

量子秘密共享研究进展与展望

廖骏, 黄磊, 费焯迎

(湖南大学信息科学与工程学院, 湖南 长沙 410082)

摘要: 在量子秘密共享 (quantum secret sharing, QSS) 中, 秘密的分发者将秘密信息编码在量子态上发送给参与者, 参与者通过协作才能恢复加密信息。基于量子力学的基本原理, QSS在理论层面具备实现无条件安全秘密共享的潜力, 这一特性使其成为学术界和产业界的研究热点。为系统梳理QSS的研究脉络与发展趋势, 对QSS研究工作进行了全面调研与深入分析。在调研过程中, 将QSS分为离散变量和连续变量两大类。首先对这两类QSS的发展历程展开详细阐述, 系统总结各协议在量子态类型、共享秘密类别、门限设定方式及验证方法等方面的关键特征。在此基础上, 结合未来实际应用需求, 对QSS的发展方向进行前瞻性探讨。未来的QSS技术不仅需要在实际应用中尽可能逼近理论层面的无条件安全性, 还需具备便捷高效的实施特性以提升可行性, 同时要满足大规模量子网络构建对规模性的要求。此外, 高实用性 (适应多样化实际需求)、低耦合普适性 (模块化设计以增强系统灵活性) 及跨领域拓展性 (与其他技术领域融合) 也将成为重要发展方向。在技术实现层面, 当前QSS仍面临诸多挑战, 如具备灵活性与通用性的QSS方案相对匮乏、计算和通信资源开销较大、缺乏具备兼容性和通用性的秘密分割与重构算法。这些技术瓶颈亟待突破, 以推动QSS从理论研究向实际应用的转化。

关键词: 量子通信; 量子秘密共享; 纠缠态; 相干态

中图分类号: TN918.1

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025039

Progress and prospect of quantum secret sharing

LIAO Qin, HUANG Lei, FEI Zhuoying

College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

Abstract: In quantum secret sharing (QSS), secret information was encoded onto quantum states by a secret distributor and distributed to participants, where decoding could only be achieved through cooperative efforts. Based on the fundamental principles of quantum mechanics, QSS was theoretically recognized to possess the potential for unconditional security, which established its status as a research hotspot in both academic and industrial communities. To systematically map the research lineage and developmental trends of QSS, comprehensive investigations and in-depth analyses of QSS studies were conducted. Throughout the research process, QSS schemes were categorized into two primary classes: discrete variable and continuous variable. The evolutionary trajectories of these two

收稿日期: 2025-01-13; 修回日期: 2025-03-17

基金项目: 国家自然科学基金 (62101180); 湖南省重点研发计划 (2025QK3011)

Foundation Items: The National Natural Science Foundation of China (62101180), The Key Research and Development Program of Hunan Province (2025QK3011)

引用格式: 廖骏, 黄磊, 费焯迎. 量子秘密共享研究进展与展望[J]. 网络与信息安全学报, 2025, 11(4): 1-14.

Citation Format: LIAO Q, HUANG L, FEI Z Y. Progress and prospect of quantum secret sharing[J]. Chinese Journal of Network and Information Security, 2025, 11(4): 1-14.

categories were elaborated in detail, with key features—including types of quantum states, categories of secrets, threshold configurations, and verification methodologies—systematically summarized and compared across protocols. Building on this foundation, forward-looking discussions regarding future development directions of QSS were proposed, aligned with practical application requirements. It was concluded that future QSS technologies should not only approach theoretical unconditional security in real-world implementations but also exhibit high operational efficiency to enhance feasibility while meeting scalability demands for large-scale quantum network construction. Furthermore, high practicality (adapting to diverse application scenarios), low-coupling universality (enabling modular design for improved flexibility), and cross-domain extensibility (integration with other technological fields) were identified as critical developmental priorities. In addition, technical challenges related to the practical implementation of QSS were systematically examined. It was recognized that a scarcity of QSS schemes integrating both flexibility and universality persists. Other major challenges included high computational and communication overhead, as well as the absence of compatible and universal algorithms for secret splitting and reconstruction.

Keywords: quantum communications, quantum secret sharing, entangled state, coherent state

0 引言

秘密共享^[1]是信息安全领域的关键技术之一,其核心在于将敏感信息分割成若干份,并分散存储于多个参与者处,以确保只有当参与者满足预设条件(如达到指定数量、符合特定权限组合等)时,才能通过协同合作解密并还原完整信息。秘密共享的目标是保护数据的隐私性和完整性,即使在某些参与者不可信的情况下仍能实现这一目标。秘密共享技术具有丰富的应用场景,涵盖通信、数据存储、金融、医疗保健等领域。在秘密共享方案中,角色可以分为分发者和参与者两类。分发者负责将原始秘密分割成若干份额(Share)并分发给参与者,确保每个参与者仅持有部分信息而无法单独还原完整秘密。唯有满足指定条件(如多个参与者协作或达到特定阈值)时,这些份额才能被重新组合以恢复原始秘密^[2]。1979年,Shamir^[3]和Blakley^[4]分别提出了经典的门限秘密共享协议。在此类协议中,分发者将秘密分割为 n 个份额并分发给 n 个参与者,满足以下特性:任意 k 个参与者合作即可恢复秘密,而任意少于 k 个的参与者无法获取关于秘密的任何信息。这种方案被称为 (k,n) 门限秘密共享。

经典秘密共享的安全性通常依赖离散对数问题与多项式插值的计算复杂度。这类方案通过数学难题的设计,确保攻击者无法在有限时间内通过计算逆向推导出原始秘密^[5-7]。然而,量子计算的突破对传统密码学假设构成威胁。随着量子计算机的研发与量子算法的优化,原本在经典计

算模型中难以解决的离散对数问题可能被量子算法高效破解^[8-10]。例如,Shor算法^[11]已被证明能够在量子计算机上快速求解离散对数问题,这直接动摇了经典秘密共享方案的理论安全基础。因此,在量子计算时代,经典秘密共享的安全性亟须增强。

在上述背景下,量子秘密共享(quantum secret sharing, QSS)被提出^[12-13]。QSS依托量子力学原理构建安全框架,具备理论层面的无条件安全性。此外,QSS不仅能满足多方参与的量子通信需求,还能有效解决传统方案中不可信参与者带来的安全隐患,因此自提出以来便迅速成为学术界和产业界关注的焦点,相关研究持续升温。

根据密钥编码所依赖的物理量类型,QSS协议可分为离散变量量子秘密共享(discrete-variable quantum secret sharing, DVQSS)和连续变量量子秘密共享(continuous-variable quantum secret sharing, CVQSS)两大类。DVQSS将密钥信息编码在本征值呈离散分布的物理观测量上,如单光子的偏振态;而CVQSS将密钥信息编码在本征值呈连续变化的物理观测量上,如光场的正交分量。在发展历程上,DVQSS率先问世。DVQSS凭借清晰的理论架构和可验证性,一经提出便引发学界的广泛研究。目前,DVQSS已建立完备的安全性证明体系,并通过大量实验验证了其可行性与可靠性。相较之下,CVQSS虽起步较晚,但其凭借理论安全码率更高、实际探测成本低廉,以及与经典光通信系统天然兼容等

显著优势,近年来在学术研究与技术开发领域实现快速突破,成为量子密码学领域的新兴研究热点。后续章节将分别围绕DVQSS与CVQSS的技术演进、核心突破及应用拓展展开深入探讨。

