方 B_{i+2}. 当最后一个接收方接收到量子序列后, 该过程结束.

Step 7) (信息仲裁): 当最后一个接收者 B_{i+2} 接收并恢复上一个接收者发送的量子序列后, 他会在之前先后接收到的两组量子序列 $\overline{S}_i$ 和 $\overline{S}_{i+1}$ 中分别保留其中一个量子序列. 此时 B_{i+2} 拥有一组完整的量子序列 $\overline{S}_i\overline{S}_{i+1}\overline{S}_{i+2}$, B_{i+2} 与 A 进行通信, 对所拥有的这组完整的序列进行验证. A 会告知接收方 B_{i+2} 打乱顺序后的各量子序列的对应测量基, 在接收方 B_{i+2} 完成测量后, A 根据测量结果进行验证. 如果测量结果与之前保存的打乱后的量子序列信息相等, 说明量子序列的传输过程正常, 执行下一步骤. 否则, 则说明在之前的序列传输过程中有接收者对量子序列进行了伪造, 终止该协议.

Step 8) (量子序列回传): 当量子序列传输到最后一个接收方时, 此时每一接收方都拥有一个最开始传输的量子序列 $\overline{S}_i$, 即量子序列 $\overline{S}_i$ 已经完成传输, 在量子序列回传阶段, 序列 $\overline{S}_i$ 不再参与传输. 所以在接收方 B_{i+2} 完成验证后, 他会将剩余的量子序列 $\overline{S}_{i+1}$ 和 $\overline{S}_{i+2}$ 经过相关操作后先后发送给下一个接收方 B_i. 对于接收方 B_i, 在每次接收并恢复上一个接收方 B_{i+2} 发送的量子序列, 他会分别保留其中一个量子序列 $\overline{S}_{i+1}$ 和 $\overline{S}_{i+2}$, 此时接收方 B_i 也拥有一组完整的量子序列 $\overline{S}_i\overline{S}_{i+1}\overline{S}_{i+2}$, 而且序列 $\overline{S}_{i+1}$ 也完成了传输, 即每个接收方都拥有该序列. 之后接收方 B_i 会将剩余的最后一个量子序列 $\overline{S}_{i+2}$ 发送给下一个参与者 B_{i+1}, 此时, 所有参与者都拥有恢复秘密信息所需的所有量子序列 $\overline{S}_i\overline{S}_{i+1}\overline{S}_{i+2}$.

Step 9) (仲裁与秘密恢复): 当量子序列回传阶段最后一个接收方 B_{i+1} 得到了序列 $\overline{S}_i\overline{S}_{i+1}\overline{S}_{i+2}$ 后, 与 A 进行通信, 执行和 Step 7) 相同的信息仲裁操作. 如果 A 检测两个量子序列信息不相等, 说明在序列回传过程中, 有接收方对序列进行了伪造, 终止该协议; 否则, 说明量子序列回传过程正常, A 会与各个接收方进行通信, 将量子序列的初始位置及测量基告诉他们, 各个接收方以此可以测

量得到量子序列 $\overline{S}_i\overline{S}_{i+1}\overline{S}_{i+2}$, 恢复序列 S. 根据编码规则, 各个接收方对序列 S 进行测量, 最终得到 A 的初始秘密 M.

3.2 接收方的动态变化操作

考虑到协议在进行过程中, 因为一些其他不可控因素的存在, 可能会导致有参与者的退出或新的参与者加入的情况发生, 为了保证协议可以在原始所准备的正交乘积态的基础上正常进行, 设计了如下的参与者动态变化的操作:

3.2.1 当有接收方退出时

假设当接收方 B_{i+1} 退出协议时, 更改协议传输路径, 操作流程如图 2 所示. 接收方 B_i 会将自己的发送对象更改为 B_{i+2}, 同时接收方 B_i 和 B_{i+2} 会协商生成一个随机密钥 $K_{\mathrm{B}_i\mathrm{B}_{i+2}}$, 他们会使用此密钥在量子序列发送时进行相关加密操作. 为避免 B_{i+1} 之前持有的序列 $\overline{S}_{i+1}$ 可能会对协议造成影响, A 重新打乱序列 S_{i+1} 的粒子位置得到一个新的序列 $\overline{S}'_{i+1}$, A 保存这个序列并记录打乱的顺序. 在量子序列分发过程中, A 会根据此时参与者的人数准备相同数量的同一量子序列并分发给对应的参与者. 在各参与者完成量子序列的传输和回传后, 此时各接收方都得到了除 $\overline{S}'_{i+1}$ 外的量子序列, A 会将新的序列 $\overline{S}'_{i+1}$ 进行发送传输, 确保所有参与者都能得到 A 传输的新的序列 $\overline{S}'_{i+1}$. 最终各参与者都会得到恢复秘密所需的所有量子序列.

3.2.2 当有新的接收方加入时

假设当新的接收方 B_m 加入协议时, 更改协议传输路径, 操作流程如图 3 所示. 新加入的接收方默认每次都添加在之前协议流程最后一个接收方之后. 假定初始协议共 3 个接收方, 此时之前流程中的最后一个接收方 B_{i+2} 更改自己的发送对象为新加入的接收方 B_m, 同时, 接收方 B_{i+2} 和 B_i 分别与 B_m 协商生成共享密钥 $K_{\mathrm{B}_{i+2}\mathrm{B}_m}$ 和 $K_{\mathrm{B}_m\mathrm{B}_i}$, 这个共享密钥会在后面双方通信时使用. A 和 B_m 会协商生成在协议传输过程中会使用到的密钥 K_{AB_m}, 密钥的分发使用 QKD 进行发送. A 会给新加入的接收方发送随机冗余量子序列 $\overline{S}_t$, 该序列不在编码规则之中, 所以在秘密恢复过程中该序列不参加, 只起到在传输过程中的一个冗余验证作用.

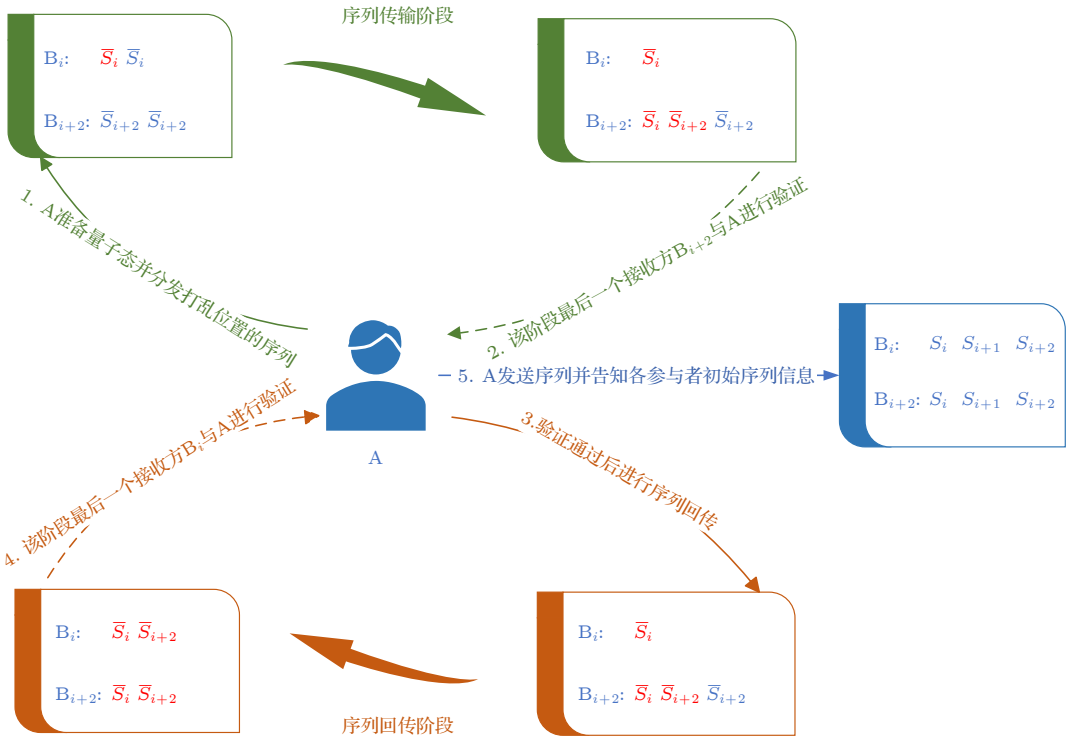

图 2 有接收方退出时的协议流程, 其中红色标注的量子序列是在传输阶段参与者进行保留的序列, 蓝色标注的量子序列是在传输阶段不同参与者的传输回合中待发送的序列

Fig. 2. The protocol flow when a receiver withdraws, the quantum sequences marked in red are the sequences that the participants retain during the transmission stage, and the quantum sequences marked in blue are the sequences to be sent in the transmission rounds of different participants during the transmission phase.

