光学学报

量子信息掩蔽

刘正昊[1,2]，许金时[1,2*]，李传锋[1,2**]

[1]中国科学技术大学中国科学院量子信息重点实验室，安徽 合肥 230026；

[2]中国科学技术大学中国科学院量子信息与量子科技创新研究院，安徽 合肥 230026

摘要 量子信息掩蔽是量子信息处理中的一个新兴概念，它将量子信息完全转移至各个量子实体的关联之中，从而使单个量子系统不再包含掩蔽前的任何信息。量子信息掩蔽在量子比特承诺、秘密共享等方面都具有重要的应用；然而与量子态的克隆、广播、隐藏等操作类似，人们无法使用一个普适的两体幺正演化来实现量子信息的掩蔽。本文系统地介绍近期量子信息掩蔽方向的一系列研究进展：首先描述了可实现量子信息掩蔽态集合的几何特征，给出掩蔽操作的实现方法，讨论了其在信息论中的含义以及与量子纠错码等概念的联系；然后介绍量子信息掩蔽的实验实现，展现量子信息掩蔽在高维体系等复杂系统中的可行性，并展示其在量子秘密共享和噪声免疫的量子通信等方面的应用。

关键词 量子信息处理；量子纠缠；量子关联；量子通信

中图分类号 O413 **文献标志码** A **doi**：10.3788/AOS202242.0327001

Quantum Information Masking

Liu Zhenghao[1,2], Xu Jinshi[1,2*], Li Chuanfeng[1,2**]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui* 230026, *China*;

[2]*CAS Centre For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui* 230026, *China*

Abstract Quantum information masking, an emerging concept in quantum information processing, refers to the complete quantum information transfer from a single quantum carrier to the correlations of multiple quantum carriers, so that any single carrier no longer contains any information of the pre-masked state. Quantum information masking has applications in the fields such as qubit commitment and secret sharing; however, similar to operations like the cloning, broadcasting, and hiding of quantum states, masking of quantum information cannot be accomplished with a universal bipartite isometry. We will provide a systematical introduction of recent progress about quantum information masking: firstly, we will describe the geometric characteristics of the maskable set, discuss the realization of the masking operation, its information-theoretical implication and its relationship with quantum error correction; secondly, we will present the experimental realizations of quantum information masking, expound the feasibility of quantum information masking in complex systems such as high-dimensional systems, and demonstrate its application in quantum secret sharing and noise-resilient quantum communication.

Key words quantum information processing; quantum entanglement; quantum correlation; quantum communication

收稿日期：2021-09-01；**修回日期**：2021-10-12；**录用日期**：2021-10-25

基金项目：国家自然科学基金(61725504，U19A2075，11774335，11821404)、国家重点研发计划(2016YFA0302700，2017YFA0304100)、中科院前沿科学重点研究计划(QYZDY-SSW-SLH003)、中国科学院基金(ZDRW-XH-2019-1)、量子通信与量子计算机重大项目引导性项目(AHY020100，AHY060300)、中央高校基本科研业务费(WK2470000026，WK2030380017)

通信作者：*jsxu@ustc.edu.cn；**cfli@ustc.edu.cn

1 引 言

量子信息学是量子力学与信息科学的融合，它以量子态叠加原理为基础来研究信息处理，并开启量子信息新技术的大门[1]。量子信息处理不仅可以用于实现隐形传态[2-4]，密集编码[5]等非经典的任务，而且可以在大数分解[6]，积和式计算[7]等具体计算任务中展现超越经典计算机的算力[8-11]。这些非经典任务的实现和计算优势的取得离不开量子纠缠[12]。1935 年，Einstein 等[13]指出，量子力学基于波函数的描述与局域实在论不能兼容：两个相隔很远且没有相互作用的微观粒子，状态可以存在相互关联，且对其中一个粒子的测量将瞬间改变另一个粒子的状态。量子纠缠的存在导致量子系统出现一系列区别于经典体系的现象，例如两个粒子可以处在多种不同的“最大纠缠态”，但在这些状态下，描述两体系统中每个单独粒子状态的“约化密度矩阵”却都是完全相同的。此时，区分不同最大纠缠态所需的信息完全包含在量子纠缠，也就是两个粒子之间的关联中。那是否有可能在更为普遍的情况下，将单个量子所携带的信息完全转入两个量子的关联之中呢？量子信息的掩蔽操作实现的就是这种将量子信息向量子关联的转移。

量子信息掩蔽是量子信息处理中一个新兴的概念。在 Modi 等原始的定义中，量子信息掩蔽指使用一个两体幺正操作，将单个量子系统所携带的信息完全转移到其与一个空白系统之间的关联中，从而两体中任何一方的约化态都不包含原先量子系统的任何信息[14]。这种协议超越经典加密手段之处在于，掩蔽的是量子信息，而不是以量子方式掩蔽经典信息。若能够实现量子信息掩蔽，不仅能够保护量子信息的安全，还可将掩蔽操作和量子系统允许叠加的特点结合起来，在量子信息处理方向取得一系列应用。然而 Modi 等发现：不存在一个普适的操作对任意纯态实现两体量子信息掩蔽，这与量子力学中的不可克隆[15]、不可广播[16]、不可删除[17]、不可隐藏[18]等一系列“行不通”定理一样，都是由于量子演化的线性特点[19]导致的。普适两体量子信息掩蔽操作的不存在性给出了进一步研究量子信息掩蔽的两个潜在方向：其一是寻找受限的两体确定性掩蔽集，也就是考虑哪些量子态是可以被同一个幺正操作所掩蔽的；其二是构造两体确定性场景之外的掩蔽操作，例如推广到多体系统或进行概率性地掩蔽。

目前，量子信息掩蔽的研究已经展示了其深远的理论意义。例如从量子力学与热力学结合的角度入手，可用信息守恒证明普适的两体掩蔽是不可实现的[20]，这有助于理解量子多体系统中的信息置乱现象，从而对黑洞信息佯谬等物理问题给出一些独特的见解[21-22]。从量子信息守恒的角度入手，可以证明不可能在不引入外界随机性的前提下，实现量子比特承诺[14, 23]，而经典比特承诺的不存在性则可以看作是量子比特承诺不存在性的一个特例。以上结论展示了量子信息掩蔽理论在信息学研究中的价值。与此同时，量子信息掩蔽也具有一定的潜在应用，如利用两体确定性掩蔽集的几何特征，可以构建量子秘密共享的协议[24]。另一方面，针对量子信息掩蔽的实验研究仍然相对较少，特别是在光学系统中，直到 2021 年才有相关实验工作的报道[25-26]。由于量子信息掩蔽与量子通信协议之间存在密切关联，掩蔽编码在光子上的“飞行量子比特”将具有广阔的应用前景。

量子信息掩蔽研究的逐步发展使得该领域中的研究结果纷纭杂沓，本文将清晰地介绍量子信息掩蔽研究的发展现状，尽可能多地涵盖对于理解该问题有所裨益的内容，如：量子信息掩蔽可适用的范围有多大，如何实验实现量子信息掩蔽，量子信息掩蔽有哪些应用，以及它与量子信息学、量子力学、物理学乃至普遍的自然科学中其他概念的关系如何？本文主要内容可简要概括如下：首先，将分别对两体和多体情况下的量子信息掩蔽给出严格的数学定义，找出实现量子信息掩蔽的映射，并研究最大可掩蔽集的性质；其次，介绍在光学系统中基于量子干涉和量子线路等方法的量子信息掩蔽的实验实现；然后展示量子信息掩蔽在诸多场景下的应用；最后，简要讨论量子信息掩蔽与量子纠错码等已经建立的概念之间的关系以及其在热力学和信息论中的意义，从而进一步展望量子信息掩蔽今后发展的方向。

2 量子信息掩蔽的定义和理论研究进展

“掩蔽”操作是指使得一些客体被掩盖在某个表面之下，从而不能被外界观察到。量子信息掩蔽的概念可以用图 1 形象地表示出来：它将量子信息完全转移至各个量子实体的关联之中，从而单个量子系统中不再包含掩蔽前的任何信息，对于单个观察者而言，原先的量子信息相当于被隐藏起来了。首先从 Modi 等最早对于量子信息掩蔽定义中的精神出发，给出一个对于纯态和混态都适用的量子信息

掩蔽的定义，而后讨论在各种情况下量子信息掩蔽操作的可行性以及可被掩蔽量子态的性质。

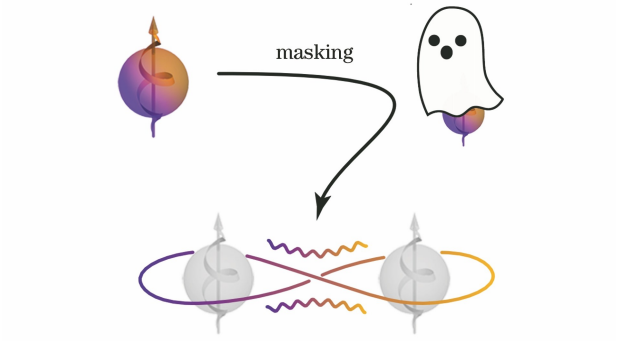

图 1　量子信息掩蔽的概念图。图中渐变线和背景表示信息所处的位置

Fig. 1 Conceptual art of quantum information masking. Gradient lines and shading indicate the site of information storage

一个两体掩蔽操作指的是使用一个线性等距映射 U 把一系列 d 维单体量子态 $\rho_s^{\mathrm{A}}\in\mathscr{H}^d$，$s\in\{1,2\cdots\}$ 映射到一系列两体量子态 $\rho_s^{\mathrm{AB}}\in\mathscr{H}^d\otimes\mathscr{H}^d$ 上，即

$$\rho_s^{\mathrm{A}}\rightarrow\rho_s^{\mathrm{AB}}=U(\rho_s^{\mathrm{A}}\otimes|0\rangle\langle 0|)\,, \tag{1}$$

其中 $\mathscr{H}^d$ 代表 d 维希尔伯特空间。从而当仅考虑单个子系统时，各个下标 s 对应的子系统状态 $\tilde{\rho}_s^{\mathrm{A}}\equiv\mathrm{Tr}^{\mathrm{B}}(\rho^{\mathrm{AB}})$ 和 $\tilde{\rho}_s^{\mathrm{B}}\equiv\mathrm{Tr}^{\mathrm{A}}(\rho^{\mathrm{AB}})$ 分别是完全相同的，亦即所有 ρ_s^{AB} 都具有相同的单体约化态：

$$\forall s,\mathrm{Tr}^{\mathrm{B}}(\rho_s^{\mathrm{AB}})=\tilde{\rho}^{\mathrm{A}},\mathrm{Tr}^{\mathrm{A}}(\rho_s^{\mathrm{AB}})=\tilde{\rho}^{\mathrm{B}}, \tag{2}$$