1 量子秘密共享概述

在QSS领域,可借助多种量子态实现信息安全分发,常见的包括纠缠态、单光子、相干态和热源等。其中,纠缠态^[14-15]体现了两个或多个粒子间的非局域关联特性,是QSS研究中应用广泛的量子态;单光子^[16-17]作为光的量子化最小单元,其偏振方向常被用作离散变量的编码载体;相干态^[18-19]属于连续谱量子态,其在相空间中的正交分量可以被用作连续变量的编码载体。此外,热源^[20-21]通过源的固有涨落或人为设计,使物理参数(如强度)产生不可预测的波动;热太赫兹源^[22-23]凭借高可用带宽优势,在短距离高速无线通信与卫星通信场景中展现出独特价值。

由于纠缠态粒子间的强关联性能够实现高效的信息分割,早期QSS方案多以纠缠态为基础构建。然而,纠缠态在实际制备过程中面临技术挑战,且随着参与者数量的增加,需要更高维度的纠缠资源支持。这导致早期基于纠缠态的QSS实验研究中的参与者规模普遍受限。为突破技术瓶颈、扩大系统容量,研究人员探索采用其他量子态实现QSS(如利用相干态和单光子等),有效推动了QSS技术向实用化方向的发展。图1直观地呈现了现有QSS方案中各类量子态的应用情况,其中标注为粗体的文献方案已通过实验验证,其余仍处于理论研究阶段。

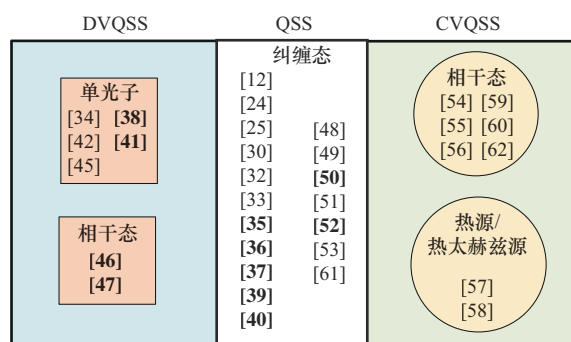


图1 现有QSS方案中各类量子态的应用情况

Figure 1 Application situations of various quantum states in the existing QSS schemes

在秘密共享体系中,待共享的秘密信息可划分为经典信息与量子信息两大类。与此同时,信息传输通道的分类更加多元化,不仅涵盖经典通道与量子通道,还包括私有通道和公共通道。其中,私有通道是经过身份验证且具备防窃听能力的信息传输路径;公共通道虽同样经过身份验证,但存在被窃听的可能性。基于上述信息载体与传输通道的不同组合,秘密共享领域逐渐形成以下3个主要研究方向。

1) 经典信息-经典通道(classical information-classical channel, CC): 共享的秘密信息为经典信息,且信息分发者与每位参与者之间均通过私有经典通道进行数据交互。

2) 经典信息-量子通道(classical information-quantum channel, CQ): 共享的秘密信息仍为经典信息,但分发者与参与者之间采用公共量子通道作为信息传输媒介。

3) 量子信息-量子通道(quantum information-quantum channel, QQ): 共享的秘密信息为量子信息,分发者与参与者之间的通信均依赖量子通道完成,且该量子通道既可以是公共通道,也可以是私有通道。

Shamir等^[3]提出的经典秘密共享方案便属于CC类别。至于CQ和QQ类别的典型示例,将在后续章节详细阐述。此外,下文还将介绍有学者借助图态这一量子资源,成功实现了上述3种秘密共享方案,为该领域的研究提供了新的思路与方法。

2 离散变量量子秘密共享

早期的QSS研究以DVQSS为主导方向,在量子态的选择与应用层面,绝大多数方案采用纠缠态或单光子作为实现DVQSS的核心载体。纠缠态可以将秘密信息分割为多个部分,天然适配于秘密拆分场景;然而,由于量子态制备技术的局限性,纠缠态的高效制备始终面临挑战。鉴于此,研究人员提出基于单光子的DVQSS方案。在这些DVQSS方案中,既有基于理论构建的方案,也有通过实验验证的方案,已形成相对完备的体系。接下来,将系统梳理DVQSS的发展脉络。

1999年, Hillery等^[12]提出了首个QSS方案,在此将其称为HBB方案。在该方案中,秘密分发者将秘密信息调制至Greenberger-Horne-

Zeilinger (GHZ) 态, 基于 GHZ 态的纠缠特性完成秘密分割, 并将分割后的量子信息分发给不同参与者。只有当所有参与者协同合作、共享各自持有的量子态信息时, 才能实现原始秘密的无损恢复。HBB 方案基于公共量子通道传输经典信息, 属于 CQ 类别, 其要求只有当所有参与者协作才能正确恢复秘密。在 HBB 方案的基础上, 研究人员持续优化技术实现路径。Karlsson 等^[24]采用两粒子纠缠态替代三粒子 GHZ 态, 显著降低了 QSS 系统的实现复杂度。此外, 该方案探讨了存在不诚实参与者与窃听者的场景下, 如何构建稳健的 QSS 协议安全防护体系。同年, Cleve 等^[25]基于量子纠错码的思想提出了首个 (k, n) 门限 QSS 方案。该方案将量子态作为共享秘密, 属于 QQ 类别, 允许部分参与者通过协作完成秘密恢复, 相较于 HBB 方案展现出更高的灵活性。Cleve 等的研究不仅实现了技术突破, 更在理论层面极大地丰富了 QSS 体系, 通过严谨推导提出多个核心定理并完成证明, 其中两项关键定理对后续研究产生了深远影响。

定理 1 若一个 (k, n) 门限 QSS 方案满足 $n > k$, 则 $(k, n-1)$ 门限 QSS 方案可以通过丢弃一个份额的方式来实现。

定理 2 传统秘密共享的 (k, n) 门限方案仅需满足 $n \geq k$ 。而 QSS 门限方案必须满足约束条件 $n < 2k$ 。这是因为若存在满足 $n \geq 2k$ 的门限方案, 便能够选取两个互不相交、各包含 k 个份额的子集, 各自重建出一个独立的量子态秘密。但这种情况与量子不可克隆定理相悖。

2000 年, Gottesman 等^[26]对具有一般访问结构的 QSS 方案展开深入研究, 并取得了一系列重要成果。该研究进一步将 QQ 类型的 QSS 方案细分为纯态 QSS 和混态 QSS。纯态 QSS 是指将秘密量子态直接编码在纯态之上, 混态 QSS 则表示秘密量子态的部分或全部编码载体为混态。同时, 他们证明了关于纯态方案的若干定理, 揭示了纯态方案所具备的一些独特性质。然而, 研究同时表明, 一般情况下的 QSS 方案多属于混态方案。例如, 在纯态方案中, 存在一个显著特性, 即授权集 (能够成功恢复秘密的份额集合) 恰好是未授权集 (无法恢复秘密

的份额集合) 的补集。这意味着在纯态方案下, 当把份额分为两组时, 必然会产生一个授权集和一个未授权集。与之形成对比的是, 在混态方案中, 有时可能会出现两个未授权集的情况。此外, 研究还证明了每一个混态方案都可以描述为丢弃了一个份额的纯态方案。研究人员进一步指出, 不可克隆定理和单调性 (如果一个参与者集合属于授权集, 那么包含该集合的更大集合同样也是授权集) 是制约 QSS 方案存在性的关键因素。这些定理的提出, 进一步完善了 QSS 的理论体系, 为后续研究提供了坚实的理论基础。

