听《Battles of Cryptographic: Algorithms in Hardware and Software: Toward Choosing the Most Efficient and Flexible Post-Quantum Cryptography Standard》有感

Kris Gaj是美国乔治梅森大学（George Mason University，U.S.A.）欧洲经委会（ECE）系教授。他是密码工程研究小组（CERG）的联席主任，参与了从AES到PQC的大多数以前和现在的密码竞赛。特别是，他的团队在2010-2012年领导了新哈希函数标准SHA-3和2016-2018年新认证密码组合CAESAR的硬件评估。他目前的研究和教学兴趣包括密码工程和硬件安全，特别关注后量子公钥密码系统、秘密密钥算法和密码破译的新硬件体系结构和嵌入式系统实现的开发，以及密码硬件和EM的基准测试。层叠茎、高级合成、软硬件协同设计和侧通道分析。

报告围绕着后量子密码术（PQC）开展，PQC指的是一类新的密码算法，可以抵抗所有已知的使用量子计算机的攻击，但同时也可以自己使用传统的计算平台来实现，例如智能手机平板电脑、笔记本电脑和基于集成电路的硬件加速器PQC是加密对全面量子计算机新威胁的响应，并预计将在未来十年或二十年内开发。PQC的主要目标是取代现有的公钥加密标准，保护大部分的互联网流量，如rsa和椭圆曲线加密（ECC）。密码竞赛已经成为开发密码标准的一种普遍接受的方式。这一过程在最近的比赛中表现得特别好，如SHA-3和CAESAR。在这些竞赛中，候选人在硬件和软件方面的表现已经成为一个非常重要的评价因素，在多个候选人中有明显的区别，有足够的安全实力。美国国家标准技术研究所于2016年发起的PQC标准化进程已进入第二轮，共有26名候选人，代表了5个主要PQC组。到目前为止，对候选人的评估主要集中在他们的安全性和通用微处理器的效率上。本次讲座的目的是通过使用新的方法，如软件/硬件协同设计和高级综合，为早期、系统和全面研究最有希望的PQC候选的硬件和嵌入式系统效率奠定基础。有了这一基础，我们相信完全硬件和软件/硬件实现的开发时间可以大大缩短，允许公平和全面的基准测试最有希望的候选人，以及公平选择最有效和灵活的算法作为未来的美国和事实上的全球PQC密码标准杆。下一个5~10年很可能会带来自20世纪70年代中期公开密钥密码术发明以来最大的密码学革命。该项目将为所有相关研究人员提供一个独特的机会，以影响未来密码标准的选择，这些标准可能在未来十年内开发和部署，并将继续使用。

量子算法对于传统密码系统的冲击是由于量子算法相对于经典算法在一些问题上具有一定的加速性（可以简单理解为量子算法具有高度的并行计算能力）。例如，在传统计算机上需要亚指数计算时间的大整数分解问题，在量子计算机上多项式时间内就可求解。然而，量子算法相对于传统算法的“指数”加速性并不是对所有数学问题都成立。事实上，对于某些问题（如NP完全问题、基于格、基于编码和基于多变元方程的数学问题），量子算法相对于传统算法并没有明显的优势。紧跟着Shor算法的出现，国内外密码学家已对基于格、基于编码和基于多变元方程密码方案展开了大量的研究，力图设计可以对抗量子计算机的经典密码算法，并统称这些研究为后量子密码学。

通过这次讲座，我粗浅地了解了量子算法的原理以及研究意义，区分了量子算法的诞生对传统加密方法带来的冲击，开阔了视野。