上述定义保证了掩蔽后每个粒子本身都不携带原先量子态 ρ_s^{A} 的任何信息。将掩蔽操作前的单体量子态所构成的集合 $\mathscr{M}=\{\rho_s^{\mathrm{A}}|s\in\{1,2\cdots\}\}$ 称为对应于线性等距映射 U 的可掩蔽集。

2.1　量子信息两体掩蔽的非普适性

Modi 等发现，由于量子力学中量子态演化的线性特点，不存在一个普适的量子信息掩蔽操作，可以将任意的量子态掩蔽至两体间的关联中。简要地复述文献[14]中的证明。假设一个等距映射 U 可以掩蔽量子态 $|\psi_0\rangle$ 和 $|\psi_1\rangle$，掩蔽操作分别得到 $|\Psi_0\rangle$ 和 $|\Psi_1\rangle$，若该映射是普适的，则它也能够掩蔽 $\mu|\psi_0\rangle+\nu|\psi_1\rangle$，并且由于 U 为线性的，掩蔽后得到的量子态是 $\mu|\Psi_0\rangle+\nu|\Psi_1\rangle$。由(2)式，$\rho^{\mathrm{B}}=\mathrm{Tr}^{\mathrm{A}}[(\mu|\Psi_0\rangle+\nu|\Psi_1\rangle)(\mu^*\langle\Psi_0|+\nu^*\langle\Psi_1|)]$，展开等号右边有

$$\mathrm{Tr}^{\mathrm{A}}(\mu\nu^*|\Psi_0\rangle\langle\Psi_1|+\mu^*\nu|\Psi_1\rangle\langle\Psi_0|)=0。 \tag{3}$$

另一方面，由于 $|\psi_0\rangle$ 和 $|\psi_1\rangle$ 都是 $\tilde{\rho}^{\mathrm{A}}$ 的纯化，可以将其写为 Schmidt 分解的形式：$|\Psi_0\rangle=\sum_k\sqrt{\lambda_k}|a_k\rangle|b_k^{(0)}\rangle$，$|\Psi_1\rangle=\sum_k\sqrt{\lambda_k}|a_k\rangle|b_k^{(1)}\rangle$。代入(3)式并两边求 B 粒子在 $|b_j^{(0)}\rangle$ 下的期望得

$$\lambda_j(\mu v^*\langle b_j^{(1)}|b_j^{(0)}\rangle+\mu^* v\langle b_j^{(0)}|b_j^{(1)}\rangle)=0。 \tag{4}$$

(4)式对任意的 μ，ν 都成立，意味着要么 $\langle b_j^{(0)}|b_j^{(1)}\rangle=0$，要么 μ，ν 的选取存在一定限制，都与掩蔽操作的普适性矛盾。因此，普适的两体量子信息掩蔽操作是不存在的。

2.2　量子信息两体掩蔽的最大可掩蔽集

既然不存在普适的量子信息两体掩蔽操作，那么量子信息的掩蔽在哪些场景下仍然是适用的呢？如果待掩蔽的态没有布满整个 Hilbert 空间，而是局限于一个受限的子集内，则量子信息掩蔽仍然是有可能实现的，例如凡是对易的量子态都可以被同一个等距映射所掩蔽[25,27]；这些量子态同时也是可广播的[16]。包含整个态空间中所有可掩蔽态的受限子集称为最大可掩蔽集。

为了说明存在一些操作可以实现对于一部分量子态的掩蔽，可以首先考虑经典信息的加密，从而得到一些启发。经常用到两个概念：加密和编码。两者都是将信息转化为另一种格式的操作。不同之处在于，加密强调对于信息的还原依赖于特定的解密方法，因此第三方很难破解；而编码则强调对信息使用的操作方法是公开的，因此获得编码后的信息就容易反推出编码前的信息。具体到量子信息掩蔽而言，对于窃听者由于使用的操作是未知的，所以掩蔽是一个加密过程，而对于发送者则是一个编码过程。一种可行的经典信息加密手段是使用流密码：发送方生成一个随机数序列(称为“加密数据流”)，将待发送的数据与加密数据流做按位异或操作，而后分别向接收方发送异或操作后的数据和加密数据流。可以证明这两个数据流都不包含加密前的任何信息[28]，因此起到了和量子信息掩蔽相类似的效果。接收方得到两串数据流之后，再对他们执行一次按位异或操作就可将原先待发送的信息解码出来。在量子力学中，对应于经典异或门的操作是量子受控非门(CNOT)。考虑将一个 CNOT 门作用在叠加态上的情况，此时系统发生的演化为

$$\mathrm{CNOT}\{[a|0\rangle+b\exp(\mathrm{i}\phi)|1\rangle]\otimes|0\rangle\}\rightarrow a|00\rangle+b\exp(\mathrm{i}\phi)|11\rangle,$$

注意演化之后，系统的两个单体约化态都为 $\tilde{\rho}=a|0\rangle\langle 0|+b|1\rangle\langle 1|$，与相位 ϕ 无关，因此所有的确定比例的量子比特叠加态以及其概率混合都可被

CNOT 门掩蔽。如图 2(a) 所示，这些态在量子比特的 Bloch 球表示上构成一个圆盘。进一步地，由于可以使用一个幺正旋转变换将 Bloch 球上的圆盘做任意旋转，因此使用 CNOT 门辅以幺正旋转，可以实现对于 Bloch 球上每个圆盘所对应的量子态的掩蔽。根据上述观察结果，Modi 等猜想对于高维量子系统，每个可掩蔽集在态空间的几何表示下，仍然都处于一个圆盘上[14]。

对于两体掩蔽一个量子比特，输出两个量子比特的情况，Liang 等[24]证明上述的“圆盘猜想”，并且给出实现掩蔽操作的等距映射的解析形式。借助任意高维量子态使用正交向量的展开形式[29]可以证明，每一个将 d 维系统映射为 $d\times d$ 维两体系统的掩蔽映射，其掩蔽集都落在态空间中的一个 d^2-1 维的圆盘上[25]。对于映射后两体系统的希尔伯特空间维数不等于 $d\times d$ 的情况，结论则更为复杂。Ding 等[30]指出，对于所有待掩蔽态维数 $d>2$ 的情况，当约化态的谱存在简并时，均可能构造出形式不为单个圆盘的最大可掩蔽集；尤其是当约化态为最大混态时，通过显式构造可知，掩蔽集不可被有限个圆盘覆盖。因此，利用约化态中谱的简并性，可以构造出性质奇特的可掩蔽集。

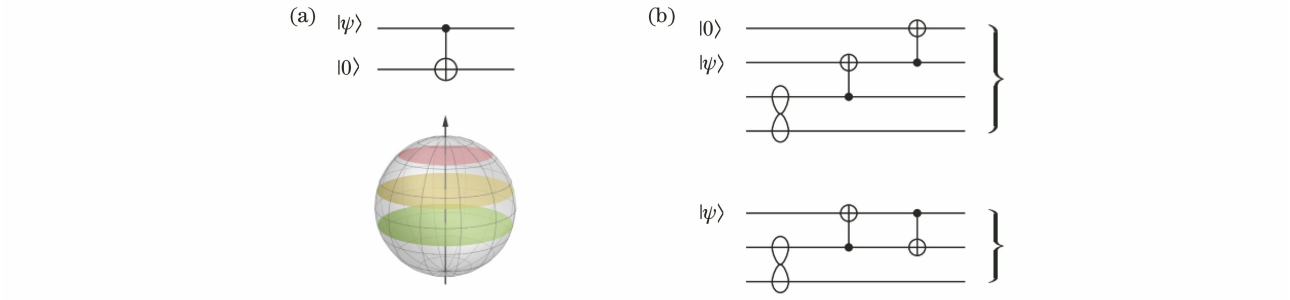

图 2　实现量子信息掩蔽的线路。(a)使用一个量子受控非门就可以在量子比特态空间实现受限的两体量子信息掩蔽，上图为量子受控非门在量子线路中的符号，下图的 Bloch 球表示中，每一个圆盘上的态都对应一个最大掩蔽集；(b)对于高维量子信息实现四体掩蔽和三体掩蔽的量子线路；构造方法源自参考文献[31]。线路之间的“8”字型连接表示对应的两体子系统处于最大纠缠态

Fig. 2 Circuit realizing quantum information masking. (a) A quantum controlled-NOT gate can realize bipartite quantum information masking in the limited qubit state space. Top: symbol of the quantum controlled-NOT gate in quantum circuit. Bottom: each state on a disk in the Bloch sphere corresponds to a maximum masking set; (b) realization of quadpartite and tripartite masking of high-dimensional quantum information; the composition is derived from reference [31]. "8"-shaped connection between the lines indicates that the corresponding bipartite subsystem is maximally entangled

“圆盘猜想”对于分析量子信息掩蔽的安全性具有重要的作用。从两体掩蔽的定义本身来看，被掩蔽的信息原则上是相当安全的。由于掩蔽后的约化密度矩阵对于任何可掩蔽态都是相同的，即使一个窃听者已知使用的掩蔽映射，在缺少两个输出粒子中的任何一个的情况下，他都不可能还原出被掩蔽前的量子态；即使窃听者对无穷份拷贝进行最优测量，也只能确定出可掩蔽集的参数，而无法进一步找出具体被掩蔽的量子态。然而，实际使用时，量子信息掩蔽的安全性还要受到使用的掩蔽操作的制约。对于量子比特而言，若在可掩蔽集所在的圆盘上随意猜测一个点 ρ'，那么平均来说与实际被掩蔽的量子态 ρ_0 之间的迹距离[32]将达到 $\frac{1}{2}\|\rho'-\rho_0\|_1=0.45\sqrt{1-z^2}$[33]，其中 z 是圆盘在 Bloch 球中的截距。可见当圆盘的截距接近 1 时，若窃听者已知使用的掩蔽映射，又获得了掩蔽后输出的其中一个粒子，就可能从中提取大量的信息；这是因为此时圆盘的面积已经大大缩小，上面包含的点代表的量子态都十分接近。另一方面，当圆盘接近 Bloch 球的球心时，其具有较大的面积，此时可掩蔽集参数则很难帮助进一步确定被掩蔽的量子信息。

在量子力学中，各个本征状态的叠加可以存在不同的相位，从而表示量子系统状态的密度矩阵可以包含复数的元素。如果要求密度矩阵仅包含实数元素，那么就等于人为地要求了量子态叠加时携带的相位是相同的，服从该约束条件的“实数量子力学”具有一些非平凡的性质[34-35]。Zhu[36]指出，实数量子力学中所有的量子态都可以被一个操作同时掩蔽，而且实数量子力学中所有态的集合，在普通的复数量子力学中也构成一个最大可掩蔽集。另一方面，如果一组单体密度矩阵的线性生成空间等于整