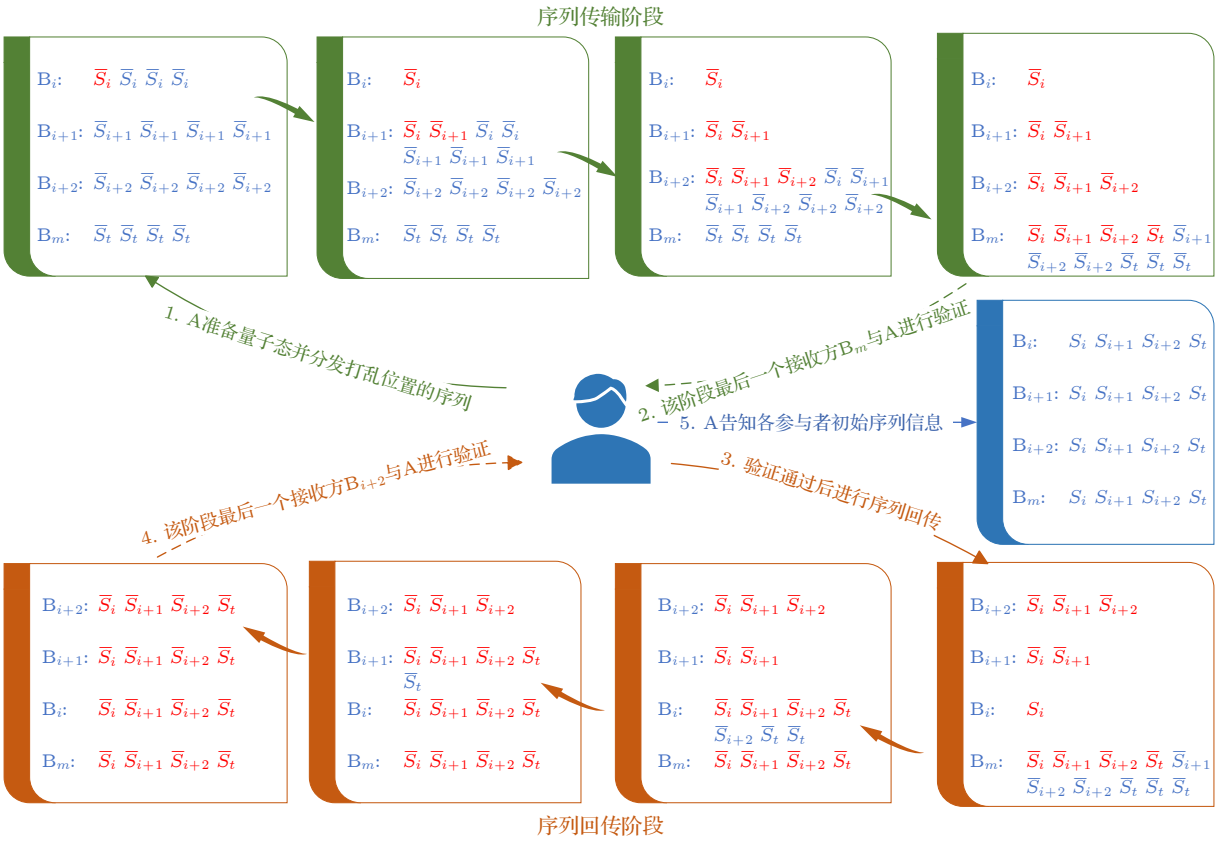

图 3 有新的接收方加入时的协议流程, 其中红色标注的量子序列是在传输阶段参与者进行保留的序列, 蓝色标注的量子序列是在传输阶段不同参与者的传输回合中待发送的序列

Fig. 3. The protocol flow when a new receiver joins, the quantum sequences marked in red are the sequences that the participants retain during the transmission stage, and the quantum sequences marked in blue are the sequences to be sent in the transmission rounds of different participants during the transmission phase.

在该协议中, 只有确认量子序列传输阶段和量子序列回传阶段中传输的量子序列都正常时, 秘密分发者 A 才会将各个量子序列的初始位置和状态告诉各接收者. 所以, 为了避免过多的新的接收方加入协议导致传输过程中存在太多的量子序列, 我们设定新加入接收方的人数不得超过初始选定的 n 部系统的正交乘积态数 n. 当人数过多时, 可以根据此时具体人数重新选定正交乘积态, 根据新的正交乘积态进行协议的量子序列传输.

4 例 子

为了更清楚地说明我们的协议, 提出了以下示例. 为了方便起见, 不考虑窃听检测. 假设秘密分发者 A 共享的秘密 $M=011110$, 根据编码规则将会准备量子态 $|\psi_2\rangle$, $|\psi_4\rangle$, $|\psi_3\rangle$. 初始化阶段各个参与者共享 3 位密钥, 即 $K_{\mathrm{AB}_0}=010$, $K_{\mathrm{AB}_1}=101$, $K_{\mathrm{AB}_2}=011$, $K_{\mathrm{B}_0\mathrm{B}_1}=110$, $K_{\mathrm{B}_1\mathrm{B}_2}=101$. 对于准备的各个量子态, 取出相同位置的粒子可以得到如下量子序列:

$$S_0=|1\rangle,|0\rangle,|+\rangle,$$
$$S_1=|+\rangle,|1\rangle,|0\rangle,$$
$$S_2=|0\rangle,|-\rangle,|1\rangle.$$

此时, A 会打乱序列 S_i 中各个粒子的初始位置进行重新排序, 得到新的量子序列 $\overline{S}_i$ 进行传输, 同时 A 会记录量子序列的初始位置信息. 假设打乱位置后得到的量子序列 $\overline{S}_i$ 为

$$\overline{S}_0=|1\rangle,|+\rangle,|0\rangle,$$
$$\overline{S}_1=|1\rangle,|0\rangle,|+\rangle,$$
$$\overline{S}_2=|0\rangle,|1\rangle,|-\rangle.$$

在 A 将各个量子序列发送给对应接收方之前, A 会根据他与各接收方之间共享的密钥对量子序列进行线性变换操作, 即 $\widetilde{S}_i=H^{K_{\mathrm{AB}_i}}\overline{S}_i$. 其中, 当 $K_{\mathrm{AB}_i}=0$ 时, $H^{K_{\mathrm{AB}_i}}=I$, 当 $K_{\mathrm{AB}_i}=1$ 时, $H^{K_{\mathrm{AB}_i}}=H$. 根据这个变换规则, 借助每一位密钥的具体值

