# 清华大学高等研究院
# Institute for Advanced Study, Tsinghua University
## 密码学学术报告
## Cryptology Seminars

**Title：** 量子密钥分发的一些理论进展
Some developments in quantum key distributions

**Speaker:** Heng Fan (范桁)
中国科学院物理研究所研究员

**Time：3:15 pm, Wednesday, Sept 19, 2012**
**(2:45~3:15pm, Tea, Coffee, and Cookie)**

**Venue:** Conference Hall 322, Science Building, Tsinghua University

**Abstract:**大家普遍采用的量子密钥分发是基于 BB84 协议及其相关发展的。对高维系统的研究局限于两种简单的推广，我们提出这种推广其实存在多种形式。在安全性的证明方面，我们发现原来的两种最优化标准并不能给出相同的条件。我们同时研究了一种基于量子 mean king 问题的新型量子密钥协议，给出了其最一般的形式，并证明其在二维系统可以比 BB84 协议提供更安全的边界，从而对实际应用提供了另外一种选择。

**范桁，** 男,中国科学院物理研究所研究员，中科院“百人计划”入选者（2005）。90 年北京大学毕业，96 年西北大学博士学位。1999-2005 先后在东京大学、加州大学洛杉矶做研究工作。2005 年至今在物理所工作。在量子信息和量子计算、凝聚态理论、场论和统计等研究中取得成果。发表 SCI 文章 110 余篇,其中 Nature 子刊(Nat.Commun.)一篇, Phys.Rev.Lett.三篇, Nucl.Phys.B 八篇,Springer 出版综述性书章节一篇，论文被引用近 1000 次，单篇最高引用 90 次。现 973 项目课题负责人。1999 年曾以第一获奖人获省级科技进步二等奖一项。主要学术贡献：在量子克隆领域有一系列工作，其中相位克隆被美国、意大利、中国等多个实验组实现，论文得到引用；在数学物理量子统计方面，解决了八顶角模型带边界的精确解(NPB)，共形场的任意子构造(PRL)；在量子信息和凝聚态多体系统研究方面，解决了固体共价键态的纠缠计算(PRL)，结果被 PRL 摘要里引用。最近指出凝聚态模型中不同的量子相在进行绝热量子计算中的能力是不同的（Nat.Commun.）。在量子纠缠、量子关联理论方面，解决了多个纠缠态局域可分辨性问题(PRL)。在实验和理论结合方面，首次在室温固态系统(金刚石氮色心)实现相位克隆。