个希尔伯特空间，那么他们对应的量子态构成一个信息完备集；任何信息完备集必不可以被掩蔽。

上面已经讨论了量子信息两体掩蔽的最大可掩蔽集的一些可能的形式。一个进一步的问题是：可掩蔽的量子态在整个态空间所占的比例如何？由于信息完备集无法被掩蔽，因此可掩蔽集的维度应当比整个态空间的维度要小。Liang 等[37]指出，若使用 Haar 测度来进行衡量，那么可掩蔽集在整个态空间中总是具有零测度，这可以形象地理解为在高维 Bloch 球中，任何可掩蔽集都对应于一个厚度为 0 的超平面或超曲面；最大可掩蔽集的几何特征将在量子秘密共享方面发挥作用。另一方面，尽管可掩蔽集必为零测度的定理在一定程度上限制了量子信息掩蔽的适用范围，可实现量子信息掩蔽的态的资源仍是相当丰富的。例如在维度 d 为偶数的希尔伯特空间中，总可以通过显式构造，得到一个维度至少为 $d(d-1)$ 的可掩蔽集[25]，且该掩蔽集在 d 维欧式空间表示中具有非零的体积测度。因此可掩蔽集的维度也存在一个下限，从而两体掩蔽仍然是一种有效的量子信息处理手段。

2.3　量子信息的多体掩蔽和概率掩蔽

本小节将讨论确定性两体掩蔽之外实现量子信息掩蔽的方法。尽管一般来说不可能将任意的量子信息存放在两体关联中，但是存放进三体或更多体之间的关联却是有可能的。在多体量子信息掩蔽中，一个线性等距映射将量子态转移至多个量子系统之间的关联中，使每个子系统都不携带关于原先量子态的任何额外信息，也就是每个约化态都与入射态无关。Li 等[38]给出一种十分巧妙的构造，借助数学中正交拉丁方阵的语言，可以将任意 $d\neq 2,6$ 维希尔伯特空间 $\mathcal{H}^d$ 中的量子信息转入 $\mathcal{H}^d\otimes\mathcal{H}^d\otimes\mathcal{H}^d$ 中的三体关联上；$\mathcal{H}^2$ 的多体完全掩蔽则需要至少使用 4 个目标量子比特才能够实现[39-40]。在此简要地复述通过正交拉丁方阵构造掩蔽操作的过程。一个 d 阶拉丁方阵 $\boldsymbol{\Lambda}^d$ 是一个 $d\times d$ 维矩阵，其元素 $(\boldsymbol{\Lambda}^d)_{ij}\in\mathbb{Z}_d$ 在每一行和每一列中都不重复。如果两个拉丁方阵 $\boldsymbol{\Lambda}_1^d$，$\boldsymbol{\Lambda}_2^d$ 对应位置中的元素组成的二元组的集合 $\{\{(\boldsymbol{\Lambda}_1^d)_{ij},(\boldsymbol{\Lambda}_2^d)_{ij}\}\,|\,i,j\in\{1,2,\cdots,d\}\}$ 不包含重复的元素，则称他们是正交的。将 d 维希尔伯特空间中的一组正交完备基矢记为 $\{|1\rangle,|2\rangle,\cdots,|d\rangle\}$，并定义矩阵 $\boldsymbol{\Gamma}^d$，$(\boldsymbol{\Gamma}^d)_{ij}=j$，那么映射

$$|i\rangle\rightarrow\frac{1}{\sqrt{d}}\sum_{j=1}^{d}|(\boldsymbol{\Gamma}^d)_{ij}\rangle\otimes|(\boldsymbol{\Lambda}_1^d)_{ij}\rangle\otimes|(\boldsymbol{\Lambda}_2^d)_{ij}\rangle,\tag{5}$$

可以掩蔽 $\mathcal{H}^d$ 中所有的量子态。上面的构造仅仅用到正交拉丁方阵的存在性[41]，实际操作起来掩蔽 d 维量子信息时，原则上还需要给出一对 d 阶正交拉丁方阵的具体形式。但是由于奇数阶的正交拉丁方阵可以方便地构造出来[38]，对于偶数维的量子态，总可以将其通过直和操作嵌入到高一维的奇数阶希尔伯特空间中，再将量子信息掩蔽 $\mathcal{H}^{d+1}\otimes\mathcal{H}^{d+1}\otimes\mathcal{H}^{d+1}$ 维的三体关联中。因此该构造方法也方便被运用于实际的量子信息处理任务。

在当前阶段的数字式量子计算机中，操作者可以使用的往往是一系列标准化的门操作[42]，使用模块化门操作构造量子信息的多体掩蔽操作有助于研究量子多体系统的行为，如量子信息置乱[22,43]、多体局域化[44-45]以及奇异物相的涌现[46-48]。文献[38]证明，$\mathcal{H}^d$ 中的量子信息总是可以被掩蔽在 $(\mathcal{H}^d)^{\otimes 2d}$ 的量子关联之中，也就是使用额外的 $2d-1$ 个 d 维量子比特，可以实现对一个 d 维量子比特的掩蔽。Shang 等[31]将 CNOT 门在高维下推广为钟表算符，借鉴量子隐形传态中的量子线路，进一步发展了多体量子信息掩蔽，构造出图 2(b) 所示的量子线路，可以将任意维度的量子信息转移至相同维度四体和三体关联内的掩蔽操作形式。

尽管量子信息掩蔽不可在两体下对于所有量子态普适地完成，然而类似的非普适操作在量子力学中是广泛的，且他们允许概率性地实现，例如可以实现非正交量子态的概率性克隆[49-50]。在文献[51-52]中，定义了量子信息的概率性掩蔽操作，这种操作可以被理解为在两体量子信息掩蔽的基础上，额外引入一个辅助量子比特，在对整体进行幺正操作后附加一个后选择，当辅助量子比特的值与目标相同时，量子信息转移到两体关联之中。对于一组线性独立的态，可以实现量子信息的概率性掩蔽[51]，且掩蔽的成功率与被掩蔽量子态之间的内积有关。适用于整个态空间的两体量子信息概率性掩蔽则是不可能的[52]。除此之外，还可实现量子信息的近似掩蔽；一个 ε-近似两体量子信息掩蔽定义为在操作之后，每个条件态与理想结果的保真度均高于 $1-\varepsilon$。若输入、输出态空间的维度分别为 d，d'，仅当 $\varepsilon\geqslant(\sqrt{1+36/\min(d,d')}-1)/36$ 时，可对整个态空间中的量子态实现两体的近似量子信息掩蔽。对于高维量子态，近似量子信息掩蔽将更为困难，不可能对所有量子态实现高保真度的掩蔽，因此上述结果从另一个角度表明，量子信息的不可普适掩蔽定理具有较强的鲁棒性[52]。

3　量子信息掩蔽的光学实现

随着量子信息掩蔽理论的发展逐步推进，该方向的实验研究也逐渐深入，并开始受到越来越广泛的关注。实验研究量子信息的掩蔽，尤其是基于光子编码的光量子信息的掩蔽，不仅可以对理论的结果给出直接检验，从而对量子力学的基础取得更为深刻的理解，而且有助于研究量子信息掩蔽在实际场景下的可行性及应用，进而设计出一些新的量子信息处理协议，在一些量子保密通信的应用场景中发挥优势。

实现光量子信息的掩蔽首先要在线性光学的框架下，将量子信息编码在光子上。光子具有丰富的自由度，例如偏振、路径、轨道角动量、时间窗口等[53]，他们均可用于进行量子信息处理，而对应的实现方法则各有不同。例如在偏振编码中，光子的水平和竖直偏振状态分别对应于量子比特的$|0\rangle$和$|1\rangle$两个本征态，常将其对应地记为$|\mathrm{H}\rangle$和$|\mathrm{V}\rangle$；在路径编码中，每一条不同的路径都代表高维量子态中一个不同的本征状态。基于线性光学的光量子处理具有模式数高、读写精度高、免疫环境噪声等一系列突出优势；另一方面，由于光子之间不进行相互作用，因此可实现的门操作深度较为有限，尤其是在偏振编码下，受控非门[54]和受控相位门[55-57]将损失88%的光子，且不能在两个已经经历过受控门操作的光子上进行。因此实现光量子信息的掩蔽有两种可行的途径，一是通过模块化的门操作[58]，辅以优化的量子线路来实现，二是通过光子之间波函数的干涉[59]，直接进行量子信息的掩蔽。下面通过介绍两个实验，分别展示两种途径的实现方法。

3.1　基于光子间波函数干涉的光量子信息掩蔽

在量子力学发展的早期，Dirac 曾提出一个著名的观点：每个光子都只会与自身发生干涉，不同的光子之间从来都不发生干涉[60]。然而对粒子全同性研究的发展给人们带来了全新的认识[61]。全同光子之间波函数的干涉是光的量子特性的一种重要的体现，被广泛用于量子力学基础问题的研究[62-64]，量子纠缠资源的制备[65-67]以及量子态的受控操作[68-70]等任务中。Liu 等[25]借助全同双光子波函数的量子干涉，报道了光学系统中实现了最大可掩蔽集的两体量子信息掩蔽。实验装置如图 3 所示，他们使用非线性晶体中光子的参量下转换现象制备两个波长相同，偏振处于直积态的光子，使用偏振自由度在其中一个光子上编码一个量子比特，并且使得另一个光子处于偏振叠加的状态。随后将两个光子在一个偏振分束棱镜上干涉，并且通过光子符合探测技术筛选出从偏振分光棱镜出射后沿不同方向前进的光子对，导致两个光子的偏振状态向一个纠缠的投影基$|\mathrm{HH}\rangle\langle\mathrm{HH}|-|\mathrm{VV}\rangle\langle\mathrm{VV}|$投影[71]，从而以 50%的效率实现了量子信息掩蔽映射，掩蔽操作的成功率高出光学受控非门三倍以上。进一步地，他们在双光子波函数干涉前使用波片组施加一幺正旋转操作来进行基底变换，使得可掩蔽集从 Bloch 球纬线环绕的圆盘扩展到 Bloch 球内的任意圆盘。实验数据可总结为图 4 中的结果。实验中，观察到五个位于 Bloch 球上同一圆盘的量子态均可被同一操作掩蔽，从而在量子比特场景下直接检验了量子信息掩蔽的圆盘猜想。掩蔽后的两个接收方的约化密度矩阵较理论值的迹距离平均值为2.81×10^{-2}，因此每个仅接收到其中一个光子的接收方几乎得不到原先量子态的任何信息。另一方面，掩蔽后整个两体量子态与理论值的保真度为 97.7%，表明原先量子态的信息仍然较好地保留在两体关联中，达到了量子信息掩蔽操作的目的。

