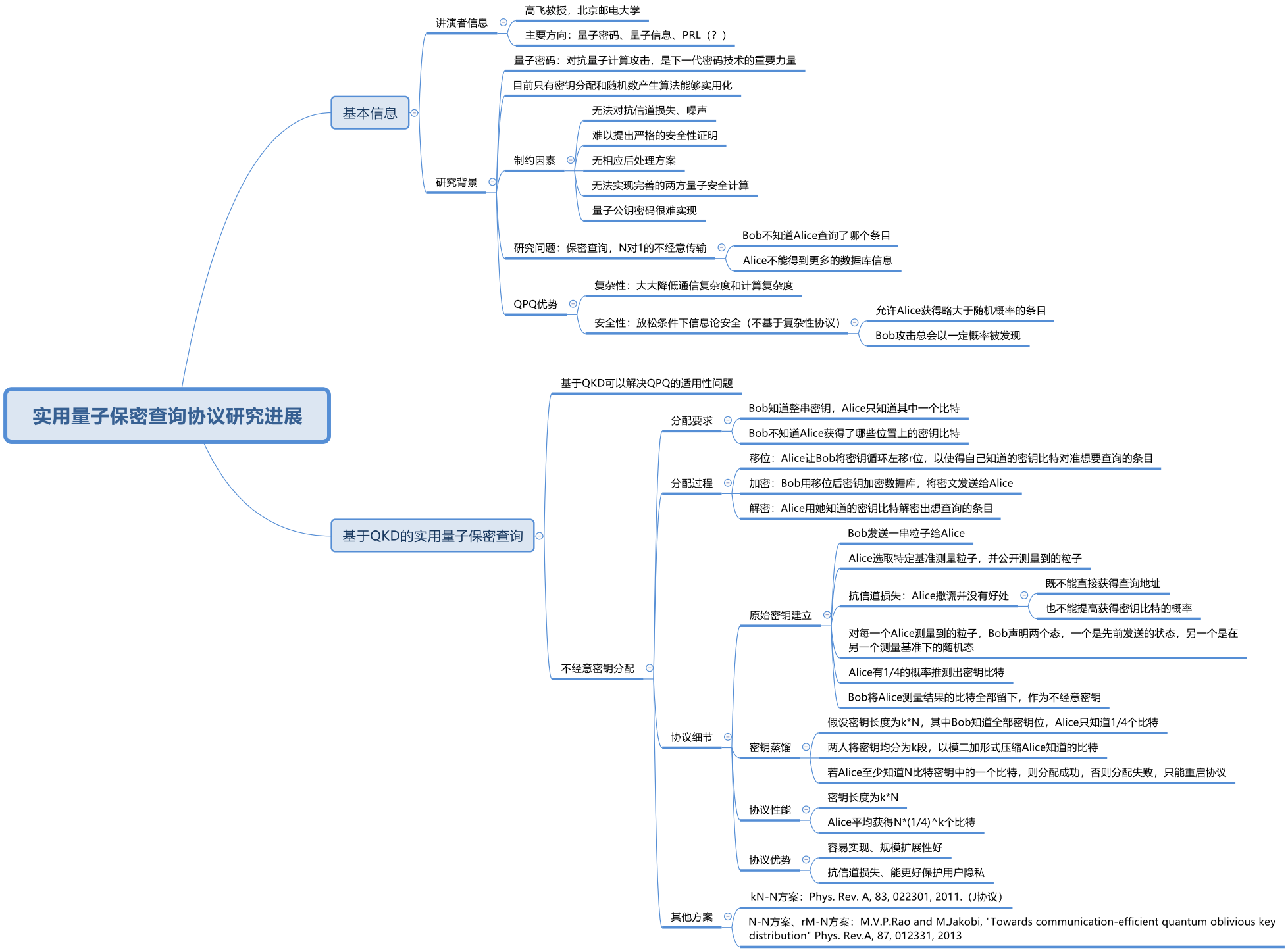
实用量子保密查询协议研究进展
基本信息
讲演者信息
高飞教授，北京邮电大学
主要方向：量子密码、量子信息、PRL（？）
研究背景
量子密码：对抗量子计算攻击，是下一代密码技术的重要力量
目前只有密钥分配和随机数产生算法能够实用化
制约因素
无法对抗信道损失、噪声
难以提出严格的安全性证明
无相应后处理方案
无法实现完善的两方量子安全计算
量子公钥密码很难实现
研究问题：保密查询，N对1的不经意传输
Bob不知道Alice查询了哪个条目
Alice不能得到更多的数据库信息
QPQ优势
复杂性：大大降低通信复杂度和计算复杂度
安全性：放松条件下信息论安全（不基于复杂性协议）
允许Alice获得略大于随机概率的条目
Bob攻击总会以一定概率被发现
基于QKD的实用量子保密查询
基于QKD可以解决QPQ的适用性问题
不经意密钥分配
分配要求
Bob知道整串密钥，Alice只知道其中一个比特
Bob不知道Alice获得了哪些位置上的密钥比特
分配过程
移位：Alice让Bob将密钥循环左移r位，以使得自己知道的密钥比特对准想要查询的条目
加密：Bob用移位后密钥加密数据库，将密文发送给Alice
解密：Alice用她知道的密钥比特解密出想查询的条目
协议细节
原始密钥建立
Bob发送一串粒子给Alice
Alice选取特定基准测量粒子，并公开测量到的粒子
抗信道损失：Alice撒谎并没有好处
既不能直接获得查询地址
也不能提高获得密钥比特的概率
对每一个Alice测量到的粒子，Bob声明两个态，一个是先前发送的状态，另一个是在另一个测量基准下的随机态
Alice有1/4的概率推测出密钥比特
Bob将Alice测量结果的比特全部留下，作为不经意密钥
密钥蒸馏
假设密钥长度为k*N，其中Bob知道全部密钥位，Alice只知道1/4个比特
两人将密钥均分为k段，以模二加形式压缩Alice知道的比特
若Alice至少知道N比特密钥中的一个比特，则分配成功，否则分配失败，只能重启协议
协议性能
密钥长度为k*N
Alice平均获得N*(1/4)^k个比特
协议优势
容易实现、规模扩展性好
抗信道损失、能更好保护用户隐私
其他方案
kN-N方案：Phys. Rev. A, 83, 022301, 2011.（J协议）
N-N方案、rM-N方案：M.V.P.Rao and M.Jakobi, "Towards communication-efficient quantum oblivious key distribution" Phys. Rev.A, 87, 012331, 2013