

基于高维 GHZ 态的动态分层量子秘密共享协议

陈克勤, 邹峥, 蔡彬彬, 林崧

(福建师范大学计算机与网络空间安全学院, 福建 福州 350007)

摘要: 量子秘密共享是量子密码的一个重要研究分支。提出了一种基于高维 GHZ (greenberger-horne-zeilinger) 态的动态分层量子秘密共享协议。协议将所有参与者划分为多个层级, 每个层级之间参与者的数量以及共享的秘密信息可以互不相同。协议充分利用高维 GHZ 态各粒子之间的纠缠特性, 使处于同一层级的所有参与者只需要进行局域测量, 之后通过合作即可恢复得到当前层级的秘密信息。并且, 每一个参与者还能够恢复得到所有低于其所在层级的秘密信息, 但无法得到高于当前层级的秘密信息, 体现了所提协议的层次性。协议在实现分层结构的同时, 还允许秘密信息的分发者在不改变某一层级所有原参与者已持有份额的情况下, 实现该层级内多个参与者的动态加入和退出, 使所提协议具有更好的灵活性和通用性。此外, 给出数学证明对所提协议的正确性进行了验证。协议的安全性分析结果表明, 所提协议能够抵御常见的截获-重发攻击、测量-重发攻击、纠缠-测量攻击和特洛伊木马攻击, 以及内部不诚实参与者的合谋攻击。

关键词: 量子秘密共享; 动态; 分层; GHZ 态

中图分类号: TN918.2

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024072

Dynamic hierarchical quantum secret sharing protocol based on high-dimensional GHZ state

CHEN Keqin, ZOU Zheng, CAI Binbin, LIN Song

College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350007, China

Abstract: Quantum secret sharing is an important research branch of quantum cryptography. A novel dynamic hierarchical quantum secret sharing protocol based on high-dimensional GHZ (Greenberger-Horne-Zeilinger) state was proposed. In the presented protocol, participants were divided into multiple layers, with the number of participants and the shared secret in each layer being allowed to differ. Based on the entanglement characteristics between particles in high-dimensional GHZ states, all participants at the same layer could cooperate to recover the secret of the

收稿日期: 2024-04-25; 修回日期: 2024-09-06

通信作者: 蔡彬彬, cbb@fjnu.edu.cn

基金项目: 国家自然科学基金 (61976053, 62171131); 福建省自然科学基金 (2022J01186, 2023J01533)

Foundation Items: The National Natural Science Foundation of China (61976053, 62171131), The Natural Science Foundation of Fujian Province (2022J01186, 2023J01533)

引用格式: 陈克勤, 邹峥, 蔡彬彬, 等. 基于高维 GHZ 态的动态分层量子秘密共享协议[J]. 网络与信息安全学报, 2024, 10(5): 134-144.

Citation Format: CHEN K Q, ZOU Z, CAI B B, et al. Dynamic hierarchical quantum secret sharing prototol based on high-dimensional GHZ state[J]. Chinese Journal of Network and Information Security, 2024, 10(5): 134-144.

current layer by performing local measurements. Moreover, each participant was able to obtain the shared secrets at lower layers, but not those at higher layers. In addition to the realization of the hierarchical structure, the proposed protocol also allowed each layer to dynamically add or delete multiple participants without changing the shares held by original participants, which provided better flexibility and generality. The correctness of the proposed protocol was verified through mathematical proof. In addition, security analysis results showed that the proposed protocol could resist intercept-and-resend attack, measure-and-resend attack, entangle-and-measure attack, Trojan horse attack, as well as collusion attacks from internal participants.

Keywords: quantum secret sharing, dynamic, hierarchical, GHZ state

0 引言

秘密共享^[1]是一种安全通信保护技术,它允许将秘密信息拆分成多个份额分发给各个参与者,只有满足特定条件,如所有参与者共同合作,才能够恢复得到原始秘密信息。1999年, Hillery等^[2]将传统秘密共享的思想与量子力学原理相结合,提出了首个量子秘密共享(quantum secret sharing, QSS)协议,协议基于GHZ(greenberger-horne-zeilinger)态实现三方秘密共享。此后,基于量子特性进行的秘密共享协议研究引起人们极大的关注^[2-14]。2003年,Guo等^[4]基于非纠缠态提出多方QSS协议,协议的理论信息传输效率接近100%。2005年,Yang和Gao^[5]通过酉操作对单光子序列进行秘密信息编码,实现多方与多方之间的秘密共享。2018年,Qin等^[12]基于GHZ态提出多方QSS协议,与文献^[5]相同,协议双方均由多个参与者组成且共享同一个秘密信息,只有双方各自的所有参与者共同合作才能够恢复得到秘密信息。

2012年,Hsu等^[15]基于EPR对(Einstein-podolsky-rosen pairs)的纠缠变换^[16],提出在协议执行期间能够对参与者进行动态增加和删除的QSS协议,这类QSS协议被称为动态量子秘密共享(dynamic quantum secret sharing, DQSS)协议^[15,17-24]。与传统QSS协议中秘密信息的分发者需要在协议之初对参与者的人数进行确定相比,DQSS的提出增加了协议设计的灵活性。2017年,Qin等^[18]基于高维GHZ态提出新的DQSS协议,协议在同一更新周期内可增加或删除多个参与者,且该过程可由某一指定参与者代替发送方执行。Yang等^[19]指出文献^[18]提出的协议虽然能够抵御窃听攻击,但是协议中参与者的不诚实行为(如参与者在退出时提交了伪造的份额)将影

响协议的正常进行。为了能够对参与者的诚实性进行检验,其在文献^[18]的工作基础上增加了验证功能。

在上述QSS协议中,所有参与者进行秘密信息恢复时仅具有相同的权利,每个参与者的地位都是平等的。然而,在某些情况下需要对协议中参与者的权利进行划分,意味着对秘密信息进行恢复的能力不同,为此提出了分层量子秘密共享(hierarchical quantum secret sharing, HQSS)协议^[25-32]。2010年,Wang等^[25]基于六粒子簇态提出HQSS协议,协议中高层级的参与者进行秘密信息恢复时需要合作的参与者人数小于低层级参与者需要的合作人数,即拥有更大的权利。文献^[25-28]基于多种纠缠态设计各种HQSS协议,这些协议仅允许各层共享同一秘密信息。然而在一些应用场景中人们希望各层级拥有不同的秘密信息,如某公司董事需要与各经理分享与生产经营相关的高度敏感信息,而与工人分享工作时间表。在Qin等^[29]基于高维纠缠态设计的HQSS协议中,每个参与者都被分配到多个层级中的某一层,每一层级拥有不同的秘密信息。协议的层次性体现在高层级的参与者能够恢复得到其所在层以及所有更低层级的秘密信息,而低层级的参与者无法恢复得到更高层级的秘密信息。但协议是静态的,未能实现参与者的增加和删除。为了满足一些应用场景对协议动态性的需要,如公司需要对员工进行录用或开除、升职或降职,本文基于高维GHZ态提出一种动态分层量子秘密共享(dynamic hierarchical quantum secret sharing, DHQSS)协议。协议将每个参与者分配到某一层级,各层级参与者的数量以及共享的秘密信息可以互不相同,且每一层的参与者在恢复本层秘密信息的同时还能够得到所有更低层级的秘密信