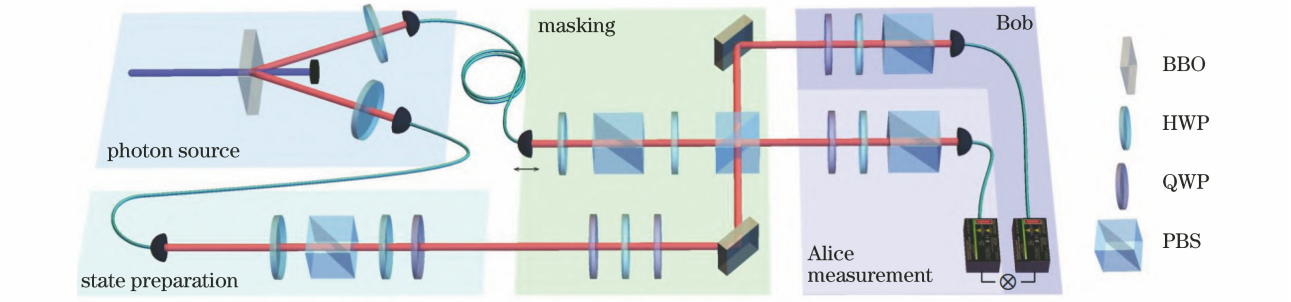

图 3　使用双光子波函数干涉实现量子信息掩蔽的实验装置[25]。BBO：非线性晶体；HWP：半波片；QWP：四分之一波片；PBS：偏振分光棱镜

Fig. 3　Experimental configuration of quantum information masking based on two-photon interference[25]. BBO: beta barium borate (nonlinear crystal); HWP: half-wave plate; QWP: quarter-wave plate; PBS: polarizing beam splitter

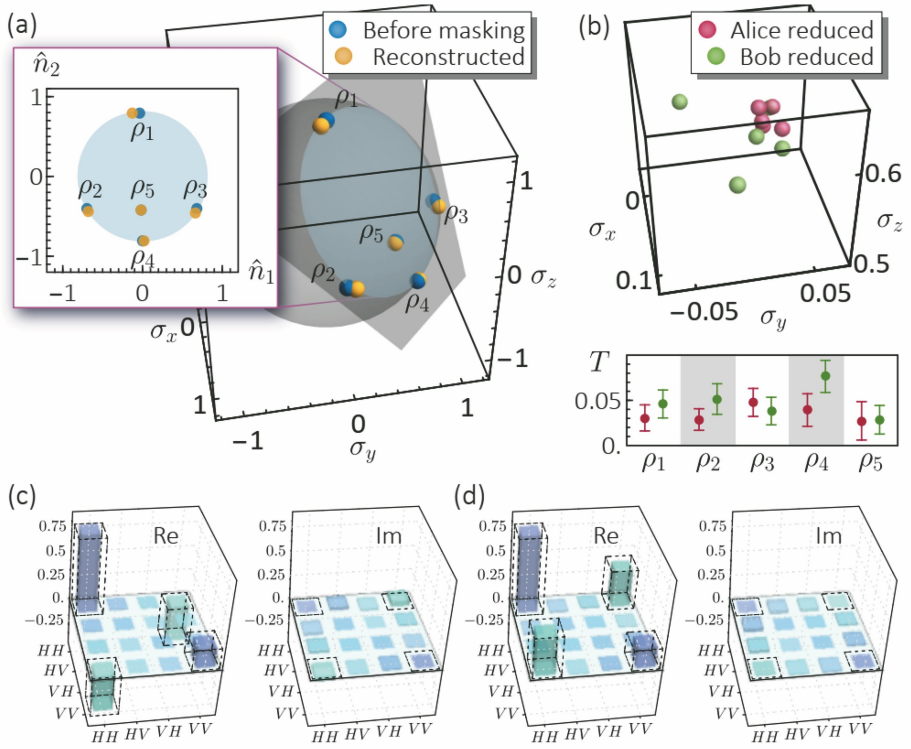

图 4　使用双光子波函数干涉实现量子信息掩蔽的实验结果[25]。(a)一个量子比特空间中的可掩蔽圆盘，数据点为五个圆盘上的量子态及经过掩蔽操作后，数值实现逆映射还原出的量子态在 Bloch 球上的表示；(b)对圆盘上掩蔽操作后测得的约化态几乎落在同一点，内插图量化了掩蔽后约化态与理论预言之间的迹距离；(c)(d)分别对应于掩蔽量子态 ρ_1 和 ρ_4 后量子态层析得到的两体密度矩阵，虚线为理论预言

Fig. 4　Experimental results of quantum information masking using two-photon interference[25]. (a) A qubit maskable disk represented on the Bloch sphere. The data points are five quantum states on the maskable disk and the recovered state from masking, deduced by numerically invert the masking isometry; (b) marginal states of the five data points after masking almost completely overlap; the inset quantifies the trace distance between the experimental results and the theoretical predictions of the marginal states; (c)(d) bipartite density matrix after masking ρ_1 and ρ_4 inferred from quantum state tomography. The dashed boxes show the theoretical predictions

在文献[25]中，作者还直接验证了可掩蔽集的零测度，方法是首先将光量子掩蔽机初始化在掩蔽 Bloch 球每条纬线的状态，而后对待掩蔽的态做一微扰，使其沿纬线或经线方向移动，观察掩蔽机中输出的态的变化。实验结果(参见图 5)表明，当被掩蔽的态沿纬线方向有一小位移(在 Bloch 球上纬度不变)时，掩蔽操作后两体系统的约化态仍然几乎保持不变；相反，当被掩蔽的态沿经线方向有一小位移(在 Bloch 球上纬度改变)时，掩蔽操作后两体系统的约化态出现显著改变。进一步地，使用微扰前后约化态之间的迹距离[32]来表征约化态改变的程度，发现迹距离在小范围内正比于输入量子态在 Bloch 球上纬度的改变。因此，理想状态下可掩蔽集确实处在一个厚度为 0 的圆盘上，从而在整个态空间中具有零体积测度。

使用光子干涉法进行量子信息掩蔽，除了上面提到的增加了成功效率之外，还具有两个优势。一是方便扩展到高维量子信息系统，只要将高维量子信息按照类似于质因数分解算法中的方式，按位编码到多个光子的偏振状态上[6,8,72-73]，再逐位掩蔽编码后得到的量子比特，就可以实现对于高维光量子信息的掩蔽；另外双光子在偏振分束棱镜上干涉时也允许携带额外的路径自由度[74-76]。二是适用于非成对的光子，例如一个脉冲激发固态色心系统生成的真单光子[77-79]，其携带的量子信息也可以以较好的效果被一个弱相干光所掩蔽。

3.2　基于模块化门操作的光量子信息掩蔽

光子的量子行走是现代量子信息学和光子学研究的重要手段，它被广泛应用于量子精密测量[80-82]、加速量子计算[83-84]、测量拓扑不变量[85-86]以及探索新奇物理机制[87-88]等一系列研究工作中，且可以构造出模块化的门操作，从而实现高维系统的任意演

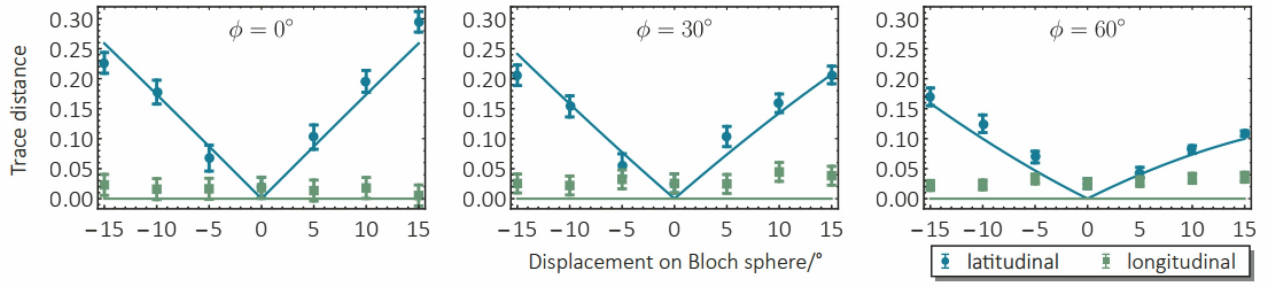

图 5　量子比特可掩蔽集的零体积测度[25]。每张图都给出当输入态沿经线或纬线偏离不同纬度的参考态时，掩蔽后输出态的其中一个约化密度矩阵与参考态被掩蔽后约化密度矩阵的迹距离，迹距离为 0 表示掩蔽成功。在当前实验设置下，可掩蔽圆盘被 Bloch 球上的纬线包围。在今后所有插图中，误差棒对应于光子计数统计导致的标准偏差，实现给出理论计算结果

Fig. 5　Zero volume measure of the qubit maskable set[25]. Each subfigure shows the trace distance between one of the reduced density matrix of the output state after masking and the reduced density matrix of the masked reference state when the input state deviates from the reference state on different latitudes along a parallel or a meridian. A trace distance of 0 indicates the success of masking. Under this experimental configuration, the maskable disks are encircled by the line of constant latitudes on the Bloch sphere. The error bars show the standard deviations deduced from the photon counting statistics, and the solid curves depict the theoretical predictions

化和测量[89]。Zhang 等[26]使用光量子行走技术，实现了实数量子力学中量子信息的掩蔽，并首次在实验上将量子信息掩蔽推广到高维系统。他们首先同时使用光子的路径和偏振自由度，混合编码一个四维实数量子系统。而后利用模块化的光学量子行走实现掩蔽等距映射所需的各种门操作，从而在输出端得到掩蔽后的量子态。为了实现离散时间光量子行走，该工作使用方解石晶体的双折射效应构造了偏振分束器。实验装置见图 6，当光子通过方解石晶体时，按照其偏振状态的不同，偏振方向垂直于晶体光轴的光子仍然在原先的路径上行进，而另一本征偏振的光子则沿着光轴方向分开一段距离。因此，通过摆放一个光轴方向合适的偏振分束器阵列，在其中辅以波片，对光子进行偏振状态的调节，就可以实现不同行进路线上光子波函数的干涉，进而构造量子门操作。掩蔽操作后输出的量子态包含两个量子比特，分别编码在一个光子的路径和偏振自由度上；再结合光量子态裂变技术[90]，原则上还可以进一步将两个自由度上的量子态转移到两个光子的偏振状态上，实现掩蔽后两个量子比特的空间分离。

实验中，观测到对于每个输入光量子行走模块的实数量子态，掩蔽操作后得到的偏振或路径约化态几乎都是一个最大混合态，因此在每个自由度上几乎都没有任何关于掩蔽前量子态的任何信息；与此同时，通过量子态验证[91]可知，掩蔽操作得到的两自由度密度矩阵与最大纠缠态的保真度对于每个入射态都超过 98%，从而达到将量子信息完全转入两体关联的效果。进一步分析发现，掩蔽操作后量子态两自由度之间的纠缠度与入射态是否为实数量子态密切相关：图 7 中的理论分析和实验结果表明，

