电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2014, Vol. 36 » Issue (3) :645-649 DOI: 10.3724/SP.J.1146.2013.00818

格上基于身份的单向代理重签名

江明明*① 胡予濮① 王保仓① 来齐齐① 刘振华②*

①(西安电子科技大学综合业务网理论与关键技术国家重点实验室 西安 710071)
②(西安电子科技大学数学与统计学院 西安 710071)

Identity-based Unidirectional Proxy Re-signature over Lattice

Jiang Ming-ming① Hu Yu-pu① Wang Bao-cang① Lai Qi-qi① Liu Zhen-hua②*

①(State Key Laboratory of Integrated Service Networks, Xidian University, Xi’an 710071, China)
②(School of Mathematics and Statistics, Xidian University, Xi’an 710071, China)

摘要 代理重签名是简化密钥管理的重要工具，能够提供路径证明和简化证书管理等。目前的代理重签名方案都是基于整数分解与离散对数的，其在量子环境下都不安全。针对这个问题，该文利用原像抽样技术与固定维数的格基委派技术，基于格上的小整数解问题(Small Integer Solution, SIS)的困难性，构造了格上基于身份的代理重签名方案。该方案具有单向性，多次使用性等性质。与其它具有相同性质的基于身份的代理重签名相比，该方案具有验证开销小，渐近复杂度低等优点。

关键词： 代理重签名 格 高斯抽样 小整数解问题

Abstract： Proxy re-signature is an important tool for simplifying key management, and can be used to prove a proof for a path, manage group signatures, simplify certificate management and so on. Currently, proxy re- signature schemes are based on large integer factorization and discrete logarithm which are not security in quantum setting. For this problem, the first identity-based proxy re-signature scheme over lattices is constructed in this paper, which uses preimage sampleable technology and lattice basis delegation in fixed dimension technology. Its security is based on the hardness of Small Integer Solution (SIS) problem. This scheme possesses the properties of unidirectional, multi-use and so on. Compared with the previous schemes which have the same properties, the proposed scheme has the advantage of low verification cost and low asymptotic computational complexity.

Keywords： Proxy re-signature Lattice Gaussian sampling Small Integer Solution (SIS) problem

Received 2013-06-07;

本文基金:

国家自然科学基金(61173151, 61173152, 61100229)资助课题

通讯作者: 江明明： 男，1984年生，博士生，研究方向为格公钥密码、数字签名. Email: jiangmm3806586@126.com