依次对量子序列的粒子进行变换:

$$\widetilde{S}_0 = H^{K_{\mathrm{AB}_0}}\overline{S}_0 = H^{010}\overline{S}_0 = |1\rangle, |0\rangle, |0\rangle,$$

$$\widetilde{S}_1 = H^{K_{\mathrm{AB}_1}}\overline{S}_1 = H^{101}\overline{S}_1 = |-\rangle, |0\rangle, |1\rangle,$$

$$\widetilde{S}_2 = H^{K_{\mathrm{AB}_2}}\overline{S}_2 = H^{011}\overline{S}_2 = |0\rangle, |-\rangle, |1\rangle.$$

在每一个接收方 B_i 恢复量子序列 $\widetilde{S}_i$ 后, 对序列执行线性变换 $H^{K_{\mathrm{AB}_i}}$ 得到

$$\mathrm{B}_0: \quad \overline{S}_0 = H^{K_{\mathrm{AB}_0}}\widetilde{S}_0 = H^{010}\widetilde{S}_0 = |1\rangle, |+\rangle, |0\rangle.$$

$$\mathrm{B}_1: \quad \overline{S}_1 = H^{K_{\mathrm{AB}_1}}\widetilde{S}_1 = H^{101}\widetilde{S}_1 = |1\rangle, |0\rangle, |+\rangle.$$

$$\mathrm{B}_2: \quad \overline{S}_2 = H^{K_{\mathrm{AB}_2}}\widetilde{S}_2 = H^{011}\widetilde{S}_2 = |0\rangle, |1\rangle, |-\rangle.$$

可以看出, 通过对 A 所发送的量子序列继续执行线性变换操作, 可以恢复 A 在开始阶段准备发送给各个接收方 B_i 的量子序列. 该线性变换操作主要借助于通信双方的共享密钥信息和一个酉矩阵.

在秘密揭示阶段, 对量子序列的相关变换操作与上面所提到的类似, 这里不再进行详细介绍. 当 A 确认在量子序列回发阶段中信息传输是安全的, 他会将量子序列 $\overline{S}_i$ 的正确位置信息及测量基告诉各个接收方 B_i, 此时接收方可以恢复初始的量子序列 S. 根据编码规则, 各个接收方可以恢复 A 的初始秘密 M.

5 安全性分析

本节我们对协议在进行过程中可能存在内部不诚实的参与者和外部恶意攻击者的攻击行为进行分析.

5.1 内部攻击

相比于外部恶意攻击者的攻击行为, 内部不诚实的参与者的攻击性会更强, 因为这些不诚实的参与者会直接参与协议的过程, 也会获得一些协议进行中使用到的秘密信息. 这里主要分析了内部不诚实的参与者可能会进行的伪造攻击和共谋攻击.

5.1.1 伪造攻击

伪造攻击是指恶意参与者试图提交伪造的共享量子序列以扰乱秘密恢复的过程. 在 QSS 协议中, 伪造攻击是一种容易被忽视但又很重要的攻击行为. 假设在该协议中存在恶意接收方, 在量子序列传输阶段, 恶意接收方会故意伪造自己的量子序列并将其发送给其他接收方, 这种伪造是不可行的. 因为在量子传输阶段, 当最后一个接收方在收到量子序列后, 他会与 A 通信进行粒子的测量验证, 因为只有 A 知道所传输的量子态信息, 如果发现最后一个接收方收到的量子序列的测量结果与初始传输的量子序列状态不一样, 则 A 会终止该协议, 防止错误的量子序列进入下一阶段. 同样, 在量子回传阶段, 最后一个接收方在收到量子序列后也会与 A 进行通信验证, 如果存在恶意参与者对序列进行了伪造, A 会发现伪造攻击的存在并终止协议.

5.1.2 共谋攻击

共谋攻击是指多个恶意参与者联合起来, 试图恢复秘密或破坏系统. 假设存在最坏情况, 即有 $n-1$ 个恶意接收方, 他们会共享自己所拥有的量子序列, 但是恢复初始秘密信息需要 n 个量子序列. 为了恢复秘密信息, 他们必须要得到 A 发送给最后一个接收方的量子序列, 这个过程等同于进行外部攻击. 通过后面对外部攻击分析可知, 当粒子数 n 较多时, 最终攻击行为被检测到概率无限接近于 1. 而且, 每一个接收方的量子序列是经过 A 打乱顺序后所发送的, 他们不知道这些量子序列的初始位置, 所以, 多个恶意接收方通过共谋攻击想直接得到秘密信息是不可行的.

5.2 外部攻击

与内部不诚实参与者的攻击不同, 外部攻击者是来自外部的非法窃听者. 在量子序列传输过程中, 外部窃听者 Eve 可能会发动一些常见的攻击. 我们将主要对拦截-重发 (intercept-resend, IR) 攻击、拦截-测量-重发 (intercept-measure-resend, IMR) 攻击和纠缠-测量攻击及特洛伊木马攻击进行分析.

5.2.1 拦截-重发攻击

假设 Eve 是一个外部窃听者, 她可以在量子序列分发和传输阶段对序列拦截, 进行攻击. 当 Eve 截取量子序列后, 她会将自己准备好的错误的量子序列发送给参与者. 然而, 由于诱饵粒子是随机地进行选择并插入到序列的随机位置, Eve 无法区分信息粒子与诱饵粒子, 因此在伪造序列时需对所有位置进行基猜测. 若 Eve 伪造的粒子与诱饵粒子处于相同基 (如均为 Z 基), 其量子态与原始诱饵态一致的概率为 1/2 (因诱饵态在基内随机生

成); 若伪造粒子与诱饵粒子处于不同基 (如诱饵粒子为 Z 基而伪造粒子为 X 基), 接收方通过原始基测量时能以 1/2 的概率获得正确结果. Eve 成功窃听单个粒子的概率为 1/2, 最终被检测到的概率为 $1-(1/2)^n$, 其中 n 为量子序列中的粒子个数. 当粒子数目 n 足够大时, 被检测到的概率接近于 1. 所以 Eve 无法通过该攻击从中获取到任何有用的信息.

5.2.2 拦截-测量-重发攻击

在量子通信中, 针对拦截测量重发攻击的检测机制如下: 当攻击者 Eve 对传输的量子比特序列进行截获时, 她会随机选择 Z 基或 X 基对每个粒子实施测量, 并根据测量结果制备对应量子态转发给接收方. 值得注意的是, 发送方在传输前已将随机选取的诱饵粒子插入量子序列的随机位置. 由于 Eve 无法识别诱饵粒子的具体位置, 当其对诱饵粒子进行测量时: 若采用正确测量基 (如对 $|0\rangle$, $|1\rangle$ 用 Z 基, 对 $|+\rangle$, $|-\rangle$ 用 X 基), 那么她就可以通过窃听检测; 若采用错误测量基 (如对 $|0\rangle$, $|1\rangle$ 用 X 基或对 $|+\rangle$, $|-\rangle$ 用 Z 基), 将有 1/2 的概率因量子态坍缩引入错误, 但仍存在 1/2 的概率未被发现. 所以在拦截测量重发攻击中, 攻击者 Eve 通过单粒子窃听检测的概率为 $\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}=\frac{3}{4}$, 即该攻击会以 $1-(3/4)^n$ 的概率被检测到. 当粒子数足够大, 被检测到的概率接近于 1, 所以该攻击无法实现.