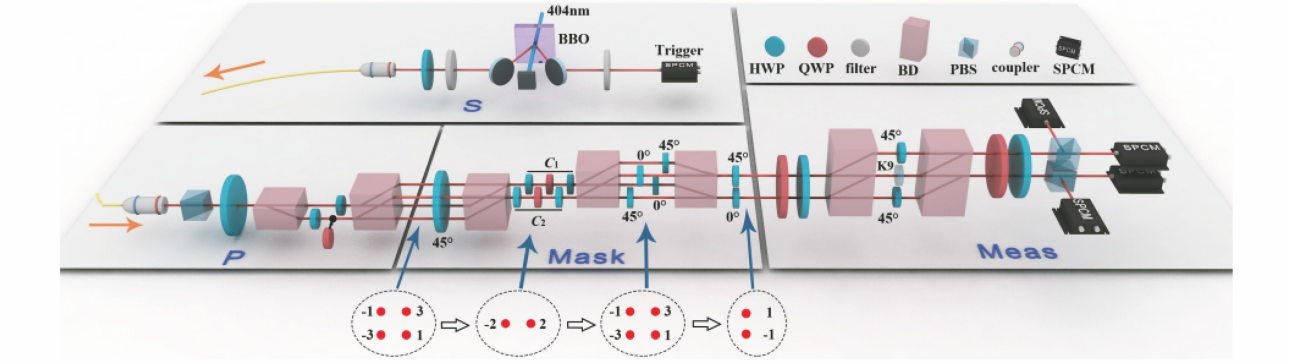

图 6　使用量子行走实现实数量子信息掩蔽的实验装置[26]。BD：方解石晶体光学分束器；SPCM：单光子计数模块

Fig. 6　Experimental setup realizing real qudit information masking using quantum walks[26]. BD: calcite crystal optical beam splitter; SPCM: single photon counting module

衡量出射态纠缠度的 concurrence[92] 与衡量入射态与实空间距离的 robustness of imaginarity[34] 存在单调依赖的关系。因此当入射态不再是实数量子态时，出射态也将不再是最大纠缠态，从而两个约化密度矩阵将不再是最大混态，而是携带与入射态相关的额外信息。因此说明，实数量子态的集合是量子信息两体掩蔽的一个最大可掩蔽集。

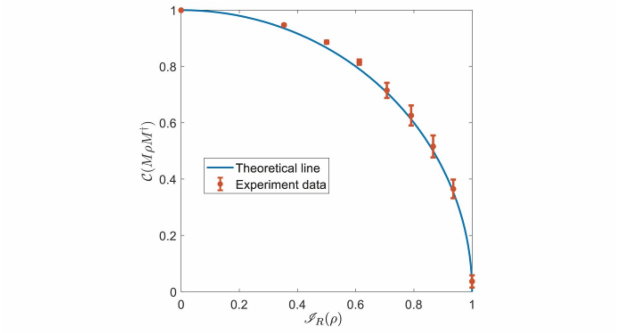

图 7　实数量子信息掩蔽操作下，输出态的纠缠度 concurrence 与表征输入态与实空间距离的 robustness of imaginarity 的关系[26]。使用的量子态集合是量子比特的最大叠加态

Fig. 7 Relationship between the concurrence of the output state from quantum information masking under the subtheory of real quantum mechanics and the robustness of imaginarity of the input state that characterizes the distance from the real state space[26]. Testbed set of quantum states is the qubit maximally superposition states

4　量子信息掩蔽在量子通信中的应用

量子信息掩蔽不但具有丰富的理论基础，而且已经可以在光学装置中实验实现。由于掩蔽是将量子信息放置在不同量子实体非定域的关联之中，因此它可能在量子通信场景下具有一些有益的性质：首先，由于量子信息在被掩蔽后完全处于量子纠缠之中，因此可以受到一定的噪声保护，可以从不破坏纠缠的噪声环境下被恢复出来；其次，由于掩蔽后每个单独的量子实体都不携带先前的任何信息，因此量子信息掩蔽操作可以天然地抵抗外界的窃听；另外，量子信息掩蔽的最大可掩蔽集具有明确的几何性质，利用这些性质也有可能构造出实用的量子通信协议。

4.1　免疫环境噪声

在一些量子通信场景中，可能需要通过非理想的信道传输量子态，然而量子信道中出现的环境噪声将使输出的量子态出现误差，进而导致传输的量子信息损坏或丢失。幸运地是，信道中噪声的形式常常是有迹可循的。例如当使用光纤传输一个偏振量子比特时，一种经常出现的噪声是光纤弯曲等因素导致的双折射[93]，它会使得两个本征偏振态之间出现一个相对相位。若使用同一根光纤传输两个光子，那么两个光子受到的噪声作用应该相同，将这种在不同量子上具有相同作用的噪声称为集体噪声。通过将信息转入量子关联之中，量子信息掩蔽可以提供一种在实际的量子通信网络中克服已知形式的集体噪声的途径。

下面将以量子比特系统的两体掩蔽为例来加以讨论。对于量子比特系统而言，生成元为 $\sigma_{\hat{n}}^{\mathrm{A}}+\sigma_{\hat{n}}^{\mathrm{B}}$ 的两体集体噪声 $\exp(\mathrm{i}\theta\sigma_{\hat{n}}^{\mathrm{A}})\exp(\mathrm{i}\theta\sigma_{\hat{n}}^{\mathrm{B}})$ 对于支撑在基矢 $\{|\hat{n}^{+}\hat{n}^{-}\rangle,|\hat{n}^{-}\hat{n}^{+}\rangle\}$ 上的量子态只造成一个整体相位的影响。其中，$|\hat{n}^{\pm}\rangle$ 对应于泡利算符 $\hat{\sigma}\cdot\hat{n}=n_x\sigma_x+n_y\sigma_y+n_z\sigma_z$ 本征值为 ±1 的本征态。为了将一个量子态转入两体纠缠，并在免疫集体噪声的子空间中加以保护，应当将其作为受控量子比特，以 $\{|\hat{n}^{+}\rangle,|\hat{n}^{-}\rangle\}$ 代替 $\{|0\rangle,|1\rangle\}$ 作为计算基矢，向一个空白的受控量子比特进行一次 CNOT 操作，最后再翻转受控量子比特。上述操作与 2.2 节中所述实现量子信息掩蔽的操作，只相差最后一步局域的翻转，对于可掩蔽集没有影响，容易检验，其对应的可掩蔽集方程可以表述为 $\hat{n}\cdot\boldsymbol{r}=n_xx+n_yy+n_zz$，且为一个常数。因此，可以利用两体掩蔽操作将可掩蔽的量子态放入一个特定形式的免疫噪声的子空间中，从而两体量子信息掩蔽提供了一种使用量子关联来保护量子信息的方法。

借助量子信息掩蔽来保护量子信息的思路类似于自旋回波效应[94]，本质都是执行两次含有噪声的演化，通过翻转系统的状态使得两次噪声的效果互相抵消，区别在于两次演化是依次进行，还是分别作用在两个单独的量子比特上。在量子信息掩蔽的概念被抽象出之前，类似自旋回波的方法已在光纤网络中被用于克服本征偏振模式之间的相对相位误差，实现量子信息的无噪声传输[95]，因此，基于量子信息掩蔽的量子信息保护也有望于未来在线性光学系统中取得一定的应用。

4.2　量子秘密共享

是否可能将一个量子态包含的信息拆分到多个量子实体中，只有将他们组合起来才能恢复出原先的量子信息？量子秘密共享[96-99]实现的就是这样一

种功能。一个(k,n)编码的量子秘密共享协议将量子态分为 n 个组分,其中任意 k 个组分都可用于恢复出原先的量子态,而没有任何 $k-1$ 个组分可以还原出原先量子态的信息。为了方便起见,在 $n=k$ 的情况下,也将上面的协议简称为 n 方量子秘密共享。通过借助光子的能量-时间纠缠[100]和偏振纠缠[101-103]等非经典特性,多种多样的量子秘密共享协议已经在光学系统中取得了实验实现。

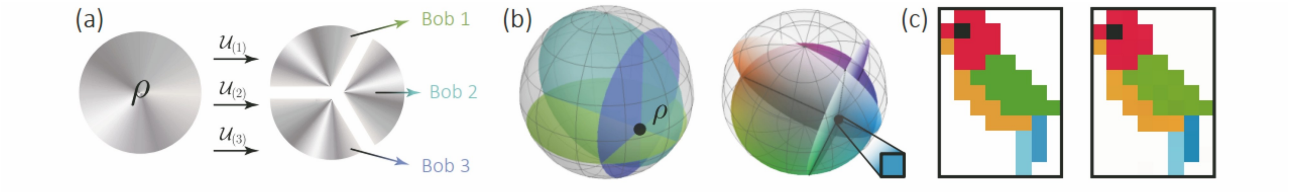

图 8　基于量子信息掩蔽的量子秘密共享方案[25]。(a)量子秘密共享的概念图,三个接收方使用各自的约化态信息可还原出被掩蔽前的量子态。(b)通过量子信息掩蔽实现量子秘密共享和进行图片传输的原理。每个接收方均可使用自身的约化态信息将传输前的量子态锁定在 Bloch 球中的一个圆盘上,而三个接收方对比信息后即可完全确定量子态在 Bloch 球中的位置;量子比特的 Bloch 球与颜色空间又具有同构性,因此可以实现量子比特与颜色的一一对应。(c)使用量子秘密共享进行图片传输的结果,左右两子图分别为原始图片和使用量子信息掩蔽进行传输后重构的结果

Fig. 8　Quantum secret sharing using quantum information masking. (a) Conceptual art of quantum secret sharing[25]. Three receivers use their corresponding marginal state to reconstruct the masked quantum state. (b) schematic plot of quantum secret sharing and image transmission through quantum information masking. Each receiver can use its own marginal state to fix the location of quantum state on a disk in the Bloch sphere, so three receivers can completely determine the position of the quantum state in the Bloch sphere after comparing their information. Moreover, the Bloch sphere and the color space are isomorphic establishing the one-to-one correspondence between the qubit states and all possible colors. (c) result of image transmission using quantum secret sharing. The left and right panels are the original and reconstruction image after transmission using quantum information masking

按照定义可知,两体量子信息掩蔽本身就可以在最大掩蔽集内实现一个两方量子秘密共享。借助量子比特最大可掩蔽集的几何性质,Liang 等[24]将该协议推广到适用于任意的量子比特纯态,并进一步发展和实验展示了适用于任意量子比特混态的三方量子秘密共享[24]。以三方共享的实验工作为例介绍基于最大可掩蔽集性质的量子秘密共享(见图 8),该方法的实质在于秘密分发者使用三个不同的等距映射掩蔽同一个量子态,从而得到三个两体量子态,再将每个两体态中的一个光子发送给一个接收方,自己留下另一个光子。在秘密共享协议开始前,三个接收者都已经被告知发送给自己的光子所使用的掩蔽等距映射。由于每个接收者仅得到一个光子,因此他们只能通过测量,确定掩蔽操作前的量子态在 Bloch 球中对应圆盘的截距,却不能具体解码出掩蔽前的量子态;对于每个独立的接收者而言,圆盘上的每个态都是等可能出现的。为了实现解码过程,三个接收者应当使用经典通信对比他们的信息,从而在几何上使三个圆盘所在的平面在 Bloch 球内交于一点,该点的位置即给出了被掩蔽前的量子态。在实验中[25],该量子秘密共享协议被用于分享一张图片,得到的图片与原图的互关联系数达到 99.35%。

