专题: 量子信息处理

量子秘密共享研究现状与展望*

尹华磊 1)#† 沈建宇 2)# 陈诺 2)# 陈增兵 2)

1) (中国人民大学物理学院, 北京 100872)

2) (南京大学物理学院, 南京 210093)

(2025 年 4 月 30 日收到; 2025 年 6 月 24 日收到修改稿)

随着量子通信和量子计算的快速发展, 人们对数据隐私保护和分布式量子信息处理的需求不断增高. 量子秘密共享作为经典秘密共享的量子延伸, 借助量子力学的基本原理可以在多方之间安全地共享信息, 提供了信息安全的新范式. 作为多方安全量子通信和分布式量子计算的重要基础, 量子秘密共享一经提出便受到广泛关注. 当前, 量子秘密共享研究已经包含经典和量子的场景, 在理论与实验上不断取得新的进展. 但在实际应用中仍然面临着量子信道噪声、设备不完美及量子资源受限等诸多困难和挑战, 实用性和安全性仍然难以兼顾. 本文将简要介绍不同技术路线下量子秘密共享的研究现状, 总结近年来量子秘密共享的发展趋势, 并对其未来的发展方向进行讨论和展望.

关键词: 量子秘密共享, 量子通信, 量子纠缠, 多方量子协议

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.74.20250586

CSTR: 32037.14.aps.74.20250586

1 引 言

作为现代密码学的一个重要分支, 经典的秘密共享方案最早在 1979 年由 Shamir[1] 和 Blakley[2] 分别独立提出, 是最重要的信息安全密码协议之一. 秘密共享方案的核心思想是将共享的秘密拆分成 n 个子秘密并分发给参与者. 只有当合作的参与者人数达到授权人数 k 时, 共享的秘密才得以被恢复. 任何参与者人数小于授权人数的情况, 共享的秘密都无法被恢复, 并且无法得到有关秘密的任何信息. 此外, Shamir[1] 和 Blakley[2] 证明, 对于任意 k 和 n 的取值均存在相关的 (k,n) 门限方案. 这有效阻止了内部人员窃听导致的秘密信息泄露. 秘密共享的提出为电信系统、互联网以及分布式计算机等现代信息技术提供了可靠安全的通信.

量子密钥分发 (quantum key distribution, QKD) 是目前最接近实际应用的量子技术之一[3–5]. 随着 QKD 的设备和技术逐渐成熟, 量子通信网络用户不断增加, 多用户量子通信协议的需求开始彰显[6–10]. 利用量子资源的秘密共享被称为量子秘密共享 (quantum secret sharing, QSS). QSS 利用量子资源在多方之间共享秘密信息. 1999 年, Hillery 等[11] 基于 GHZ (Greenberger-Horne-Zeilinger) 态提出了第 1 个 QSS 协议. 同年, Cleve 等[12] 基于量子纠错编码理论, 提出了量子 (k,n) 门限方案. 此后, 基于这两篇文章, 各种类型的 QSS 协议被相继提出, 并在实验上得到证明. 与经典的秘密共享不同, QSS 中秘密的信息分割与分发是基于对分布式量子态的局域测量来实现的, 因此 QSS 允许在存在窃听的情况下安全地分配共享的份额. 同时不同于 QKD, QSS 是多方的通信过程, 允许更丰富、

* 国家自然科学基金 (批准号: 12274223) 资助的课题.

同等贡献作者.

† 通信作者. E-mail: hlyin@ruc.edu.cn

更灵活的量子通信. 但 QSS 不仅需要排除外部的窃听行为, 还需要防范通信各方潜在的内部欺骗行为, 因此 QSS 对其协议有更严格的要求.

秘密共享问题可以分为 3 个子问题[13]. 1) CC. 分发者通过分发者和参与者之间私人信道以及每对参与者之间的经典私人信道来共享经典信息. 2) CQ. 分发者通过分发者和参与者之间公共信道以及每对参与者之间的经典或者量子信道来共享经典信息. 3) QQ. 分发者通过分发者和参与者之间共享的公共或者私人的量子信道以及每对参与者之间的经典或者量子信道来共享量子信息. 如图 1 所示, 根据不同的分类方法, QSS 可以分为不同的类型, 但总的来说 QSS 主要研究的就是 CQ 和 QQ 两个子问题. QSS 一方面可以利用量子资源增强经典秘密共享的安全性, 有效抵抗公共信道的窃听行为. 另一方面量子信息的秘密共享, 将为大规模多方量子网络和分布式量子计算的构建提供重要技术支持. 因此 QSS 逐渐成为量子信息技术的一个研究焦点. 本文将分别从共享经典信息的 QSS 和共享量子信息的 QSS 两个主要方向, 梳理和介绍近年来不同技术路线下 QSS 的研究进展与现状, 并对 QSS 的研究趋势和未来的研究方向进行总结和展望.

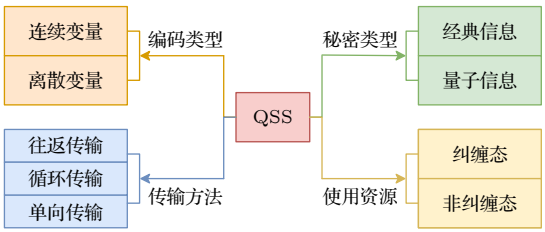

图 1 QSS 协议的类型

Fig. 1. Types of QSS protocol.

2 经典量子秘密共享 (CQ)

2.1 使用纠缠态的经典量子秘密共享

使用纠缠态的经典量子秘密共享指利用量子纠缠态来对经典比特进行秘密共享. 由 Hillery 等[11]于 1999 年提出的 QSS 协议展示了如何使用 GHZ 态去对经典信息和量子信息进行分割与重构, 这个协议也被称为 HBB 协议. 在共享经典信息的 HBB 协议中, Alice, Bob 和 Charlie 分别随机在基 $|\pm x\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$ 和 $|\pm y\rangle=(|0\rangle\pm \mathrm{i}|1\rangle)/\sqrt{2}$ 中对三粒子 GHZ 态进行测量:

$$|\psi\rangle_{\mathrm{ABC}}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{\mathrm{ABC}}, \tag{1}$$

下标 A, B, C 分别表示属于 Alice, Bob 和 Charlie 的粒子. 三方的测量结果具有关联性, 关联结果如表 1 所示. 通过这些关联性 Alice, Bob 和 Charlie 根据一定的编码规则可以得到一个二进制的密钥串, 满足 $k_{\mathrm{A}}=k_{\mathrm{B}}\oplus k_{\mathrm{C}}$. 只有 Bob 和 Charlie 合作才能知道 Alice 的比特, 实现了秘密共享.

表 1 三方测量结果的关联性

Table 1. Correlation of the measurement results from three parties.

		Alice			
		$\|+x\rangle$	$\|-x\rangle$	$\|+y\rangle$	$\|-y\rangle$
Bob	$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|-y\rangle$	$\|+y\rangle$
	$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|+y\rangle$	$\|-y\rangle$
	$\|+y\rangle$	$\|-y\rangle$	$\|+y\rangle$	$\|-x\rangle$	$\|+x\rangle$
	$\|-y\rangle$	$\|+y\rangle$	$\|-y\rangle$	$\|+x\rangle$	$\|-x\rangle$

但原始的 HBB 协议是不安全的, 不诚实的参与者可以在不引入任何错误的情况下获得所有信息[14]. 2005 年, 通过利用四光子纠缠源制备 GHZ 态, Chen 等[15]首次对 HBB 协议进行了实验实现, 在此之前仅证明了使用伪 GHZ 态[16]实验实现 QSS 的可行性. 在这些方案中, 识别多粒子 GHZ 状态也是必要的. 一般来说, Bell 态的识别比 GHZ 态的识别要容易得多, 大量基于 Bell 态的 QSS 协议被提出[17,18]. 2019 年, Williams 等[19]基于 Bell 态提出并实验演示了一个使用偏振纠缠光子对的实用三方 QSS 协议. 如图 2 所示, 偏振纠缠 QSS 协议依赖泵浦偏振来制备所需的量子态, 而不是在光子对产生后再进行调制. 这一方面可以对产生的纠缠态进行高速调制, 另一方面使得协议不易受损耗的影响, 可以有效保证 QSS 的性能.

三方的 QSS 很快被得到证明, QSS 向着四方乃至更多方的 QSS 发展[20]. 一种高纠缠四光子态[21]也被证明可以实现四方 QSS[22], 表明了利用多光子纠缠实现安全多方量子通信的可行性. Yu 等[23]利用多能级系统构造出了多方 QSS 的一般方案, 并给出了有效测量的一致性条件:

$$A+B+C+\cdots+\Omega=0 \mod d, \tag{2}$$

$$a+b+c+\cdots+\omega=0 \mod d, \tag{3}$$

其中大写字母表示测量基, 小写字母表示给定正交

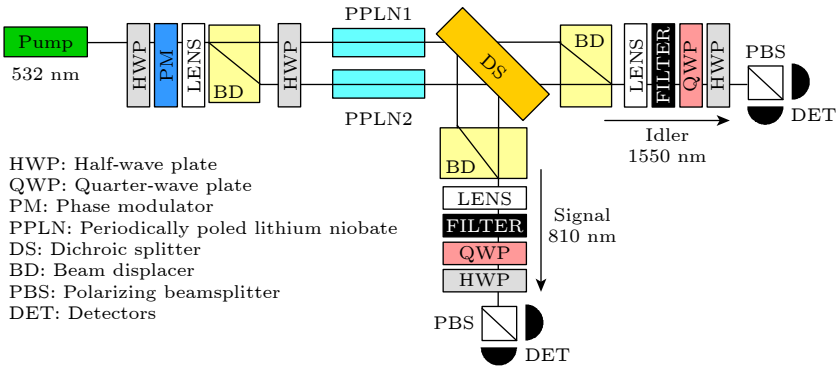

图 2 偏振纠缠光子源示意图[19]

Fig. 2. Schematic of the polarization-entangled photon source[19].

测量基中的向量. 如同 Hillery 等[11] 最初的方案, 参与者首先利用本地操作和经典通信 (local operations and classical communication, LOCC) 确定 (2) 式是否满足, 如果满足, 则 (3) 式表达的就是各方建立的密钥关系. 如果不满足, 则丢弃本轮结果. 对抗截获-重发等攻击的能力对 QSS 的安全性来说非常重要. 常见的二能级系统的 QSS 方案[11] 检测到截获-重发攻击的概率仅为 25%, 因此增强抵抗此类攻击能力的一个最直接的办法就是使用更高维的量子系统来实现 QSS. 更高维的量子系统使得 QSS 协议更加复杂, 攻击者截获-重发攻击未被检测到的概率将大幅降低. 使用非常高维的互无偏基 (mutually unbiased bases, MUBs) 的方案原则上能够完美抵抗此类攻击. 但另一方面, 这也将使得协议需要耗费更多的量子资源, d 维量子系统 QSS 协议的效率只有 $1/d$. 但采用 Xiao 等[24] 提出的基于测量基加密的高效 QSS 方案之后, QSS 协议的效率将能够从 $1/d$ 提高至 100%.

虽然纠缠态的使用能够使窃听者难以单独篡改或者窃取部分信息, 具有很强的安全性. 但是对于使用纠缠态的情况, 增加和删除参与者往往需要改变系统的维度, 这将不得不对源进行复杂的更改, 限制了其可扩展性. 为了解决这一问题, Xiao 等[25] 利用单纠缠光子对源和波分复用技术[26] (wavelength-division multiplexing) 提出了一种在全连接量子网络架构[27] 中的高效源无关 QSS 协议. 基于该量子网络体系, 网络提供商利用单纠缠光子对源产生两体纠缠并通过波分复用技术将两体纠缠分发到多个用户, 该协议可以在不改变纠缠源和网络用户硬件的情况下进行多方扩展, 在城域网以及更大规模量子网络的构建中具有很大的应用潜力.