息, 而得不到高于该层级的秘密信息。与其他 HQSS 协议相比, 本文所提协议具有以下优点。

1) 允许每一层在不改变该层参与者已持有份额的情况下同时实现多个参与者的增加或删除, 具有较好的灵活性。

2) 秘密的恢复仅要求各层参与者具备单粒子测量的能力, 提高协议的实用性和高效性。

3) 基于高维 GHZ 态的性质设计安全验证机制, 保证量子资源传输过程的安全性的同时实现参与者诚实性验证。

1 预备知识

1.1 量子秘密共享

定义 1 QSS 协议基于量子力学原理进行设计, 实现将秘密信息拆分成多个份额分发给每个参与者, 只有合法的授权参与者集合才能够恢复秘密。QSS 协议的算法定义可以概括为以下几个阶段和步骤。

1) 初始化阶段

输入: 参与者集合 $P = \{P_1, \dots, P_n\}$, 秘密信息 S 。

输出: 参与者的份额集合 $\sigma = \{\sigma_1, \dots, \sigma_n\}$ 。

操作: 分发者基于秘密信息 S 以及协议操作为每个参与者选择份额 σ_i 。

2) 分发阶段

输入: 编码后的经典信息或量子态。

输出: 每个参与者接收的经典信息或量子态。

操作: 分发者将编码后的秘密信息或量子态发送给所有参与者。

3) 恢复阶段

输入: 来自授权参与者集合的份额。

输出: 秘密信息 S 。

操作: 授权参与者集合按照协议规定的操作通过合作恢复秘密信息 S 。

一个完善的 QSS 协议需要满足以下性质。

1) 协议正确性^[33]: 对于一个合法的授权参与者集合 $A \subseteq \{P_1, \dots, P_n\}$, A 中的参与者通过合作, 基于他们的份额能够恢复得到秘密信息 S 。

2) 协议安全性: 对于任何未授权的参与者

集合 $B \subseteq \{P_1, \dots, P_n\}$, 通过合作并不能为他们提供关于秘密信息 S 的任何信息。

1.2 d 维 GHZ 态

在 d 维 Hilbert 空间中, Z 基和 X 基的定义如下。

$$\begin{aligned} |Z_j\rangle &= \{|j\rangle, j = 0, 1, \dots, d-1\} \\ |X_j\rangle &= \{|J_j\rangle, j = 0, 1, \dots, d-1\} \end{aligned} \quad (1)$$

其中, $|J_j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} |k\rangle$, $\omega = e^{\frac{2\pi i}{d}}$ 。对任意 $j, k \in \{0, 1, \dots, d-1\}$ 有 $|\langle Z_j | X_k \rangle| = \frac{1}{\sqrt{d}}$, 因此 Z 基

和 X 基被认为是一组共轭基, 这意味着使用 $Z(X)$ 基对一个 $X(Z)$ 基量子态进行测量, 将得到完全随机的结果, 只有选择了相同的测量基才能够正确识别量子态。

d 维 GHZ 态表示为

$$|\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n} \quad (2)$$

使用 X 基对 $|\varphi\rangle$ 中的每个粒子进行测量, 测量结果表示为 $e_1, e_2, \dots, e_n \in \{0, 1, \dots, d-1\}$, 则有

$$e_1 + e_2 + \dots + e_n = 0 \quad (3)$$

此处及后文的“+”都表示模 d 和运算。

1.3 受控非门(CNOT 门, Control-NOT gate)

对于两个 d 维量子态 $|i\rangle, |j\rangle$, d 维 CNOT 门^[34]定义如下。

$$\text{CNOT}(|i\rangle, |j\rangle) = (|i\rangle, |i+j\rangle) \quad (4)$$

其中, $|i\rangle$ 作为控制比特, $|j\rangle$ 作为目标比特。

2 高维 GHZ 态的 DHQSS 协议

2.1 DHQSS 协议

协议将 $N = \sum_{i=1}^m n_i$ 个参与者分为 m 层, 同一层级的所有参与者共享一个 n 比特秘密信息。以第 i 层为例, 假设该层共有 n_i 个参与者 $\{\text{Bob}_{i,1}, \text{Bob}_{i,2}, \dots, \text{Bob}_{i,n_i}\}$, 发送者 Alice 想要发送给该层的秘密信息为 $S_i = s_{i,1} s_{i,2} \dots s_{i,n}$, 只有第 i 层的所有参与者共同合作才能够恢复得到 S_i , 其中 $s_{i,j} \in \{0, 1\}$, $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$ 。此外, 第 i 层的所有参与者还能够恢复得到所有低于 i

层, 即 $(i+1) \sim m$ 层 (协议以第一层为最高层、第 m 层为最低层) 的秘密信息。协议的具体步骤如下。

1) Alice 首先制备 $n+h$ 个 d ($d=2^m$) 维 GHZ 态 $|\varphi_1\rangle = \dots = |\varphi_{n+h}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n_i+1}$, 并计算 $u_{i,1} = \sum_{g=i}^m 2^{g-1} \cdot s_{g,1}, \dots, u_{i,n} = \sum_{g=i}^m 2^{g-1} \cdot s_{g,n}$ 。

2) Alice 将由每个 GHZ 态第 y 个粒子组成的粒子序列 Q_y ($y=1, 2, \dots, n_i$) 发送给对应的参与者 $\text{Bob}_{i,y}$, 并保留每个 GHZ 态的最后一个粒子。

3) 确定每个参与者都收到各自的粒子序列后, Alice 随机选择 $(h_1 + h_2) (< h)$ 个位置的粒子, 要求该层级的所有参与者使用 Z 基对 h_1 个指定位置的粒子进行测量, 使用 X 基对另外 h_2 个指定位置的粒子进行测量, 并公布各自的测量结果 (假设 Alice 选择了每个 GHZ 态的前 $h_1 + h_2$ 个粒子, $\text{Bob}_{i,y}$ 对应的测量结果为 $(b_{y,1}, \dots, b_{y,h_1}, b_{y,h_1+1}, \dots, b_{y,h_1+h_2})$ 。

4) Alice 使用相应的基对这 $h_1 + h_2$ 个位置的粒子进行测量, 得到测量结果 $a_1, \dots, a_{h_1+h_2}$ 。根据每个参与者公布的测量结果, Alice 检测是否满足

$$\begin{cases} b_{1,j} = b_{2,j} = \dots = b_{n_i,j} = a_j, 1 < j \leq h_1 \\ b_{1,j} + \dots + b_{n_i,j} + a_j = 0, h_1 < j \leq h_1 + h_2 \end{cases} \quad (5)$$