上述使用量子信息掩蔽实现的量子秘密共享,相比先前的方案具有两点显著的优势。其一是安全性,即使窃听者截获其中一个接收方的光子,由于其缺少掩蔽映射的相关信息,也将无法参与到量子秘密共享中还原出量子态;若使用伪造的掩蔽映射,甚至有可能在重构时得到 Bloch 球之外的非物理态,导致窃听者被发现。其二是发送方在完成量子信息掩蔽后,无需像在量子隐形传态中一样,按照自身保留的态指示接收方在收到的态上进行泡利算符操作,从而该协议适用于经典通信受限的场景;发送方保留的态还可在事后用于验证三个接收方分享的信息,进一步增加了协议的安全性。另一方面,由于在高维下掩蔽集具有更加丰富的几何特性,因此在高维下构造相应的量子秘密共享协议将是一个有趣的开放性问题。

4.3　量子信息掩蔽与比特承诺的关系

比特承诺[104]是现代密码学中的一个重要的协议,该协议要求发送方向接收方承诺一个比特的值,并在稍晚的时刻揭示该比特的值,从而向接收方证明该比特的值确实与其承诺的相同。在整个过程中,发送方不能够改变用于承诺的比特上的信息。形象地说,一次比特承诺可以被理解为发送方向一个黑盒子中放入一张记录信息的纸条,锁上盒子后

向接收方宣称记录的信息，在揭示阶段将锁的钥匙交给接收方。那么比特承诺协议的安全性如何呢？由于在揭示阶段开始前，发送方一直持有黑盒子的钥匙，因此他总是可以重新打开盒子，更换其中纸条的内容，从而完成作弊。上述结论并非偶然：任何仅包含发送方向接收方单向通信的比特承诺协议都存在安全漏洞[105]，即使使用量子纠缠的资源也不能在非相对论框架下完成无条件安全的比特承诺[106-108]。

量子信息掩蔽协议的出现似乎为借助量子力学实现比特承诺带来了新的转机：既然掩蔽操作后量子信息被完全放置在了两体关联中，是否有可能仅通过两体掩蔽来实现比特承诺呢？遗憾地是，答案是否定的，究其原因在于对掩蔽后两体态中每个粒子的操作都可能改变量子关联的形式，因此给予发送方和接收方作弊的机会。以 CNOT 门实现的掩蔽操作来举例分析。前面已经提到其实现的映射是 $\mathrm{CNOT}\{[a|0\rangle+b\exp(\mathrm{i}\varphi)|1\rangle]\otimes|0\rangle\}\rightarrow a|00\rangle+b\exp(\mathrm{i}\varphi)|11\rangle$。不妨考虑发送方希望承诺的态是 $|\tilde{\psi}_1\rangle=a|0\rangle+b|1\rangle$ 和 $|\tilde{\psi}_2\rangle=a|0\rangle+b\exp(\mathrm{i}\varphi)|1\rangle$ 中的一个，它们被掩蔽之后分别得到 $|\tilde{\psi}_1\rangle=a|00\rangle+b|11\rangle$ 和 $|\tilde{\psi}_2\rangle=a|00\rangle+b\exp(\mathrm{i}\varphi)|11\rangle$，当 $\langle\tilde{\psi}_1|\tilde{\psi}_2\rangle=0$ 时就回到经典比特承诺的情况。诚然，在两体掩蔽操作后发送方和接收方的约化态都不随初态的选择而变化，但是 $|\tilde{\Psi}_1\rangle$ 和 $|\tilde{\Psi}_2\rangle$ 可以被一个单体的幺正演化联系起来：发送方和接收方都可以通过对自己手中的粒子施加一个相位门，使得承诺的量子态发生转换。因此，即使形式上具有诸多类似之处，仅仅使用两体量子信息掩蔽仍然不足以实现无安全漏洞的比特承诺协议。

上面的两体掩蔽操作中，输入等距映射的辅助量子态都是置于一个纯的空白态 $|0\rangle\langle 0|$ 上。若允许将在系统中引入额外的随机性，允许辅助量子态处于混合态，结论则会有所不同。文献[23]提出一种基于对混合的辅助态进行量子信息掩蔽，实现无条件安全比特承诺的方法，让中间人使用一次一密的方式构造随机形式的掩蔽映射，发送方将掩蔽后得到的两体态中的一个粒子与待承诺的态共同做贝尔态测量，测量结果即为承诺的内容。在揭示阶段，中间人公布单次密码表的结果，结合发送方承诺的内容即可做掩蔽操作的逆映射，恢复出承诺的量子态。一次一密的手段已经在直接量子通信[109-110]等场景中展示了广泛的应用，其在量子信息掩蔽和比特承诺协议中的角色进一步展示了随机性作为一种资源在量子信息处理中的重要性[111]。

5　总结与讨论

5.1　量子信息掩蔽在交叉学科中的意义

尽管量子信息掩蔽是最近三年才出现的全新概念，但其中的很多思想都可追溯到早期量子信息学发展中已出现的概念。例如借鉴量子隐形传态[2]的思想，取消其中的经典通信部分就可以构造多体量子信息掩蔽的映射[31,38,]。一个两体量子信息掩蔽的过程也可以被认为是实现了一个量子纠错码[14]；结合量子纠错码的思想，也可对多体量子信息掩蔽的定义做出另一种基于多体约化密度矩阵的推广[112]，该定义下量子信息掩蔽的结果对于比特反转形式的噪声具有一定的免疫性[113]。量子纠错码是未来最终实现大规模容错量子计算的重要理论工具，限于篇幅所限不展开讨论，推荐文献[114-115]，可进一步了解相关的内容。

量子信息两体掩蔽的非普适性可以被认为是量子信息不可隐藏的一个推论。量子信息的不可隐藏定理[18]指出：若一个量子系统所包含的信息被擦除，那么该信息必须完全转移至量子系统之外的环境，而不能部分保留/隐藏在系统与环境的关联中。事实上，已经通过实验证明，使用合适的操作，可以将散逸至环境中的量子信息重新提取出来，提取的过程完全不涉及量子信息最初始时刻所属的系统[116]。按照上述定义可知，若在量子信息的两体掩蔽场景中，将两个子系统分别当做量子信息隐藏场景中的系统与环境，即可由不可隐藏定理证得两体掩蔽的非普适性。进一步地讲，不可普适掩蔽定理还可以认为是“互信息守恒”原理的推论[20]。考察一个量子两体系统 AB 和外界环境 R 之间的关联，记系统 X 的信息熵为 $S(X)$，两个系统 X，Y 间的互信息为 $I(X,Y)\equiv S(X)+S(Y)-S(XY)$，它代表了两个系统之间的状态互相关联的程度。由于 ABR 共同构成了一个封闭系统，有 $S(AR)=S(B)$，$S(BR)=S(A)$，从而

$$I(A:R)+I(B:R)=2S(R)。\tag{6}$$

(6)式表明，当使用互信息表征系统之间的关联强度时，一个两体量子系统的两个约化态在掩蔽操作前后与外界环境存在的关联是守恒的，因此不可能将初始时刻与外界关联状态不同的一些量子态同时掩蔽，使得在掩蔽之后达到一个相同的条件态。相反，若考虑将经典信息掩蔽在量子关联中的过程，

就会发现由于经典信息是完全可以区分的，它们可以被认为与外界环境没有关联，因此互信息守恒不禁止对经典信息的普适掩蔽。实际上为了实现经典信息的掩蔽，只需将它们编码在正交的贝尔态上[14]。正交的量子态对应的密度矩阵是对易的，因此它们可以同时被克隆或掩蔽[25,36]。

任意量子信息不可被两体掩蔽和隐藏的结论在黑洞信息佯谬问题中也具有重要的影响。使用广义相对论可以证明黑洞的“无毛定理”，也就是除了质量，角动量和电荷之外，黑洞不能够携带任何信息[117]。Hawking[118]发现尽管黑洞表面的时空曲率使光子都无法逃逸，真空中的涨落却会导致黑洞缓慢地向外界辐射。问题在于辐射出的光子应当与掉入黑洞的光子处于纠缠的状态，按照无毛定理，黑洞将摧毁落入光子的信息，使得逃逸的光子处在失去信息的最大混合态上，这与量子力学线性演化导致的信息守恒原则形成尖锐的矛盾，因此被称为黑洞信息佯谬[119]。解决该佯谬的一种途径是假定黑洞与所有辐射出的光子处于纠缠状态，从而虽然黑洞本身不再携带量子信息，这一部分信息却仍然保留在黑洞与外界的关联中[119-122]。两体掩蔽的非普适性排除了上述解释的可能性：其携带的信息能够置于两体关联中的量子态在所有量子态的空间中测度为零，因此所有信息都处在量子关联中的假定是非常人为的，不可能用来化解黑洞信息佯谬。上述讨论展示了量子信息掩蔽深刻的热力学和信息学背景。

5.2 量子信息掩蔽的发展趋势与开放性问题

对量子信息掩蔽的研究不断深化人们对量子信息理论，量子物理学乃至整个自然科学的理解。在下一阶段，量子信息掩蔽的相关研究将有望在理论和实验两个方向同时进一步得到扩展。从理论上讲，量子信息掩蔽研究的发展，将使其与量子信息学中其他概念的联系更加紧密，并催生出一些新的研究方向，如研究随机性资源在量子信息任务中的作用[20,123]、研究多体系统中的量子信息置乱和混沌现象[124-125]、推导新型不确定性关系[126-127]等等。另一方面，还可以定义更广义的量子信息掩蔽操作，使得多体系统中任何 k 个子系统组成的复合系统均不包含待掩蔽的任何信息[112]，或使用局域操作使量子信息扩散到先前存在的纠缠中[128]。同时，对于量子信息掩蔽本身的理论研究仍有一些开放性问题亟待解决，例如是否存在一个适用于所有量子态的 $\mathscr{H}^6\to\mathscr{H}^6\otimes\mathscr{H}^6\otimes\mathscr{H}^6$ 掩蔽映射[39]？对于 d 维量子信息的两体掩蔽，使最大可掩蔽集具有非零测度的子空间维数应为多少？这些问题目前仍然没有定论。

从实验上讲，量子信息掩蔽实验研究中存在两个引人注目的待解决问题。第一是目前阶段所有光量子信息掩蔽的实验都旨在研究量子信息的两体掩蔽，因此没有一个实验可以实现整个希尔伯特空间中所有量子态的掩蔽。要实现所有量子态的掩蔽至少需要使用 4 个量子比特或者 3 个三维量子比特，因此对实验技术和光路的设计将构成更大的挑战。第二是迄今为止，所有光量子信息掩蔽的实验都是使用量子态层析来论证恢复出量子信息的可行性，因此只能统计性地重构出被掩蔽系综的信息，而不能在单次掩蔽操作后立即实现被掩蔽量子信息在接收端的重新构建。要实现已掩蔽信息在远距离的恢复，除了直接进行掩蔽映射的逆运算之外，还可以使用类似于量子隐形传态中使用的前馈控制技术，将一个光子的状态通过经典通信转化为另一个光子上需要执行的操作，从而达到重构量子态的目的。目前阶段，使用电光调制器在各个光子之间进行高速的经典通信已经是非常成熟的技术[129-130]，可以期望不久的将来就有望实现最大可掩蔽集中量子信息的掩蔽及远距离重构，从而量子信息掩蔽有望作为一种安全可靠的量子通信手段得到广泛的应用。

参 考 文 献

[1] Bennett C H, DiVincenzo D P. Quantum information and computation[J]. Nature, 2000, 404(6775): 247-255.