5.2.3 纠缠-测量攻击

纠缠-测量攻击是量子保密通信中的一种典型窃听策略, 攻击者通过操控量子纠缠现象实施信息截取. 在该攻击模型中, 窃听者 Eve 会拦截通信信道中传输的量子态序列, 同时制备特定辅助量子态 $|a_i\rangle$. 为避免引发异常检测, Eve 将运用统一操作 $U_{\rm a}$ 使辅助量子态与截获的量子粒子形成纠缠关联. 通过后续对辅助量子系统实施量子测量操作, Eve 试图从测量结果中解析出机密信息. 这种攻击会破坏量子态的相干特性, 可能造成传输信息的完整性受损, 进而威胁量子通信系统的保密性. 其中对于诱骗粒子施加的统一操作 $U_{\rm a}$ 可以表示为

$$U_{\rm a}|0\rangle|a_i\rangle=\alpha|0\rangle|a_1\rangle+\beta|1\rangle|a_2\rangle, \tag{1}$$

$$U_{\rm a}|1\rangle|a_i\rangle=\gamma|0\rangle|a_3\rangle+\delta|1\rangle|a_4\rangle, \tag{2}$$

$$\begin{aligned}U_{\rm a}|+\rangle|a_i\rangle&=\frac{1}{\sqrt{2}}\left(U_{\rm a}|0\rangle|a_i\rangle+U_{\rm a}|1\rangle|a_i\rangle\right)=\frac{1}{\sqrt{2}}\left(\alpha|0\rangle|a_1\rangle+\beta|1\rangle|a_2\rangle+\gamma|0\rangle|a_3\rangle+\delta|1\rangle|a_4\rangle\right)\\&=\frac{1}{\sqrt{2}}\left(\alpha\frac{|+\rangle+|-\rangle}{\sqrt{2}}|a_1\rangle+\beta\frac{|+\rangle-|-\rangle}{\sqrt{2}}|a_2\rangle+\gamma\frac{|+\rangle+|-\rangle}{\sqrt{2}}|a_3\rangle+\delta\frac{|+\rangle-|-\rangle}{\sqrt{2}}|a_4\rangle\right)\\&=\frac{1}{2}\left[|+\rangle\left(\alpha|a_1\rangle+\beta|a_2\rangle+\gamma|a_3\rangle+\delta|a_4\rangle\right)+|-\rangle\left(\alpha|a_1\rangle-\beta|a_2\rangle+\gamma|a_3\rangle-\delta|a_4\rangle\right)\right],\end{aligned} \tag{3}$$

$$\begin{aligned}U_{\rm a}|-\rangle|a_i\rangle&=\frac{1}{\sqrt{2}}\left(U_{\rm a}|0\rangle|a_i\rangle-U_{\rm a}|1\rangle|a_i\rangle\right)=\frac{1}{\sqrt{2}}\left(\alpha|0\rangle|a_1\rangle+\beta|1\rangle|a_2\rangle-\gamma|0\rangle|a_3\rangle-\delta|1\rangle|a_4\rangle\right)\\&=\frac{1}{\sqrt{2}}\left(\alpha\frac{|+\rangle+|-\rangle}{\sqrt{2}}|a_1\rangle+\beta\frac{|+\rangle-|-\rangle}{\sqrt{2}}|a_2\rangle-\gamma\frac{|+\rangle+|-\rangle}{\sqrt{2}}|a_3\rangle-\delta\frac{|+\rangle-|-\rangle}{\sqrt{2}}|a_4\rangle\right)\\&=\frac{1}{2}\left[|+\rangle\left(\alpha|a_1\rangle+\beta|a_2\rangle-\gamma|a_3\rangle-\delta|a_4\rangle\right)+|-\rangle\left(\alpha|a_1\rangle-\beta|a_2\rangle-\gamma|a_3\rangle+\delta|a_4\rangle\right)\right].\end{aligned} \tag{4}$$

其中 $|a_i\rangle$ 是辅助量子的初始状态, $|a_1\rangle$, $|a_2\rangle$, $|a_3\rangle$, $|a_4\rangle$ 是 Eve 可以进行区分的 4 个状态, 参数 α, β, γ, δ 满足 $|\alpha|^2+|\beta|^2=|\gamma|^2+|\delta|^2=1$.

对于 (1) 式和 (2) 式, 为了防止 Eve 的辅助量子与量子态 $|0\rangle$, $|1\rangle$ 纠缠后被检测到, 需要满足条件 $\beta=\gamma=0$. 此时, 在 Eve 未被发现的情况下, Eve 的酉算子 $U_{\rm a}$ 会对 $|+\rangle$, $|-\rangle$ 产生影响, 即:

$$\begin{aligned}U_{\rm a}|+\rangle|a_i\rangle&=\frac{1}{\sqrt{2}}\left(U_{\rm a}|0\rangle|a_i\rangle+U_{\rm a}|1\rangle|a_i\rangle\right)=\frac{1}{\sqrt{2}}\left(\alpha|0\rangle|a_1\rangle+\delta|1\rangle|a_4\rangle\right)\\&=\frac{1}{\sqrt{2}}\left(\alpha\frac{|+\rangle+|-\rangle}{\sqrt{2}}|a_1\rangle+\delta\frac{|+\rangle-|-\rangle}{\sqrt{2}}|a_4\rangle\right)=\frac{1}{2}\left[|+\rangle(\alpha|a_1\rangle+\delta|a_4\rangle)+|-\rangle(\alpha|a_1\rangle-\delta|a_4\rangle)\right],\end{aligned} \tag{5}$$

$$U_{\rm a}|-\rangle|a_i\rangle=\frac{1}{\sqrt{2}}\left(U_{\rm a}|0\rangle|a_i\rangle-U_{\rm a}|1\rangle|a_i\rangle\right)=\frac{1}{\sqrt{2}}\left(\alpha|0\rangle|a_1\rangle-\delta|1\rangle|a_4\rangle\right)$$
$$=\frac{1}{\sqrt{2}}\left(\alpha\frac{|+\rangle+|-\rangle}{\sqrt{2}}|a_1\rangle-\delta\frac{|+\rangle-|-\rangle}{\sqrt{2}}|a_4\rangle\right)=\frac{1}{2}[|+\rangle(\alpha|a_1\rangle-\delta|a_4\rangle)+|-\rangle(\alpha|a_1\rangle+\delta|a_4\rangle)]\,. \quad (6)$$

同样, 对于 (5) 式和 (6) 式, 为了防止 Eve 的辅助量子与量子态 $|+\rangle$, $|-\rangle$ 纠缠后被检测到, 需要满足条件 $\alpha\,|a_1\rangle-\delta\,|a_4\rangle=0$, 即 $\alpha\,|a_1\rangle=\delta\,|a_4\rangle$.

通过以上分析可以得到, 如果 Eve 进行纠缠-测量攻击, 但在辅助粒子与截取的序列粒子纠缠后仍未被发现, 此时对于诱骗粒子施加的操作 $U_{\rm a}$ 应满足以下关系式:

$$U_{\rm a}|0\rangle|a_i\rangle=\alpha|0\rangle|a_1\rangle, \quad (7)$$

$$U_{\rm a}|1\rangle|a_i\rangle=\delta|1\rangle|a_4\rangle=\alpha|1\rangle|a_1\rangle, \quad (8)$$

$$U_{\rm a}|+\rangle|a_i\rangle=\frac{1}{2}|+\rangle(\alpha|a_1\rangle+\delta|a_4\rangle)=\alpha|+\rangle|a_1\rangle, \quad (9)$$

$$U_{\rm a}|-\rangle|a_i\rangle=\frac{1}{2}|-\rangle(\alpha|a_1\rangle+\delta|a_4\rangle)=\alpha|-\rangle|a_1\rangle. \quad (10)$$

由 (7) 式—(10) 式可以发现, 在未被发现的情况下, Eve 在对粒子执行 $U_{\rm a}$ 操作后, 她只能得到 $|a_1\rangle$ 有关的信息, 无法正确区分出 $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ 的状态. 所以, 在不被发现的情况下, Eve 在纠缠-测量攻击中无法获得有关共享秘密的有效信息.

5.2.4 特洛伊木马攻击

当 QSS 协议以光子为载体时, 延迟光子攻击与不可见光子攻击两类特洛伊木马威胁尤为突出, 其核心在于攻击者通过向量子设备注入特制光子, 窃取密钥信息或破坏协议的安全性. 但是, 通过配备波长滤波器和光子数拆分器[37,38], 可以有效地防御特洛伊木马的攻击.

