

量子力学和相对论的美妙结合：成功实现互不信任终端之间的安全比特承诺

合肥微尺度物质科学国家实验室潘建伟教授及同事张强、彭承志等在国际上首次实现了无条件安全“比特承诺”，在解决如何在相互不信任的通信终端之间直接建立信任的问题上实现了突破。该实验研究成果于近日发表在国际权威物理学杂志《物理评论快报》上，被评价为“密码学的重要进展”和“该领域的先驱实验”。美国物理学会《物理·焦点》栏目也对该成果进行了专题报道。

实现“比特承诺”是指成功建立如下通信机制：甲乙双方为互不信任的终端，甲方可以对某未发生事件做出是或否的预测（即0或1），然后该预测将在事件发生后的某个确定时刻对乙方公布。比特承诺的核心在于确保乙方不能在甲方预测公布前窃听到相关信息，同时也必须保证甲方不能在做出预测后修改结果。这样，甲乙双方都可以确信对方遵守了承诺，从而建立信任并实现通信。

为实现安全“比特承诺”，各国科学家在过去几十年中进行了不懈努力。其中，经典密码学有两种解决方案，即使用第三方公共平台或者利用计算复杂性假设。然而，这两种方案都被证实存在安全隐患，即无法实现“无条件安全”。1997年，加拿大科学家Mayers和Lo分别独立证明，即使是量子保密通信本身也无法保证无条件安全“比特承诺”的建立。2012年，剑桥大学的Adrian Kent教授提出，只有同时利用量子力学和狭义相对论，才能实现无条件安全比特承诺。潘建伟小组通过其自主开发的高速量子保密通信技术和自由空间高速光通信技术，结合西班牙科学家A. Cabello和M. Curty的理论分析，成功地实验验证了Kent教授的理论方案，将互不信任终端之间互相欺骗的几率降低到6%以下，在世界上首次实现了互不信任终端之间的安全“比特承诺”。这一奠基性的研究成果可以被广泛应用于互联网金融、公共随机数产生、设计零知识证明协议、安全计算等领域，开拓了量子通信新的研究方向。



实验室简讯

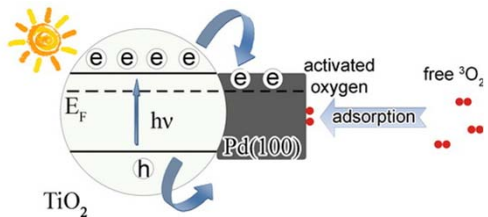
◆熊宇杰教授获2013年度中国化学会青年化学奖

熊宇杰教授多年来一直致力于无机功能材料的可控合成、纳米制造与集成组装，共发表学术论文80余篇，论文总引用7000余次(H index 45)。自2011年6月在我校工作后，入选首批“国家青年千人计划”，围绕催化固体材料的界表面和电荷行为调控开展研究，在《J. Am. Chem. Soc.》、《Angew. Chem. Int. Ed.》、《ACS Nano》等期刊发表通讯作者论文10余篇。

研究进展

复合结构催化剂设计取得重要进展

合肥微尺度物质科学国家实验室熊宇杰教授课题组基于先前在分子活化过程中金属和氧分子间电荷转移的发现(J. Am. Chem. Soc. 2013, 135, 3200)，通过与武晓君教授和罗毅研究团队的张群副教授在材料设计与合成、理论模拟和先进表征中的“三位一体化”合作，再次取得重要进展。研究人员首次以超快光谱和动力学测量为探针，揭示了金属表面等离激元导致的热电子会直接注入n-型半导体带，与肖特基势垒驱动的电荷转移形成竞争关系。在阐明微观作用机制的基础上，研究人员得以通过光强调控这一简单而有效的手段，优化催化剂在氧分子活化和有机氧化反应中的活性。这项突破性研究进展，有助于加深人们对光催化剂复合材料设计的认识，也对阐明有机化学界在氧化反应中广泛使用氧化物载体的原理具有重要意义。该工作近日在线发表在《德国应用化学》杂志上，论文的共同第一作者是博士生龙冉和毛可可。



玻璃化转变研究取得重要进展

合肥微尺度物质科学国家实验室和物理系的徐宁教授研究组一直从事非晶固体本质和非晶液-固转变的理论研究，研究组的博士生王利近和徐宁教授研究发现，玻璃化转变温度完全可以由零温玻璃的结构和振动特性来预言，从而从固体视角对玻璃化转变做出了崭新的诠释。他们独辟蹊径地从零温玻璃的角度解释了过冷液体中吸引作用的非微扰作用，这种结构差异使得有吸引作用的玻璃拥有比纯排斥作用的玻璃更高的特征振动频率和更弱的低频振动模的局域化，从而使得有吸引作用的玻璃更稳定并具有更高的玻璃化转变温度，相应的过冷液体动力学就会有显著差异。更重要的是，从零温玻璃的结构和振动特性出发，王利近博士和徐宁教授提出了完全由零温玻璃的结构和振动物理量表征的玻璃化转变温度的经验表达式，该表达式给出的结果与计算机模拟的结果很好地定量吻合。该研究表明玻璃化转变完全可以从固态玻璃的特性来理解，因此为玻璃化转变的研究开辟了全新的思路。该研究的论文发表于2月7日的《物理评论快报》[Phys. Rev. Lett. 112, 055701 (2014)]。