[2] Bennett C H, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels[J]. Physical Review Letters, 1993, 70(13): 1895.

[3] Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation[J]. Nature, 1997, 390(6660): 575-579.

[4] Hu X M, Zhang C, Liu B H, et al. Experimental high-dimensional quantum teleportation[J]. Physical Review Letters, 2020, 125(23): 230501.

[5] Bennett C H, Wiesner S J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states[J]. Physical Review Letters, 1992, 69(20): 2881.

[6] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science, November 20-22, Santa Fe, NM, USA. New York: IEEE Press, 1994: 124-

134.

[7] Aaronson S, Arkhipov A. The computational complexity of linear optics[C]//Proceedings of the 43rd annual ACM symposium on Theory of computing - STOC '11, June 6-8, 2011. San Jose, California, USA. New York: ACM Press, 2011: 333-342.

[8] Martín-López E, Laing A, Lawson T, et al. Experimental realization of Shor's quantum factoring algorithm using qubit recycling [J]. Nature Photonics, 2012, 6(11): 773-776.

[9] Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574(7779): 505-510.

[10] Zhong H S, Wang H, Deng Y H, et al. Quantum computational advantage using photons[J]. Science, 2020, 370(6523): 1460-1463.

[11] Arrazola J M, Bergholm V, Brádler K, et al. Quantum circuits with many photons on a programmable nanophotonic chip [J]. Nature, 2021, 591(7848): 54-60.

[12] Schrödinger E. Die gegenwärtige Situation in der Quantenmechanik[J]. Naturwissenschaften, 1935, 23(48): 807-812.

[13] Einstein A, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete?[J]. Physical Review, 1935, 47(10): 777.

[14] Modi K, Pati A K, Sen(De) A, et al. Masking quantum information is impossible[J]. Physical Review Letters, 2018, 120(23): 230501.

[15] Wootters W K, Zurek W H. A single quantum cannot be cloned[J]. Nature, 1982, 299(5886): 802-803.

[16] Barnum H, Caves C M, Fuchs C A, et al. Noncommuting mixed states cannot be broadcast [J]. Physical Review Letters, 1996, 76(15): 2818.

[17] Pati A K, Braunstein S L. Impossibility of deleting an unknown quantum state[J]. Nature, 2000, 404(6774): 164-165.

[18] Braunstein S L, Pati A K. Quantum information cannot be completely hidden in correlations: implications for the black-hole information paradox [J]. Physical Review Letters, 2007, 98(8): 080502.

[19] Schrödinger E. An undulatory theory of the mechanics of atoms and molecules[J]. Physical Review, 1926, 28(6): 1049.

[20] Lie S H, Jeong H. Randomness cost of masking quantum information and the information conservation law[J]. Physical Review A, 2020, 101(5): 052322.

[21] Hayden P, Preskill J. Black holes as mirrors: quantum information in random subsystems[J]. Journal of High Energy Physics, 2007, 2007(9): 120.

[22] Sekino Y, Susskind L. Fast scramblers[J]. Journal of High Energy Physics, 2008, 2008(10): 065.

[23] Lie S H, Kwon H, Kim M S, et al. Quantum one-time tables for unconditionally secure qubit-commitment[J]. Quantum, 2021, 5: 405.

[24] Liang X B, Li B, Fei S M. Complete characterization of qubit masking[J]. Physical Review A, 2019, 100(3): 030304.

[25] Liu Z H, Liang X B, Sun K, et al. Photonic implementation of quantum information masking [J]. Physical Review Letters, 2021, 126(17): 170505.

[26] Zhang R Q, Hou Z B, Li Z H, et al. Experimental masking of real quantum states[J]. Physical Review Applied, 2021, 16(2): 024052.

[27] Du Y X, Guo Z H, Cao H X, et al. Masking quantum information encoded in pure and mixed states [J]. International Journal of Theoretical Physics, 2021, 60(7): 2380-2399.

[28] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[29] Kimura G. The Bloch vector for N-level systems [J]. Physics Letters A, 2003, 314(5/6): 339-349.

[30] Ding F, Hu X Y. Masking quantum information on hyperdisks[J]. Physical Review A, 2020, 102(4): 042404.

[31] Shang W M, Zhang F L, Chen J L. Quantum information masking basing on quantum teleportation[EB/OL]. (2021-03-04)[2021-08-01]. https://arxiv.org/abs/2103.03126.

[32] Nielsen M A, Chuang I L. Quantum computation and quantum information [M]. Cambridge: Cambridge University Press, 2000.

[33] García-Pelayo R. Distribution of distance in the spheroid[J]. Journal of Physics A: Mathematical and General, 2005, 38(16): 3475-3482.

[34] Hardy L, Wootters W K. Limited holism and real-vector-space quantum theory[J]. Foundations of Physics, 2012, 42(3): 454-473.

[35] Wu K D, Kondra T V, Rana S, et al. Operational resource theory of imaginarity[J]. Physical Review Letters, 2021, 126(9): 090401.

[36] Zhu H J. Hiding and masking quantum information in complex and real quantum mechanics [J]. Physical Review Research, 2021, 3(3): 033176.

[37] Liang X B, Li B, Fei S M, et al. Impossibility of masking a set of quantum states of nonzero measure [J]. Physical Review A, 2020, 101(4): 042321.

[38] Li M S, Wang Y L. Masking quantum information in multipartite scenario [J]. Physical Review A, 2018, 98(6): 062306.

[39] Han K Y, Guo Z H, Cao H X, et al. Quantum multipartite maskers vs. quantum error-correcting codes[J]. EPL (Europhysics Letters), 2020, 131(3): 30005.

[40] Shang W M, Zhang F L, Zhou J, et al. Qubit masking in multipartite qubit system [J]. Modern Physics Letters A, 2021, 36(21): 2150156.

[41] Dey A. Orthogonal Latin Squares and the Falsity of Euler's conjecture[M]//Bhatia R, Rajan C S, Singh A I. Connected at Infinity II. Texts and readings in mathematics. Gurgaon: Hindustan Book Agency, 2013, 67: 1-17.

[42] Preskill J. Quantum Computing in the NISQ era and beyond[J]. Quantum, 2018, 2: 79.

[43] von Keyserlingk C, Rakovszky T, Pollmann F, et al. Operator hydrodynamics, OTOCs, and entanglement growth in systems without conservation laws[J]. Physical Review X, 2018, 8(2): 021013.

[44] Anderson P W. Absence of diffusion in certain random lattices [J]. Physical Review, 1958, 109(5): 1492.

[45] Abanin D A, Altman E, Bloch I, et al. Colloquium: many-body localization, thermalization, and entanglement [J]. Reviews of Modern Physics, 2019, 91(2): 021001.

[46] Yao N Y, Potter A C, Potirniche I D, et al. Discrete time crystals: rigidity, criticality, and realizations[J]. Physical Review Letters, 2017, 118(3): 030401.

[47] Heyl M. Dynamical quantum phase transitions: a review[J]. Reports on Progress in Physics. Physical Society (Great Britain), 2018, 81(5): 054001.

[48] Mi X, Ippoliti M, Quintana C, et al. Observation of time-crystalline eigenstate order on a quantum processor[EB/OL]. (2021-07-28)[2021-08-01]. https://arxiv.org/abs/2107.13571.

[49] Duan L M, Guo G C. Probabilistic cloning and identification of linearly independent quantum states [J]. Physical Review Letters, 1998, 80(22): 4999.

[50] Pati A K. Quantum superposition of multiple clones and the novel cloning machine[J]. Physical Review Letters, 1999, 83(14): 2849.

[51] Li B, Jiang S H, Liang X B, et al. Deterministic versus probabilistic quantum information masking [J]. Physical Review A, 2019, 99(5): 052343.

[52] Li M S, Modi K. Probabilistic and approximate masking of quantum information [J]. Physical Review A, 2020, 102(2): 022418.

[53] Flamini F, Spagnolo N, Sciarrino F. Photonic quantum information processing: a review [J]. Reports on Progress in Physics, 2019, 82(1): 016001.

[54] O'Brien J L, Pryde G J, White A G, et al. Demonstration of an all-optical quantum controlled-NOT gate[J]. Nature, 2003, 426(6964): 264-267.

[55] Okamoto R, Hofmann H F, Takeuchi S, et al. Demonstration of an optical quantum controlled-NOT gate without path interference [J]. Physical Review Letters, 2005, 95(21): 210506.

[56] Kiesel N, Schmid C, Weber U, et al. Linear optics controlled-phase gate made simple [J]. Physical Review Letters, 2005, 95(21): 210505.

[57] Langford N K, Weinhold T J, Prevedel R, et al. Demonstration of a simple entangling optical gate and its use in bell-state analysis[J]. Physical Review Letters, 2005, 95(21): 210504.

[58] Englert B G, Kurtsiefer C, Weinfurter H. Universal unitary gate for single-photon two-qubit states [J]. Physical Review A, 2001, 63(3): 032303.

[59] Hong C K, Ou Z Y, Mandel L. Measurement of subpicosecond time intervals between two photons by interference[J]. Physical Review Letters, 1987, 59(18): 2044.

[60] Dirac P M. The principles of quantum mechanics [M]. Oxford: Oxford University Press, 1930.

[61] Glauber R J. Dirac's famous dictum on interference: one photon or two? [J]. American Journal of Physics, 1995, 63(1): 12.

[62] Proietti M, Pickston A, Graffitti F, et al. Experimental test of local observer independence [J]. Science Advances, 2019, 5(9): eaaw9832.

[63] Wang K, Xu Q, Zhu S N, et al. Quantum wave-particle superposition in a delayed-choice experiment [J]. Nature Photonics, 2019, 13(12): 872-877.

