评“区块链环境下用户身份匿名的量子委托计算协议”

邓光伟

量子信息处理与区块链均为当前热门的应用研究领域，二者可以在技术上短板互补，在应用上协同发展。区块链的去中心化、匿名性与不可篡改性，结合量子信息学相对经典密码学的优越性，可以设计出更安全、高效的场景应用协议。

以此为背景，该文重点关注了量子委托计算网络中的用户身份安全，设计出一个兼顾数据与身份盲性，且不需要可信第三方的匿名委托计算协议。该协议使用量子同态加密完成委托计算，用户在委托计算中使用环签名网络进行身份混淆，使用量子隐形传态技术对委托请求与计算结果进行传输与接收，能够匿名、定向、安全地传输量子态数据。在协议中，使用区块链技术对委托计算过程进行审批，保护交易过程的公平。在改进后的协议中，依靠区块链共识机制验证委托计算的正确性。

该文所提协议具有较高的可行性与安全性，且依靠区块链技术获得了较高的效率。除此之外，还创新性地提供了一个面向大数据环境的开放性协议框架，其不依赖于特定算法，能够灵活地替换子协议，且可迁移至其他需要身份和数据匿名的应用场景，具有良好的应用前景。

评“基于复合域 SM4 密码算法 S 盒的量子电路实现”

邓光伟

量子计算在理论上对现有的密码系统构成了严峻的威胁。对于非对称密码系统，Shor 算法可以快速破解基于大整数分解和离散对数困难问题的密码系统。因此，美国国家标准与技术研究院 (NIST) 从 2016 年开始遴选新的密码标准，以抵抗量子计算机的攻击。在对称密码领域，暂时还没有相关的机构计划制定新的密码标准用以抵抗量子计算机的攻击，但量子计算对于对称密码的威胁依然存在，如 Grover 算法能使其等价安全密钥长度减半。因此，进一步研究对称密码在量子环境下的安全性是很有必要的。

随着量子计算的发展，随之而来的一个问题是，多大规模的量子计算机将对对称密码系统构成实质性威胁，这就需要分析这些密码算法在实现时所用的量子资源。该文以我国自主研发的分组密码算法 SM4 中唯一的非线性组件 S 盒为研究对象，结合复合域和量子逻辑综合相关理论，进一步优化了实现 S 盒的量子资源。该文将为更准确地评估 SM4 算法所用量子资源提供依据，也为进一步评估其他对称密码算法所用量子资源提供参考。