若检查结果的错误率超过了某一阈值, Alice 终止协议。否则, 协议继续。

5) 每个参与者使用 X 基对剩余的粒子进行测量, 并在测量完成后通知 Alice, n_i 个参与者的测量结果表示为 $b_{1,h_1+h_2+1}, \dots, b_{1,n+h}; \dots; b_{n_i,h_1+h_2+1}, \dots, b_{n_i,n+h}$ 。

6) 确定每个参与者都完成了各自的测量后, Alice 使用 X 基对剩余的粒子进行测量, 得到测量结果 $a_{h_1+h_2+1}, \dots, a_{n+h}$ 。随后, Alice 选择 n 个测量结果 (假设 Alice 选择了 $a_{h_1+h_2+1}, \dots, a_{h_1+h_2+n}$), 基于自己测量结果以及要发送的秘密信息计算公开值 $K_1 = a_{h_1+h_2+1} + u_{i,1}, \dots, K_n = a_{h_1+h_2+n} + u_{i,n}$, 并向第 i 层的所有参与者公布 $\{K_1, K_2, \dots, K_n\}$ 。

7) 当第 i 层的所有参与者通过合作, 共享各自的测量结果后, 每个参与者都能够得到 $u_{i,1}, u_{i,2}, \dots, u_{i,n}$ 的值。之后, 基于式 (6) 计算得到第 p 层秘密信息 S_p 的第 r 个比特 $s_{p,r}$ ($i \leq p \leq m, 1 \leq r \leq n$)。最终, 第 i 层的每个参与者都能够恢复得到秘密信息 $S_i, S_{i+1}, \dots, S_m$ 。

$$s_{p,r} = \frac{1}{2^{p-1}} \left(\sum_{g=i}^m 2^{g-1} * s_{g,r} - \sum_{g=p+1}^m 2^{g-1} * s_{g,r} \right) \quad (6)$$

2.2 新的参与者加入协议

假设新的参与者 Charlie 想要加入第 i 层的 n_i 个参与者 $\{\text{Bob}_{i,1}, \text{Bob}_{i,2}, \dots, \text{Bob}_{i,n_i}\}$, 该过程需要分为两种情况进行考虑。

1) Charlie 在第 i 层参与者对粒子进行测量前加入协议。此时, Alice 制备 $n+h$ 个辅助粒子 $|0\rangle$, 通过 CNOT 门操作 (Alice 的粒子作为控制比特, 辅助粒子 $|0\rangle$ 作为目标比特) 将系统的状态变为 $|\varphi_1'\rangle = \dots = |\varphi_n'\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n_i+2}$ 。

Alice 将辅助粒子组成的粒子序列 Q_C 发送给 Charlie, 之后的步骤与原协议相同。此时, 只有 $\{\text{Bob}_{i,1}, \dots, \text{Bob}_{i,n_i}, \text{Charlie}\}$ 合作才能够恢复得到 $S_i, S_{i+1}, \dots, S_m$ 。

2) Charlie 在第 i 层参与者对粒子进行测量后加入协议。此时, Alice 选择 n 个随机数小于等于 $v_1, v_2, \dots, v_n$ ($0 \leq v_1, v_2, \dots, v_n \leq d-1$), 制备 n 个 X 基量子态 $|X_{v_1}\rangle, \dots, |X_{v_n}\rangle$ 。之后, Alice 随机在 X 基和 Z 基下制备一些诱骗粒子, 将诱骗粒子插入 $|X_{v_1}\rangle, \dots, |X_{v_n}\rangle$ 中得到序列 $Q_{C'}$ 。Alice 记录每个诱骗粒子的初始状态以及插入位置后, 将 $Q_{C'}$ 发送给 Charlie。确定 Charlie 收到 $Q_{C'}$ 后, Alice 告知 Charlie 每个诱骗粒子在 $Q_{C'}$ 中的位置以及对应的测量基, 要求 Charlie 使用相应的测量基对诱骗粒子进行测量, 并公布测量结果。Alice 对比测量结果, 若错误率超过了一定的阈值, 二者重新开始上述过程。否则, Charlie 使用 X 基对得到的 n 个粒子进行测量。Alice 在 2.1 节所述的步骤 6) 中计算 $K_1 = a_{h_1+h_2+1} + u_{i,1} - v_1, \dots, K_n = a_{h_1+h_2+n} + u_{i,n} - v_n$ (此处以及后文的 “-” 都表示模 d 减运算)。当 Alice 公布计算结果 $\{K_1, K_2, \dots, K_n\}$ 后, 通

过合作 $\{\text{Bob}_{i,1}, \dots, \text{Bob}_{i,n_i}, \text{Charlie}\}$ 可以恢复秘密信息 $S_i, S_{i+1}, \dots, S_m$, 即实现了 Charlie 的加入。

2.3 原参与者加退出协议

不失一般性, 假设第 i 层参与者 $\text{Bob}_{i,1}$ 想要退出协议, 该过程同样需要分为两种情况讨论。

1) 第 i 层参与者 $\text{Bob}_{i,1}$ 对粒子进行测量前退出协议。此时, $\text{Bob}_{i,1}$ 需要使用 X 基对所有粒子进行测量, 并公布测量结果。随后, Alice 随机选择 $k (k < h - h_1 - h_2)$ 个位置的粒子 (假设 Alice 选择了最后 k 个粒子), 要求其他 $n_i - 1$ 个参与者使用 X 基对这 k 个位置的粒子进行测量, 并公布各自的测量结果。Alice 同样使用 X 基对这 k 个位置的粒子进行测量后, 检查测量结果是否满足

$$b_{1,j} + \dots + b_{n_i,j} + a_j = 0, n + h + 1 - k \leq j \leq n + h \quad (7)$$

通过上述步骤, 即可确定 $\text{Bob}_{i,1}$ 测量结果的真实性。若发现 $\text{Bob}_{i,1}$ 为不诚实参与者, Alice 立即停止当前协议, 与其他参与者如 2.1 所述的步骤重新发起新的协议。若发现 $\text{Bob}_{i,1}$ 为诚实参与者, 则 Alice 进行安全检测, 即结合 $\text{Bob}_{i,1}$ 公布的测量结果, 在 2.1 节所述的步骤 4) 中检查剩余参与者指定粒子的测量结果是否满足

$$\begin{cases} b_{2,j} = b_{3,j} = \dots = b_{n_i,j} = a_j, 1 < j \leq h_1 \\ b_{1,j} + \dots + b_{n_i,j} + a_j = 0, h_1 < j \leq h_1 + h_2 \end{cases} \quad (8)$$