在上述 QSS 方案中, 参与者须分别从 σ_x 测量基或 σ_y 测量基中随机选择一个测量基, 这导致仅有一半的纠缠态可用于秘密共享, 该特性与量子密钥分发 (quantum key distribution, QKD) 中的 BB84 协议^[27]类似。在 BB84 协议的研究进程中, 为提升密钥分发效率, 学术界相继提出了有偏好的基选择方案 (Lo-Chau-Ardehali QKD 方案^[28]) 和基于控制键的基选择方案 (Hwang-Koh-Han QKD 方案^[29]), 这些改进方案的密钥分发效率接近 100%。受此启发, Xiao 等^[30]分别借鉴上述两种基选择策略, 成功设计出两种高效的 QSS 方案, 使 QSS 方案的效率大幅提升并趋近于 100%。此外, 传统 QSS 方案存在操作局限性, 即需要通过表格详尽列举所有可能的测量基组合及各方可能的测量结果。当参与人数较多时, 这种方式的操作流程会变得非常烦琐。为解决这一问题, Xiao 等将共享秘密信息转化为由参与者测量结果构成的二进制字符串的奇偶性表示形式, 并以此数学模型为基础, 成功地将 QSS 方案拓展至任意多方场景。

图态是一种通过图结构加以表示的多方纠缠态^[31]。在秘密共享领域中应用图态具有显著优势: 其一, 从实验角度来看, 图态是易于制备的多方纠缠态, 这为实际操作提供了便利; 其二, 图态具备集成多种不同任务的特性, 与秘密共享的应用需求高度契合; 其三, 图态能够以图形化方式呈现, 不仅可提供直观的信息流图像, 还能借助图论相关理论成果辅助证明与理解。基于上述特性, 图态成为秘密共享量子信号源的理想选

择。2008年, Markham等^[32]基于图态成功实现QSS, 并将CC、CQ和QQ这3类问题纳入统一框架体系。在常规情形下, 图态通过索引标记各顶点, 而Markham等进一步为每个顶点增设了特定标签, 顶点 v_i 的标签为 $(i, \ell_{i1}, \ell_{i2}, \ell_{i3})$ 。其中, $\ell_{ij} \in \{0, 1\}$, i 为顶点索引, ℓ_{i1}, ℓ_{i2} 用来描述经典信息的传播, ℓ_{i3} 用来描述协议的安全性。为了简化, 将 ℓ_{i3} 标签用图形表示。当 $\ell_{i3} = 1$ 时, 该顶点用□表示; 当 $\ell_{i3} = 0$ 时, 该顶点用○表示。图2(a)展示了图态对秘密共享的描述, 分发者将图态分发给4个参与者。图2(b)是当 ℓ_{12} 从顶点1移至顶点4后的图态, 此时若参与者1、2、3合作能够获得两个编码, 即 (ℓ_{22}, ℓ_{32}) , 但无法获得任何关于 (ℓ_{12}, ℓ_{42}) 编码的信息。可见, 图态可以直观地表示QSS和其中的信息流, Markham等用这种表示方式分别实现了CC、CQ和QQ3类秘密共享方案。

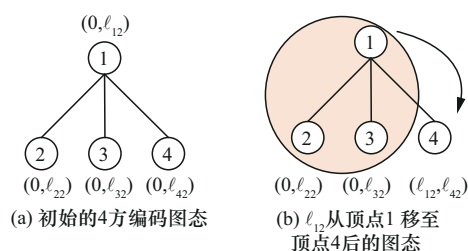


图2 4个参与者的图态表示

Figure 2 Graph representation of four participants

为提高QSS的实际安全性, Fu等^[33]提出了一种测量设备无关的QSS方案。该方案通过引入不可信方执行测量操作, 使QSS方案天然免疫所有探测器侧信道攻击, 增强了QSS系统的安全性。此外, 该方案使用传统的弱相干态实现190 km的传输距离, 远超此前利用GHZ纠缠态进行多方量子通信的预期距离, 对推动实际量子通信发展具有重要意义。之后, 针对QSS在密钥率-距离上的限制、实施技术难度和成本等问题, Li等^[34]基于单光子提出了改进的测量设备无关QSS方案。分发者和每个参与者从Z基和X基的特征态中随机选择 M 个单光子态, 并通过空分复用的量子信道将这些单光子态传输给不可信方进行测量。仿真结果表明, 该方案借助空分复用技术在3方通信场景下的传输距

离超过300 km, 在10方通信场景下的传输距离接近250 km, 突破了传统密钥率-距离的理论界限。研究还发现, 将该QSS方案应用于数字签名领域, 签名效率相较于现有协议提升超 10^7 倍, 充分展现出QSS在跨领域应用中的巨大潜力。

随着QSS理论体系的逐步成熟, 其实际应用也成为研究领域的关注焦点。2001年, Tittel等^[35]提出一种基于能量-时间纠缠的QSS实验装置。与采用三粒子纠缠GHZ态的协议不同, 该装置利用两个纠缠粒子可以模拟出第3个纠缠比特, 首次实现了基于两个以上量子比特的量子通信应用。2005年, Chen等^[36]在实验中使用超稳定高强度四光子纠缠源, 成功克服了传统多光子纠缠源强度低、稳定性差的技术瓶颈, 基于GHZ态实现了高质量QSS实验, 为后续研究奠定了关键技术基础。此后, QSS实验研究迎来了快速发展。2007年, Gaertner等^[37]成功实现了四方参与的QSS实验。2008年, Bogdanski等^[38]利用通信光纤实现了QSS实验, 展现出更高的可行性和更大的规模性。2014年, Bell等^[39]通过实验证明了基于图态的QSS。2016年, Lu等^[40]实现了(3,3)门限的QSS, 其重建量子态的保真度达到0.93。

值得注意的是, 上述QSS协议大多数都是基于纠缠态实现的, 普遍面临制备难度大、系统扩展性受限等固有缺陷。尤其是当参与人数增加时, 基于纠缠态的QSS协议的复杂度会急剧增加, 进而使得相关实验中QSS协议可支持的参与者数量极为有限。为解决参与者数量增长带来的QSS实现难题, Schmid等^[41]和Zhang等^[42]先后提出并通过实验验证了单光子顺序QSS方案, 显著提升了QSS可支持的参与者数量上限。

该方案的核心原理是, 将制备于初始极化状态的单光子按序从首位参与者传递至末位参与者, 各参与者独立对同一光子实施随机BB84型偏振旋转, 经所有参与者调制后的光子最终发送给分发者进行偏振测量。只有当所有参与者协同合作, 才能获得该光子的全部调制信息, 从而实现了量子秘密共享。由于摒弃了纠缠态的使用,

该方案大幅扩展了参与者规模，成功实现了 6 方量子秘密共享，刷新了当时的参与者数量纪录。此外，该方案所依赖的线性光学元件可基于现有光通信技术实现，具备较高的实用价值。总体而言，与基于纠缠态的 QSS 方案相比，该方案在可行性与规模性方面优势显著，引起了学术界的广泛关注与深入研究。不过，该方案在安全性方面尚存在争议^[43-44]。研究发现，攻击者可通过特洛伊木马攻击向参与者的偏振旋转装置发送多光子信号，通过测量输出信号破解偏振旋转信息。为此，Deng 等^[45]提出了改进策略，通过双光子测量与 4 项么正操作，确保了协议在密钥分发与秘密分割过程中的安全性。

尽管 QSS 在理论研究与实验验证方面已取得诸多成果，但仍缺乏能够兼顾安全性与实用性的理想协议。针对这一现状，Shen 等^[46]提出了一种基于相干态简单相位编码的 QSS 协议。该协议规避了对难以制备的纠缠资源的依赖，同时无须进行复杂的相位随机化操作，可直接依托现有技术实现。在考虑有限长效应的条件下，仿真结果显示，该方案的传输距离可超过 230 km。此外，往返式系统实验进一步证实了其可行性——在未进行强度调制和相位随机化处理的情况下，面对 35 dB 的信道损耗，该协议仍能保持 85.3 bit/s 的密钥率，这一性能优于 QSS 协议的其他实验表现。随后，Wang 等^[47]在有限脉冲相干态场景中对该协议展开实验验证，通过灵活调整脉冲强度与基选择概率，实现了 192 ~ 432 bit/s 的密钥率，为构建安全且实用的量子多方计算网络提供了全新解决方案。