2.2 使用非纠缠态的经典量子秘密共享

虽然纠缠态的使用使得窃听者无法在不被察觉的情况下获取秘密信息, 给 QSS 协议提供了安全性的保障. 但是就目前来看, 纠缠态的制备需要复杂的实验设备, 仍然很难被高亮度、高保真度地产生、操控和分发[28–32]. 同时由于纠缠态易受光子损耗、偏振畸变等环境噪声的影响, 导致纠缠退化, 难以远距离传输[33], 这限制了 QSS 系统的密钥率和稳定性, 使得 QSS 方案的可靠性大大降低. 2003 年, Guo 等[34] 基于 BB84 QKD 协议首次提出了不依赖纠缠的 QSS 协议, 仅需要使用两量子比特乘积态就能完成共享密钥的建立. 随后, 大量研究表明, 在共享经典信息的 QSS 中纠缠并不是必须的.

2.2.1 单量子比特量子秘密共享

为规避多光子纠缠源的使用, 单光子 QSS 协议应运而生[35–37]. 实验上, 实现单光子 QSS 方案最常见的方案是基于光的偏振[35]. 除此之外还可以利用单光子和零光子的叠加态来构建单量子比特. 2005 年, Schmid 等[38] 基于单光子提出了一种使用单量子比特的 QSS 协议. 在这个协议中, 秘密共享的任务不再需要多粒子纠缠 GHZ 态, 而只需要在一个传递的单量子比特上对其相位进行局域操作就可以实现. 在这里, 量子比特的初态制备为 $|+x\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$. 然后量子比特在各参与者中依次传递, 每个参与者都用如下酉相位算子作用在这个量子比特上:

$$\hat{U}_j(\varphi_j)=\begin{cases}|0\rangle\to|0\rangle,\\ |1\rangle\to \mathrm{e}^{\mathrm{i}\varphi_j}|1\rangle,\end{cases} \tag{4}$$

其中随机选取 $\varphi_j\in\{0,\pi,\pi/2,3\pi/2\}$. 那么通过所有参与者后的量子比特将处于状态:

$$|x_N\rangle\frac{1}{\sqrt{2}}(|0\rangle+\mathrm{e}^{\mathrm{i}\sum_j^N\varphi_j}|1\rangle). \tag{5}$$

当各参与者的类型满足 $\cos(\sum_j^N\varphi_j)=\pm1$ 时, 最后一位参与者在基 $|\pm x\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$ 上能够测得 ±1, 此时量子比特有效 (可通过特定的选择使得量子比特总是有效). 此时由于 φ_j 满足余弦关系式, 当最后一位参与者宣布测量结果后, 任何 $N-1$ 方子集都能推断出剩余一方的 φ_j 值, 实现秘密共享.

与纠缠态的方案相比, 单个量子比特更具有实验可实现性和可扩展性. 文献 [38] 中就利用线性光学元件和光子偏振态分析给出了 6 个参与方的实验演示, 是当时实现的量子协议中积极执行的参与方最多的. 除了实验演示外, 单量子比特 QSS 也在光纤中得到实现. 电信级的相位调制器是偏振敏感的, 而在单模光纤中受双折射效应影响, 激光脉冲的偏振会缓慢随机的变化, 这很大程度上影响了相位调制器的正确作用. Bogdanski 等 [39] 基于偏振控制系统和偏振不敏感相位调制器, 在 Sagnac 中提出了补偿单模光纤双折射效应的概念, 解决了单模光纤中双折射漂移的问题 [40], 实现了第 1 个在 1550 nm 单模光纤网络上使用相位编码单量子比特协议的 Sagnac QSS 方案 (三方和四方). 随后, Ma 等 [41] 也在 50 km 单模光纤网络上实现了使用相位编码的鲁棒的三方单光子 QSS 方案, 能见度高达 99.4%. 这表明了单量子比特 QSS 在实际系统中具有良好的应用潜力, 在电信光纤网络上实现量子秘密共享是可行的. 但值得注意的是, 二维的单量子比特 QSS 在安全性方面仍存在一定限制 [42,43], 容易受到特洛伊木马的攻击 [44]. 窃听者可以向参与者的基站发送信号, 并通过测量输出信号来明确地的确定参与者所拥有的私密信息.

另一方面, 一些基于纠缠态的 QSS 协议是可以转化为非纠缠态的. 例如扩展到 d 能级系统的 GHZ 态协议 [23] 可以转化为单个 qudit 顺序传输的协议 [45]. 而在高维形式下, 二维单量子比特顺序传输 QSS 协议的安全漏洞得以解决. 因此更高维的单 qudit QSS 协议被相继提出. 制造高维的单 qudit 一般有两种方式, 一种是利用光子本身的自由度, 一种是利用路径的自由度. 光子本身自由度最常见的就是光子的偏振, 但偏振只有两个自由度, 限制了向更高维度的扩展. 而光子的轨道角动量 [46,47] (orbital angular momentum, OAM) 能够提供无穷维的希尔伯特空间, 为实现高维的量子信息过程提供了一条新途径, 因此可以用来实现单 qudit QSS. Pinnell 等 [48] 利用 OAM 实现了 10 方 QSS 的实验演示, 如图 3(a) 所示. 另外还可以使用经过不同的路径的系列光子的组合来制造 qudit. 例如在信道中使用三臂类马赫-曾德尔干涉仪可以产生单个 qutrit, 从而实现三方 QSS[49], 如图 3(b) 所示.

值得注意的是, 很多理论上基于单光子的 QSS 协议实验上都选择使用弱相干光来实现 [39,41,48,49]. 虽然单光子的产生与纠缠态相比已经更加容易, 但单光子在实验上仍然难以高效地产生和控制. 弱相干光可以通过普通激光源结合可调谐衰减器 (如中性密度滤光片等) 来进行制备, 实验实现简单、技术成熟, 具有高稳定性和易操作性. 另一方面, 单光子源的光子产生率往往较低, 而弱相干光则可以通过调整激光功率和重复频率来提高光子的产生率. 同时, 弱相干光可以使用标准光纤传输, 不需要额外的光子管理技术, 在现有技术下更容易实现远距离传输. 因此弱相干光常常被用作单光子源的替代方案. 但弱相干光的使用会损失单光子带来的安全性. 由于弱相干光服从泊松分布, 其无法避免地存在多光子成分, 这使得弱相干光无法无条件安全地抵御光子数分裂 (photon-number-splitting, PNS) 攻击 [50,51]. 不过, 在实际部署中这种攻击可以通过诱骗态 [52–54] 或者在 QSS 协议中增加额外的安全补偿机制来减轻.

2.2.2 相位编码量子秘密共享

为了抵抗 PNS 攻击, 并进一步简化实验装置, Inoue 等 [55] 基于差分相移 (differential-phase-shift, DPS) 的 QKD, 提出了一种 DPS-QSS[56]. 与之前的协议不同, DPS-QSS 的密钥信息储存在相邻脉冲的相对相位中, 并且需要 Charlie 随机选择脉冲时隙进行测量, 如图 4(a) 所示. 而 PNS 攻击者选择和 Charlie 相同时隙对光子进行计数的概率很低, 因此这个协议对抵抗 PNS 攻击具有很好的鲁棒性. DPS-QSS 的提出为量子秘密共享的实用化、可行化开辟了一条新的路径. 但遗憾的是, Inoue

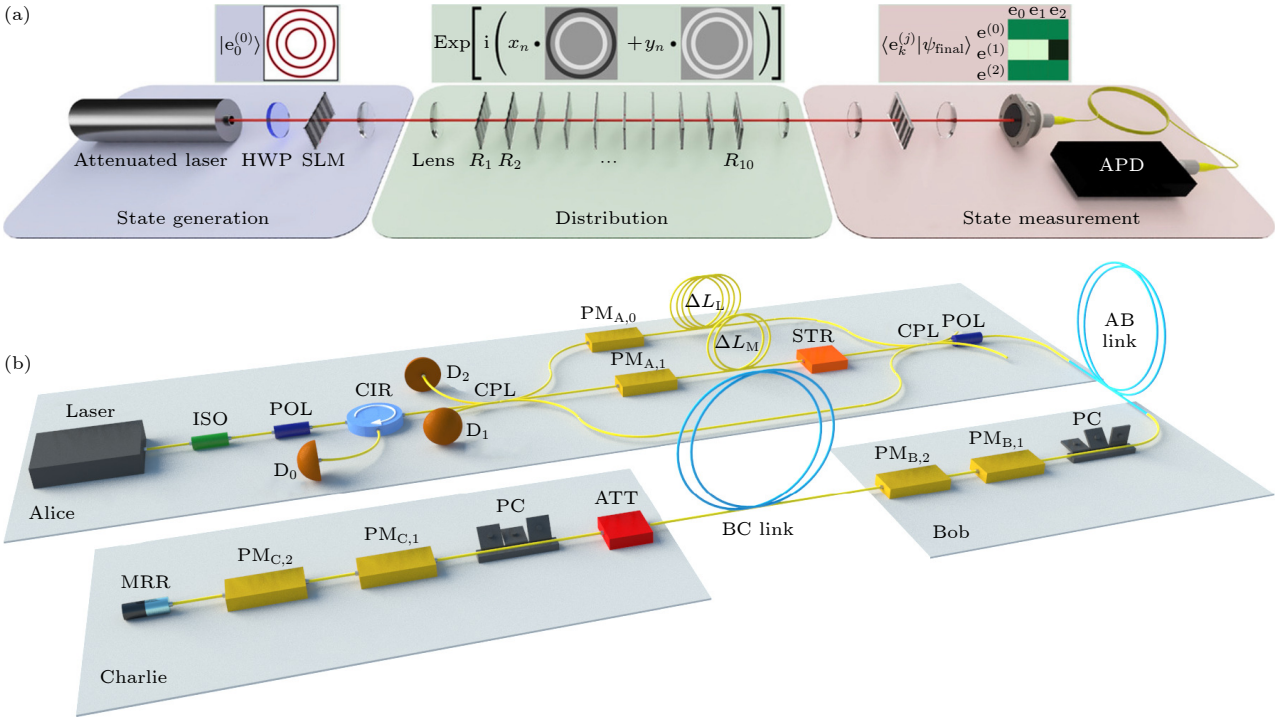

图 3 实现高维单 qudit QSS 的两种方法 (a) 使用光子轨道角动量[48]; (b) 使用多臂类马赫-曾德尔干涉仪[49]

Fig. 3. Two methods for achieving high-dimensional single-qudit QSS: (a) Using the orbital angular momentum of photons[48]; (b) using the multi-arm Mach-Zehnder-like interferometer[49].

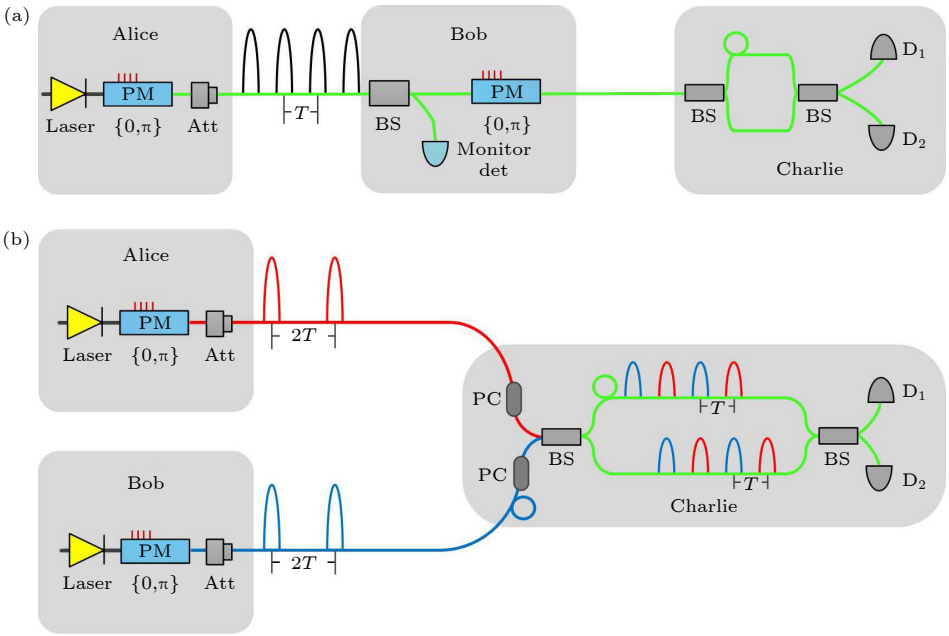

图 4 DPS-QSS 协议的配置[57] (a) 典型 DPS-QSS 的实验配置; (b) 使用双场的 DPS-QSS 的实验配置

Fig. 4. Configuration of DPS-QSS protocol[57]: (a) Setup of typical DPS-QSS; (b) setup of DPS-QSS using a twin field.