通过安全检测后, Alice 与其他参与者使用 X 基对各自的粒子进行测量, 当 Alice 计算并公布 $\{K_1, K_2, \dots, K_n\}$ 后, 结合 $\text{Bob}_{i,1}$ 公布的测量结果, 剩余参与者 $\{\text{Bob}_{i,2}, \dots, \text{Bob}_{i,n_i}\}$ 通过合作即可恢复得到秘密信息 $S_i, S_{i+1}, \dots, S_m$ 。

2) 在第 i 层参与者 $\text{Bob}_{i,1}$ 对粒子进行测量后退出协议。由于在此之前进行了安全检测, $\text{Bob}_{i,1}$ 只需要公布剩余 $n + h - h_1 - h_2$ 个粒子的测量结果。同样 Alice 随机选择 k 个位置的粒子, 利用情况 1) 的方法对 $\text{Bob}_{i,1}$ 公布的测量结果的真实性进行检测。确定 $\text{Bob}_{i,1}$ 公布了正确的测量结果后, Alice 计算并公布 $\{K_1, K_2, \dots, K_n\}$, 剩余的 $n_i - 1$ 个参与者不需要 $\text{Bob}_{i,1}$ 的参与即可恢复得到秘密信息 $S_i, S_{i+1}, \dots, S_m$ 。

3 协议分析

本节将对协议的正确性以及安全性进行分析。

析, 并将本文所提协议与其他 HQSS 协议进行比较分析。

3.1 正确性分析

定理 1 使用 X 基对 GHZ 态 $|\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n}$

中的每个粒子进行测量, n 个粒子的测量结果表示为 $e_1, e_2, \dots, e_n \in \{0, 1, \dots, d-1\}$, 则 $e_1 + \dots + e_n = 0$ 。

证明 Z 基和 X 基分别表示为 $|Z_j\rangle = \{|j\rangle, j = 0, 1, \dots, d-1\}$, $|X_j\rangle = \{|J_j\rangle, j = 0, 1, \dots, d-1\}$, 其中 $|J_j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} |k\rangle$ 。由 $|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{-kj} |J_k\rangle$, 其中 $\omega = e^{\frac{2\pi i}{d}}$, $|\varphi\rangle$ 在 X 基下可以表示为

$$\begin{aligned} |\varphi\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n} = \\ &= \frac{1}{\sqrt{d}} \left(\frac{1}{\sqrt{d}} \sum_{k_1=0}^{d-1} \omega^{-jk_1} |J_{k_1}\rangle \right) \dots \left(\frac{1}{\sqrt{d}} \sum_{k_n=0}^{d-1} \omega^{-jk_n} |J_{k_n}\rangle \right) = \\ &= \frac{1}{(\sqrt{d})^{n+1}} \sum_{k_1, \dots, k_n=0}^{d-1} \sum_{j=0}^{d-1} \omega^{-j(k_1 + \dots + k_n)} |J_{k_1}\rangle \dots |J_{k_n}\rangle \quad (8) \end{aligned}$$

使用 X 基对 $|\varphi\rangle$ 中的每个粒子进行测量, 测量结果表示为 $e_1, e_2, \dots, e_n$, 则有

$$\begin{aligned} |\varphi\rangle &= \frac{1}{(\sqrt{d})^{n+1}} \\ &= \sum_{k_1, \dots, k_n=0}^{d-1} \sum_{j=0}^{d-1} \omega^{-j(k_1 + \dots + k_n)} |J_{k_1}\rangle \dots |J_{k_n}\rangle = \\ &= \frac{1}{(\sqrt{d})^{n+1}} \sum_{j=0}^{d-1} \omega^{-j(e_1 + \dots + e_n)} |e_1 \dots e_n\rangle \quad (9) \end{aligned}$$

若 $e_1 + e_2 + \dots + e_n \neq 0$, 则:

$$\begin{aligned} &= \frac{1}{(\sqrt{d})^{n+1}} \sum_{j=0}^{d-1} \omega^{-j(e_1 + \dots + e_n)} = \\ &= \frac{1}{(\sqrt{d})^{n+1}} \sum_{j=0}^{d-1} e^{-\frac{2\pi i}{d} j(e_1 + \dots + e_n)} = \\ &= \frac{1}{(\sqrt{d})^{n+1}} \frac{1 - e^{-\frac{2\pi i}{d} (e_1 + \dots + e_n)d}}{1 - e^{-\frac{2\pi i}{d} (e_1 + \dots + e_n)}} = \\ &= \frac{1}{(\sqrt{d})^{n+1}} \frac{1 - 1}{1 - e^{-\frac{2\pi i}{d} (e_1 + \dots + e_n)}} = 0 \quad (10) \end{aligned}$$

若 $e_1 + e_2 + \dots + e_n = 0$, 则

$$\frac{1}{(\sqrt{d})^{n+1}} \sum_{j=0}^{d-1} \omega^{-j(e_1 + \dots + e_n)} = \frac{1}{(\sqrt{d})^{n+1}} \sum_{j=0}^{d-1} 1 = \frac{1}{(\sqrt{d})^{n-1}}$$

因此, 使用 X 基对 $|\varphi\rangle$ 中的 n 个粒子进行测量, 得到的测量结果应满足 $e_1 + \dots + e_n = 0$ 。

引理 1 协议中当 Alice 公布 $K_r^i = u_{i,r} + a_r^i$ 后, 第 i 层的参与者通过合作即可恢复得到 $u_{i,r} = K_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i$ 。

证明 由定理 1 有 $a_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i = 0$, 则 $K_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i = u_{i,r} + a_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i = u_{i,r}$ 证毕。

引理 2 当参与者 Charlie 在第 i 层参与者进行粒子测量后加入协议, Alice 计算并公布 $K_r^i = u_{i,r} + a_r^i - v_r$, 则原第 i 层的参与者需要与 Charlie 合作才能够恢复得到 $u_{i,r} = K_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i + v_r$, 其中, v_r 是 Charlie 粒子的测量结果。

证明 由定理 1 可知

$$a_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i = 0 \quad (11)$$

若原 n_i 个参与者在无 Charlie 参与的情况下进行秘密信息的恢复, 则有

$$\begin{aligned} K_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i &= u_{i,r} + a_r^i - v_r + \\ b_{1,r}^i + \dots + b_{n_i,r}^i &= u_{i,r} - v_r \end{aligned} \quad (12)$$

即原 n_i 个参与者无法恢复得到正确的 $u_{i,1}, \dots, u_{i,n}$, 从而无法对秘密信息进行恢复。当它们与 Charlie 合作时, 有

$$\begin{aligned} K_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i + v_r &= \\ u_{i,r} + a_r^i - v_r + b_{1,r}^i + \dots + b_{n_i,r}^i + v_r &= u_{i,r} \end{aligned} \quad (13)$$

证毕。

引理 3 第 i 层参与者 Bob _{$i,1$} 进行粒子测量后退出协议, Alice 计算并公布 $K_r^i = u_{i,r} + a_r^i$ 后, 第 i 层剩余参与者通过合作即可恢复得到 $u_{i,r}$ 。