3 连续变量量子秘密共享

基于连续变量 (continuous-variable, CV) 实现的 QSS 具有诸多显著优势。一方面，它能够借助现有技术完成高保真度的测量；另一方面，它与经典光通信系统能够良好兼容，并且平均每个脉冲所承载的原始信息量较为可观。鉴于这些优势，部分学者将基于纠缠态的 DVQSS 方案拓展至 CV 领域，进而提出了 CVQSS 方案。然而，这些早期的 CVQSS 方案依旧面临纠缠态制备困难的问题，同时对信道损耗的容忍度极低。为解决这些弊端，其他学者提出了基于相干态实现的

CVQSS 方案。

2002 年，Tyc 等^[48]基于光学干涉法提出了首个 CVQSS 方案，并对 $(k, 2k-1)$ 门限的 CVQSS 方案展开了深入探讨。依据上述定理 1 和定理 2，一般情形下， (k, n) 方案 (满足 $n \leq 2k-1$) 可以通过丢弃份额 $(2k-n-1)$ 的方式来实现。在 $(k, 2k-1)$ 门限的 QSS 方案中，分发者的量子态为 Φ ， k 个参与者协作才能获得态 $\Phi_{\text{out}} \in \mathcal{H}^{\otimes 2k-1}$ 。在理想情况下， Φ_{out} 是秘密态 ψ 和 $k-1$ 对纠缠态的积，纠缠态分别存在于由授权参与者组成的访问结构和由非授权参与者组成的敌对结构中。这种设计结构能够有效保障敌对结构无法获取任何关于秘密态 ψ 的信息。

Tyc 等引入了一个 CV 表示的秘密态 $|\psi\rangle$ ： $\psi(x) = \langle x | \psi \rangle$ ，其中， $|x\rangle$ 是正交位置运算符 $\hat{x}$ 的本征态。 k 个参与者的正交位置构成了一个 k 维向量空间，定义为 $\mathbf{X} \equiv (x_1, \dots, x_k)^T$ ，分发者对其进行一个特定的线性映射：

$$L: \mathbb{R}^k \rightarrow \mathbb{R}^{2k}: \mathbf{X} \mapsto L(\mathbf{x}) = [x_1, L_1(\mathbf{X}), \dots, L_{2k-1}(\mathbf{X})]^T \quad (1)$$

线性映射 L 使得 $\{x_1, L_1, \dots, L_{2k-1}\}$ 的任意一个 k 元子集的分量都是线性无关的，分发者使用线性映射 L 将 ψ 编码到纠缠态中：

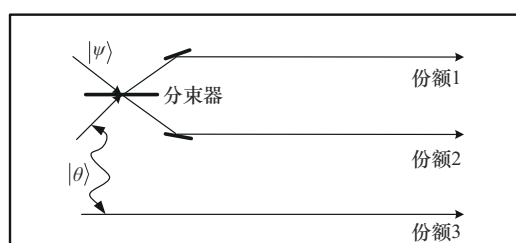
$$|\Phi\rangle = \int_{\mathbb{R}^k} \psi(x_1) |L_1(\mathbf{X})\rangle_1 \cdots |L_{2k-1}(\mathbf{X})\rangle_{2k-1} d^k \mathbf{X} \quad (2)$$

该编码使任意 k 个份额协作可以恢复 ψ ，因此实现了秘密共享。

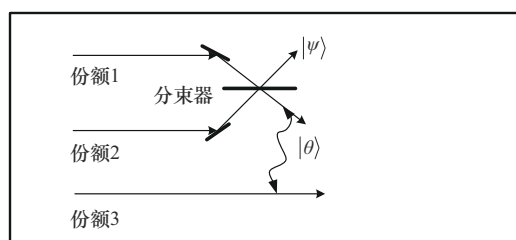
图 3 展示了 $(2,3)$ 门限 QSS 方案的编码和重建过程。其中图 3(a) 展示了秘密信息的编码过程，图 3(b) 展示了份额 1 (参与者 1) 和份额 2 (参与者 2) 协作重建秘密的过程，图 3(c) 展示了份额 1 (参与者 1) 和份额 3 (参与者 3) 协作重建秘密的过程。

2003 年，Lance 等^[49]在 Tyc 等研究基础上，提出了一种更容易实现的基于电光前馈回路的 CVQSS 改进方案。2004 年，Lance 等^[50]基于连续变量 3 方纠缠态实现了 $(2,3)$ 门限的 CVQSS 方案，并将该方案推广到适用于任意门限的秘密共

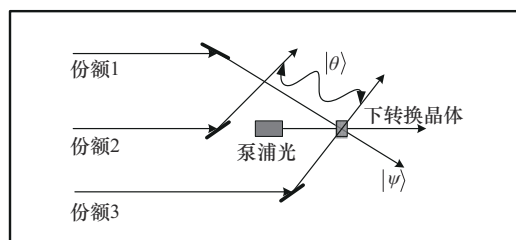
享场景。由于采用连续变量实现, 该方案在参与者数量增加时, 所需量子态保持不变。实验数据显示, 该方案在保真度 (0.73 ± 0.04)、信号传输效率和重建噪声等关键指标上均优于经典秘密共享方案, 尤其在低噪声环境下的信号传输性能表现突出。



(a) 秘密信息的编码过程



(b) 份额1和份额2协作重建秘密的过程



(c) 份额1和份额3协作重建秘密的过程

图3 (2,3)门限QSS方案的编码和重建过程

Figure 3 Encoding and reconstruction procedures for a (2,3) QSS threshold scheme

为降低QSS的实用化门槛, 一些学者致力于将DVQSS方案扩展到CV领域, 进而提出相应的CVQSS方案。Lau等^[51]将Markham等^[32]提出的QSS框架拓展至连续变量系统, 提出基于簇态的QSS方案, 并证明无论是经典信息还是量子信息, 都可以通过公共或私有通道发送簇态来实现共享。研究表明, 当簇态处于无限压缩状态时, 未达到规定门限数量的参与者无法获取任何关于秘密的信息, 从而保障了秘密的安全性; 然而, 当簇态处于实际的有限压缩状态时, 则会存在一定程度的信息泄露。因此, Lau等建议采用基准

方法来评估有限压缩情况下方案的安全性。在经典信息共享方面, 研究人员计算了从每个簇态中能够提取的安全密钥数量, 用于对秘密信息进行编码; 在量子信息共享方面, 通过估计建立高保真隐形传态信道传输秘密态所需的簇态数量, 实现量子信息的安全共享。此外, Lau等以(2,3)和(3,5)门限的QSS方案为例, 对方案的安全性展开了深入讨论, 并给出了密钥率计算公式。这种安全性分析方法具有良好的通用性, 能够推广应用于使用其他量子信号源的方案, 包括CQ和QQ类型的方案。上述基于GHZ态和簇态实现的QSS方案, 由于其量子相关特征的不平衡性, 难以实现均衡的秘密共享率。Zhou等^[52]将文献[40]提出的方案拓展到CV领域, 提出了基于多方束缚纠缠(bound entanglement, BE)态的QSS协议, 该协议能够实现均衡的秘密共享率。均衡的秘密共享率是指从两个正交分量中提取的密钥率完全平衡, 这一特性可以有效提升QSS的性能与安全性。在Zhou等提出的方案中, 分发者首先在4方BE态上调制一个秘密信息, 然后将BE态的子模式分别发送给4个参与者。得益于4个被授权的参与者之间共享的非定域且确定的BE态, 该QSS方案能够在存在窃听者和不诚实参与者的复杂环境下, 有效保护秘密信息的安全性。研究人员对使用BE态和其他纠缠态的密钥率进行了对比仿真, 结果显示基于BE态的QSS方案从两个正交分量中提取的密钥率是完全平衡的, 充分验证了基于BE态的QSS方案具有均衡的秘密共享率。Kogias等^[53]将HBB方案^[12]拓展至CV领域, 提出了一种可行的基于纠缠的CVQSS方案, 并推导了协议在渐近密钥率下的所有(k, n)门限方案实现无条件安全的充分条件。一旦满足该条件, 便能确保方案在面对窃听者的一般攻击、任意欺骗策略及不诚实参与者攻击时, 均具备无条件安全性。以(2,2)门限方案为例, 可信方Alice准备一个3方CV纠缠态, 保留其中一个模式, 同时通过单独的未知量子通道将其他模式分别发送给不可信参与者Bob和Charlie, 则Alice的测量结果 X_A 与单独的Bob的测量结果 X_B 或Charlie的测量结果 X_C 不存在关联, 但与 X_B, X_C 的组合存在关联。例如, 测量结果满足