最初提出的方案无法抵御特洛伊木马的攻击. 2021 年 Gu 等[57] 结合双场[58–60] 提出了使用双场的 DPS-QSS 协议. 如图 4(b) 所示, 该协议与文献[56] 中的协议是等价的, 但由于使用双场, Alice 的脉冲不需要顺序经过 Bob 并被 Bob 调制, 因此该方案可以安全地抵御特洛伊木马的攻击. 但是 DPS-QSS 协议仍然存在安全局限性, 只能抵抗个体攻击 (例如 PNS 攻击和光束分裂攻击), 而无法抵抗更强大的相干攻击[61](coherent attacks). 2023 年, Shen 等[62] 进一步提出了一种可以抵抗相

干攻击的 QSS 协议, 并通过在相干态上对逻辑位进行相位调制编码, 消除了对强度调制和相位随机化的要求, 简化了实验设置, 为实现 QSS 的安全性和实用性的结合问题提供了解决途径. 但协议[62]针对不同参与者在一些步骤中表现出不对称性, 因此需要事先了解窃听者的身份, 并可能引入安全漏洞. 随后 Wang 等[63]对协议[62]进行了修正, 对所有参与者采用对称程序, 消除了协议[62]因不对称基选择而产生的安全漏洞.

2.3 连续变量量子秘密共享

根据编码类型, 除了前文提到的离散变量 QSS (discrete-variable QSS, DV-QSS) 之外, 还有连续变量 QSS (continuous-variable QSS, CV-QSS). 传统的 QSS 主要利用离散的量子比特实现, 而 CV-QSS 则是在光场的正交分量 (振幅 $\hat{x}$ 和相位 $\hat{p}$) 中对密钥位进行编码. 因其高效的信息编码方式, 成熟的光学实现技术以及较高的容错能力, CV-QSS 成为 QSS 乃至量子密码学的一个重要研究方向. 在 Grosshans 和 Grangier[64]将连续变量引入量子密码学后不久, Tyc 等[65]提出了首个 CV-QSS 协议. 随后 Lance 等[66]对 Tyc 的协议进行了扩展, 利用电光前馈技术验证了 (2, 3) 门限 CV-QSS 协议的可行性, CV-QSS 正式进入历史舞台. 2017 年, Kogias 等[67]给出了 CV-QSS 同时对抗窃听者和不诚实参与者的充分条件, 这适用于所有 (k,n) 门限 CV-QSS 方案.

实现 CV-QSS 的一种方法是使用 Einstein-Podolsky-Rosen (EPR) 纠缠态 ($\hat{a}_{\rm EPR1}$ 和 $\hat{a}_{\rm EPR2}$) 和光的热态 (thermal states)($\hat{\nu}_1^{\rm T}$ 和 $\hat{\nu}_2^{\rm T}$) 来制备束缚纠缠 (bound entanglement, BE) 态, 并将秘密信息 $a_s(a_s^*)$ 调制到 BE 态中[68]:

$$\hat{b}_{1(2)} = (\hat{a}_{\rm EPR1} \pm \hat{\nu}_1^{\rm T} + a_s)/\sqrt{2}, \tag{6}$$

$$\hat{b}_{3(4)} = (\hat{a}_{\rm EPR2} \pm \hat{\nu}_2^{\rm T} + a_s^*)/\sqrt{2}, \tag{7}$$

BE 态处于可分离态和自由纠缠态之间, 其无法表示为分离态的形式, 同时其也是不可提纯的, 无法通过 LOCC 来提纯纠缠[69–71]. 从 (6) 式和 (7) 式中可以看到, 每个子模式都存在较大的噪声背景, 任何一个玩家都无法检索到调制信号比较小的秘密信息. 只有当足够多的参与者合作进行组合噪声测量时, 秘密信息才得以揭示. 除了束缚纠缠态外, 连续变量簇态[72]、连续变量 GHZ 态[73]、连续变量图态[74]等连续变量纠缠态也在逐渐被广泛运用到 QSS 的研究当中. 但正如前文对于离散变量纠缠态所讨论的那样, 使用连续变量纠缠态的 QSS 由于其仍然基于多方纠缠, 当参与者的数目很大时在现有技术下难以实现. 同时, 虽然相比于使用纠缠态的 DV-QSS, 使用纠缠态的 CV-QSS 能够和现代光通信技术有更好的兼容, 但其仍然面临着难以容忍的信道损耗[67].

为避免纠缠态的使用, 基于弱相干态的顺序 CV-QSS 协议被提出[75], 这进一步提高了 CV-QSS 与现代光通信技术的兼容性及其实用性. 同时与单量子比特顺序 QSS 方案相比, 此方案具有天然的抵抗特洛伊木马攻击的能力. 随后, 这个思想被进一步扩展到基于热态[76]和基于离散调制相干态[77,78]的 CV-QSS, 促进了 CV-QSS 的发展. 但不幸的是, 大多数相干态的 CV-QSS 协议要求所有参与者在自己的站点准备自己的激光源, 这种成本是巨大的. 并且所有参与者的独立激光源之间的相位需要严格锁定, 信号同步问题难以解决. 更重要的是, 由于 CV-QSS 要求每个参与者将自己的本振 (local oscillator, LO) 信号通过不安全的信道发送给分发者, 因此本振信号很容易成为攻击者攻击的目标. 2022 年, Liao 等[79]提出了一种基于即插即用 (plug-and-play) 结构[80]和双相调制 (dual-phase modulation) 策略的 CV-QSS 方案, 解决上述问题. 但这需要在不受信任的量子通道中传输未调制的量子信号, 可能会引入新的漏洞. 随后 Liao 等[81]进一步基于本地 LO (local LO, LLO) 技术提出了 LLO-CVQSS 的方案, 彻底堵住了 CV-QSS 系统中传输 LO 导致的可能遭受各种攻击的漏洞. 除此之外, 对于 CV-QSS, 由于经销商的联合测量, 来自其他参与者的信道过剩噪声 (channel excess noises) 的叠加将会使密钥率大幅降低[75,76,79]. 利用将其密钥信息编码到光场的不同边带[82]的多边带调制方法[83], 分发者可以使用单个外差检测器 (heterodyne detector) 提取多个参与者的信息, 并且由于每个参与者的量子信道透射率 (quantum channel transmittance) 和信道过剩噪声等信道参数的评估是独立的, QSS 的量子密钥率和传播距离显著提高. 同时, 利用该方法的硬件架构, 只需要切换经典的后处理程序就可以实现 QSS 和会议密钥协商[84–86](conference key agreement) 的灵活切换. Richter 等[87]也实验演示了一个具有量子加

密敏捷性 (quantum cryptoagility) 和多功能性的系统, 能够在同一平台上实现连续变量量子数字签名 (quantum digital signatures)[88]、连续变量 QSS 和连续变量 QKD[89–91]. 这种利用同一硬件支持不同量子密码协议切换的系统将大幅增加量子通信设备的通用性.

2.4 量子秘密共享的安全性保障

传统的 QSS 会利用信号的扰动检测来保障安全. 发送方通常会将发送的一部分量子比特作为检测比特. 根据量子不可克隆定理, 量子态无法被完美复制, 任何窃听行为都会对量子态造成干扰, 从而在传输的量子比特中引入错误. 因此可以对信号的扰动进行检测来判断通信是否遭到窃听. 通过计算错误比特和总检测比特的比值可以得到量子比特误码率, 如果量子比特误码率超过了某一阈值 (信道固有误码率), 则说明存在窃听者, 本轮通信将被放弃. 这很大程度上提高了 QSS 的安全性. 但是信号扰动检测会损失一部分比特用于检测, 降低了通信效率. 同时在某些攻击 (如特洛伊木马攻击) 的情况下, 误码率可能不会明显上升造成误判. 2021 年, Gu 等[92] 受环回 (round-robin) 差分相移 QKD[93] 和双场 QKD[58] 的启发, 提出了一个不监测信号扰动的三用户 QSS 协议, 即环回 QSS. 这个协议面向内部和外部攻击者是无条件安全的, 并且密钥率能够打破 Pirandola-Laurenza-Ottaviani-Banchi 界限[94]. 环回 QSS 由于其高噪声容忍和抗信号干扰等固有优势, 有较好的应用前景, 但其对可变延迟马赫-曾德尔干涉仪的要求限制了其实际应用.

使用纠缠态的 QSS 即使光源部分被攻击者控制, 只要测量端能够被完美表征并进行测量错误率即可获得安全秘密共享, 因此可以实现光源设备无关的安全性. 但使用单光子或者相干光的 QSS 则是完全依赖于设备的完美表征, 因此设备的不完善性会给实际系统带来安全漏洞. 诸如致盲攻击[95–97]、时移攻击[98]、波长攻击[99]、偏振旋转攻击[100]、饱和攻击[101] 等针对测量设备的侧信道攻击[102](side-channel attacks) 会给量子通信系统的安全性造成极大的威胁. 测量设备无关 (measurement-device-independent, MDI) 的量子通信技术[103] 通过引入不信任的第三方进行来执行测量, 利用后选择纠缠免除了探测器必须由合法分发者保护的必要性, 为侧信道攻击提供了解决方案. 2015 年, Fu 等[104] 提出了第一个 MDI-QSS 协议, 利用后选择 GHZ 态和诱骗态[52,105] 实现了对测量设备攻击和 PNS 攻击的抵抗, 实验装置如图 5 所示. 随后 MDI-QSS 在离散变量[106–109] 和连续变量[110,111] 领域得到广泛发展. 尽管 MDI-QSS 不需要使用纠缠资源, 但传输效率仍然会随着用户数量的增加呈指数级下降. 2023 年, Li 等[112] 基于全光量子中继[113] 和自适应 MDI-QKD[114] 中的空间复用 (spatial multiplexing) 和自适应操作提出了一种更加高效实用的 MDI-QSS. 当通信方的数量增加时, 协议的传输效率可以保持不变, 并在至少 10 个通信方的情况下打破网络上的速度-距离界限[94]. 除了测量设备外, 不完美光源同样会造成侧信道信息泄露, 威胁 QSS 的安全性. 为消除所有实际不完美设备的

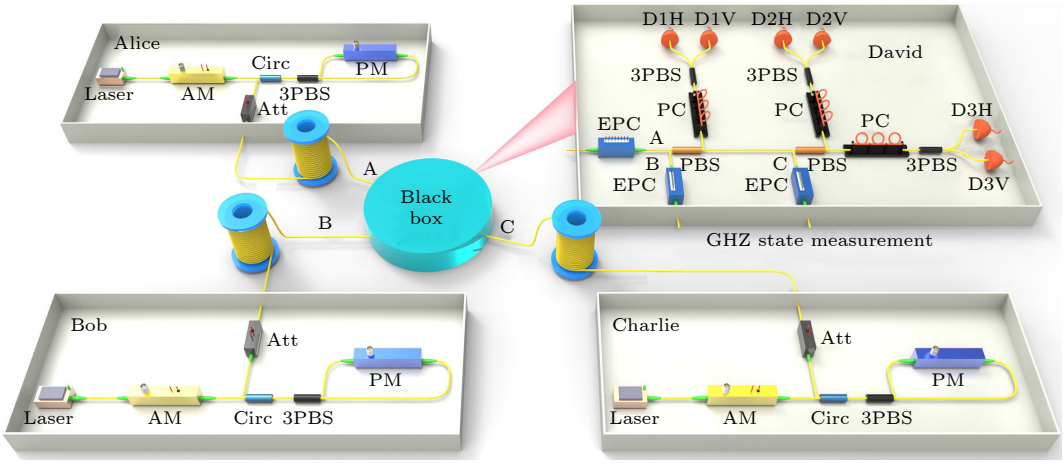

图 5 MDI-QSS 装置的示意图[104]

Fig. 5. Schematic of the MDI-QSS setup[104].

安全漏洞, 设备无关 (device-independent, DI) 的 QSS 被提出[115–117]. 但在实际通信过程中, 目前的 DI-QSS 的性能仍然较低, 尚未有效实现.