证明 由定理 1 有 $a_r^i + b_{1,r}^i + \dots + b_{n_i,r}^i = 0$ 。

因此, 当 Bob _{$i,1$} 退出后, 剩余 $n_i - 1$ 个参与者基于 Bob _{$i,1$} 公布的测量结果, 有

$$\begin{aligned} K_r^i + b_{1,r}^i + b_{2,r}^i + \dots + b_{n_i,r}^i &= u_{i,r} + a_r^i + b_{1,r}^i + \\ b_{2,r}^i + \dots + b_{n_i,r}^i &= u_{i,r} \end{aligned} \quad (14)$$

证毕。

值得注意的是, 由引理 2 可以看出, 当 Charlie 加入后, 第 i 层原参与者与 Charlie 通过合

作最终恢复得到的秘密信息仍是 $S_i, S_{i+1}, \dots, S_m$, 与 Charlie 加入前的秘密信息相同, 因此所提协议满足前向安全性 (指即使长期使用的主密钥泄露也不会导致历史的会话密钥泄露)。同理, 由引理 3 可知, 当 Bob _{$i,1$} 退出后, 第 i 层剩余参与者通过合作最终恢复得到的秘密信息仍是 $S_i, S_{i+1}, \dots, S_m$, 与 Bob _{$i,1$} 退出前的秘密信息相同, 因此所提协议满足后向安全性 (指协议在密钥泄露的情况下, 不会对未来通信内容的安全性产生影响)。

3.2 安全性分析

3.2.1 外部攻击

协议中存在两个过程涉及量子态传输: Alice 将制备好的粒子序列发送给对应参与者、参与者加入时 Alice 制备新的粒子序列发送给该参与者。为了获取秘密信息, 窃听者 Eve 在粒子传输的过程中可能采取如截获-重发攻击、测量-重发攻击、纠缠-测量攻击以及特洛伊木马攻击。

1) 截获-重发攻击

在量子密码协议分析中, 截获-重发攻击指的是在秘密分发阶段, 窃听者可能截取量子信道中传输的量子比特, 并向接收者发送随机制备的其他量子比特。

在 2.1 节所述协议的步骤 2) 中, Alice 将制备好的粒子序列发送给对应的参与者。假设 Eve 截获 Alice 发送给 Bob _{i} 的粒子序列 Q_i , 并向 Bob _{i} 发送由自己随机制备的伪粒子序列 Q_i' (伪粒子序列中的每个粒子随机处于 X 基或 Z 基下的某一种状态), 企图通过对截获的粒子序列进行测量得到相关秘密信息。然而 Alice 将在随后进行的安全检测中察觉 Eve 这一行为。虽然 Q_i 中的每个粒子都是在 Z 基下进行制备的, 但 Eve 并不知道 Alice 在安全检测中会选择哪些粒子, 以及要求每个参与者使用哪些基对每个粒子进行测量, 因此 Eve 通过安全检测的概率为 $\left(\frac{1}{2} \times \frac{1}{d} + \frac{1}{2} \times \frac{1}{d}\right)^{h_1 + h_2} = \left(\frac{1}{d}\right)^{h_1 + h_2}$, 其中 h_1 和 h_2 是 Alice 要求参与者分别使用 X 基和 Z 基进行测量的粒子数。可以看出, 当 $h_1 + h_2$ 的值足够大时, Eve 通过安全检测的概率趋近于 0。

当新的参与者 Bob _{j} 加入协议时, Alice 需要

重新制备粒子序列发送给 Bob_j。若 Bob_j 在原参与者对粒子进行测量前加入协议, 由于 Alice 通过 CNOT 门操作使 Bob_j 收到的粒子与原参与者的粒子间对应形成纠缠, 因此分析过程同上, Eve 通过安全检测的概率为 $\left(\frac{1}{d}\right)^{h_1+h_2}$ 。若在原参与者对粒子进行测量后加入协议, Alice 将根据选择的 n 个随机数制备对应 X 基下的量子态, 插入诱骗粒子后发送给 Bob_j。此时, Eve 截获该粒子序列, 并向 Bob_j 发送一个随机制备的粒子序列。之后在 Alice 与 Bob_j 进行安全检测中, 检测到 Eve 存在的概率为 $1 - \left(\frac{1}{2} \times \frac{1}{d} + \frac{1}{2} \times \frac{1}{d}\right)^k = 1 - \left(\frac{1}{d}\right)^k$, 其中, k 是 Alice 插入诱骗粒子的数量, 当 k 的值足够大时, Eve 通过安全检测的概率趋近于 1。综上, 本文所提协议能够抵御第三方的截获-重发攻击。

2) 测量-重发攻击

在窃听者截获信道中的量子比特后, 先对截获的粒子进行测量, 再根据得到的测量结果发送适当的量子态给接收者。窃听者采取的这种外部攻击被称为测量-重发攻击^[35]。

假设截获了粒子序列 Q_i 后, 对 Q_i 中的每个粒子, Eve 随机使用 X 基或 Z 基进行测量, 根据测量结果制备相同的量子态后将得到的粒子序列 Q'_i 发送给 Bob_j。由于 Eve 并不知道安全检测中 Alice 会选择哪些粒子, 以及要求参与者使用哪些基对每个粒子进行测量, 若 Eve 选择了错误的测量基进行测量, 对应制备的量子态仍有 $1/d$ 的概率通过安全检测。因此, Eve 的窃听行为不被发现的概率为 $\left(\frac{1}{2} + \frac{1}{2} \times \frac{1}{d}\right)^{h_1+h_2} = \left(\frac{d+1}{2d}\right)^{h_1+h_2}$, 当 $h_1 + h_2$ 的值足够大时这个概率趋近于 0。

当新的参与者 Bob_j 加入协议时, Alice 需要重新制备粒子序列发送给 Bob_j。若 Bob_j 在原参与者进行粒子测量前加入协议, 由于 Bob_j 收到的序列 Q_j 中每个粒子都与原参与者的粒子间对应存在纠缠, 因此分析同上, Eve 通过安全检测的概率为 $\left(\frac{d+1}{2d}\right)^{h_1+h_2}$ 。若 Bob_j 在原参与者进行粒子测量后加入协议, 由于无法得到 Q_j 中诱骗粒

子的初始态以及插入位置的相关信息, Eve 通过窃听检测的概率为 $\left(\frac{1}{2} + \frac{1}{2} \times \frac{1}{d}\right)^k = \left(\frac{d+1}{2d}\right)^k$, 当 k 的值足够大时这个概率趋近于 0。综上, 本文协议能够抵御第三方的测量-重发攻击。

3) 纠缠-测量攻击

纠缠-测量攻击^[36]指的是窃听者在截获信道中的量子比特后, 经由酉操作使自己的附加粒子与截获的粒子形成纠缠。将截获的合法粒子重发给接收者后, 窃听者从自己的附加粒子中获取信息。