$X_A \approx -X_B + X_C$, 则可以用 $\bar{X} = -X_B + X_C$ 描述 X_B , X_C 组合, 并用于估计 X_A 与 $\bar{X}$ 的互信息等, 从而证明只要满足:

$$V_{X_A|\bar{X}} \max \{V_{P_A|P_C}, V_{P_A|P_B}\} < e^{-2} \quad (3)$$

就能够保证上述无条件安全性。最后, 该研究还展示了如何将密钥率下界推广至 (k, n) 门限的 CVQSS 方案。

然而, 上述提及的 CVQSS 方案均依赖纠缠态实现, 在实验中难以实施, 且 Kogias 等提出的方案对信道损耗的容忍度极低。在此背景下, Grice 等^[54]提出了一种采用传统激光器和零差探测器的 CV 顺序 QSS 方案, 提高了 QSS 的安全性和实用性。

该方案如图 4 所示, 其核心思想区别于所有参与者共同调制单光子模式, 而是让每个参与者将本地制备好的相干态, 通过高度不对称分束器 (highly asymmetric beam splitter, HABS) 注入相同的时间-空间模式中。这一设计有效避免了窃听者对量子态制备过程的访问与干扰, 使方案具备抵御特洛伊木马攻击的能力。通过合理选择分束比, 能够将每个参与者引入的额外损耗控制在极低水平, 从而使该协议适用于大规模参与者的场景。

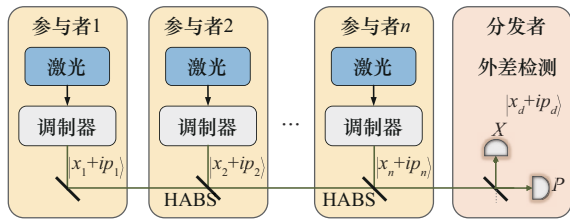


图 4 CV 顺序 QSS 方案示意图

Figure 4 Schematic diagram of CV sequential QSS scheme

Grice 等提出的 QSS 方案属于 (n, n) 门限的 CVQSS, 要求所有参与者相互协作, 才能成功恢复秘密信息。为提高方案的灵活性以更好地契合实际应用需求, Wang 等^[55]运用拉格朗日插值法对秘密的分发与恢复过程进行了优化, 进而提出一种改良版的基于弱相干态的 (t, n) 门限的 QSS 方案。相较于 (n, n) 门限 QSS 方案, 该方案显著提高了灵活性, 能够满足更多实际场景下的秘密共享需求。对于一个 (t, n) 门限 QSS 方案, 将每个合法参与者记作 $C_j, l \in \{1, 2, \dots, t\}, j \in \{1, 2, \dots, n\}$ 。

其中, l 表示其在 t 个合法参与者集合中的序号, j 表示其在 n 个参与者集合中的序号。在该方案的秘密分发流程中, 分发者首先利用原始数据生成秘密 S 。具体过程如下: 首先生成一个多项式

$$f(x) = S + Z_1 x + Z_2 x^2 + \dots + Z_{t-2} x^{t-2} + Z_{t-1} x^{t-1} \quad (4)$$

其中, $Z_1 = S \bmod x_{l_1}, Z_2 = S \bmod x_{l_2}, \dots, Z_t = S \bmod x_{l_t}$ 。 x_{l_j} 是分发者通过数据替换得到 B_j 的 $x_j, l \in \{1, 2, \dots, t\}, j \in \{1, 2, \dots, n\}$ 。然后, 通过多项式计算可以得到 $\{f(x_{l_1}), f(x_{l_2}), \dots, f(x_{l_t})\}$ 。接下来, 分发者通过泡利 (Pauli) 操作对 $f(x_{l_j})$ 进行重新编码。为防范窃听行为, 分发者需要准备一些诱饵粒子, 并将它们随机插入编码序列之中。同时, 分发者须记录每个诱饵粒子的初始状态和位置。之后, 分发者将这些将编码后的秘密份额及包含诱饵粒子的序列对应发送给每个合法参与者 C_j 。当分发者宣布每个诱饵粒子的初始插入状态和位置后, 则可以确定 C_j 的私钥为 $\{x_j, f(x_{l_j})\}$ 。最后, t 个合法参与者运用拉格朗日插值算法进行计算, 便可恢复出秘密 S 。

$$f(x) = f(x_{l_1})\psi_1 + f(x_{l_2})\psi_2 + \dots + f(x_{l_t})\psi_t = S + Z_1 x + Z_2 x^2 + \dots + Z_{t-1} x^{t-1} \quad (5)$$

$$\text{其中, } \psi_k = \prod_{l=1, l \neq k}^t \frac{x - x_{l_j}}{x_{k_j} - x_{l_j}}.$$

上述研究工作主要聚焦于 CVQSS 理论方案的提出与优化, 但在实际应用层面, 这些方案仍面临诸多亟待解决的问题。其一, 各方案要求每个参与者在本地部署激光器与调制设备, 不仅成本高昂, 且操作不便; 其二, 大量不同类型的激光器协同工作时, 信号同步问题难以攻克; 其三, 在相干探测机制下, 参与者须经不可信量子信道向分发者发送本振光 (local oscillator, LO), 使得 CVQSS 系统极易遭受 LO 漏洞攻击。为应对这些挑战, Liao 等^[56]提出一种往返式双相位调制 CVQSS 方案。在此方案中, 分发者先制备相干态并发送给参与者进行调制, 调制完成后返还分

发者执行测量。这一设计使得参与者无须在本地部署激光器，且有效解决了信号同步难题。同时，发送方可以在本地生成LO，可以抵御针对LO的各类攻击，大幅提升了CVQSS系统的实际安全性。

文献[54-56]提出的方案均采用高斯调制相干态（Gaussian modulation coherent state, GMCS）实现QSS，在一定程度上增强了CVQSS的可行性。然而，GMCS方案在实际应用层面存在调制格式复杂、对调制误差的容忍度低，须配备高稳定性、高消光比的调制器等固有限制，导致成本居高不下，尤其在大规模应用场景下更加显著。此外，随着传输速率的不断提升，现有有源调制技术难以在QSS框架下实现高速、精确的量子态制备。针对这些问题，2020年Wu等^[57]提出利用热源实现CVQSS，摆脱了对高消光比调制器的依赖，为QSS的实现提供了更便捷的路径。2021年，Liu等^[58]提出使用热太赫兹（thermal terahertz, THz）源作为信息编码载体，通过卫星间无线链路传输，验证了多参与者长距离星际THz-CVQSS方案的可行性，为星际量子通信网络的构建提供了重要参考。

