论文中文摘要

作者姓名：张强

论文题目：多光子纠缠及其在量子信息中的应用

作者简介：：张强，男， 1979 年 12 月出生，2001 年 9 月师从于中国科学技术大学潘建伟教授，于 2006 年 7 月获博士学位。

中 文 摘 要

本论文主要内容是对光子纠缠源的产生，操纵以及其在量子信息上的应用进行的实验研究。

我们在实验上进一步发展了多光子纠缠源技术。利用光参量下转换产生的纠缠光子对和线性光学手段，我们在国际上首次实验实现了六光子干涉和两光子复合系统的量子态隐形传输；我们首次实验实现了四维纠缠光子对制备并在此基础上对两光子 GHZ 定理进行了检验；我们首次实验实现了纠缠光子对的同步；我们首次在实验上实现了容错量子密码。

量子态隐形传输能够在遥远两地传递量子态而不需要传递携带量子态的物理系统。它不但是量子通讯的核心内容，也在大量的量子计算协议中扮演了重要的角色。人们已经在光子系统和离子系统分别实验实现了它，最近长距离的量子态隐形传输和开放目的的量子态隐形传输也纷纷被实验验证。但很不幸的是，直到现在为止，所有的相关实验都只能隐形传输一个量子比特，隐形传输两个或更多比特组成的复合系统在实验领域仍然是个巨大的挑战。同时要实现远距离量子通讯和量子计算，仅仅单量子比特的量子态隐形传输是远远不够的，复合系统的量子态隐形传输也是量子信息研究中的一个长期目标。我们在国际上首次实验实现了两比特复合系统的量子态隐形传输。我们在实验干涉六个光子的基础上，隐形传输了两个光子的任意极化态。在实验中，平均保真度是 0.75±0.03，远远超过了两粒子系统的克隆界限。我们的实验不止是复杂系统量子态隐形传输的重要一环，而且在实验中发展起来的六光子干涉技术可以立即被应用于一系列的量子通讯和量子计算协议中，比如多阶段量子接力，容错量子计算，普适量子纠错码和一次性量子计算。

我们发展并且应用两光子四维纠缠态在世界上首次实验检验了两粒子非统计型定域实在论，在我们的检验中并没有利用传统此类实验所需的上下文实在论假设。实验结果跟量子力学预言符合，同定域实在论的预言矛盾。我们也简短的讨论了在实验中发展的技术在量子信息研究中的应用。

我们在实验上同步了由两台独立的同步不相干激光器泵浦产生的纠缠光子对。我们将同步的纠缠光子对进行了纠缠交换，由此产生的量子纠缠以 3.2 个标准差违背了 Bell 不等式。实验中发展的技术不仅在线性光学量子信息处理中有着重要应用，而且为定域实在论的检验提供了新的手段。

我们利用两光子消相干自由子空间实验实现了容错量子密码。我们的装置在联合噪声带来的比特翻转错误情况下可以实现安全的量子密钥分配，在同样的噪声情况下，传统的 BB84 协议是不能产生密钥的。本实验利用极化空间进行编码，所以不需要进行坐标轴校正。这一

特性将在未来的自由空间量子通讯中有重要应用。同时也可以传递任意抗噪声的量子态。

除了在实验上的研究之外，我们也发现了基于盲基矢的量子密码的安全性漏洞，并且给出了改进方案。

我们在实验中发展起来的技术将在未来的远程量子通讯，线性光学量子计算，量子力学基础检验等重要科学问题的研究中起到重要作用。

关键词：多光子纠缠，量子密码，线性光学

Experimental Multi-photon Entanglement and Applications in Quantum Information

Zhang Qiang

ABSTRACT

The present dissertation is mainly about experimental generation, manipulation of multi-photon entanglement and its applications in quantum information.

We have further developed the multi-photon interference techniques. By making use of polarization entangled photon pairs via parametric down-conversion and linear optics, in this dissertation, we report for the first time the experimental realization of quantum teleportation a composite system, of four-dimension entanglement and the test of two photon GHZ theorem, of synchronization of entangled photon paris, and of fault-tolerant quantum key distribution.

Quantum teleportation, a way to transfer the state of a quantum system from one location to another, is central to quantum communication and plays an important role in a number of quantum computation protocols. Previous experimental demonstrations have been implemented with single photonic or ionic qubits. However, teleportation of single qubits is insufficient for a large-scale realization of quantum communication and computation. Here, we present the experimental realization of quantum teleportation of a two qubit composite system. In the experiment, we develop and exploit a six-photon interferometer to teleport an arbitrary polarization state of two photons. The observed teleportation fidelities for different initial states are all well beyond the state estimation limit of 0.40 for a two-qubit system. Not only does our six-photon interferometer provide an important step towards teleportation of a complex system, it will also enable future experimental investigations on a number of fundamental quantum communication and computation protocols.

We develop and exploit a source of two-photon, four-dimensional entanglement to report the first twoparticle all-versus-nothing test of local realism with a linear optics setup, but without resorting to a noncontextuality assumption. Our experimental results are in good agreement with quantum mechanics while in extreme contradiction to local realism. Potential applications of our experiment are briefly discussed.

We report the generation of independent entangled photon pairs from two synchronized but mutually incoherent laser sources. The quality of synchronization is confirmed by observing a violation of Bell's inequality with 3.2 standard deviations in an entanglement swapping experiment. The techniques developed in our experiment are not only important for realistic linear optical quantum-information processing, but also enable new tests of local realism.

We experimentally implement a fault-tolerant quantum key distribution protocol with two photons in a decoherence-free subspace. It is demonstrated that our protocol can yield a good key rate even with a large bit-flip error rate caused by collective rotation, while the usual realization of the Bennett-Brassard 1984 protocol cannot produce any secure final key given the same channel. Since the experiment is performed in polarization space and does not need the calibration of a reference frame, important applications in free-space quantum communication are expected. Moreover, our method can also be used to robustly transmit an arbitrary two-level quantum state in a type of decoherence-free subspace.

Besides for the experimental research, in the end of the thesis we also report a flaw of the quantum key distribution protocol based on blind bases and a feasible solution to it.

The techniques developed in this dissertation would dramatically facilitate progresses in many important fields of scientific research, including long distance quantum communication, linear optics quantum computation and test of the foundation of quantum mechanics.

Key words: multi-photon entanglement, quantum cryptography, linear optics