QSS 的概念首次提出时, 使用的是量子典型特征的纠缠态来共享经典信息. 但由于纠缠态制备、控制和传输在当前技术条件下实现较为困难、实用性较低. 因此使用单光子的非纠缠态的 QSS 协议被相继提出, 但单光子目前在实验上依然难以高效地产生和控制, 并且与目前的通信光纤有适配性差异. 于是, 作为单光子和纠缠态的替代方案, 使用相干光 QSS 协议被提出, 并得益于其成熟的实验技术在光纤网络上迅速得到实现. 仍需指出的是, 单光子和相干光的使用会损失纠缠态带来的安全性, 相干光也比单光子更容易受到光子数分裂攻击. 为此, 诱骗态、环回、MDI 等方法被使用以提高 QSS 的安全性. 近年来提出的 QSS 协议已经能很好地抵御外部攻击和内部成员攻击等一系列安全性问题. 因此, 虽然近年来, 纠缠态的制备、控制和传输已经取得一系列重要突破[118–125], 但是对于共享经典信息的 QSS 来说纠缠态的使用已经不具备明显优势. 相反, 使用非纠缠态的 QSS 因其高稳定性、易操作性和光纤适配性, 具有更高的实用价值. 但在量子信息的秘密共享领域, 纠缠态仍然发挥着不可替代的作用.

3 量子信息的秘密共享 (QQ)

量子信息的秘密共享 (QQ) 的概念渊源最早可追溯至由 Bennett 等[126] 在 1993 年所提出的量子隐形传态, 发送者借助于量子纠缠资源, 可以在不传递物理粒子的情况下将未知量子态信息传递给接收者. QQ 即可被认为是多方量子隐形传态的一个应用. 1999 年, Hillery 等[11] 使用 GHZ 态和 Bell 基测量提出了首个 QQ 方案, Alice 将未知量子态传送给她的代理组 Bob 和 Charlie, 代理组成员之间仅有一人能够在 Alice 处 Bell 基的测量结果和另一位成员的信息下对量子态秘密进行重构, 因此 QQ 也被称为量子信息分割 (quantum information splitting, QIS) 或量子态共享 (quantum state sharing, QSTS). 本节将依次讨论离散变量情况下 QQ 中的对称性方案、非对称分层方案与基于一种重要量子资源态, 图态的方案, 然后介绍 QQ 中的连续变量方案, 最后展示对纠缠态进行共享和多方量子秘密直接传输的重要工作. 现存 QQ 方案重要的问题主要包括秘密共享方案结构与参与者数量的拓展, 方案共享信息从单量子比特态、多量子比特态到高维量子态的拓展, 以及衡量量子资源消耗、操作复杂度和通信成本, 对具有更高效率方案的研究.

3.1 对称性量子信息秘密共享方案

(k,n) 门限方案是一类具有对称性的重要秘密共享方案. 在 (k,n) 门限方案中, 对于恢复秘密的要求仅为参与者数量. 数量达到门限 k 的任意参与者均成为授权者集合, 合作时可以完美恢复秘密, 少于 k 位参与者的集合则被拒绝访问任何关于秘密的信息. 1999 年, Cleve 等[12] 首次定义了 QQ 中的 (k,n) 门限方案并基于量子纠错码给出了一种通用的构造方式, 与文献 [11] 共同成为 QQ 领域的开创性工作. 设量子态秘密 $|s\rangle$ 的维度为 s, 选择素数 q 满足 $\max(n,s)\leqslant q\leqslant 2\max(n,s)$, 构造有限域 $\mathbb{F}_q$, 其中 $\mathbb{F}=\mathbb{Z}_q$. 对于 $s\in\mathbb{F}$, 可将量子态 $|s\rangle$ 编码为 n 个份额:

$$|s\rangle\mapsto\sum_{c\in\mathbb{F}_q^k,c_{k-1}=s}|p_c(x_0),\cdots,p_c(x_{n-1})\rangle,\tag{8}$$

其中, 多项式 $p_c(t)$ 定义为 $p_c(t)=c_0+c_1t+\cdots+c_{k-1}t^{k-1}$, 系数 $(c_0,c_1,\cdots,c_{k-1})\in\mathbb{F}^k$, 坐标 $x_0,x_1,\cdots,x_{n-1}$ 选取为 $\mathbb{F}$ 上互不相同的 n 个点, 所分发的子份额则为多项式在某个坐标 x_i 上的取值 $p_c(x_i)$.

对于共享量子信息的情况, 量子不可克隆原理要求量子态秘密不可被多次恢复, 限制了 $k\geqslant n/2$. 在所有编码后全局态为纯态的 (k,n) 方案中, 授权集与未授权集均为互补, 即满足条件 $n=2k-1$. 在 $(k,2k-1)$ 门限方案的基础上丢弃份额可以直接得到其他 $k\leqslant n<2k-1$ 方案, 但此时将为混合态方案. 一般而言, Cleve 等[12] 给出的方案需要使用高维量子比特的混合态.

(k,k',n) 斜坡方案为 (k,n) 门限的一种弱化, 在进行秘密共享 n 名参与者中, 任何 k 及以上名参与者的集合能够完美访问秘密, 任何 k' 及以下名参与者无法获取任何秘密信息, 其他情况则面临着量子态秘密泄露的风险. 当 $k'=k-1$ 时, 斜坡方案就成为 (k,n) 门限方案. Senthoor 和 Sarvepalli[127] 在 Cleve 等[12] 工作的基础上构建了一个通用的通信高效量子门限秘密共享方案, 其结合斜坡方案和

标准门限方案, 通过在参与者人数高于门限时根据实际需求灵活选择任意数量的参与方, 提高了秘密恢复的通信效率.

在固定结构的方案之外, 实际情况下, 秘密分发者可能会根据工作需要增加或减少成员, 重新对新代理组进行秘密分发面临高昂的成本, 为此提出了动态量子秘密共享方案 (dynamic quantum secret sharing, DQSS), 其在共享经典信息和量子信息的过程中允许对接收者代理组进行更改. DQSS 源于 CQ 情形下由 2011 年 Yang 等 [128] 首次提出的 (k,n) 门限方案中进行成员扩展的协议. 2012 年, Jia 等 [129] 基于星形簇态, 提出了一种 CQ 和 QQ 的动态方案. 利用星状簇态在泡利测量下的可扩展性, 分发者能够在子份额被分发前与分发后两个阶段对代理组进行增减成员的调整. 若子份额已被分发, 添加新成员则额外需要一名原始成员的授权, 无需重新分配所有份额. Sun 等 [130] 使用单光子偏振态和 CNOT 门操作和 Bell 基测量, 能够在允许增加新用户的代理组中共享量子秘密, 该方案成员扩展的过程无需任何原代理组成员的协助. 但目前工作基本均局限于 (n,n) 门限方案的架构.

量子纠缠是量子隐形传态和 QQ 方案的核心, 纠缠态的特殊性质为处理量子信息任务提供了很好的支持. 自 Hillery 等 [11] 以来, 提出了许多基于不同纠缠态的 QQ 方案设计, 包括 Bell 态 [131–135]、GHZ 态 [11,136]、簇态 [137]、W 态 [138] 等. 在这些方案中, 所有接收者均有能力恢复被发送的未知量子态, 权限结构具有一定的对称性, 因此这一类方案也被称为对称量子信息分割.

在 Hillery 等 [11] 最先的 GHZ 态方案中, 分发者 Alice 将一个初始 GHZ 态 (其中 3 个粒子 a, b, c 分别由 Alice 和接收者 Bob, Charlie 持有) 与秘密量子态 $|\psi\rangle_{\rm A}=\alpha|0\rangle_{\rm A}+\beta|1\rangle_{\rm A}$ 结合, 可得

$$\begin{aligned}|\Psi\rangle &= |\psi\rangle_{\rm A}\otimes\frac{1}{\sqrt{2}}(|000\rangle_{\rm abc}+|111\rangle_{\rm abc})\\ &=\frac{1}{2}\Big[|\Psi^+\rangle_{\rm Aa}(\alpha|00\rangle_{\rm bc}+\beta|11\rangle_{\rm bc})\\ &\quad+|\Psi^-\rangle_{\rm Aa}(\alpha|00\rangle_{\rm bc}-\beta|11\rangle_{\rm bc})\\ &\quad+|\Phi^+\rangle_{\rm Aa}(\beta|00\rangle_{\rm bc}+\alpha|11\rangle_{\rm bc})\\ &\quad+|\Phi^-\rangle_{\rm Aa}(-\beta|00\rangle_{\rm bc}+\alpha|11\rangle_{\rm bc})\Big],\end{aligned}\tag{9}$$

其中,

$$\begin{aligned}|\Psi^{\pm}\rangle_{\rm Aa}&=\frac{1}{\sqrt{2}}\left(|00\rangle_{\rm Aa}\pm|11\rangle_{\rm Aa}\right),\\ |\Phi^{\pm}\rangle_{\rm Aa}&=\frac{1}{\sqrt{2}}\left(|01\rangle_{\rm Aa}\pm|10\rangle_{\rm Aa}\right).\end{aligned}\tag{10}$$

因此, 通过 Alice 对 A, a 粒子 Bell 基测量的结果可以确认秘密量子态的振幅信息, 再结合另一位成员 Bob 对他所拥有粒子的测量结果, Charlie 即可执行相应修正操作在自己的量子比特上恢复原始秘密.

相较于其他纠缠态方案, Bell 态方案具有更好的灵活性和可拓展性, 减轻了方案对复杂纠缠态量子资源的依赖. Li 等 [131] 首次利用纠缠交换与 GHZ 基测量设计了 n 名参与者对单量子比特态的共享方案, Yuan 等 [134] 使用两个 EPR 对, 通过 Bell 基测量和接收者处的单比特酉操作, 能够实现两量子比特态的三方安全共享. Shi 等 [135] 结合 Bell 态和 CNOT 门操作, 提出了一种高效、低资源消耗的多方量子态共享方案, 在向 n 名参与者共享两量子比特态时仅需 n 个 Bell 态的量子资源.

W 态是一类区别于 GHZ 态的多体纠缠态:

$$\begin{aligned}|W_n\rangle_{123}=\frac{1}{\sqrt{2+2n}}\big(&|100\rangle+\sqrt{n}{\rm e}^{{\rm i}\theta}|010\rangle\\ &+\sqrt{n+1}{\rm e}^{{\rm i}\phi}|001\rangle\big).\end{aligned}\tag{11}$$

其中 n 为实数, θ, ϕ 为相位. W 态的三体纠缠度为 0. 相较于 GHZ 态, W 态具有更好的鲁棒性, 在丢失任意一个粒子后, W 态中剩余的两粒子仍保持部分纠缠, 不易退相干 [139]. 利用此类纠缠态, Agrawal 等 [140] 已经实现了双方量子隐形传态. Nie 等 [138] 进一步提出了基于 W 态对任意三量子比特态量子态进行三方秘密共享的方案, 结合三量子比特冯·诺依曼测量结果和局域酉算符操作, 可以实现确定性传输. 簇态 [137] 方案的原理本质上与上述方案类似, 实现了单量子比特态和双量子比特态的三方共享.

3.2 非对称分层量子秘密共享方案

Gottesman[141] 基于 QQ 的 (k,n) 门限方案, 对非对称性的量子信息分割做过初步讨论, 他提出可以对门限方案中的子秘密份额进行捆绑, 向参与者分配不同数量份额, 从而实现复杂结构或部分特定要求. 2010 年, Wang 等 [142] 使用一种 4 量子比特纠缠态 $|\chi\rangle$, 首次提出了非对称分割量子信息的

分层量子秘密共享方案 (hierarchical quantum sharing, HQSS), 这一类量子秘密共享方案考虑到参与者之间具有不同属性带来的能级划分, 例如在公司决策中董事长、经理和普通员工之间具有上下级关系, 不同权限能级的接收者在恢复量子秘密时需要不同的协作条件. 随后他们又提出了基于 6 量子比特簇态 [143] 和 t 量子比特 ($t \geqslant 3$) 图态 [144] 的分层 QQ 方案. 由 Shukla 等 [145] 进一步给出了一个在 n 方接收者中实现分层量子秘密共享的通用方案, 基于 4 量子比特 $|\Omega\rangle$ 态或 4 量子比特簇态. 这些方案均依赖特定多粒子纠缠态来支持分层结构的划分, 使得在分发者进行特定测量后坍缩的量子态下, 普通成员在某些基上只能得到相关测量结果, 因此仅当普通成员合作时无法恢复秘密. 正由于构建非对称性的分层 QQ 方案的纠缠态具有很强的特殊性, 分层 QQ 方案在实际部署和更一般的通用结构设计上都面临极大的挑战.