相较于GMCS，离散调制相干态（discrete modulation coherent state, DMCS）在实际实验中展现出显著优势，包括制备更简单、抗干扰能力更强、远距离传输误码率更低，且传输距离更远。基于此，Liao等^[59]于2021年提出基于DMCS的QSS方案，并证明该方案在集体高斯攻击下的组合安全性，仿真结果显示其在渐进极限条件下传输距离可达100 km以上。随后，Liao等^[60]进一步提出多环离散调制CVQSS方案，通过相移键控（phase shift keying, PSK）对相干态进行不同幅度的离散调制，从而使相干态在相空间中分布于多个幅度环上，如图5所示。研究人员对2环16态和3环32态CVQSS进行了深入分析，仿真结果表明，相较于传统CVQSS方案，多环离散调制在最大参与者数量和最远传输距离上均有明显提升。此外，在调制态数目相同的情况下，与单环离散调制相比，多环离散调制可显著降低探测器分辨DMCS的错误率，有效提升了CVQSS系统的性能。

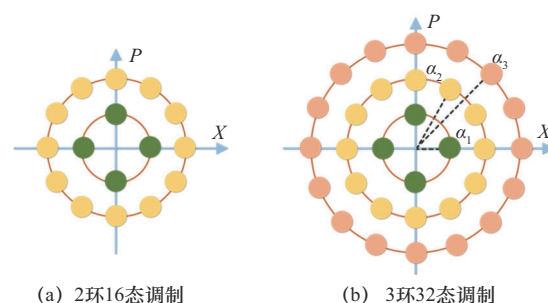


图5 多环离散调制
Figure 5 Multi-ring discrete modulation

为了提高CVQSS的实际安全性，Wu等^[61]基于CV的GHZ态提出了一种测量设备无关的CVQSS方案。在该方案中，分发者和两个参与者各自保留双模压缩态的一个模式，将另一个模式发送给不可信的第4方进行测量。基于公布的测量结果，分发者保持数据不变，参与者则对自身数据进行替换操作，使分发者和参与者之间的数据呈现GHZ态特性，即满足特定关系式： $\hat{X}_1 - \hat{X}_2 \rightarrow 0$ ， $\hat{X}_2 - \hat{X}_3 \rightarrow 0$ ， $\hat{P}_1 + \hat{P}_2 + \hat{P}_3 \rightarrow 0$ 。其中，分发者的数据为 $(\hat{X}_1, \hat{P}_1)$ ，两个参与者的数据分别为 $(\hat{X}_2, \hat{P}_2)$ 和 $(\hat{X}_3, \hat{P}_3)$ 。凭借这些基于 $\hat{P}$ 正交分量的关系式，可以实现QSS。该测量策略赋予方案抵御所有探测器侧信道攻击的能力，大幅提高了安全性。此外，研究团队对存在窃听者与不可信参与者时的方案安全性展开了论证，在安全性分析过程中，分别探讨了纠缠克隆攻击与相干攻击场景下的安全性表现。仿真结果显示，相干攻击会显著压缩最远传输距离，其攻击效果相较于纠缠克隆攻击更为突出。Liao等^[62]基于更容易实现的相干态构建了测量设备无关的CVQSS方案。与传统CVQSS相比，该方案具有更低的过噪声、更高的原始数据利用率，并且在参与者数量变化时展现出局域稳定性，这些特性使其在构建大规模量子通信网络方面极具潜力。此外，研究团队还提出3种变体方案，以适配不同类型量子通信网络的实际需求。

4 总结与展望

通过梳理QSS的发展脉络可知，QSS方案存在一些关键属性，如所采用的量子态类型、共享秘密的类别、实现的门限机制等。为便于把握QSS的发展趋势，现将相关文献中的这些关键属性汇总于表1，按DVQSS和CVQSS分类，并在

表1 QSS方案属性汇总
Table 1 Summary of QSS schemes attributes

文献	时间 (年)	QSS类型	量子态	共享秘密类型	QSS 门限	验证方法
[12]	1999	DV	纠缠态	经典信息	(2, 2)和(3, 3)	理论推导
[24]	1999	DV	纠缠态	量子态	(2, 2)	理论推导
[25]	1999	DV	纠缠态	量子态	(k, n)	理论推导
[35]	2001	DV	纠缠态	经典信息	(2, 2)	实验验证
[30]	2004	DV	纠缠态	经典信息	(k, n)	理论推导
[36]	2005	DV	纠缠态	经典信息	(2, 2)	实验验证
[41]	2005	DV	单光子	经典信息	(5, 5)	实验验证
[42]	2005	DV	单光子	经典信息	(n, n)	理论推导
[45]	2005	DV	纠缠态	量子信息	(n, n)	理论推导
[37]	2007	DV	纠缠态	经典信息	(3, 3)	实验验证
[38]	2008	DV	单光子	经典信息	(4, 4)	实验验证
[32]	2008	DV	纠缠态	均有	(n, n)、(3, 4)和(3, 5)	理论推导
[39]	2014	DV	纠缠态	均有	(3, 4)	实验验证
[33]	2015	DV	纠缠态	经典信息	(2, 2)	理论推导
[40]	2016	DV	纠缠态	量子态	(3, 3)	实验验证
[34]	2023	DV	单光子	经典信息	(n, n)	理论推导
[46]	2023	DV	相干态	经典信息	(2, 2)	实验验证
[47]	2024	DV	相干态	经典信息	(2, 2)	实验验证
[48]	2002	CV	纠缠态	量子态	(k, n)	理论推导
[49]	2003	CV	纠缠态	量子态	(2, 3)	理论推导
[50]	2004	CV	纠缠态	量子态	(2, 3)	实验验证
[51]	2013	CV	纠缠态	均有	(2, 3)和(3, 5)	理论推导
[61]	2016	CV	纠缠态	经典信息	(2, 2)	理论推导
[53]	2017	CV	纠缠态	经典信息	(k, n)	理论推导
[52]	2018	CV	纠缠态	经典信息	(3, 4)	实验验证
[54]	2019	CV	相干态	经典信息	(n, n)	理论推导
[55]	2020	CV	相干态	经典信息	(k, n)	理论推导
[57]	2020	CV	热源	经典信息	(n, n)	理论推导
[58]	2021	CV	热太赫兹源	经典信息	(n, n)	理论推导
[59]	2021	CV	相干态	经典信息	(n, n)	理论推导
[56]	2022	CV	相干态	经典信息	(n, n)	理论推导
[60]	2023	CV	相干态	经典信息	(n, n)	理论推导
[62]	2025	CV	相干态	经典信息	(n, n)	理论推导

每个类别下依据时间顺序排列各QSS方案。

总体来看，DVQSS是最早被提出的类型，QSS前期研究也以DVQSS为主；CVQSS虽提出时间较晚，但同样获得了深入研究。在量子态使用方面，QSS从早期依赖纠缠态，逐渐发展为采用更容易制备的其他量子态，有效降低了实际实现QSS的难度。共享秘密类型主要集中于经典信息，涉及量子态共享的方案相对较少。在QSS门限的实现上，可容纳的参与者数量也在逐步增加。

具体到DVQSS方案，早期多采用纠缠态作为量子载体，后续出现了基于单光子态、图态等实现的方案。DVQSS的理论体系与实验验证均较为成熟，但由于纠缠态制备困难，实验验证方案中的参与者数量普遍受限。对于CVQSS方案，使用的量子态以相干态为主，部分方案也采用纠缠态；早期研究涉及量子态秘密共享，后期则聚焦于经典信息；在QSS门限实现上，早期包含一般情况下的 (k,n) 门限方案，后期以 (n,n) 门限研究为主；目前提出的方案多为理论构想，经过实验验证的相对较少。

