后量子安全的格盲签密方案

俞惠芳，白璐
西安邮电大学网络空间安全学院，中国西安市，710121

摘要：盲签密能够保证签密消息的盲性和不可追踪性，可以同时实现盲签名和公钥加密。大多数盲签密都是基于传统数论问题。随着量子计算技术的发展，传统盲签密面临着严峻的安全威胁。作为有前途的抗量子计算候选密码系统，格密码系统在学术领域引起越来越多关注。本文通过将盲签密应用于格密码系统，提出一种后量子安全的格盲签密方案（PQ-LBSCS）。PQ-LBSCS具有格密码体制和盲签密技术的优点。在标准模型中PQ-LBSCS基于带错误学习问题和小整数解问题被证明是安全的。Matlab仿真结果表明PQ-LBSCS比已有方案更高效。PQ-LBSCS安全性强、计算效率高，使其在电子商务、移动通信、智能卡等领域具有广泛应用前景。

关键词：格密码系统；盲签密；抗量子计算；带错误学习问题；最短向量问题
https://doi.org/10.1631/FITEE.2000099