延迟光子攻击中, 攻击者利用量子设备对光子响应的时间窗口漏洞, 向发送端发射与工作波长相近的间谍光子. 这些光子进入发送端后, 会激发设备产生携带密钥信息的光子, 并被攻击者预先植入的反射装置反射回接收端. 对于这一威胁, 可以在量子设备中集成波长滤波器. 波长滤波器基于光的干涉和衍射原理, 通过构建特定的光学结构选择性透过协议工作波长光子, 屏蔽邻近波长间谍光子, 从源头阻断攻击者利用非工作波长光子窃取信息的途径. 同时, 引入光子数分离器 (PNS) 对接收光子进行采样分析, 分离统计光子数目, 当检测到异常多的光子脉冲率, 即可识别延迟光子攻击.

不可见光子攻击则是攻击者向接收端发射不可见的异频光子, 这些光子不会触发正常的检测机制, 却能与接收端设备相互作用, 干扰设备对合法光子的处理, 从而窃取密钥信息. 针对这一攻击方式, 可以在接收端加装窄带光学滤波器. 该滤波器仅允许与工作波长严格匹配的光子通过, 对攻击者发射的不可见异频光子形成物理阻断, 确保接收端仅处理合法的通信光子, 有效抵御不可见光子攻击.

6 模拟与讨论

本节将使用 IBM Qiskit 进行协议的电路模拟并讨论协议性能.

6.1 基于 IBM Qiskit 的仿真

为验证所提出的基于正交乘积态的量子秘密共享协议在实际操作中的可行性与核心步骤的正确性, 我们利用 IBM Qiskit 框架进行了仿真实验. 实验模拟重点关注协议的核心量子环节: 特定正交乘积态的制备, 量子态的传输变换及恢复过程. 模拟主要在 Qiskit 的 AerSimulator 上进行, 模拟包含测量采样的实际执行过程. 同时, 我们利用 Statevector 方法精确验证量子态矢量的演化是否正确. 模拟中使用的具体参数严格遵循协议第 3 节的定义.

首先, 我们模拟了协议所需的正交乘积态的制备过程. 根据协议要求, 我们为目标正交乘积态 (例如 $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, $|\psi_4\rangle$) 设计了高效的量子电路. 这些电路通常从初态 $|0\rangle^{\otimes n}$ 出发, 通过精心组合的量子门操作构建目标态. 我们以 $|\psi_2\rangle=\frac{1}{\sqrt{2}}|1\rangle_1(|0\rangle+|1\rangle)_2|0\rangle_3$ 和 $|\psi_4\rangle=\frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2(|0\rangle-|1\rangle)_3$ 这两个正交乘积态的制备为例进行了模拟.

图 4 展示了制备目标正交乘积态 $|\psi_2\rangle=\frac{1}{\sqrt{2}}\times|1\rangle_1(|0\rangle+|1\rangle)_2|0\rangle_3$ 的量子电路及其仿真结果. 该电路从初态 $|0\rangle^{\otimes 3}$ 出发, 通过在第 1 个量子比特 $\rm q_1$ 上应用 X 门 (产生 $|1\rangle_1$), 在第 2 个量子比特 $\rm q_2$ 上应用 H 门 (产生叠加态 $(|0\rangle+|1\rangle)_2$), 并保持第 3 个

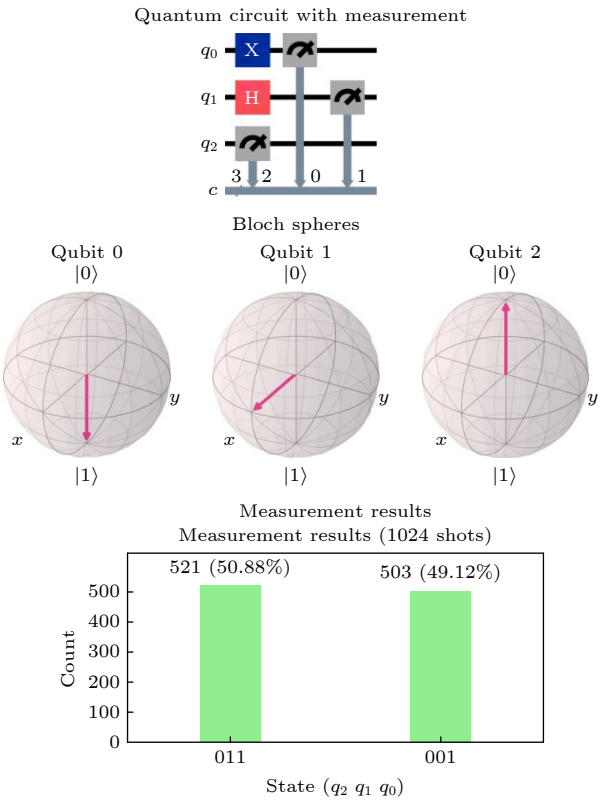

图 4 正交乘积态 $|\psi_2\rangle$ 的制备及仿真结果

Fig. 4. Preparation and simulation results of orthogonal product state $|\psi_2\rangle$.

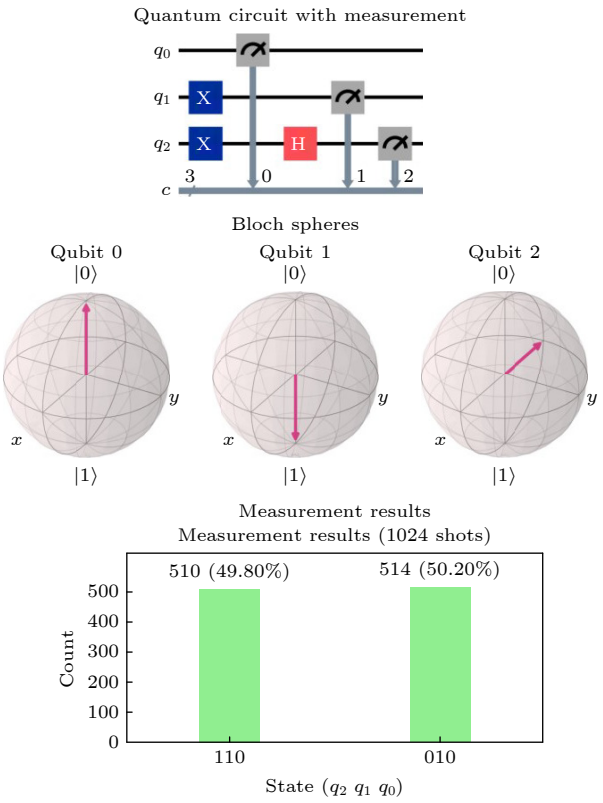

图 5 正交乘积态 $|\psi_4\rangle$ 的制备及仿真结果

Fig. 5. Preparation and simulation results of orthogonal product state $|\psi_4\rangle$.

量子比特 q_3 为 $|0\rangle_3$, 最后进行测量. 布洛赫球分析确认制备的态矢量与 $|\psi_2\rangle$ 完全一致. 由于 q_2 处于叠加态, 测量时应以等概率 (各约 50%) 坍缩到基态 $|1\rangle_1|0\rangle_2|0\rangle_3$ 或 $|1\rangle_1|1\rangle_2|0\rangle_3$; 1024 次测量采样的统计结果为 $|100\rangle$ (对应 $|1\rangle_1|0\rangle_2|0\rangle_3$) 占 49.12%, $|110\rangle$ (对应 $|1\rangle_1|1\rangle_2|0\rangle_3$) 占 50.88%, 非常接近理论预期, 充分验证了该量子电路制备 $|\psi_2\rangle$ 态的可行性.