综上所述，当前QSS研究仍存在诸多空白与不足。例如，针对一般情况下的 (k,n) 门限QSS方案的实验验证仍较为缺乏，如何进一步提升QSS系统可容纳的参与者数量也有待深入研究。

自QSS概念被提出以来，其理论体系不断完善，安全性也逐步得到严格证明。为进一步提升QSS的可行性与拓展性，研究者相继提出一系列改进方案。通过梳理相关研究发现，QSS的发展呈现以下3个显著特点。

1) 安全性持续强化。尽管QSS基于量子力学基本原理在理论上具备无条件安全性，但受技术发展水平的限制和攻击模型的影响，实际QSS系统难以实现绝对安全。因此，降低这些因素对安全性的影响成为重要发展方向。例如，Grice等^[54]提出的QSS方案可以有效抵御特洛伊木马攻击，显著提升了系统的安全性。

2) 可行性逐步提升。为解决纠缠态实验制备困难问题，研究人员采用单光子、相干态等量子态替代纠缠态实现QSS；针对基于高斯调制相干

态的QSS方案中高稳定性、高消光比调制器导致的高成本问题（尤其在参与者规模较大时），引入热源实现QSS的方案有效降低了调制成本；此外，针对相干态QSS方案中参与者须自备激光器引发的高成本与信号同步难题，使用往返式和双相位调制实现QSS成功解决了上述问题。随着研究的深入，QSS的可行性与实用性得到了显著提高。

3) 规模不断扩展。早期QSS实验的参与者数量十分有限，而量子通信网络化已成为必然趋势，因此后续基于单光子和相干态的QSS方案不断突破参与者人数上限，为构建大规模量子通信网络奠定了坚实基础。

尽管QSS在安全性、可行性和规模方面取得了重大进展，但仍存在诸多亟待解决的问题。结合当前研究现状，未来QSS的发展趋势主要体现在以下3个方面。

1) 实用性优化。在实际应用场景中，参与者动态调整 and 不同方案整合是常见需求，而现有QSS方案往往未充分考虑这些问题，严重制约了其在动态环境中的应用。未来的QSS方案应具备动态调整功能，支持参与者灵活加入或退出，并确保系统安全性不受影响；同时，需要设计兼容性机制，实现不同QSS方案的高效整合，并在整合过程中进行严格的安全验证，避免引入新的安全隐患。此外，若能有效满足参与者与分发者角色转换等实际需求，将大幅提升QSS的实用性和推广价值。

2) 普适性增强。具备普适性的QSS系统应具备模块化、低耦合的特性。以测量设备无关的QSS方案为例，其测量设备与量子操作模块相互独立的解耦设计显著提升了系统灵活性。然而，部分传统方案依赖特定量子态实现固定门限QSS，导致模块间高度耦合，通用性受限。未来，QSS的发展应致力于降低模块间的依赖程度，如实现量子态模块的独立化，即支持任意量子态用于秘密共享，从而增强系统的健壮性，扩大其适用范围。

3) 拓展性延伸。经典秘密共享技术已广泛应用于电子投票、数字图像处理 and 生物特征识别等众多领域，相比之下，QSS目前仍主要停

留在理论研究阶段, 实际应用较少。尽管已有学者将 QSS 应用于数字签名领域并取得显著效果, 但未来 QSS 的应用潜力仍有待进一步挖掘。例如, 可探索将其应用于量子门限认证、量子安全多方计算等协议的构建, 以提升安全性和实用性, 推动 QSS 在更多现实场景中的落地应用。

在 QSS 的实际技术实现层面, 当前仍面临诸多挑战, 具体体现在以下 3 个方面。

1) 方案缺少灵活性: 目前, 大多数 QSS 方案为 (n, n) 门限方案, 这种设计在部分参与者缺席或存在恶意行为时, 会导致秘密信息无法恢复, 严重限制了方案在复杂环境下的适用性和拓展性。

2) 计算与通信资源消耗较大。现有 QSS 方案在粒子制备与测量过程中需要消耗大量计算和通信资源; 同时, 由于缺乏简洁高效的份额分配与秘密恢复机制, 整体执行成本较高。

3) 量子态秘密共享的通用性不足。在涉及量子态的 QSS 协议中, 经典信息须先转换为量子态再进行传输。然而, 目前尚未形成通用且兼容的量子态分割与重构方法, 这一技术短板极大地阻碍了相关协议的广泛应用。

参考文献:

- [1] GONG X Q, HU P, SHUM KW, et al. A zigzag-decodable ramp secret sharing scheme[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(8): 1906-1916.
- [2] KOMARGODSKI I, NAOR M, YOGEV E. Secret-sharing for NP[J]. Journal of Cryptology, 2017, 30(2): 444-469.
- [3] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.
- [4] BLAKLEY G R. Safeguarding cryptographic keys[C]//Proceedings of 1979 International Workshop on Managing Requirements Knowledge. Piscataway: IEEE Press, 1979: 313-318.
- [5] JACKSON W A, MARTIN K M. Perfect secret sharing schemes on five participants[J]. Designs, Codes and Cryptography, 1996, 9(3): 267-286.
- [6] YANG C C, CHANG T Y, HWANG M S. A (t, n) multi-secret sharing scheme[J]. Applied Mathematics and Computation, 2004, 151(2): 483-490.
- [7] HUANG W T, LANGBERG M, KLEWER J, et al. Communication efficient secret sharing[J]. IEEE Transactions on Information Theory, 2016, 62(12): 7195-7206.
- [8] MARIANTONI M, WANG H, YAMAMOTO T, et al. Implementing the quantum Von Neumann architecture with superconducting circuits[J]. Science, 2011, 334(6052): 61-65.
- [9] BARENDT R, KELLY J, MEGRANT A, et al. Superconducting quantum circuits at the surface code threshold for fault tolerance[J]. Nature, 2014, 508(7497): 500-503.
- [10] JOHNSON M W, AMIN M H, GILDERT S, et al. Quantum annealing with manufactured spins[J]. Nature, 2011, 473(7346): 194-198.
- [11] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303-332.
- [12] HILLERY M, BUŽEK V, BERTHIAUME A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3): 1829-1834.
- [13] YANG W, HUANG L, SHI R, et al. Secret sharing based on quantum Fourier transform[J]. Quantum Information Processing, 2013, 12(7): 2465-2474.
- [14] GREENBERGER D M. GHZ (Greenberger-Horne-Zeilinger) theorem and GHZ states[M]//Compendium of quantum physics. Heidelberg: Springer, 2009: 258-263.
- [15] ERHARD M, MALIK M, KRENN M, et al. Experimental greenberger-horne-zeilinger entanglement beyond qubits[J]. Nature Photonics, 2018, 12(12): 759-764.
- [16] LOUNIS B, ORRIT M. Single-photon sources[J]. Reports on Progress in Physics, 2005, 68(5): 1129-1179.
- [17] BULLER G S, COLLINS R J. Single-photon generation and detection[J]. Measurement Science and Technology, 2009, 21(1): 012002.
- [18] ZHANG W M, GILMORE R. Coherent states: theory and some applications[J]. Reviews of Modern Physics, 1990, 62(4): 867-928.
- [19] SANDERS B C. Entangled coherent states[J]. Physical Review A, 1992, 45(9): 6811-6815.
- [20] QI B, EVANS P G, GRICE W P. Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution[J]. Physical Review A, 2018, 97(1): 012317.
- [21] BAI D Y, HUANG P, MA H, et al. Passive-state preparation in continuous-variable measurement-device-independent quantum key distribution[J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2019, 52(13): 135502.
- [22] OTTAVIANI C, WOOLLEY M J, EREMENTCHOUK M, et al. Terahertz quantum cryptography[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(3): 483-495.
- [23] LIU X, ZHU C H, CHEN N, et al. Practical aspects of terahertz wireless quantum key distribution in indoor environments[J]. Quantum Information Processing, 2018, 17(11): 1-20.
- [24] KARLSSON A, KOASHI M, IMOTO N. Quantum entanglement for secret sharing and secret splitting[J]. Physical Review A, 1999, 59(1): 162-168.
- [25] CLEVE R, GOTTESMAN D, LO H K. How to share a quantum secret[J]. Physical Review Letters, 1999, 83(3): 648-651.