3.3 基于图态的量子信息秘密共享

图态是一类基于图的多粒子纠缠态. 这类纠缠态具有高度的非局域性质, 是目前实验室中最容易获得的多方资源量子态之一. 图态几乎可以编写所有的多方协议, 被提议为基于测量的量子计算、量子纠错和盲量子计算等各种多方量子信息处理任务中的主要资源态之一. 基于图态的量子秘密共享协议由于其使用的纠缠资源态, 天然具备了与复杂网络协议集成以及在纠缠扩展功能上进一步开发的能力. 图 6 为线性簇态、星形图态 (即 GHZ 态)、树形图态、环形图态、二维方格图态等类型图态.

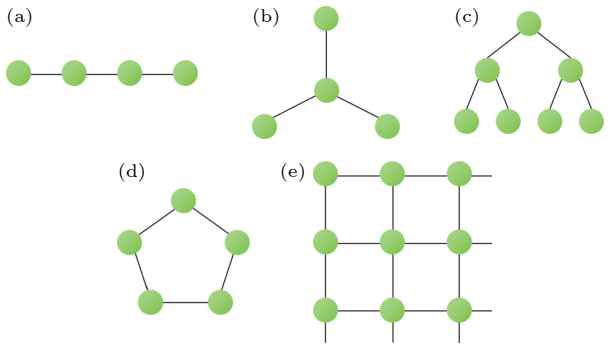

图 6 图态类型 (a) 线性簇态; (b) 星形图态; (c) 树形图态; (d) 环形图态; (e) 二维方格图态

Fig. 6. Types of graph states: (a) Linear cluster state; (b) star-shaped graph state; (c) tree-shaped graph state; (d) ring-shaped graph state; (e) 2D square graph state.

图态本身具有的图形直观地展示了各个部分复杂的纠缠, 提供了一种简化. 图的复杂连接性结构可以支持多样化的各种信息访问结构, 在量子网络的多层复杂通信协议的实现上极具发展前景.

给定一个包含 n 个顶点的无向图 $G = (V, E)$, 其中顶点集合 $V = \{v_i\}$ 表示量子比特, 边集合 $E = \{e_{ij} = (v_i, v_j)\}$ 表示量子比特之间存在的纠缠. 每个顶点上量子比特初始定义为 $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ 态, 对所有存在边相互连接的量子比特进行受控相位门 $\mathrm{CZ} = \mathrm{diag}(1, 1, 1, -1)$ 操作, 即可得到 n 阶图态:

$$|G\rangle = \prod_{e \in E} CZ_e |+\rangle^{\otimes n}. \tag{12}$$

图态可以通过稳定子生成元的方式来表示, 对于图态中任意第 i 个顶点, 其稳定子算符为

$$K_i = X_i Z_{N(i)}, \tag{13}$$

其中, $N(i)$ 表示图态 G 中与顶点 i 存在边连接的相邻顶点集合, $Z_{N(i)} = \bigotimes_{u \in N(i)} Z_u$.

图态由其稳定子算符的本征方程唯一确定, 这通常也被称为图态的不动点性质:

$$X_i Z_{N(i)} |G\rangle = |G\rangle. \tag{14}$$

在图态的标准框架上, Markham 等 [13] 通过给图态中的顶点附加额外的标签信息, 对稳定子算符作用下部分图态之间的等价性质进行证明, 从而对图态中信息的可访问性给出直观展示.

除去为图态提供了一个优雅的图形化表征之外, 图的相关结论可以被用来对量子性质进行辅助证明和理解. 图论理论为量子光学实验中复杂纠缠态的可构造性提供了新的分析方法 [146]. 图所给出的“流”概念刻画了量子秘密共享协议中秘密信息从分发者到授权者集合的传输路径 [147], 研究 [148,149] 进一步指出了图态中弱奇支配性质在基于图态的量子秘密共享协议中的关键作用. 事实上, 在图态提供的框架下经典信息和量子信息情景下的秘密共享可以形成优雅的统一 [13]. Keet 等 [150] 进一步把由二维量子比特构成的图态扩展至素数维度量子比特的图态, 广义图态下可以实现所有允许的访问结构, 为共享更高维度的经典和量子秘密提供了有用的框架.

基于图态的 CQ 方案中的授权者集合需要满足以下可访问性条件.

可访问性: 给定一个图 $G=(V, E)$, 如果存在集合 $B \subseteq V$, 使得 $\exists D \subseteq B$ 满足 $|D|=1 \mod 2$ 且 $\mathrm{Odd}(D) \subseteq B$, 则称该顶点集 B 具有可访问性, 其中 $\mathrm{Odd}(D)=\{v \in V \mid |N(v) \cap D|=1 \mod 2\}$.

基于图态的 CQ 方案是完美的, 未授权集合 (即所有不满足可访问性的集合) 都被证明具有弱奇支配集 (weak odd domination, WOD 集) 性质. WOD 集的约化密度矩阵与秘密无关, 因此任何未授权集合无法获取任何关于秘密的信息.

WOD 集: 当存在 $C \subseteq V \setminus B$, 使得 $B \subseteq \mathrm{Odd}(C)$ 时, 集合 B 是 WOD 集.

在 QQ 方案的情形下, 授权者集合 B 在满足可访问性条件之外, 量子不可克隆原理还额外要求 B 的补集为 WOD 集. 给定一个 n 阶图态 $G=(V, E)$, Gravier 等[149] 给出 QQ 协议如下.

1) 加密. 分发者将量子态秘密 $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$ 编码为 $|\Psi\rangle=\alpha|G_0\rangle+\beta|G_1\rangle$, 其中 $|G_0\rangle=|G\rangle$, $|G_1\rangle=Z_V|G\rangle$.

2) 分发. 将 $|\Psi\rangle$ 的每个量子比特分发给对应参与者.

3) 量子态秘密重构. 设集合 B 为授权者集合, B 满足可访问性, 且 B 的补集 $V \setminus B$ 为 WOD 集. 即 $\exists C, D \subseteq B$ 使得 $V \setminus B \subseteq \mathrm{Odd}(C)$, $|D|=1 \mod 2$, 且 $\mathrm{Odd}(D) \subseteq B$.

若参与者选择在 $u \in B$ 上恢复秘密, 则集合 $B \setminus \{u\}$ 中每个参与者将自己的量子比特传递给 u. u 额外使用一个辅助量子比特 $(|0\rangle+|1\rangle)/\sqrt{2}$, 与集合 B 中的量子比特一起构成一个 $(|B|+1)$ 个量子比特的系统, 在其上施加酉算符操作 $\frac{1}{\sqrt{2}}\begin{pmatrix} I & U \\ -U & I \end{pmatrix}$, 其中 $U=(-1)^{|G_D|}X_D Z_{\mathrm{Odd}(D)}$, 可以得到 $\alpha|0\rangle \otimes |G_0\rangle+\beta|1\rangle \otimes |G_1\rangle$.

再对其施加酉算符操作 $\begin{pmatrix} I & 0 \\ 0 & U' \end{pmatrix}$, 其中 $U'=(-1)^{|G_C|}X_C Z_{V \setminus \mathrm{Odd}(C)}$, 则有 $(\alpha|0\rangle+\beta|1\rangle) \otimes |G\rangle$, 秘密在第 1 个量子比特上被重建.

与 CQ 方案不同, 基于图态的 QQ 方案通常是不完美的, 即除了满足可访问性的授权者集合外, 存在其他集合可能会携带部分关于秘密的信息, 可以通过向上述协议引入一次一密来构造量子信息的量子秘密共享 (k, n) 门限方案. 分发者随机选择两个经典比特 $p, q \in \{0, 1\}$ 作为一次一密的密钥, 对量子态 $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$ 施加 $X^p Z^q$ 操作后再利用上述协议对加密后的新量子态 $|\alpha|p\rangle+\beta(-1)^q|1-p\rangle$ 进行共享. 经典比特 p, q 通过经典信息的 (k, n) 门限方案分发给参与者, 确保了仅当授权者集合 B 的大小 $|B| \geqslant k$ 时, 可恢复 p, q, 规模低于门限 k 的参与者集合将无法获得关于秘密的任何信息.

在 3.1 节已表述了由文献所给出的通用 QQ (k, n) 门限方案, 随着参与者数量的增加, 该方案将面临子份额量子态维度无限扩张的问题. 图态方法允许不依赖于参与者数量, 以较低维度的量子比特纯态设计秘密共享方案, 但会存在无法构造所有门限方案的缺陷. 在量子不可克隆原理的基础上, 基于图态的量子秘密共享 (k, n) 门限方案的门限下界进一步改进为 $k>0.506n$. 目前基于图态的量子秘密共享门限方案的构造均会导致准全体一致协议, 即 $k=n-\mathcal{O}(n)$. Gravier 等[149] 通过随机图证明了对于足够大的 n, 高概率性存在图 G 满足 $k \leqslant 0.811n$, 但尚且没有准全体一致协议的显式构造. 判定一个给定图态 G 的门限是否大于一个给定参数被证明是 NP 完全问题, 人们无法有效地验证一个随机生成的图态是否存在一个小的门限.

Bell 等[151] 首次在全光装置上实现了基于图态的量子秘密共享, 制备图态的主要技术手段从利用自发参量下转换源产生的纠缠光子概率性制备[152] 已经发展到利用原子单个记忆自旋发射的一系列单光子的确定性生成[153], 目前已经突破了简单的一维链型和星型图态, 在实验上实现了二维环型和树型图态的融合生成[154]. 基于芯片的光子图态制备也不断取得进展[155]. 虽然目前生成的光子图态规模尚小, 但原则上可以通过量子逻辑门的操作等方式将它们结合在一起扩展形成更大、更复杂的图态. 具有灵活连接性与能够在原子状态中长期储存信息的图态仍有待研究.

3.4 基于连续变量的量子信息秘密共享

2003 年, Lance 等[66] 提出并实验实现了一种基于连续变量的 $(2, 3)$ 门限量子信息秘密共享方案, 并且为区别于共享经典信息的 QSS. 如图 7 所示, 这个协议利用 1 : 1 分束器将一个秘密相干态 $\hat{a}_{\mathrm{in}}$ 与 EPR 对 $\hat{a}_{\mathrm{EPR1}}$ ($\hat{a}_{\mathrm{EPR2}}$) 中的一个进行干涉, 编码成一个三方纠缠. 分发者进一步使用与正交振幅具有相同相关性的高斯白噪声 (Gaussian white noise) $\delta\mathcal{N}$ 对三方纠缠进行调制, 共享的组分变为

$$\hat{a}_1 = (\hat{a}_{\rm in} + \hat{a}_{\rm EPR1} + \delta\mathcal{N})/\sqrt{2}, \tag{15}$$

$$\hat{a}_2 = (\hat{a}_{\rm in} - \hat{a}_{\rm EPR1} - \delta\mathcal{N})/\sqrt{2}, \tag{16}$$

$$\hat{a}_3 = \hat{a}_{\rm EPR2} + \delta\mathcal{N}^*, \tag{17}$$

其中 $\hat{a}_{\rm in} = (\hat{X}^+ + {\rm i}\hat{X}^-)/\sqrt{2}$, (+) 和 (−) 分别表示振幅和相位正交分量, $\delta\mathcal{N} = (\delta\mathcal{N}^+ + {\rm i}\delta\mathcal{N}^-)/2$ 是高斯噪声, $*$ 表示复共轭. 三方纠缠产生之后, 分别分发给 3 个参与者. 秘密重构阶段, 如果是参与者 1 和参与者 2 合作, 则利用 1:1 分束器的马赫-曾德尔干涉仪来重构量子态. 如果是参与者 1 (参与者 2) 和参与者 3 合作, 则利用一个 2:1 分束器和一个电光前馈环来重构量子态, 这个过程会更加复杂[156]. 正如 Lance 的方案中所提到的, 连续变量量子信息秘密共享的实现需要依赖前馈技术. 而前馈技术涉及到光-电和电-光的转换, 这种转换过程限制了量子信息秘密共享的带宽. 因此, 要拓宽量子信息秘密共享的带宽就要避免涉及到这种光与电之间的转换, 去构建全光的量子信息秘密共享体系. 虽然理论上使用相位不敏感放大器 (phase-insensitive amplifier, PIA) 可以避免前馈技术的使用[157], 但是耦合到 PIA 放大输出态的噪声难以直接控制, 一直以来实验实现较为困难. 2023 年, Chen 等[158] 利用基于双 Λ 构型四波混频过程的低噪声 PIA 代替了光电前馈技术, 实现了确定性的 (2, 3) 门限全光量子信息秘密共享, 在 1.4—2.4 MHz 的带宽范围内重构态的保真度均内超过经典极限. 与 Lance 等[66] 不同, Chen 等[158] 方案中重建态的形式与秘密态是相同的, 不需要对重构态进行后验 (posteriori) 就能得到有意义的保真度. 这为全光宽带量子网络的构建提供了一条途径.