Alice 将制备好的粒子序列 Q_i 发送给 Bob_i, Q_i 中每个粒子的密度矩阵为

$$\rho_i = \text{tr}_{1,\dots,i-1,i+1,\dots,n_i+1} \left(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^{\otimes n_i+1} \times \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \langle j|^{\otimes n_i+1} \right) = \text{tr}_{1,\dots,i-1,i+1,\dots,n_i+1} \left(\frac{1}{d} \sum_{j=0}^{d-1} |j\rangle^{\otimes n_i+1} \times \sum_{j=0}^{d-1} \langle j|^{\otimes n_i+1} \right) = \frac{1}{d} \sum_{j=0}^{d-1} |j\rangle \langle j| = \frac{I_d}{d} \quad (15)$$

其中, I_d 是 $d \times d$ 维单位矩阵。可以看出, 每个粒子都是密度矩阵为 I_d/d 的最大混合态。

若 Eve 截获 Q_i , 通过制备辅助粒子 $|E\rangle$ 并施加酉操作 U_E , 使 $|E\rangle$ 与 Q_i 中的粒子对应形成纠缠, 这一过程可以表示为

$$\begin{cases} U_E |0\rangle |E\rangle = a_{0,0} |0\rangle |e_{0,0}\rangle + a_{0,1} |1\rangle |e_{0,1}\rangle + \dots + a_{0,d-1} |d-1\rangle |e_{0,d-1}\rangle \\ \vdots \\ U_E |d-1\rangle |E\rangle = a_{d-1,0} |0\rangle |e_{d-1,0}\rangle + a_{d-1,1} |1\rangle |e_{d-1,1}\rangle + \dots + a_{d-1,d-1} |d-1\rangle |e_{d-1,d-1}\rangle \end{cases} \quad (16)$$

其中, $|e_{ij}\rangle$ ($ij \in \{0,1,\dots,d-1\}$) 是施加了酉操作后辅助粒子的状态, 并且有

$$\begin{cases} |a_{0,0}|^2 + |a_{0,1}|^2 + \dots + |a_{0,d-1}|^2 = 1 \\ |a_{1,0}|^2 + |a_{1,1}|^2 + \dots + |a_{1,d-1}|^2 = 1 \\ \vdots \\ |a_{d-1,0}|^2 + |a_{d-1,1}|^2 + \dots + |a_{d-1,d-1}|^2 = 1 \end{cases} \quad (17)$$

Eve 为了能够隐藏自己的攻击行为, 需要满足

$$\begin{cases} a_{0,1} = a_{0,2} = \cdots = a_{0,d-1} = 0 \\ a_{1,0} = a_{1,2} = \cdots = a_{1,d-1} = 0 \\ \vdots \\ a_{d-1,0} = a_{d-1,1} = \cdots = a_{d-1,d-2} = 0 \end{cases} \quad (18)$$

因此, 对 Q_i 中的粒子施加酉操作 U_E 的最终结果可以简化为

$$\begin{cases} U_E|0\rangle|E\rangle = |0\rangle|e_{0,0}\rangle \\ U_E|1\rangle|E\rangle = |1\rangle|e_{1,1}\rangle \\ \vdots \\ U_E|d-1\rangle|E\rangle = |d-1\rangle|e_{d-1,d-1}\rangle \end{cases} \quad (19)$$

即 $U_E|j\rangle|E\rangle = |j\rangle|e_{j,j}\rangle, j \in \{0,1,\dots,d-1\}$ 。

Eve 的辅助粒子 $|E\rangle$ 的密度矩阵为

$$\begin{aligned} \rho_E &= \text{tr}_1 \left(\frac{1}{d} \sum_{j=0}^{d-1} (U_E|j\rangle|E\rangle)(\langle j|\langle E| U_E^\dagger) \right) = \\ &= \text{tr}_1 \left(\frac{1}{d} \sum_{j=0}^{d-1} (|j\rangle|e_{j,j}\rangle)(\langle j|\langle e_{j,j}|) \right) = \\ &= \frac{1}{d} \sum_{j=0}^{d-1} |e_{j,j}\rangle\langle e_{j,j}| \end{aligned} \quad (20)$$

可以看出, $|E\rangle$ 是一个完全混合态, 在不引入任何错误的情况下, Eve 对 $|E\rangle$ 的测量并不能为它带来任何有用的信息。此外, 由于 Eve 的辅助粒子与 Alice 以及各参与者的粒子间存在纠缠, 基于式 (5) 可以看出, 若与 $|E\rangle$ 纠缠的粒子在安全检测中被 Alice 选择使用 X 基测量, 只有当 $|E\rangle$ 的测量结果为 0 时才能掩盖 Eve 的存在, 因此, Eve 将以 $\left(\frac{1}{2} + \frac{1}{2} \times \frac{1}{d}\right)^{h_1+h_2} = \left(\frac{d+1}{2d}\right)^{h_1+h_2}$ 的概率通过安全检测, 而当 $h_1 + h_2$ 的值足够大时, 这个概率趋近于 0。

当新的参与者 Bob_j 加入协议时, Alice 需要重新制备粒子序列发送给 Bob_j。若 Bob_j 在原参与者进行粒子测量前加入协议, 安全分析过程同上。若 Bob_j 在原参与者进行粒子测量后加入协议, Eve 通过酉操作 U_E 使 $|E\rangle$ 与 Q_j 中的粒子间对应形成纠缠。对于 Z 基下的诱骗粒子, 由前文可知, U_E 的作用可以表示为 $U_E|j\rangle|E\rangle = |j\rangle|e_{j,j}\rangle$ 。对于 X 基下的诱骗粒子, U_E 的作用可以表示为

$$\begin{aligned} U_E|J_j\rangle|E\rangle &= U_E \left(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj}|k\rangle \right) |E\rangle = \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} U_E|k\rangle|E\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj}|k\rangle|e_{k,k}\rangle \end{aligned} \quad (21)$$

其中, $j \in \{0,1,\dots,d-1\}$ 。由于 $|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{-kj}|J_k\rangle$, 则有

$$\begin{aligned} U_E|J_j\rangle|E\rangle &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj}|k\rangle|e_{k,k}\rangle = \\ &= \frac{1}{\sqrt{d}} \left(\sum_{k=0}^{d-1} \left(\sum_{i=0}^{d-1} \omega^{k(j-i)} |J_i\rangle \right) |e_{k,k}\rangle \right) = \\ &= \frac{1}{\sqrt{d}} \left(|J_0\rangle \sum_{k=0}^{d-1} \omega^{k(j-0)} |e_{k,k}\rangle + \cdots + \right. \\ &\quad \left. |J_{d-1}\rangle \sum_{k=0}^{d-1} \omega^{k(j-(d-1))} |e_{k,k}\rangle \right) \end{aligned} \quad (22)$$