- [26] GOTTESMAN D. Theory of quantum secret sharing[J]. *Physical Review A*, 2000, 61(4): 042311.
- [27] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[J]. *Theoretical Computer Science*, 2014, 560: 7-11.
- [28] LO H K, CHAU H F, ARDEHALI M. Efficient quantum key distribution scheme and a proof of its unconditional security[J]. *Journal of Cryptology*, 2005, 18(2): 133-165.
- [29] HWANG W Y, KOH I G, HAN Y D. Quantum cryptography without public announcement of bases[J]. *Physics Letters A*, 1998, 244(6): 489-494.
- [30] XIAO L, LONG G L, DENG F G, et al. Efficient multi-party quantum secret sharing schemes[J]. *Physical Review A*, 2004, 69(5): 052307.
- [31] LU C Y, ZHOU X Q, GÜHNE O, et al. Experimental entanglement of six photons in graph states[J]. *Nature Physics*, 2007, 3(2): 91-95.
- [32] MARKHAM D, SANDERS B. Graph states for quantum secret sharing[J]. *Physical Review A*, 2008, 78(4): 042309.
- [33] FU Y, YIN H L, CHEN T Y, et al. Long-distance measurement-device-independent multiparty quantum communication[J]. *Physical Review Letters*, 2015, 114(9): 090501.
- [34] LI C L, FU Y, LIU W B, et al. Breaking the rate-distance limitation of measurement-device-independent quantum secret sharing[J]. *Physical Review Research*, 2023, 5(3): 033077.
- [35] TITTEL W, ZBINDEN H, GISIN N. Experimental demonstration of quantum secret sharing[J]. *Physical Review A*, 2001, 63(4): 042301.
- [36] CHEN Y, ZHANG A, ZHAO Z, et al. Experimental quantum secret sharing and third-man quantum cryptography[J]. *Physical Review Letters*, 2005, 95(20): 200502.
- [37] GAERTNER S, KURTSIEFER C, BOURENNANE M, et al. Experimental demonstration of four-party quantum secret sharing[J]. *Physical Review Letters*, 2007, 98(2): 020503.
- [38] BOGDANSKI J, RAFIEI N, BOURENNANE M. Experimental quantum secret sharing using telecommunication fiber[J]. *Physical Review A*, 2008, 78(6): 062307.
- [39] BELL B A, MARKHAM D, HERRERA-MARTÍ D A, et al. Experimental demonstration of graph-state quantum secret sharing[J]. *Nature Communications*, 2014, 5(1): 1-12.
- [40] LU H, ZHANG Z, CHEN L K, et al. Secret sharing of a quantum state[J]. *Physical Review Letters*, 2016, 117(3): 030501.
- [41] SCHMID C, TROJEK P, BOURENNANE M, et al. Experimental single qubit quantum secret sharing[J]. *Physical Review Letters*, 2005, 95(23): 230505.
- [42] ZHANG Z, LI Y, MAN Z. Multiparty quantum secret sharing[J]. *Physical Review A*, 2005, 71(4): 044301.
- [43] HE G P. Comment on experimental single qubit quantum secret sharing[J]. *Physical Review Letters*, 2007, 98(2): 028901.
- [44] HE G P, WANG Z D. Single qubit quantum secret sharing with improved security[J]. *Quantum Information & Computation*, 2010, 10(1): 28-40.
- [45] DENG F G, LI X H, LI C Y, et al. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs[J]. *Physical Review A*, 2005, 72(4): 044301.
- [46] SHEN A, CAO X Y, WANG Y, et al. Experimental quantum secret sharing based on phase encoding of coherent states[J]. *Science China Physics, Mechanics & Astronomy*, 2023, 66(6): 260311.
- [47] WANG Y Z, SUN X R, CAO X Y, et al. Experimental coherent-state quantum secret sharing with finite pulses[J]. *Physical Review Applied*, 2024, 22(4): 044018.
- [48] TYC T, SANDERS B C. How to share a continuous-variable quantum secret by optical interferometry[J]. *Physical Review A*, 2002, 65(4): 042310.
- [49] LANCE A M, SYMUL T, BOWEN W P, et al. Continuous variable (2,3) threshold quantum secret sharing schemes[J]. *New Journal of Physics*, 2003, 5(1): 4.
- [50] LANCE A, SYMUL T, BOWEN W, et al. Tripartite quantum state sharing[J]. *Physical Review Letters*, 2004, 92(17): 177903.
- [51] LAU H, WEEDBROOK C. Quantum secret sharing with continuous-variable cluster states[J]. *Physical Review A*, 2013, 88(4): 042313.
- [52] ZHOU Y, YU J, YAN Z, et al. Quantum secret sharing among four players using multipartite bound entanglement of an optical field[J]. *Physical Review Letters*, 2018, 121(15): 150502.
- [53] KOGIAS I, XIANG Y, HE Q, et al. Unconditional security of entanglement-based continuous-variable quantum secret sharing[J]. *Physical Review A*, 2017, 95(1): 012315.
- [54] GRICE W P, QI B. Quantum secret sharing using weak coherent states[J]. *Physical Review A*, 2019, 100(2): 022339.
- [55] WANG Y, JIA B, MAO Y, et al. Improving continuous variable quantum secret sharing with weak coherent states[J]. *Applied Sciences*, 2020, 10(7): 2411.
- [56] LIAO Q, LIU H, GONG Y, et al. Practical continuous-variable quantum secret sharing using plug-and-play dual-phase modulation[J]. *Optics Express*, 2022, 30(3): 3876-3892.
- [57] WU X, WANG Y, HUANG D. Passive continuous-variable quantum secret sharing using a thermal source[J]. *Physical Review A*, 2020, 101(2): 022301.
- [58] LIU C, ZHU C, LI Z, et al. Continuous-variable quantum secret sharing based on thermal terahertz sources in inter-satellite wireless links[J]. *Entropy*, 2021, 23(9): 1223.
- [59] LIAO Q, LIU H, ZHU L, et al. Quantum secret sharing using discretely modulated coherent states[J]. *Physical Review A*, 2021, 103(3): 032410.
- [60] LIAO Q, LIU X, OU B, et al. Continuous-variable quantum secret sharing based on multi-ring discrete modulation[J]. *IEEE Transactions on Communications*, 2023, 71(10): 6051-6060.
- [61] WU Y, ZHOU J, GONG X, et al. Continuous-variable

measurement-device-independent multipartite quantum communication[J]. Physical Review A, 2016, 93(2): 022325.

- [62] LIAO Q, HUANG L, FEI Z, et al. Measurement-device-independent continuous-variable quantum secret sharing[J]. Adv Quantum Technol, 2025, 8(8): 2400505.

[作者简介]



廖骥 (1990-), 男, 湖南长沙人, 博士, 湖南大学副教授, 主要研究方向为量子保密通信、量子计算和网络安全。



黄磊 (2000-), 男, 江西上饶人, 湖南大学硕士生, 主要研究方向为量子保密通信。



费焯迎 (2000-), 女, 河南许昌人, 湖南大学硕士生, 主要研究方向为量子保密通信。