[64] Tschernig K, Müller C, Smoor M, et al. Direct observation of the particle exchange phase of photons[J]. Nature Photonics, 2021, 15(9): 671-675.

[65] Browne D E, Rudolph T. Resource-efficient linear optical quantum computation [J]. Physical Review Letters, 2005, 95: 010501.

[66] Lo Franco R, Compagno G. Indistinguishability of elementary systems as a resource for quantum information processing [J]. Physical Review

Letters, 2018, 120(24): 240403.

[67] Sun K, Wang Y, Liu Z H, et al. Experimental quantum entanglement and teleportation by tuning remote spatial indistinguishability of independent photons[J]. Optics Letters, 2020, 45(23): 6410-6413.

[68] Zhou X Q, Ralph T C, Kalasuwan P, et al. Adding control to arbitrary unknown quantum operations [J]. Nature Communications, 2011, 2: 413.

[69] Ru S H, Wang Y L, An M, et al. Realization of a deterministic quantum Toffoli gate with a single photon[J]. Physical Review A, 2021, 103(2): 022606.

[70] Wang F R, Ru S H, Wang Y L, et al. Experimental demonstration of a quantum controlled-SWAP gate with multiple degrees of freedom of a single photon[J]. Quantum Science and Technology, 2021, 6(3): 035005.

[71] Bodiya T P, Duan L M. Scalable generation of graph-state entanglement through realistic linear optics[J]. Physical Review Letters, 2006, 97(14): 143601.

[72] Lu C Y, Browne D E, Yang T, et al. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits [J]. Physical Review Letters, 2007, 99(25): 250504.

[73] Lanyon B P, Weinhold T J, Langford N K, et al. Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement[J]. Physical Review Letters, 2007, 99(25): 250505.

[74] Kim Y, Kim Y S, Lee S Y, et al. Direct quantum process tomography via measuring sequential weak values of incompatible observables [J]. Nature Communications, 2018, 9(1): 1-6.

[75] Liu Z H, Zhou J, Meng H X, et al. Experimental test of the Greenberger-Horne-Zeilinger-type paradoxes in and beyond graph states [J]. Npj Quantum Information, 2021, 7(1): 1-8.

[76] Zhang A N, Zhan H, Liao J J, et al. Quantum verification of NP problems with single photons and linear optics [J]. Light: Science & Applications, 2021, 10(1): 1-11.

[77] Berhane A M, Jeong K Y, Bodrog Z, et al. Bright room-temperature single-photon emission from defects in gallium nitride[J]. Advanced Materials, 2017, 29(12): 1605092.

[78] Wang J F, Zhou Y, Wang Z Y, et al. Bright room temperature single photon source at telecom range in cubic silicon carbide[J]. Nature Communications, 2018, 9: 4106.

[79] Li Q, Zhou J Y, Liu Z H, et al. Stable single photon sources in the near C-band range above 400 K[J]. Journal of Semiconductors, 2019, 40(7): 072902.

[80] Hou Z B, Tang J F, Shang J W, et al. Deterministic realization of collective measurements via photonic quantum walks [J]. Nature Communications, 2018, 9(1): 1-7.

[81] Wu K D, Bäumer E, Tang J F, et al. Minimizing backaction through entangled measurements [J]. Physical Review Letters, 2020, 125(21): 210401.

[82] Hou Z B, Jin Y, Chen H Z, et al. "super-Heisenberg" and Heisenberg scalings achieved simultaneously in the estimation of a rotating field [J]. Physical Review Letters, 2021, 126(7): 070503.

[83] Tang H, di Franco C, Shi Z Y, et al. Experimental quantum fast hitting on hexagonal graphs [J]. Nature Photonics, 2018, 12(12): 754-758.

[84] Xu X Y, Huang X L, Li Z M, et al. A scalable photonic computer solving the subset sum problem [J]. Science Advances, 2020, 6(5): eaay5853.

[85] Xu X Y, Wang Q Q, Pan W W, et al. Measuring the winding number in a large-scale chiral quantum walk[J]. Physical Review Letters, 2018, 120(26): 260501.

[86] Xu X Y, Wang Q Q, Heyl M, et al. Measuring a dynamical topological order parameter in quantum walks[J]. Light: Science & Applications, 2020, 9(1): 1-11.

[87] Xiao L, Qu D K, Wang K K, et al. Non-Hermitian Kibble-Zurek mechanism with tunable complexity in single-photon interferometry [J]. PRX Quantum, 2021, 2(2): 020313.

[88] Wang K K, Xiao L, Budich J C, et al. Simulating exceptional non-Hermitian metals with single-photon interferometry[J]. Physical Review Letters, 2021, 127(2): 026404.

[89] Kurzyński P, Wójcik A. Quantum walk as a generalized measuring device [J]. Physical Review Letters, 2013, 110(20): 200404.

[90] Vitelli C, Spagnolo N, Aparo L, et al. Joining the quantum state of two photons into one[J]. Nature Photonics, 2013, 7(7): 521-526.

[91] Zhu H J, Hayashi M. Efficient verification of pure quantum states in the adversarial scenario [J]. Physical Review Letters, 2019, 123(26): 260504.

[92] Wootters W K. Entanglement of formation of an arbitrary state of two qubits [J]. Physical Review Letters, 1998, 80(10): 2245.

[93] Ulrich R, Rashleigh S C, Eickhoff W. Bending-

induced birefringence in single-mode fibers [J]. Optics Letters, 1980, 5(6): 273-275.

[94] Hahn E L. Spin echoes[J]. Physical Review, 1950, 80(4): 580.

[95] Xu J S, Yung M H, Xu X Y, et al. Robust bidirectional links for photonic quantum networks [J]. Science Advances, 2016, 2(1): e1500672.

[96] Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting [J]. Physical Review A, 1999, 59(1): 162.

[97] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing [J]. Physical Review A, 1999, 59 (3): 1829.

[98] Cleve R, Gottesman D, Lo H K. How to share a quantum secret[J]. Physical Review Letters, 1999, 83(3): 648.

[99] Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes [J]. Physical Review A, 2004, 69(5): 052307.

[100] Tittel W, Zbinden H, Gisin N. Experimental demonstration of quantum secret sharing [J]. Physical Review A, 2001, 63(4): 042301.

[101] Chen Y A, Zhang A N, Zhao Z, et al. Experimental quantum secret sharing and third-man quantum cryptography [J]. Physical Review Letters, 2005, 95(20): 200502.

[102] Gaertner S, Kurtsiefer C, Bourennane M, et al. Experimental demonstration of four-party quantum secret sharing[J]. Physical Review Letters, 2007, 98(2): 020503.

[103] 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.

[104] Blum M. Coin flipping by telephone. CRYPTO, 1981, 1981: 11-15

[105] Canetti R, Fischlin M. Universally composable commitments [M] // Kilian J. Advances in cryptology—CRYPTO 2001. Lecture notes in computer science. Heidelberg: Springer, 2001, 2139: 19-40.

[106] Lo H K, Chau H F. Is quantum bit commitment really possible?[J]. Physical Review Letters, 1997, 78(17): 3410.

[107] Mayers D. Unconditionally secure quantum bit commitment is impossible [J]. Physical Review Letters, 1997, 78(17): 3414.

[108] Adlam E, Kent A. Device-independent relativistic quantum bit commitment[J]. Physical Review A, 2015, 92(2): 022315.

[109] Deng F G, Long G L. Secure direct communication with a quantum one-time pad[J]. Physical Review A, 2004, 69(5): 052319.

[110] Gu B, Zhang C Y, Cheng G S, et al. Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel [J]. Science China Physics, Mechanics and Astronomy, 2011, 54(5): 942-947.

[111] Schmid D, Rosset D, Buscemi F. The type-independent resource theory of local operations and shared randomness[J]. Quantum, 2020, 4: 262.

[112] Shi F, Li M S, Chen L, et al. k-uniform quantum information masking[J]. Physical Review A, 2021, 104(3): 032601.

[113] Hu M Y, Chen L. Genuine entanglement, distillability and quantum information masking under noise[EB/OL]. (2021-02-01)[2021-08-01]. https://arxiv.org/abs/2102.00673.

[114] Lidar D A, Brun T A, Brun T. Quantum error correction[M]. Cambridge: Cambridge University Press, 2013.

[115] Grimsmo A L, Puri S. Quantum error correction with the Gottesman-Kitaev-Preskill code[J]. PRX Quantum, 2021, 2(2): 020101.

[116] Samal J R, Pati A K, Kumar A. Experimental test of the quantum no-hiding theorem [J]. Physical Review Letters, 2011, 106(8): 080401.

[117] Misner CW, Thorne KS, Wheeler JA. Gravitation. Macmillan; 1973.

[118] Hawking S W. Black hole explosions?[J]. Nature, 1974, 248(5443): 30-31.

[119] Page D N. Is black-hole evaporation predictable? [J]. Physical Review Letters, 1980, 44(5): 301.

[120] Hooft G. On the quantum structure of a black hole [J]. Nuclear Physics B, 1985, 256: 727-745.

[121] Kalara S, Nanopoulos D V. Black holes, membranes, wormholes and superstrings [M]. Singapore: World Scientific, 1993.

[122] Fiola T M, Preskill J, Strominger A, et al. Black hole thermodynamics and information loss in two dimensions[J]. Physical Review D, 1994, 50(6): 3987.

[123] Yuan X, Zhou H Y, Cao Z, et al. Intrinsic randomness as a measure of quantum coherence[J]. Physical Review A, 2015, 92(2): 022124.

[124] Yamaguchi K, Watamura N, Hotta M. Quantum information capsule and information delocalization by entanglement in multiple-qubit systems [J]. Physics Letters A, 2019, 383(12): 1255-1259.

[125] Hotta M, Yamaguchi K. Strong chaos of fast scrambling yields order: emergence of decoupled quantum information capsules[J]. Physics Letters

A, 2020, 384(3): 126078.

[126] Liang X B, Li B, Huang L, et al. Optimal approximations of available states and a triple uncertainty relation[J]. Physical Review A, 2020, 101(6): 062106.

[127] Wang D, Ming F, Hu M L, et al. Quantum-memory-assisted entropic uncertainty relations[J]. Annalen Der Physik, 2019, 531(10): 1900124.

[128] Mohan B, Sohali, Srivastava C, et al. Quantum information can remain without physical body in volatile form[EB/OL]. (2021-05-05)[2021-08-01]. https://arxiv.org/abs/2105.03250.

[129] Prevedel R, Hamel D R, Colbeck R, et al. Experimental investigation of the uncertainty principle in the presence of quantum memory and its application to witnessing entanglement[J]. Nature Physics, 2011, 7(10): 757-761.

[130] Chaves R, Carvacho G, Agresti I, et al. Quantum violation of an instrumental test [J]. Nature Physics, 2018, 14(3): 291-296.