为了在安全检测中隐藏自己的攻击行为, Eve 需要满足 $\sum_{k=0}^{d-1} \omega^{k(j-i)} |e_{k,k}\rangle = 0$, 其中, $i \in \{0,1,\dots,d-1\}$ 且 $i \neq j$, 则 U_E 的作用最终可以表示为

$$\begin{cases} U_E|j\rangle|E\rangle = |j\rangle|e_{j,j}\rangle \\ U_E|J_j\rangle|E\rangle = |J_j\rangle \sum_{k=0}^{d-1} |e_{k,k}\rangle \end{cases} \quad (23)$$

可以看出, 在不引入任何错误的情况下, 无论使用什么辅助粒子, $|E\rangle$ 的测量并不能为 Eve 带来任何有用的信息。综上, 本文所提协议在面对第三方的纠缠-测量攻击时是安全的。

4) 特洛伊木马攻击

若协议中使用的量子比特是光子, 当面对第三方施加的特洛伊木马攻击^[37]时可能是不安全的。一般来说, 特洛伊木马攻击包括延迟光子攻击和不可见光子攻击。为了抵御延迟光子攻击, 协议的参与方需要具备辨别是否存在多光子信号的能力, 即判断接收到的是多光子还是单光子, 每个参与者需要在接收设备前设置一个光子数分配器 (photon number splitter, PNS), 并使用正确的基对信号进行测量。若光子速率过高, 则认为存在多光子信号, 应终止本次传输。为了抵御不可见光子攻击, 每个参与者需要在接收设备前放置一个过滤器, 滤光片只允许波长接近工作信

号的光子进入,从而防止第三方不可见光子进入协议双方的设备。

3.2.2 内部攻击

协议面临的内部攻击主要以参与者之间合谋攻击的形式出现,即多个不诚实参与者企图通过合作,获取其他诚实参与者的份额,目的是不需要诚实参与者的参与即可恢复秘密信息。这里,讨论一种极端情况下的合谋攻击。假设第 i 层 $n_i - 1$ 个参与者 $\{\text{Bob}_{i,1}, \dots, \text{Bob}_{i,k-1}, \text{Bob}_{i,k+1}, \dots, \text{Bob}_{i,n_i}\}$ 企图在没有参与的情况下进行秘密信息的恢复。为了达到这一目的,它们截获由 Alice 发往 $\text{Bob}_{i,k}$ 的粒子序列 Q_k 。由上文分析可知,当用于安全检测的粒子数 h_1 和 h_2 足够大时,不诚实参与者的任何攻击行为都将被察觉。此外,由于 Alice 保留了每个 GHZ 态的最后一个粒子,进行合谋攻击的参与者并不能够根据已有的 $n_i - 1$ 个测量结果推测出 $\text{Bob}_{i,k}$ 的测量结果。因此,本文所提协议在面对内部参与者的合谋攻击时是安全的。

3.3 比较分析

下面将给出其他 HQSS 协议^[29-30,32]与本文协议的比较,比较结果如表 1 所示。

从表 1 可以看出,文献[29]基于特殊的高维纠缠态设计 HQSS 协议,协议实现高层级参与者对本层以及所有更低层级秘密信息的访问,即层次性的体现。但协议是静态的,并未实现参与者的动态增加和删除。此外,该协议所需量子资源的特殊性将进一步增加协议的实现难度。文献[30]基于四粒子簇态的纠缠特性,实现对任意多比特量子态的分层秘密共享。但除了未实现动态性外,协议仅允许将参与者划分为有限的两个不同层级,存在一定局限性。文献[32]基于单

调张成方案(monotone span program, MSP)提出 DHQSS 协议,在满足层次性的同时实现各层级参与者的动态增加和删除。但协议并未对参与者的诚实性进行检验,参与者的不诚实行为将影响协议秘密信息的恢复。此外,该协议的实现要求参与者能够进行量子比特测量的同时具备对量子比特施加量子傅里叶变换和 Pauli 算子的能力,一定程度上增加了协议的复杂程度。

本文提出的 DHQSS 协议在多个方面进行了改进和优化。与文献[29]类似,本文协议实现了高层级参与者对所有更低层级秘密信息的访问,除此之外,还允许各层级在不改变原参与者已持有份额的情况下实现参与者的动态增加和删除,进而灵活实现参与者所处层级的升降。并且,本文在协议中增加了参与者诚实性验证机制,提高协议灵活性的同时能够保证上述功能的安全执行。此外,协议允许发送者为各层级选择不同的秘密信息,避免了对同一秘密信息的单一恢复。实现秘密信息的恢复仅要求每个参与者具备单粒子测量的能力,而不需要对量子比特施加其他操作,使得本文协议在具有更为广泛应用场景的同时提高了协议的灵活性和高效性。

4 结束语

依据高维 GHZ 态中所有粒子使用 X 基和 Z 基测量时呈现的不同性质,本文提出一种动态分层量子秘密共享协议。在本文所提协议中,每个参与者都被分配到某一层级,处于同一层级的所有参与者通过合作即可恢复得到其所在层以及更低层的秘密信息。在协议实施的过程中,只有秘密信息的分发者需要进行量子态的制备、分发以及对量子态施加 CNOT 门操作,各层级的参与者只需要具备最基本的单粒子测

表 1 其他 HQSS 协议与本文协议的比较

Table 1 The comparison among the other HQSS protocols and proposed protocol

协议	量子资源	秘密类型	参与者施加酉操作	动态增加和删除参与者	各层级的秘密信息
文献[29]	高维纠缠态	经典信息	否	否	不同
文献[30]	簇态	量子态	X, Y, Z, H 门操作	否	相同
文献[32]	量子安全直接通信	经典信息	量子傅里叶变换和 Pauli 算子	是	相同
本文	高维 GHZ 态	经典信息	否	是	不同

量能力,降低各层级参与者的操作难度。最后,本文通过截获-重发攻击、测量-重发攻击、纠缠-测量攻击、特洛伊木马攻击以及内部不诚实参与者的合谋攻击对协议进行分析,说明了本文所提协议的安全性。

参考文献:

