格上高效的身份基签名

陈江山[1,2]，胡予濮[1]，梁红梅[2]，高雯[3]
[1]西安电子科技大学综合业务网理论及关键技术国家重点实验室，中国西安市，710071
[2]闽南师范大学数学与统计学院，中国漳州市，363000
[3]西安邮电大学网络空间安全学院，中国西安市，710061

摘要：随着电子信息技术的飞速发展，数字签名已成为人们生活中不可或缺的一部分。由于证书管理的局限性，传统的公钥证书密码系统无法满足现有需求。基于身份的密码系统避免了证书管理问题。量子计算机的发展给传统密码学带来严峻挑战。后量子密码学研究势在必行。目前，几乎所有后量子基于身份的签名方案都是利用高斯采样技术或陷门技术构建的。但是，这两种技术对计算效率有很大影响。为克服该问题，采用Lyubashevsky签名方案构造了格上基于身份的签名方案。基于格上的最短向量问题，该方案既不使用高斯采样技术也不使用陷门技术。在随机谕言机模型中，可以证明该方案对适应性选择的消息和身份攻击是不可伪造的。其安全性级别是强不可伪造的，比其他方案存在性不可伪造的安全性更高。与其他有效方案相比，所提方案在计算复杂度和安全性方面具有优势。

关键词：身份基签名；格；强不可伪造性；随机谕言机模型
https://doi.org/10.1631/FITEE.1900318