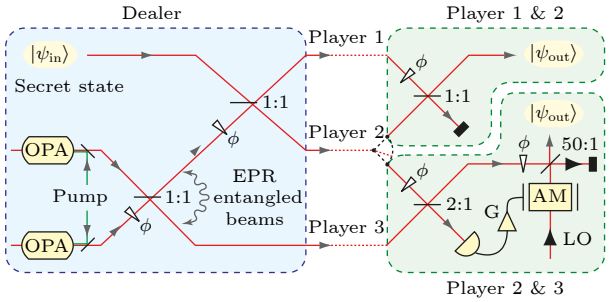

图 7 连续变量 (2, 3) 门限量子信息秘密共享方案示意图[66]

Fig. 7. Schematic of the (2, 3) threshold quantum information secret sharing scheme for continuous variable[66].

3.5 共享纠缠态的量子信息秘密共享

前面所提到的已经实现的一些量子信息秘密共享的方案[66,151,158] 中, 共享的都是纯量子比特态, 纠缠态的共享和恢复仍然没有实现. 2016 年 Lu 等[159] 通过使用一个六光子纠缠态演示了一个 (3, 3) 量子门限方案. 在这个方案中, 共享的保密量子态可以被有效地重建, 并且重建的量子态的保真度能够达到 93%. 如图 8 所示, 分发者将共享的量

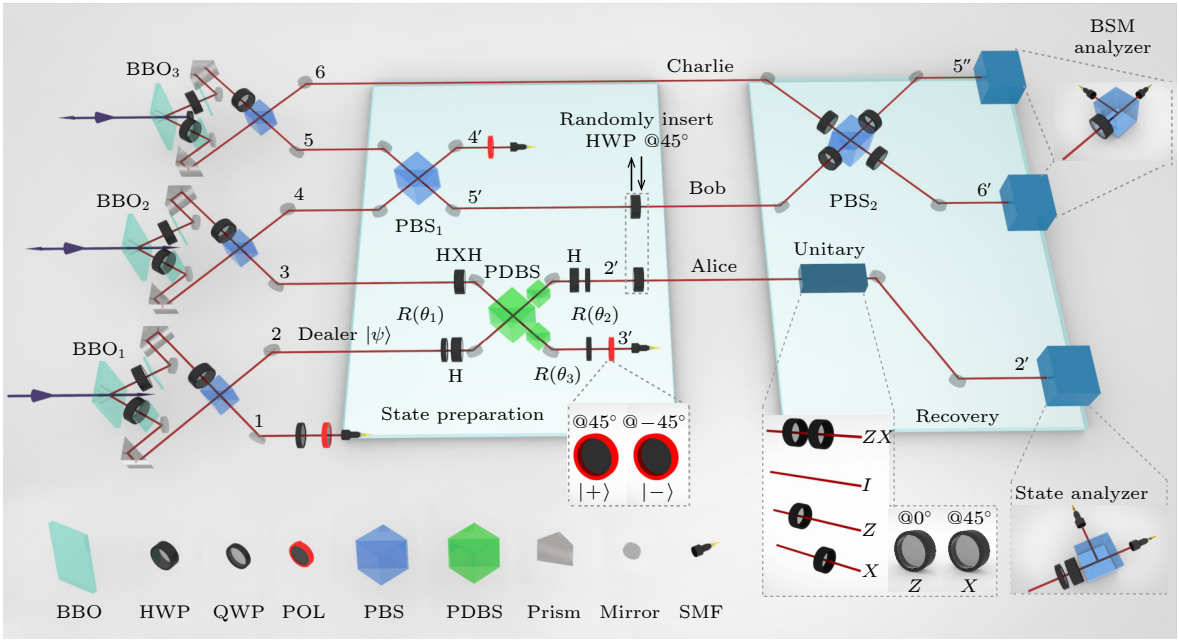

图 8 共享纠缠态的量子信息秘密共享实验装置示意图[159]

Fig. 8. Schematic of the experimental setup for quantum information secret sharing of entangled states[159].

子态 $|\psi\rangle=\alpha|H\rangle+\beta|V\rangle$, 并将其编码在一个三光子混合态中, 然后分发给三位参与者. 当且仅当其中两个参与者在他们的光子上进行 Bell 态测量之后, 第 3 个参与者才能根据他们的测量结果 $\{|\Phi^+\rangle,|\Phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle\}$ 对自己的光子施加相应的酉操作 $\{XZ,I,Z,X\}$, 从而恢复 $|\psi\rangle$, 其中 X,Z 是 Pauli 算子, I 是单位算子. Lu 等 [159] 进一步表明, 恢复量子态的纠缠见证 (entanglement witness) $\langle\mathcal{W}\rangle=-0.24\pm0.02<0$, 恢复的量子态仍然与 EPR 对的另一半纠缠在一起, 证明了利用这个方案也可以实现纠缠态的共享和恢复.

3.6 多方量子秘密直接传输

2020 年, Lee 等 [160] 提出了一种多方量子秘密直接传输的 QQ 协议, 并通过一个实验有效验证了他们的量子态传输. 其允许任意数量的分发者将量子态共享给任意数量的接收者, 并且在传输过程中任何一个子方都无法完全访问量子秘密. 协议中 n 名发送者利用 n 粒子 GHZ 态对所共享的量子秘密进行编码, 并和 m 名接收者集合共享一个由 $(n+m)$ 粒子的 GHZ 态作为量子信道, 每名发送方对自己持有的子秘密份额粒子和信道粒子进行分布式 Bell 基测量, 接收方根据所有测量结果在他们持有的 m 个信道粒子上联合施加逻辑泡利操作共同恢复量子态秘密. 去中心化传输无需依赖可信中间节点, 秘密始终由多方进行共享, 避免了单点失效风险, 对量子网络的安全性与容错性有重要意义.

4 总结与展望

二十多年来 QSS 繁荣发展, 表 2 列出了不同类型的 QSS 方案及其特点. 从纠缠态到单光子再到相干光, QSS 不断优化使用的资源, 使其更适配当前的技术水平并更好地兼容电信光纤网络, 增加其实用性. 同时, 环回、MDI 等协议提出也在不断提高着 QSS 的安全性. 但是实用的 QSS 往往面临着安全性问题, 而具有较高安全性的 QSS 又对技术有较高的要求. 迄今为止, 仍然缺乏兼顾实用性和安全性的 QSS 协议. 因此, 找到一个兼具实用性和安全性的 QSS 协议将是未来 QSS 研究的一个重要方向. 值得注意的是, 不论是共享经典信息的 QSS 还是共享量子信息的 QSS, 长久以来都一直受困于传输距离的限制无法远距离传输. 由于量子不可克隆定理, 量子信号无法像经典通信那样直接放大, 量子中继器 [161] 成为实现长距离量子通信的关键技术. 未来, 随着量子中继技术的进一步发展 [114,162,163], 人们不用担心衰减和噪声对通过长光纤发送的量子态的影响, QSS 的距离限制问题将得到解决. 同时量子中继还将为 QSS 提供更灵活的设置. 一方面通过引入中继节点可以构建多点到多点的量子网络, 可以实现动态的参与者选择和调整. 另一方面量子中继器可以缓存部分量子信息,

表 2 不同 QSS 方案的特点

Table 2. Characteristics of different QSS schemes.

QSS方案	特点
使用纠缠态的QSS	由于纠缠特性, 即使光源部分被攻击者控制, 只要测量端能够被完美表征并进行测量错误率即可获得安全的秘密共享. 但目前实验上高效制备纠缠态仍具有较大困难
使用单光子的QSS	相比于纠缠态, 单光子更容易制备和分发, 更具实验性和扩展性. 但仍与目前的通信光纤有适配性差异且容易受到特洛伊木马的攻击
使用相干光的QSS	实验实现简单, 与标准光纤适配更容易实现远距离传输, 具有高稳定性和易操作性. 但相干光存在多光子成分, 无法抵御光子数分裂攻击
离散变量的QSS	利用光子偏振态 $\|H\rangle$ 和 $\|V\rangle$ 或轨道角动量来编码密钥比特, 系统对损耗不敏感、测量和判别精度高. 但信道容量低、单光子制备困难
连续变量的QSS	利用光场的正交分量 $\hat{x}$ 和 $\hat{p}$ 来编码密钥比特, 相比于离散变量可以确定性实现. 但大多数方案要求独立激光源及激光源之间的信号同步, 并且易受到本振攻击
环回QSS	不用监测信号扰动, 密钥率能打破Pirandola-Laurenza-Ottaviani-Banchi界限. 但需要使用可变延迟马赫-曾德尔干涉仪限制了其实际应用
测量设备无关的QSS	能够消除测量端设备不完美带来的攻击风险, 有效增强系统的安全性. 但大多数协议传输效率仍然会随着用户数量的增加呈指数级下降
设备无关的QSS	能够消除所有实际不完美设备的安全漏洞. 但目前协议的性能仍然较低, 尚未有效实现

允许在不同时刻进行量子操作对接, QSS 可以在更宽松的同步条件下运行. 最终能够实现长距离安全实用的 QSS. 此外, 目前提出的 QSS 协议大多是单功能的, 即只能实现 QSS 协议本身, 只有少数协议能在相同硬件实现多种量子密码协议的切换. 要想更进一步地扩展 QSS 的实用性和安全性, 就需要构建具有多功能性和量子加密敏捷性的系统, 实现同一硬件下 QSS 和其他量子密码协议快速切换. QSS 作为多方量子通信的安全保障, 需要在大量用户之间共享秘密信息. 但目前的 QSS 协议大多只进行少数几方的实验演示, 远未达到多方量子通信的要求. 因此扩展 QSS 以容纳更多的用户并在实际通信网络中验证是 QSS 未来发展的一个至关重要的挑战. 在量子信息的秘密共享中, QSS 方案的设计架构很大程度上依赖于多方量子态的纠缠特性, 对于从起初的 GHZ 态到 Bell 态、簇态、W 态、图态等纠缠态的研究与使用为 QSS 方案做出了初步尝试与示范. 对于量子信息的秘密共享而言, 固定的纠缠资源态限制了 QSS 方案的一般性结构拓展, 实验室在制备与储存复杂纠缠态的局限性为量子情形下 QSS 的实际部署造成了很大的障碍. 虽然已经在 GHZ 态、EPR 对、图态等资源上进行了实验演示, 但目前对量子信息 QSS 的研究仍然十分缺乏, 大多数协议仅停留在理论阶段, 实验实现仍然困难. 量子纠错码理论与相关 QSS 方案深刻关联, 期待对于量子纠错码的研究能够为量子信息 QSS 提供更好的见解. 量子信息 QSS 依赖于量子信道的安全分发[133,164], 在随机选择部分粒子作为诱骗粒子进行窃听检测外, 通过部署波长过滤器和光子数分离器可以有效抵御特洛伊木马攻击[165]. 在噪声信道中, 可通过纠缠纯化[166]的方式蒸馏出最大纠缠态来提高量子通信的安全性, 而量子纠错码能够针对光子丢失、操作错误和不诚实参与者等问题进行容错[160,167,168], 提升了协议对噪声的鲁棒性. 但更为具体通用的方案仍待进一步研究. 与此同时, 量子信息的秘密共享作为分布式量子计算的安全基础, 要推动分布式量子计算的发展就需要实现量子信息 QSS 的可行化和实用化. 因此更加可行、高效的量子信息 QSS 协议的提出和实验也将在未来 QSS 的发展中发挥举足轻重的作用. 综上所述, QSS 未来的发展将聚焦在 4 个主要方向: 1) 实用性和安全性; 2) 多功能性和加密敏捷性; 3) 更多方用户和实际通信网络实现; 4) 量子信息 QSS 方案.