- [1] SHAMIR A. How to share a secret[J]. Communications of the ACM. 1979, 22(11): 612.
- [2] HILLERY M, BUZEK V, BERTHIAUME A. Quantum secret sharing [J]. Physical Review A. 1999, 59(3): 1829.
- [3] TITTEL W, ZBINDEN H, GISIN N. Experimental demonstration of quantum secret sharing[J]. Physical Review A. 2001, 63(4): 1829.
- [4] GUO G P, GUO G C. Quantum secret sharing without entanglement [J]. Physics Letters A. 2003, 310(4): 247-251.
- [5] YANG F L, GAO T. Quantum secret sharing between multiparty and multiparty without entanglement[J]. Physical Review A. 2005, 72(1): 012304.
- [6] XIAO L, LONG G L, DENG F G, et al. Efficient multiparty quantum secret sharing schemes[J]. Physical Review A. 2004, 69(5): 052307.
- [7] KARLSSON A, KOASHI M, IMOTO N. Quantum entanglement for secret sharing and secret splitting[J]. Physical Review A. 1999, 59 (1): 162-168.
- [8] CLEVE R, GOTTESMAN D, LO H K. How to share a quantum secret[J]. Physical Review Letters. 1999, 83(3): 648-651.
- [9] BAI C M, LI Z H, LIU C J, et al. Quantum secret sharing using orthogonal multiqubit states[J]. Quantum Information Process. 2017, 16: 304.
- [10] MASHHADI S. General secret sharing based on quantum Fourier transform[J]. Quantum Information Process. 2019, 18: 114.
- [11] CHEN X B, DOU Z, XU G, et al. A kind of universal quantum secret sharing protocol[J]. Scientific Reports. 2017, 7: 39845.
- [12] QIN H W, TANG W K S, TSO R. Multiparty to multiparty quantum secret sharing[J]. Modern Physics Letters B. 2018, 32: 1850350.
- [13] 宋云. 基于 GHZ 态局域测量的量子秘密共享[J]. 电子学报, 2019, 47(7):1443-1448.
SONG Y. Quantum secret sharing based on GHZ states local measurements[J]. Acta Electronica Sinica, 2019,47(7):1443-1448.
- [14] BAI C M, ZHANG S, LIU L. Quantum secret sharing for a class of special hypergraph access structures[J]. Quantum Information Process. 2022, 21: 119.
- [15] HSU J L, CHONG S K, HWANG T, et al. Dynamic quantum secret sharing[J]. Quantum Information Process.2013, 12: 331.
- [16] ZUKOWSKI M, ZEILINGER A. "Event-Ready-Detectors" Bell experiment via entanglement swapping[J]. Physical Review Letters.1993, 71(26): 4287-4290.
- [17] LIAO C H, YANG C W, HWANG T, et al. Dynamic quantum secret sharing protocol based on GHZ state[J]. Quantum Information Process. 2014, 13: 1907.
- [18] QIN H W, DAI Y. Dynamic quantum secret sharing by using d-dimensional GHZ state[J]. Quantum Information Process. 2017, 16:64.
- [19] YANG C W, TSAI C W. Participant attack and improving dynamic quantum secret sharing using d-dimensional GHZ state[J]. Modern Physics Letters A. 2020, 35: 2050024.
- [20] DU Y T, BAO W S. Dynamic quantum secret sharing protocol based on two-particle transform of Bell state[J]. Chinese Physics B. 2018, 27: 080304.
- [21] SONG Y, LI Z H, LI Y M. A dynamic multiparty quantum direct secret sharing based on generalized GHZ states[J]. Quantum Information Process. 2018, 17: 244.
- [22] YANG C W, TSAI C W. Efficient and secure dynamic quantum secret sharing protocol based on Bell states[J]. Quantum Information Process. 2020, 19: 162.
- [23] LI F, CHEN T, ZHU S. Dynamic (t, n) threshold quantum secret sharing based on d-dimensional Bell state[J]. Physica A: Statistical Mechanics and its Applications. 2022, 606: 128122.
- [24] 宋秀丽, 李闯. 基于非局域正交积态的动态量子秘密共享方案[J]. 电子与信息学报, 2024, 46:3.
SONG X L, LI C. Dynamic quantum secret sharing scheme based on nonlocal orthogonal product states[J]. Journal of Electronic & Information Technology, 2024, 46:3.
- [25] WANG X W, ZHANG D Y, TANG S Q, et al. Hierarchical quantum information splitting with six-photon cluster states[J]. International Journal of Theoretical Physics. 2010, 49: 2691-2697.
- [26] SHUKLA C, PATHAK A. Hierarchical quantum communication[J]. Physics Letters A. 2013, 377(19): 1337-1344.
- [27] XU G, WANG C, YANG Y X. Hierarchical quantum information splitting of an arbitrary two-qubit state via the cluster state[J]. Quantum Information Process. 2014, 13: 43-57.
- [28] ZHA X W, MIAO N, WANG H F. Hierarchical quantum information splitting of an arbitrary two-qubit using a single quantum resource[J]. International Journal of Theoretical Physics. 2019, 58: 2428.
- [29] QIN H W, TANG W K S, TSO R. Hierarchical quantum secret sharing based on special high-dimensional entangled state[J]. IEEE Journal of Selected Topics in Quantum Electronics. 2020, 26:1-6.
- [30] TANG J, MA S, LI Q. Universal hierarchical quantum information splitting schemes of an arbitrary multi-qubit state[J]. International Journal of Theoretical Physics. 2022, 61: 209.
- [31] LAI H, PIEPRZYK J, PAN L. Dynamic hierarchical quantum secret sharing based on the multiscale entanglement renormalization ansatz[J]. Physical Review A. 2022, 106(5): 052303.
- [32] LI F, CHEN T, ZHU H, et al. Dynamic hierarchical quantum secret sharing with general access structure[J]. Quantum Information Process. 2023, 22: 320.
- [33] 贾恒越, 武霞, 张可佳, 等. 动态分等级量子比特共享协议[J]. 网络与信息安全学报, 2016, 2(12): 12-18.
JIA H Y, WU X, ZHANG K J, et al. Dynamic hierarchical quantum information sharing protocol[J]. Chinese Journal of Network and In-

formation Security. 2016, 2(12): 12-18.

[34] NIELSEN M, CHUANG I. Quantum computation and quantum Information[M]. Cambridge: Cambridge University Press. 2011: 177.

[35] 温巧燕, 秦素娟, 高飞. 量子密码协议安全性分析[J]. 密码学报, 2014, 1(2):200-210.

WEN Q Y, QIN S J, GAO F. Cryptanalysis of quantum cryptographic protocols[J]. Journal of Cryptologic Research. 2014, 1(2): 200-210.

[36] ZHANG Z J, MAN Z X. Multiparty quantum secret sharing of classical messages based on entanglement swapping[J]. Physical Review A. 2005,72: 022303.

[37] YANG Y G, SUN S J, ZHAO Q Q. Trojan-horse attacks on quantum key distribution with classical Bob[J]. Quantum Information Process. 2015, 14: 681-686.

[作者简介]



陈克勤 (1998-), 男, 福建南平人, 福建师范大学硕士生, 主要研究方向为量子密码。



邹峥 (1984-), 女, 湖南娄底人, 福建师范大学讲师, 主要研究方向为图像处理、深度学习。



蔡彬彬 (1992-), 男, 福建厦门人, 福建师范大学讲师, 主要研究方向为量子信息与计算、密码分析。



林崧 (1979-), 男, 福建福清人, 福建师范大学教授、博士生导师, 主要研究方向为量子信息与计算、信息安全。