doi:10.1631/FITEE.1700039

题目：一个格上不经意传输协议的量子安全性分析

概要：不经意传输协议（oblivious transfer, OT）因其简易的密码功能广泛应用于安全多方计算。以往 OT 协议都是基于传统数论问题（例如，离散对数，大数分解问题）所构造的，随着量子计算技术的发展，基于传统困难问题的 OT 协议安全性受到极大的威胁。因此，人们转而考虑使用后量子密码技术替代以往 OT 协议所依赖的传统困难问题。目前，已有一些基于后量子密码体制的 OT 协议被提出。然而，大多数后量子密码构造只在假设传统敌手存在的环境下证明其方案安全性。在本文中，我们在量子敌手存在的环境下，证明一个基于格公钥密码的 OT 协议（[PVW08]）的安全性。首先我们使用量子平移定理（[Unr10]）证明该协议的安全性可以完全平移到量子环境中，此外，我们还使用其他两个专用于分析后量子密码原语的分析模型（[HSS11]，[Son14]）从不同的角度对该协议进行安全性分析，从而保证我们给出的量子安全证明的正确性。我们的成果可以看作对后量子密码协议分析模型的一个实际应用实例。

关键词：不经意传输；后量子；格公钥；带差错学习；通用可复合