图 5 所示为在制备正交乘积态 $|\psi_4\rangle=(1/\sqrt{2})\times|0\rangle_1|1\rangle_2(|0\rangle-|1\rangle)_3$ 时, 相应的量子电路和仿真结果. 通过布洛赫球和测量结果的直方图, 可以发现通过该量子电路对目标量子态的制备具有可行性.

其次, 我们仿真模拟了量子态在传输过程中的变换及其恢复过程. 秘密分发者首先根据选定的秘密信息, 利用前述量子电路制备对应的正交乘积态 (如 $|\psi_2\rangle$ 或 $|\psi_4\rangle$), 并按协议将量子比特子集分配给不同参与者, 量子比特寄存器的划分模拟了粒子的物理分配过程. 核心模拟环节聚焦于通信双方在传输粒子时执行的变换操作以及接收方执行的逆变换恢复操作. 该变换操作由通信密钥和 Hadamard 算子决定: 当密钥值为 0 时, 应用恒等算子 I (即无操作); 当密钥值为 1 时, 应用 Hadamard 门 H. 接收方对接收到的粒子执行完全相同的操作 (因 $H^2=I$, 故再次应用 H 即完成逆变换), 最终测量粒子状态并与初始状态进行对比, 以验证变换和恢复过程的可行性. 我们针对态 $|\psi_2\rangle$ 和 $|\psi_4\rangle$ 中的粒子进行模拟, 具体结果将在后续内容中展示.

图 6 所示为量子态为 $|\psi_2\rangle$ 且通信密钥为 011 时的变换与恢复操作电路. 电路由四部分构成 (以虚线分割): 第 1 部分为 $|\psi_2\rangle$ 的制备电路; 第 2 部分为发送方根据密钥值 (011 表示对 q_1 无操作 (I), q_2 和 q_3 施加 H 门) 执行的变换操作; 第 3 部分为接收方执行的相同操作 (即逆变换); 最后部分为对恢复后量子态的测量. 图 7 所示为执行该电路的仿真结果, 图 7(a) 为测量结果分布, 图 7(b) 为各量子比特概率分布的预期值与实际值对比, 图 7(c) 为量子比特的稳定性分析. 结果表明: 对于基态 $|0\rangle$ 或 $|1\rangle$ 的粒子, 变换与逆变换后状态保持概率为 1; 对于叠加态 $|+\rangle$ 或 $|-\rangle$ 的粒子, 测量结果以约 50% 的概率坍缩到 $|0\rangle$ 或 $|1\rangle$, 与理论预期完全一致. 这充分验证了在量子态传输过程中应用基于密钥的变换操作及其逆操作恢复量子态的可行性.

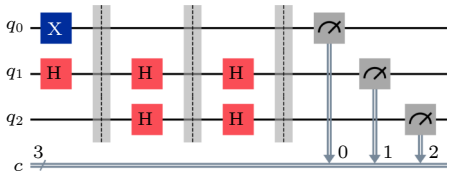

图 6 正交乘积态 $|\psi_2\rangle$ 中的粒子在密钥值为 011 情况下的变换和恢复的电路图

Fig. 6. Circuit diagram for the transformation and recovery of particles in the orthogonal product state $|\psi_2\rangle$ under the key value of 011.

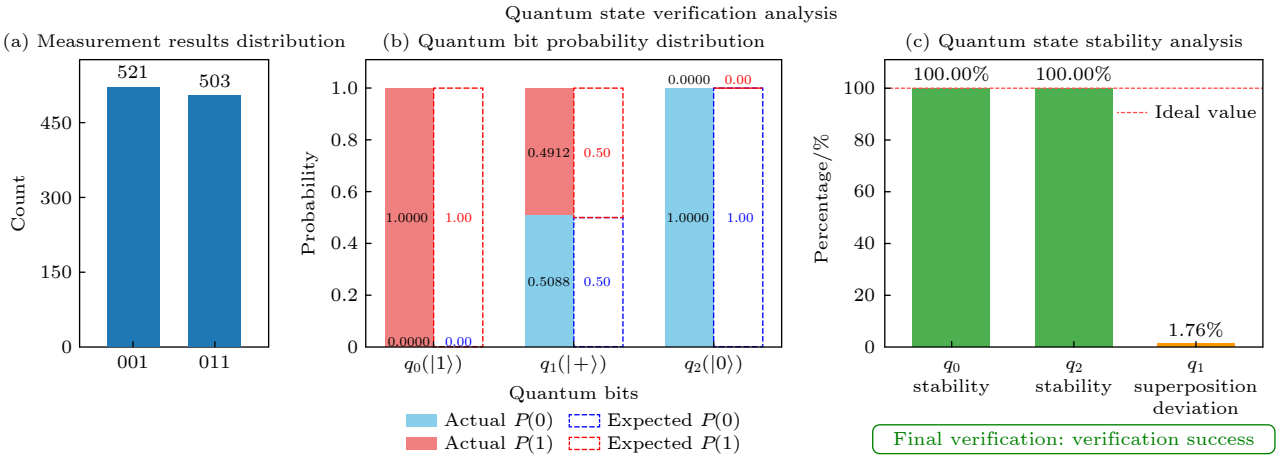

图 7 正交乘积态 $|\psi_2\rangle$ 中的粒子在密钥值为 011 情况下的变换和恢复的测量结果

Fig. 7. Measurement results for the transformation and recovery of particles in the orthogonal product state $|\psi_2\rangle$ under the key value of 011.

图 8 展示了量子态为 $|\psi_4\rangle$ 且通信密钥为 101 时的变换与恢复操作电路, 图 9 所示为执行上述电路的仿真结果. 通过分析可以发现, 该情况下量子态在进行传输前后粒子状态仍能保持一致, 满足协议的要求.

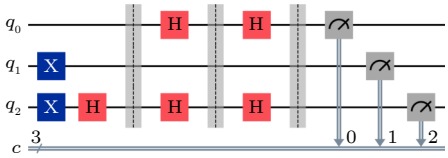

图 8 正交乘积态 $|\psi_4\rangle$ 中的粒子在密钥值为 101 情况下的变换和恢复的电路图

Fig. 8. Circuit diagram for the transformation and recovery of particles in the orthogonal product state $|\psi_4\rangle$ under the key value of 101.

综上所述, Qiskit 仿真实验成功模拟了协议的核心量子流程. 结果明确证实: 协议所需的正交乘积态可以被高保真度制备; 量子态在参与者间的传输和必要变换能够被正确执行, 这些结果为协议的理论可行性提供了重要的计算验证.

6.2 讨 论

表 1 所示为本文所提出的协议与现有的一些量子秘密共享协议 [25–29] 的对比. 文献 [39] 提出量子比特效率可以表示为 $\eta = c/q$, 其中 q 表示通过量子通道传输的总比特数 (窃听检测中使用的诱饵粒子除外), c 表示执行协议后共享的经典比特数.

