评“大数据环境下量子机器学习的研究进展及发展趋势”
王晓霆

量子机器学习是量子计算和机器学习在各自领域蓬勃发展后必然产生的交叉学科。量子计算的概念，可以追溯到二十世纪八十年代 Benioff 提出的计算机量子力学模型；而机器学习的概念，可以追溯到二十世纪四五十年代包括人工神经元在内的有关机器学习的先驱性研究。历史总是惊人的相似，两个学科在发展之初，各自领域最杰出的科学家都做出了开创性的工作：一边是图灵提出的图灵测试，另一边是费曼提出的量子计算机和量子模拟的概念；两个学科的理论基础均在二十世纪八九十年代得到了高速发展，并都在高速发展之后经历了一段“严冬”，然后在 2010 年之后得益于物理硬件上的突破而重新获得了高度关注和发展，并应运而生了量子机器学习这一交叉学科。经过近十年的发展，量子机器学习尤其是相关量子算法方面，已经获得一系列重要的进展，如该文提到的量子 K 近邻、量子支持向量机、量子主成分分析、量子神经网络等，其研究范围已经包括了经典机器学习所涉及的方方面面；然而，量子机器学习尚未被解决的重大问题依然存在，包括近两年出现的新进展和问题，亟需更多好的综述性文章做出承前启后的总结作用。

该文从一个新颖的角度，即大数据的复杂性和不确定性，对量子机器学习如何跟大数据研究相结合这一课题，做出了相关综述，系统地总结了大数据不确定性集合理论和分析方法，总结了经典机器学习的研究对象和相关算法，以及迄今为止量子机器学习领域所提出的量子算法和相关问题，并给出了一个如何结合大数据本身的科研问题探索量子机器学习新算法的思路。如何在大数据领域，获得更多有关量子机器学习的理论成果和应用场景，我们拭目以待。

评“SM4 密码算法 S 盒的量子电路实现”
徐兵杰

随着量子计算的发展，现行经典密码系统的安全性受到了严峻威胁。对于非对称密码系统，Shor 算法能够迅速破解基于大整数分解及离散对数困难问题的密码算法；对于对称密码系统，Grover 算法能使其等价安全密钥长度减半，其安全性所受的影响相比于非对称密码系统较小，但仍需引入相应措施以应对量子计算威胁。现有对称密码算法在量子环境下的安全性分析大多基于该算法可通过量子电路实现的假设之上，但目前国内外仅在 AES 算法的量子电路实现方面有少量研究，而对其他主流对称密码算法 (如 SM4) 的量子电路实现研究并未涉及。

该文针对以上研究现状，首次给出了 SM4 密码算法 S 盒的量子电路实现方案。主要基于 SM4 密码算法 S 盒的代数结构，采用 48 个量子比特，592 个量子门 (包括 NOT 门、CNOT 门和 Toffoli 门)，电路深度为 289，比较高效地构建并实现了其 S 盒的量子电路。该研究将对量子环境下 SM4 密码算法的研究产生推动作用，也丰富了对称密码在量子环境下的安全性分析。