基于自旋的量子计算与弱磁信号灵敏探测取得重要进展

合肥微尺度物质科学国家实验室杜江峰教授研究组经过三年多努力，搭建了一系列具有国际领先水平的光探测磁共振实验平台，开展基于掺杂金刚石单自旋的量子计算与弱磁信号灵敏探测等前沿科学研究，取得了一系列重要的进展。相关成果发表在2014年《自然》、《自然·物理》和《物理评论快报》上。

精确操控量子比特是量子计算的核心问题之一。对于电子自旋量子比特而言，核自旋热库噪声和驱动场噪声使得实现精确操控极具挑战性。杜江峰教授研究组利用两种新颖的方法，有效抑制了这两种噪声，实现了对单电子自旋的精确操控，相关成果发表在1月9日和2月7日的《物理评论快报》上。此外，杜江峰教授与德国斯图加特大学合作，实验实现了固态自旋体系中的量子纠错，该工作发表在1月29日的《自然》上。这些成果对未来量子计算实用化以及灵敏探测具有重要意义。

电子自旋会感受到周围环境中的核自旋热库噪声。这种磁场涨落噪声对电子自旋的影响不仅表现为破坏量子态，而且会极大制约操控量子系统的品质。杜江峰研究组荣星等发挥磁共振领域中脉冲操控优势，将一种用于对抗梯度磁场涨落噪声的动力学纠错逻辑门，拓展为抑制更为普遍的磁场涨落噪声。实验结果表明外磁场噪声被有效地抑制到六阶，量子相干时间被延长至690±40微秒，这比自由感应衰减时间长了两个数量级，也远远超过了普通脉冲控制下量子相干时间，达到了T1rho(660±80微秒)极限。该工作首次成功将对电子自旋的精确操控水平突破T2极限，推进到了T1水平，极大延长了可对电子自旋量子比特的进行操控的时间，使得更为复杂精确的操控成为可能，从而为基于电子自旋的量子计算及灵敏探测提供了关键技术[Phys. Rev. Lett. 112, 050503 (2014)]。

此外操控电子自旋的驱动场也会引入额外的噪声。当环境中自旋热库噪声被有效抑制之后，驱动场噪声将成为制约操控品质的一个重要因素。杜江峰研究组周经纬等利用快速的微波频率调制，首次实验实现时域上超过100次的Landau-Zener(LZ)隧穿，并且观测到多次隧穿形成的一种新型拉比振荡现象。理论与实验结果表明，这种新型的拉比振荡可以有效抑制驱动场引入的噪声，从而为实现精确操控提供了一种崭新的手段。该工作不仅将有助于深入理解与LZ隧穿和拉比振荡相关的重要物理过程，而且对于量子控制技术在量子计算、生物化学等领域的应用具有重要的价值[Phys. Rev. Lett. 112, 010503 (2014)]。

量子纠错也是一种可以有效对抗噪声的方案，而且是实现容错量子计算的关键。杜江峰教授与德国斯图加特大学合作，将核磁共振中的最优控制方法拓展到光探测磁共振，实现了一个电子自旋和三个核自旋构成的复杂量子系统的高精度操控，从而实现了固态自旋体系中量子纠错。这项工作为基于固态自旋体系的量子计算实用化打下了坚实的基础[Nature advance online publication 29 January 2014. doi:10.1038/nature12919]。

精确的量子操控和有效抑制环境噪声还对弱信号的灵敏检测意义重大。杜江峰研究组石发展等利用掺杂金刚石中氮-空位固态单电子自旋量子干涉仪，把微观自旋体系产生的弱磁信号转为干涉仪的相位，并利用多脉冲动力学解耦技术和外加磁场来有效抑制环境噪声，成功实现了室温大气环境下单核自旋对的探测及其原子尺度的结构分析。该工作表明动力学解耦技术结合单自旋探针是单分子结构解析和谱学分析的有力工具，可帮助我们在纳米甚至原子尺度获取物质组成和结构信息，为物理生物等各领域开展微观研究提供新的方法[Nature Physics 10, 21 (2014)]。

杜江峰教授研究组的这些工作把对自旋量子体系的操控能力提升到了一个新的水平，而且这些工作中发展出来的方法可被应用到多种重要量子比特体系，譬如量子点，离子阱，超导量子比特等。因此这些重要进展为量子计算、弱磁信号灵敏探测等前沿领域打下了坚实基础。