在 Song 等 [25] 的方案中, 经销商为秘密共享准备了 $N(n-1)$ 个广义 GHZ 态粒子, 忽略了用于进行窃听检查的诱饵粒子数量, 所以该协议的比特效率为 $1/(n-1)$. 在 Yang 等 [26] 的方案中, 每个 Bell 态都可以被用来编码 1 位主密钥. 一个经销商会产生 $n-1$ 个 Bell 态 (即 $2n-2$ 个量子比特), 忽略了使用的诱饵粒子数量. 所以, 该协议的量子比特效率为 $1/(2n-2)$. 在 Hu 等 [27] 提出的方案中, 需要 $n+1$ 个量子比特来共享 1 位秘密, 该协议的量子比特效率为 $1/(n+1)$. 在 Tian 等 [28] 的方案中, 每个 Bell 态用来编码 1 位秘密信息, 忽略窃听检查使用的诱饵粒子数量, 协议中经销商会准备 nm 个 Bell 态, 所以协议的量子效率为 $1/(2n)$. 在 Lin 等 [29] 提出的协议中, $N(n-1)+N(n-1)$ 个量子位共享 N 位秘密信息, 协议的量子比特效率为 $1/(2n-2)$. 在我们所提出的方案中, 协议中所需的量子态由秘密分发者准备, 因为使用正交乘积态进行秘密的编码, 所以准备的每一个量子态的粒

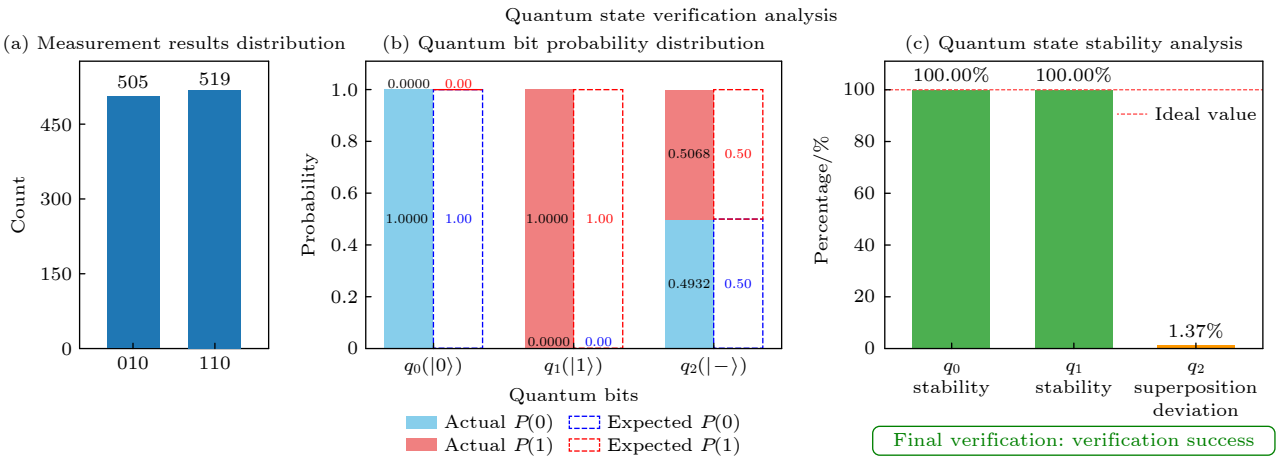

图 9 正交乘积态 $|\psi_4\rangle$ 中的粒子在密钥值为 101 情况下的变换和恢复的测量结果

Fig. 9. Measurement results for the transformation and recovery of particles in the orthogonal product state $|\psi_4\rangle$ under the key value of 101.

表 1 文献 [25–29] 的协议与我们的协议比较

Table 1. Compare the protocols in Refs. [25–29] with our protocol.

协议	[25]	[26]	[27]	[28]	[29]	提出的协议
量子态	广义GHZ态	Bell态	GHZ态	Bell态	Bell态	正交乘积态
参与者测量	单粒子测量	单粒子测量	单粒子测量	Bell态测量	Bell态/单粒子测量	单粒子测量
量子比特数(QR)	$N(n-1)$	$2n-2$	$N(n+1)$	$2nm$	$2N(n-1)$	Nn
量子效率	$\frac{1}{n-1}$	$\frac{1}{2n-2}$	$\frac{1}{n+1}$	$\frac{1}{2n}$	$\frac{1}{2n-2}$	$\frac{\lfloor\log_2 n\rfloor+1}{n}$
窃听检测资源	诱饵粒子	诱饵粒子	GHZ	诱饵粒子	诱饵粒子	诱饵粒子
准备量子位以添加代理	单光子	Bell态	d级GHZ态	Bell态	Bell态	随机量子态序列
易受合谋攻击	No	No	No	No	No	No
是否对粒子执行变换操作	No	Yes	Yes	Yes	No	Yes

子个数由参与者个数 n 确定, 而且每一个量子态可以用来表示 $\lfloor\log_2 n\rfloor+1$ 位经典信息. 所以我们的协议的量子比特效率为 $(\lfloor\log_2 n\rfloor+1)/n$.

在表 1 中其他的方面, Song 等 [25] 的协议利用广义 GHZ 态作为量子资源, Yang 等 [26]、Tian 等 [28] 和 Lin 等 [29] 使用 Bell 态, Hu 等 [27] 使用 GHZ 态, 而我们所提出的协议使用正交乘积态承载秘密信息, 而且量子态的制备相较于上述具有纠缠关系的 Bell 态和 GHZ 态更好制备. 在窃听检测方面, 除了 Hu 等 [27] 使用 GHZ 态进行窃听检测, 其他协议均使用诱饵粒子进行检测. 当有新的代理加入协议时, Song 等 [25] 的协议中需要准备单光子进行添加过程, Yang 等 [26]、Tian 等 [28] 和 Lin 等 [29]协议中需要准备 Bell 态, Hu 等 [27] 的协议需要准备 d 级 GHZ 态, 我们的协议在有新的代理加入时, 需要准备一个随机量子态冗余序列进行代理的添加, 该序列在协议中起到一个冗余验证的作用. 在对抗合谋攻击方面, 上述几个协议都可以很好地防止合谋攻击的实现. 在协议执行过程中, Yang等 [26]、Hu 等 [27] 和 Tian 等 [28] 及我们提出的协议, 都需要在量子态传输过程中对粒子进行幺正变换操作, 而 Song 等 [25] 和 Lin 等 [29] 的协议中不需要对粒子操作.

在我们的协议中, A 所发送给接收方的量子序列都是打乱顺序的, 初始状态只有 A 知道, Eve 无法正确地恢复初始的量子序列状态. 同时在量子序列传输之前, 通信双方会对传输的量子序列进行线性变换操作, 该变换依靠传输双方之间的共享密钥, 由于协议中的共享密钥都是通过 QKD 进行传输的, Eve 无法获得通信双方的共享密钥, 即无法对量子序列的线性变换进行恢复. 综上所述, 相较于其他协议, 我们提出的协议在量子资源的准备阶段, 对于量子态的制备更为容易. 在协议执行过程中, 具有仲裁身份的参与者会对秘密共享任务进行阶段性的验证, 如果在某一阶段存在量子序列传输有误的情况, 则会直接终止协议, 避免在协议执行完所有参与者都接收到量子序列后才发现传输有

误, 防止执行过多无意义的操作. 在量子效率方面, 我们提出的协议与其他协议相比具有较高的效率. 所以, 我们的协议较之前的协议更实用或更有利.

7 结 论

本文提出了一种基于正交乘积态的可验证的QSS协议, 这种正交乘积状态不能被LOCC完全区分. 依靠正交乘积态的特性和对共享信息编码的量子态位置打乱操作, 秘密拥有者和参与者可以实现秘密共享. 各个参与者共同合作可以恢复所要共享的秘密信息. 相较于利用纠缠态的粒子进行的量子秘密共享协议, 我们所使用的正交乘积态的粒子更容易制备. 同时, 考虑到在协议进行过程中, 可能会出现参与者数量的变化, 对协议中参与者的动态变化进行了设计, 可以较好实现在参与者加入或退出后协议仍然可以正常进行. 通过对可能存在的内部和外部攻击的分析, 证明了我们的协议可以安全抵御现有的伪造和拦截攻击. 同时, 利用Qiskit仿真实验成功模拟了协议的核心量子流程, 实验结果为协议的理论可行性提供了重要的计算验证. 本研究旨在为量子秘密共享领域的理论突破与应用拓展提供新的研究思路和技术支撑.