在量子时代, CQ-QSS 和 QQ-QSS 将成为高安全性场景的核心工具. 基于 QSS 的多方量子通信作为实现量子多方计算网络的关键要素, 提供了超越经典密码学限制的信息论安全. 虽然目前 QSS 仍然面临着许多挑战, 仍有一系列问题亟待解决. 但大量的研究已经表明 QSS 具有显著优势和广阔的发展前景. 在未来大型量子网络构建和分布式量子计算中, QSS 将发挥着不可替代的作用.

参考文献

[1] Shamir A 1979 *Communications of the ACM* **22** 612
[2] Blakley G R 1979 *Managing Requirements Knowledge, International Workshop on* (IEEE Computer Society) pp313–313
[3] Liao S K, Cai W Q, Liu W Y, et al. 2017 *Nature* **549** 43
[4] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, Bao Y, Wang Y, Fu Y, Yin H L, Chen Z B 2022 *PRX Quantum* **3** 020315
[5] Gu J, Cao X Y, Fu Y, He Z W, Yin Z J, Yin H L, Chen Z B 2022 *Sci. Bull.* **67** 2167
[6] Yin H L, Fu Y, Li C L, Weng C X, Li B H, Gu J, Lu Y S, Huang S, Chen Z B 2023 *Natl. Sci. Rev.* **10** nwac228
[7] Pan D, Long G L, Yin L, Sheng Y B, Ruan D, Ng S X, Lu J, Hanzo L 2024 *IEEE Commun. Surv. Tut.* **26** 1898
[8] Cao X Y, Li B H, Wang Y, Fu Y, Yin H L, Chen Z B 2024 *Sci. Adv.* **10** eadk3258
[9] Jing X, Qian C, Weng C X, Li B H, Chen Z, Wang C Q, Tang J, Gu X W, Kong Y C, Chen T S, Yin H L, Jiang D, Niu B, Lu L L 2024 *Sci. Adv.* **10** eadp2877
[10] Du Y, Li B H, Hua X, Cao X Y, Zhao Z, Xie F, Zhang Z, Yin H L, Xiao X, Wei K 2025 *Light: Sci. Appl.* **14** 108
[11] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[12] Cleve R, Gottesman D, Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[13] Markham D, Sanders B C 2008 *Phys. Rev. A* **78** 042309
[14] Qin S J, Gao F, Wen Q Y, Zhu F C 2007 *Phys. Rev. A* **76** 062324
[15] Chen Y A, Zhang A N, Zhao Z, Zhou X Q, Lu C Y, Peng C Z, Yang T, Pan J W 2005 *Phys. Rev. Lett.* **95** 200502
[16] Tittel W, Zbinden H, Gisin N 2001 *Phys. Rev. A* **63** 042301
[17] Karlsson A, Koashi M, Imoto N 1999 *Phys. Rev. A* **59** 162
[18] Zhang Z J, Gao G, Wang X, Han L F, Shi S H 2007 *Opt. Commun.* **269** 418
[19] Williams B P, Lukens J M, Peters N A, Qi B, Grice W P 2019 *Phys. Rev. A* **99** 062311
[20] Sen A, Sen U, Żukowski M 2003 *Phys. Rev. A* **68** 032309
[21] Gaertner S, Bourennane M, Eibl M, Kurtsiefer C, Weinfurter H 2003 *Appl. Phys. B* **77** 803
[22] Gaertner S, Kurtsiefer C, Bourennane M, Weinfurter H 2007 *Phys. Rev. Lett.* **98** 020503
[23] Yu I C, Lin F L, Huang C Y 2008 *Phys. Rev. A* **78** 012344
[24] Xiao L, Lu Long G, Deng F G, Pan J W 2004 *Phys. Rev. A* **69** 052307
[25] Xiao Y R, Jia Z Y, Song Y C, Bao Y, Fu Y, Yin H L, Chen Z B 2024 *Opt. Lett.* **49** 4210
[26] Ishio H, Minowa J, Nosu K 1984 *J. Lightwave Technol.* **2**

448
[27] Wengerowsky S, Joshi S K, Steinlechner F, Hübel H, Ursin R 2018 *Nature* **564** 225
[28] Bouwmeester D, Pan J W, Daniell M, Weinfurter H, Zeilinger A 1999 *Phys. Rev. Lett.* **82** 1345
[29] Pan J W, Daniell M, Gasparoni S, Weihs G, Zeilinger A 2001 *Phys. Rev. Lett.* **86** 4435
[30] Zhao Z, Yang T, Chen Y A, Zhang A N, Żukowski M, Pan J W 2003 *Phys. Rev. Lett.* **91** 180401
[31] Huang Y F, Liu B H, Peng L, Li Y H, Li L, Li C F, Guo G C 2011 *Nat. Commun.* **2** 546
[32] Pan J W, Chen Z B, Lu C Y, Weinfurter H, Zeilinger A, Żukowski M 2012 *Rev. Mod. Phys.* **84** 777
[33] Gisin N 2015 *Front. Phys.* **10** 100307
[34] Guo G P, Guo G C 2003 *Phys. Lett. A* **310** 247
[35] Deng F G, Zhou H Y, Long G L 2005 *Phys. Lett. A* **337** 329
[36] Han L F, Liu Y M, Liu J, Zhang Z J 2008 *Opt. Commun.* **281** 2690
[37] Wang T Y, Wen Q Y 2011 *Quantum Inf. Comput.* **11** 434
[38] Schmid C, Trojek P, Bourennane M, Kurtsiefer C, Żukowski M, Weinfurter H 2005 *Phys. Rev. Lett.* **95** 230505
[39] Bogdanski J, Ahrens J, Bourennane M 2009 *Opt. Express* **17** 1055
[40] Kuzin E, Nunez H C, Korneev N 1999 *Opt. Commun.* **160** 37
[41] Ma H Q, Wei K J, Yang J H 2013 *Opt. Lett.* **38** 4494
[42] Deng F G, Li X H, Zhou H Y, Zhang Z j 2005 *Phys. Rev. A* **72** 044302
[43] He G P 2007 *Phys. Rev. Lett.* **98** 028901
[44] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z, Shields A J 2015 *Phys. Rev. X* **5** 031030
[45] Tavakoli A, Herbauts I, Żukowski M, Bourennane M 2015 *Phys. Rev. A* **92** 030302
[46] Shen Y J, Wang X J, Xie Z W, Min C J, Fu X, Liu Q, Gong M L, Yuan X C 2019 *Light Sci. Appl.* **8** 90
[47] Bliokh K Y, Rodríguez-Fortuño F J, Nori F, Zayats A V 2015 *Nat. Photonics* **9** 796
[48] Pinnell J, Nape I, de Oliveira M, TabeBordbar N, Forbes A 2020 *Laser Photon. Rev.* **14** 2000012
[49] Smania M, Elhassan A M, Tavakoli A, Bourennane M 2016 *npj Quantum Inf.* **2** 16010
[50] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[51] Lütkenhaus N, Jahma M 2002 *New J. Phys.* **4** 44
[52] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[53] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[54] Lo H K, Ma X, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[55] Inoue K, Waks E, Yamamoto Y 2003 *Phys. Rev. A* **68** 022317
[56] Inoue K, Ohashi T, Kukita T, Watanabe K, Hayashi S, Honjo T, Takesue H 2008 *Opt. Express* **16** 15469
[57] Gu J, Cao X Y, Yin H L, Chen Z B 2021 *Opt. Express* **29** 9165
[58] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400
[59] Curty M, Azuma K, Lo H K 2019 *npj Quantum Inf.* **5** 64
[60] Yin H L, Chen Z B 2019 *Sci. Rep.* **9** 17113
[61] Fröhlich B, Lucamarini M, Dynes J F, Comandar L C, Tam W W S, Plews A, Sharpe A W, Yuan Z, Shields A J 2017 *Optica* **4** 163
[62] Shen A, Cao X Y, Wang Y, Fu Y, Gu J, Liu W B, Weng C X, Yin H L, Chen Z B 2023 *Sci. China Phys. Mech. Astron.* **66** 260311
[63] Wang Y Z, Sun X R, Cao X Y, Yin H L, Chen Z B 2024 *Phys. Rev. Appl.* **22** 044018
[64] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[65] Tyc T, Sanders B C 2002 *Phys. Rev. A* **65** 042310
[66] Lance A M, Symul T, Bowen W P, Sanders B C, Lam P K 2004 *Phys. Rev. Lett.* **92** 177903
[67] Kogias I, Xiang Y, He Q, Adesso G 2017 *Phys. Rev. A* **95** 012315
[68] Zhou Y Y, Yu J, Yan Z H, Jia X J, Zhang J, Xie C D, Peng K C 2018 *Phys. Rev. Lett.* **121** 150502
[69] Horodecki M, Horodecki P, Horodecki R 1998 *Phys. Rev. Lett.* **80** 5239
[70] Shor P W, Smolin J A, Thapliyal A V 2003 *Phys. Rev. Lett.* **90** 107901
[71] Jia X J, Zhang J, Wang Y, Zhao Y P, Xie C D, Peng K C 2012 *Phys. Rev. Lett.* **108** 190501
[72] Lau H K, Weedbrook C 2013 *Phys. Rev. A* **88** 042313
[73] Wu Y D, Zhou J, Gong X B, Guo Y, Zhang Z M, He G Q 2016 *Phys. Rev. A* **93** 022325
[74] Walk N, Eisert J 2021 *PRX Quantum* **2** 040339
[75] Grice W P, Qi B 2019 *Phys. Rev. A* **100** 022339
[76] Wu X D, Wang Y J, Huang D 2020 *Phys. Rev. A* **101** 022301
[77] Liao Q, Liu H J, Zhu L, Guo Y 2021 *Phys. Rev. A* **103** 032410
[78] Liao Q, Liu X Q, Ou B, Fu X Q 2023 *IEEE Trans. Commun.* **71** 6051
[79] Liao Q, Liu H J, Gong Y P, Wang Z, Peng Q Q, Guo Y 2022 *Opt. Express* **30** 3876
[80] Huang D, Huang P, Wang T, Li H, Zhou Y, Zeng G 2016 *Phys. Rev. A* **94** 032305
[81] Liao Q, Fei Z, Huang L, Fu X 2025 *Commun. Phys.* **8** 138
[82] Shen Y, Zou H, Tian L, Chen P, Yuan J 2010 *Phys. Rev. A* **82** 022317
[83] Liu S, Lu Z, Wang P, Tian Y, Wang X, Li Y 2023 *npj Quantum Inf.* **9** 92
[84] Murta G, Grasselli F, Kampermann H, Bruß D 2020 *Adv. Quantum Technol.* **3** 2000025
[85] Cao X Y, Gu J, Lu Y S, Yin H L, Chen Z B 2021 *New J. Phys.* **23** 043002
[86] Proietti M, Ho J, Grasselli F, Barrow P, Malik M, Fedrizzi A 2021 *Sci. Adv.* **7** eabe0395
[87] Richter S, Thornton M, Khan I, Scott H, Jaksch K, Vogl U, Stiller B, Leuchs G, Marquardt C, Korolkova N 2021 *Phys. Rev. X* **11** 011038
[88] Zhang Y F, Liu W B, Li B H, Yin H L, Chen Z B 2024 *Phys. Rev. A* **110** 052613
[89] Diamanti E, Leverrier A 2015 *Entropy* **17** 6072
[90] Liu W B, Li C L, Xie Y M, Weng C X, Gu J, Cao X Y, Lu Y S, Li B H, Yin H L, Chen Z B 2021 *PRX Quantum* **2** 40334
[91] Li S G, Li C L, Liu W B, Yin H L, Chen Z B 2024 *Adv. Quantum Technol.* **7** 2400140
[92] Gu J, Xie Y M, Liu W B, Fu Y, Yin H L, Chen Z B 2021 *Opt. Express* **29** 32244
[93] Sasaki T, Yamamoto Y, Koashi M 2014 *Nature* **509** 475
[94] Pirandola S, Laurenza R, Ottaviani C, Banchi L 2017 *Nat. Commun.* **8** 15043
[95] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V 2010 *Nat. Photonics* **4** 686
[96] Makarov V 2009 *New J. Phys.* **11** 065003
[97] Qin H, Kumar R, Makarov V, Alléaume R 2018 *Phys. Rev. A* **98** 012312
[98] Qi B, Fung C H F, Lo H K, Ma X 2007 *Quantum Inf.*

