学术报告听后感

报告情况：

报告题目：量子算法的构造方法和量子算法的进展情况

报告人：　龙桂鲁教授 清华大学物理系

报告时间：2019 年 9 月 24 日(星期二) 下午 13：00-14：00

报告地点：玉泉校区 工商楼二楼 200-9 数学学术报告厅

摘要：　介绍了量子算法的最新进展和可能的研究方向和问题。

正文：

这门课程最早的开题报告作业，我就写了目前正在研究的一个方向：后量子密码安全性。简单来讲，目前保障信息安全的主要途径是密码学，而密码学中的一些公钥算法如 RSA 等，在量子计算机的技术真正成熟后就会被轻易攻破。巧妙利用了量子计算机各种特性进行计算的方法称为量子算法，而我们实验室目前在研究的是用来抵御量子算法攻击的后量子算法。由于两者之间是矛与盾的关系，所以我很想了解量子算法的进展。因此前去听了这个讲座。在讲座中获取的信息记录如下：

首先，要真正利用量子特性来进行算法实现，需要支持量子计算的物理平台。目前有五种主流的方式被认为是可行的，然而其中还有两种目前还没有真正在物理层面实现，而这两种恰恰是理论效率最高的两种方法。

所以，要达到能破解当前计算复杂度的 RSA 等加密算法，量子计算硬件还有很长的发展空间。因为量子计算利用了多个量子比特之间的量子纠缠关系，今年后半年谷歌提出的被称为“量子霸权”的量子计算机其实仅实现了 50 个左右量子的纠缠，就可以高于普通计算机多倍的计算效率运行。

其次，要能更好地利用量子计算平台，需要与之适配的量子算法。这些量子算法既利用了量子的不确定性，又要用各种数学方法进行确定的计算过程。

在讲座中老师提到，构造量子算法有五种重要技术：

1. 量子相位估计
2. 酉算子线性组合
3. 量子线性算法
4. Grover 搜索
5. 量子行走

由于我研究的是后量子算法，对这些构造量子算法的技术也了解不多，但是可以看出其中存在数学基础与量子特性的结合。这个特性要求研究人员要同时对数学与物理有足够的掌握，难度较大，但又确实是量子计算中必须研究的问题。

在讲座最后，老师提到了该领域的总结与展望。其中有一条：利用对偶量子计算分析抗量子密码算法。其实仅仅是翻译的问题，这里的抗量子密码算法就是我提到的后量子密码算法。由此可见，不仅在当前密码学存在对加密算法的攻击，在基于量子计算机的算法领域，同样存在攻击与对抗。因此在量子计算硬件平台不断发展的背景下，基于此平台的量子算法与抗量子算法都将在博弈和对抗中不断发展，有很广阔的研究前景。

除了学习上的收获，老师提到的他自己的经历也让我很有感触。龙桂鲁老师自述，他是从核物理领域转去量子算法领域的，在刚刚接触的时候也对数学角度的一些知识一窍不通，而他一边继续自己领域的科研与工作，一边进行新方向的学习，每天都坚持对新知识的了解与掌握。而我现在只需要对一个领域尽可能地深入研究，我就应该做到和龙老师一样的不懈地学习，最终总能在此领域达到不低的掌握程度。