参考文献

[1] Hellman M, Diffie W 1976 *IEEE Trans. Inf. Theory* **22** 644
[2] Fujisaki E, Okamoto T 1999 *Annual international cryptology conference* Santa Barbara, California, USA, August 15–19, 1999 p537
[3] Bellare M, Desai A, Jokipii E, Rogaway P 1997 *Proceedings 38 th Annual Symposium on Foundations of Computer Science* Miami Beach, FL, USA, October 20–22, 1997 p394
[4] Feistel H 1973 *Sci. Amer.* **228** 15
[5] Shor P W 1999 *SIAM Rev.* **41** 303
[6] Grover L K 1996 *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* Philadelphia, Pennsylvania, May 22–24, 1996 p212
[7] Bennett C H, Brassard G 1984 *Proc. Workshop on the Theory and Application of Cryptographic Techniques* Santa Barbara, California, USA, August 19–22, 1984 p475
[8] Feng F Y, Zhang Q 2007 *Acta Phys. Sin.* **4** 1924 (in Chinese) [冯发勇, 张强 2007 物理学报 **4** 1924]
[9] Zhao Z, Chen Y A, Zhang A N, Yang T, Briegel H J, Pan J W 2004 *Nature* **430** 54
[10] Wang T Y, Wen Q Y 2011 *Chin. Phys. B* **20** 040307
[11] Jiang S X, Zhao B, Liang X Z 2021 *Chin. Phys. B* **30** 060303
[12] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317
[13] Zhao N, Jiang Y H, Zhou X T 2022 *Acta Phys. Sin.* **71** 150304 (in Chinese) [赵宁, 江英华, 周贤韬 2022 物理学报 **71** 150304]
[14] Deng F G, Zhou H Y, Long G L 2006 *J. Phys. A: Math. Gen.* **39** 14089
[15] Sun Y, Du J Z, Qin S J, Wen Q Y, Zhu F C 2008 *Acta Phys. Sin.* **08** 4689 (in Chinese) [孙莹, 杜建忠, 秦素娟, 温巧燕, 朱甫臣 2008 物理学报 **08** 4689]
[16] Dai Y W, Qin H Y 2015 *Chin. Phys. Lett.* **32** 100301
[17] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[18] Karlsson A, Koashi M, Imoto N 1999 *Phys. Rev. A* **59** 162
[19] Xiao L, Lu Long G, Deng F G, Pan J W 2004 *Phys. Rev. A* **69** 052307
[20] Yang Y, Wen Q, Zhu F 2007 *Sci. China Ser. G-Phys. Mech. Astron.* **50** 331
[21] Wang T Y, Wen Q Y, Chen X B, Guo F Z, Zhu F C 2008 *Opt. Commun.* **281** 6130
[22] Wang C, Zhang Y 2009 *Chin. Phys. B* **18** 3238
[23] Jia H Y, Wen Q Y, Gao F, Qin S J, Guo F Z 2012 *Phys. Lett. A* **376** 1035
[24] Hsu J L, Chong S K, Hwang T, Tsai C W 2013 *Quantum Inf. Process.* **12** 331
[25] Du Y T, Bao W S 2018 *Chin. Phys. B* **27** 080304
[26] Yang C W, Tsai C W 2020 *Quantum Inf. Process.* **19** 1
[27] Hu W, Zhou R G, Li X, Fan P, Tan C 2021 *Quantum Inf. Process.* **20** 1
[28] Tian Y, Wang J, Bian G, Chang J, Li J 2024 *Adv. Quantum Technol.* **7** 2400116
[29] Lin J, Chen C C, Huang C Y 2024 *Physica A* **638** 129615
[30] Yu S, Oh C H 2015 arXiv: 1502.01274 [quant-ph]
[31] Guo G P, Li C F, Shi B S, Li J, Guo G C 2001 *Phys. Rev. A* **64** 042301
[32] Jiang D H, Wang J, Liang X Q, Xu G B, Qi H F 2020 *Int. J. Theor. Phys.* **59** 436
[33] Jiang D H, Hu Q Z, Liang X Q, Xu G B 2020 *Int. J. Theor. Phys.* **59** 1442
[34] Walgate J, Hardy L 2002 *Phys. Rev. Lett.* **89** 147901
[35] Xu G B, Wen Q Y, Qin S J, Yang Y H, Gao F 2016 *Phys. Rev. A* **93** 032341
[36] Feng Y, Shi Y 2009 *IEEE Trans. Inf. Theory* **55** 2799
[37] Deng F G, Li X H, Zhou H Y, Zhang Z J 2005 *Phys. Rev. A* **72** 044302
[38] Li X H, Deng F G, Zhou H Y 2006 *Phys. Rev. A* **74** 054302
[39] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635

Multi-party quantum secret sharing protocol based on orthogonal product states

CHEN Yun LI Xuanbing LI Shuai †

(*School of Information Engineering, Ningxia University, Yinchuan* 750021, *China*)

(Received 27 March 2025; revised manuscript received 27 June 2025)

Abstract

Quantum secret sharing (QSS) is a cryptographic protocol that utilizes fundamental principles of quantum mechanics to securely distribute and reconstruct secret information among multiple participants. Most existing protocols rely on entangled states (such as Bell and GHZ states), but in practical applications. The preparation of entangled state is constrained by a short quantum coherence time, low state fidelity, etc., which makes it difficult to implement entangled resource-dependent QSS protocols. In this work, a novel practical and verifiable multi-party QSS protocol is proposed based on orthogonal product states, which are easier to prepare than entangled states. During the protocol preparation stage, the secret distributor first converts pre-shared classical secret information into the corresponding orthogonal product states according to the encoding rules, and pre-shares a communication key with participants via quantum key distribution (QKD), which is used to hide the initial quantum sequence information through subsequent particle transformation operations. After preparing the orthogonal product states, the distributor reorganizes the particles by position, extracting particles at the same position from each state to form new sequences, shuffling their order, then applying Hadamard operations using a pre-shared key, inserting decoy particles, and sending the sequences to the participants. After receiving it, participants conduct eavesdropping detection, use the same key for the inverse transformations, retain one particle from each sequence, and sequentially pass the remaining particles until the last participant receives a complete set, triggering state verification with the arbiter distributor. If the verification is successful, the particles will be returned to the first participant and the return stage will follow the same procedure. Only after both the transmission and return stage verifications have passed, will the distributor reveal the initial particle positions, allowing participants to collaboratively reconstruct the secret. In the protocol, the secret distributor acts as an arbitrator to verify the particle state information together with participants at designated points (the end of the transmission stage and the end of the return stage) in order to determine whether the particle-state information is error-free during transmission. If the verification fails at either stage, the protocol will be terminated immediately. Meanwhile, considering that the number of participants may change during the execution of the protocol, a dynamic scheme for personnel changes is designed to ensure the flexibility of the protocol. Through the analysis of possible internal and external attacks, It can be proven that our protocol can effectively resist the existing common attack. Using Qiskit simulation experiments, the core quantum procedures of the protocol can be successfully modeled. The experimental results provide strong computational validation of the theoretical feasibility of the protocol.

Keywords: quantum secret sharing, verifiable, orthogonal product state, dynamic change

PACS: 03.65.Aa, 03.67.Ac, 03.67.Dd **DOI:** 10.7498/aps.74.20250394

CSTR: 32037.14.aps.74.20250394

† Corresponding author. E-mail: lis@nxu.edu.cn

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于正交乘积态的多方量子秘密共享协议

陈云　李璇冰　李帅

Multi-party quantum secret sharing protocol based on orthogonal product states

CHEN Yun　LI Xuanbing　LI Shuai

引用信息 Citation: Acta Physica Sinica, 74, 170301 (2025)　DOI: 10.7498/aps.74.20250394
CSTR: 32037.14.aps.74.20250394
在线阅读 View online: https://doi.org/10.7498/aps.74.20250394
当期内容 View table of contents: http://wulixb.iphy.ac.cn