Comput. **7** 073
[99] Huang J Z, Weedbrook C, Yin Z Q, Wang S, Li H W, Chen W, Guo G C, Han Z F 2013 *Phys. Rev. A* **87** 062329
[100] Wei K, Zhang W, Tang Y L, You L, Xu F 2019 *Phys. Rev. A* **100** 022325
[101] Qin H, Kumar R, Alléaume R 2016 *Phys. Rev. A* **94** 012325
[102] Xu F, Ma X, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[103] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[104] Fu Y, Yin H L, Chen T Y, Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501
[105] Ma X, Qi B, Zhao Y, Lo H K 2005 *Phys. Rev. A* **72** 012326
[106] Gao Z, Li T, Li Z 2020 *Sci. China Phys. Mech. Astron.* **63** 120311
[107] Yang Y G, Wang Y C, Yang Y L, Chen X B, Li D, Zhou Y H, Shi W M 2021 *Sci. China Phys. Mech. Astron.* **64** 260321
[108] Liu T, Lai J, Li Z, Li T 2025 *Phys. Rev. Appl.* **23** 034057
[109] Zhang C, Zhang Q, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Zhou L, Sheng Y B 2025 *Phys. Rev. A* **111** 012602
[110] Liao Q, Huang L, Fei Z Y, Fu X Q 2025 *Adv. Quantum Technol.* **8** 2400505
[111] Wang Y, Tian C, Su Q, Wang M, Su X 2019 *Science China Information Sciences* **62** 72501
[112] Li C L, Fu Y, Liu W B, Xie Y M, Li B H, Zhou M G, Yin H L, Chen Z B 2023 *Phys. Rev. Res.* **5** 033077
[113] Azuma K, Tamaki K, Lo H K 2015 *Nat. Commun.* **6** 6787
[114] Azuma K, Tamaki K, Munro W J 2015 *Nat. Commun.* **6** 10171
[115] Roy S, Mukhopadhyay S 2019 *Phys. Rev. A* **100** 012319
[116] Zhang Q, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Zhou L, Sheng Y B 2024 *Phys. Rev. A* **110** 042403
[117] Zhang Q, Ying J W, Wang Z J, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Gu S P, Wang X F, et al. 2025 *Phys. Rev. A* **111** 012603
[118] Zhang Z, Yuan C, Shen S, Yu H, Zhang R, Wang H, Li H, Wang Y, Deng G, Wang Z, et al. 2021 *npj Quantum Inf.* **7** 123
[119] Chen X, Fu Z, Gong Q, Wang J 2021 *Adv. Photon.* **3** 064002
[120] Chopin A, Barone A, Ghorbel I, Combrié S, Bajoni D, Raineri F, Galli M, De Rossi A 2023 *Commun. Phys.* **6** 77
[121] Chen S, Peng L C, Guo Y P, Gu X M, Ding X, Liu R Z, Zhao J Y, You X, Qin J, Wang Y F, et al. 2024 *Phys. Rev. Lett.* **132** 130603
[122] Huang J, Mao J, Li X, Yuan J, Zheng Y, Zhai C, Dai T, Fu Z, Bao J, Yang Y, et al. 2025 *Nat. Photonics* **19** 471
[123] Nemirovsky-Levy L, Pereg U, Segev M 2024 *Optica Quantum* **2** 165
[124] Yan P S, Zhou L, Zhong W, Sheng Y B 2023 *Sci. China Phys. Mech. Astron.* **66** 250301
[125] Hu X M, Huang C X, Sheng Y B, Zhou L, Liu B H, Guo Y, Zhang C, Xing W B, Huang Y F, Li C F, et al. 2021 *Phys. Rev. Lett.* **126** 010503
[126] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[127] Senthoor K, Sarvepalli P K 2022 *IEEE Transactions on Information Theory* **68** 3164
[128] Yang Y G, Wang Y, Chai H P, Teng Y W, Zhang H 2011 *Opt. Commun.* **284** 3479
[129] Jia H Y, Wen Q Y, Gao F, Qin S J, Guo F Z 2012 *Phys. Lett. A* **376** 1035
[130] Sun Y, Xu S W, Chen X B, Niu X X, Yang Y X 2013 *Quantum Inf. Process.* **12** 2877
[131] Li Y, Zhang K, Peng K 2004 *Phys. Lett. A* **324** 420
[132] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2005 *Phys. Rev. A* **72** 044301
[133] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2006 *Eur. Phys. J. D* **39** 459
[134] Yuan H, Liu Y M, Zhang W, Zhang Z J 2008 *J. Phys. B* **41** 145506
[135] Shi R H, Huang L S, Yang W, Zhong H 2011 *Quantum Inf. Process.* **10** 231
[136] Pathak A, Banerjee A 2011 *Int. J. Quantum Inf.* **09** 389
[137] Muralidharan S, Panigrahi P K 2008 *Phys. Rev. A* **78** 062333
[138] Nie Y Y, Li Y H, Liu J C, Sang M H 2011 *Opt. Commun.* **284** 1457
[139] Roos C F, Riebe M, Häffner H, Hänsel W, Benhelm J, Lancaster G P T, Becher C, Schmidt-Kaler F, Blatt R 2004 *Science* **304** 1478
[140] Agrawal P, Pati A 2006 *Phys. Rev. A* **74** 062320
[141] Gottesman D 2000 *Phys. Rev. A* **61** 42311
[142] Wang X W, Xia L X, Wang Z Y, Zhang D Y 2010 *Opt. Commun.* **283** 1196
[143] Wang X W, Zhang D Y, Tang S Q, Zhan X G, You K M 2010 *Int. J. Theor. Phys.* **49** 2691
[144] Wang X W, Zhang D Y, Tang S Q, Xie L J 2011 *J. Phys. B* **44** 35505
[145] Shukla C, Pathak A 2013 *Phys. Lett. A* **377** 1337
[146] Chandran L S, Gajjala R 2024 *Quantum* **8** 1396
[147] Kashefi E, Markham D, Mhalla M, Perdrix S 2009 *Electronic Proceedings in Theoretical Computer Science* **9** 87
[148] Javelle J, Mhalla M, Perdrix S 2013 *New Protocols and Lower Bounds for Quantum Secret Sharing with Graph States* (Springer Berlin Heidelberg) pp1–12
[149] Gravier S, Javelle J, Mhalla M, Perdrix S 2013 In Hutchison D, Kanade T, Kittler J, Kleinberg J M, Mattern F, Mitchell J C, Naor M, Nierstrasz O, Pandu Rangan C, Steffen B, Sudan M, Terzopoulos D, Tygar D, Vardi M Y, Weikum G, Kučera A, Henzinger T A, Nešetřil J, Vojnar T, Antoš D, editors. *Mathematical and Engineering Methods in Computer Science*, Vol. 7721 (Berlin, Heidelberg: Springer Berlin Heidelberg) pp15–31
[150] Keet A, Fortescue B, Markham D, Sanders B C 2010 *Phys. Rev. A* **82** 62315
[151] Bell B A, Markham D, Herrera-Martí D A, Marin A, Wadsworth W J, Rarity J G, Tame M S 2014 *Nat. Commun.* **5** 5480
[152] Bell B A, Herrera-Martí D A, Tame M S, Markham D, Wadsworth W J, Rarity J G 2014 *Nat. Commun.* **5** 3658
[153] Cooper E S, Kunkel P, Periwal A, Schleier-Smith M 2024 *Nat. Phys.* **20** 770
[154] Thomas P, Ruscio L, Morin O, Rempe G 2024 *Nature* **629** 567
[155] Huang J, Chen X, Li X, Wang J 2023 *AAPPS Bulletin* **33** 14
[156] Lance A M, Symul T, Bowen W P, Tyc T, Sanders B C, Lam P K 2003 *New J. Phys.* **5** 4
[157] Lance A M, Symul T, Bowen W P, Sanders B C, Tyc T, Ralph T C, Lam P K 2005 *Phys. Rev. A* **71** 033814
[158] Chen Y, Zhu Q, Wang X, Lou Y, Liu S, Jing J 2023 *Adv. Photon.* **5** 026006
[159] Lu H, Zhang Z, Chen L K, Li Z D, Liu C, Li L, Liu N L, Ma X, Chen Y A, Pan J W 2016 *Phys. Rev. Lett.* **117** 030501
[160] Lee S M, Lee S W, Jeong H, Park H S 2020 *Phys. Rev. Lett.* **124** 060501

[161] Briegel H J, Dür W, Cirac J I, Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
[162] Azuma K, Economou S E, Elkouss D, Hilaire P, Jiang L, Lo H K, Tzitrin I 2023 *Rev. Mod. Phys.* **95** 045006
[163] Li C L, Yin H L, Chen Z B 2024 *Rep. Prog. Phys.* **87** 127901
[164] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 42317
[165] Tian Y, Wang J L, Bian G Q, Chang J Y, Li J 2024 *Adv. Quantum. Tech.* **7** 2400116
[166] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[167] And A 2012 *Commun. Theor. Phys.* **58** 661
[168] Gupta S, Sinha A, Pandey S K 2024 *Quantum Inf. Process.* **23** 58

SPECIAL TOPIC—Quantum information processing

Research status and prospects of quantum secret sharing*

YIN Hualei [1)#†] SHEN Jianyu [2)#] CHEN Nuo [2)#] CHEN Zengbing [2)]

1) (*School of Physics, Renmin University of China, Beijing* 100872, *China*)

2) (*School of Physics, Nanjing University, Nanjing* 210093, *China*)

(Received 30 April 2025; revised manuscript received 24 June 2025)

Abstract

Quantum secret sharing (QSS), as a quantum extension of classical secret sharing, uses the basic principles of quantum mechanics to share information safely among multiple parties, providing a new paradigm for information security. As a key foundation for secure multiparty quantum communication and distributed quantum computing, QSS has attracted considerable attention since its emergence. Currently, research in this field includes both classical and quantum scenarios, and continuous progress has been made in both theoretical and experimental aspects. This paper first reviews the current development of QSS for classical information. In this regard, significant and parallel progress has been made in both discrete-variable QSS and continuous-variable QSS. The QSS protocols for sharing classical information, from entangled states to single photons and then to coherent light, have been continuously optimized to better utilize available resources and achieve more efficient implementation under current technological conditions. Meanwhile, round-robin, measurement-device-independent, and other protocols have been steadily improving the security of QSS. Next, one will focus on QSS scheme for quantum secrets, which begins with the symmetry of access structures and introduces basic (k, n) threshold protocols, dynamic schemes that support adaptive agent groups, and symmetric quantum information splitting through entanglement. It further introduces hierarchical quantum secret sharing schemes for asymmetric splitting of quantum information. Considering practical laboratory conditions of quantum states as resources, an overall discussion is conducted on quantum secret sharing with graph states. Afterwards, the design of a continuous-variable scheme for quantum secret sharing is outlined, and entanglement state sharing and quantum teleportation between multiple senders and receivers are introduced. Finally, this review discusses and outlines the future development directions of QSS, thereby inspiring readers to further study and explore the relevant subjects.

Keywords: quantum secret sharing, quantum communication, quantum entanglement, multiparty quantum protocols

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.74.20250586

CSTR: 32037.14.aps.74.20250586

* Project supported by the National Natural Science Foundation of China (Grant No. 12274223).

# These authors contributed equally.

† Corresponding author. E-mail: hlyin@ruc.edu.cn

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

量子秘密共享研究现状与展望

尹华磊 沈建宇 陈诺 陈增兵

Research status and prospects of quantum secret sharing

YIN Hualei SHEN Jianyu CHEN Nuo CHEN Zengbing

引用信息 Citation: Acta Physica Sinica, 74, 160301 (2025) DOI: 10.7498/aps.74.20250586
CSTR: 32037.14.aps.74.20250586
在线阅读 View online: https://doi.org/10.7498/aps.74.20250586
当期内容 View table of contents: http://wulixb.iphy.ac.cn
