基于格的数字多签名体制

彭春燕，杜秀娟，李梅菊，刘雪珂
(青海师范大学 计算机学院，青海 西宁 810008)

摘 要： 传统的数字多签名体制大多基于大整数与离散对数困难问题，这一多签名方案在量子计算机环境下已不再安全.利用格理论上的小整数解问题（SIS）的困难性问题构造的数字多签名方案，能够抵抗量子计算机攻击.该数字多签名体制，可以分为同时签名和顺序签名两种类型.分别描述了格理论上的这两种数字多签名体制的密钥生成、签名步骤及签名验证过程，证明了基于格的数字多签名的有效性及安全性.

关键词： 格；多签名；同时签名；顺序签名

Digital Multi-signature Scheme Based on Lattice

PENG Chun-yan, DU Xiu-juan, LI Mei-ju, LIU Xue-ke

(Department of Computer, Qinghai Normal University, Xining 810008, China)

Abstract： The traditional digital multi-signature scheme mostly based on large integer factorization and the discrete logarithm problems, which has not been secure in quantum environment. The paper presents a new lattice-based multi-signature scheme that can resist the quantum attack using the hardness of average-case short integer solution problem (SIS). Multi-signature includes two types: simultaneous signature and sequential signature. The paper describes respectively the key generation, multi-signature generation and multi-signature verification of the two multi-signature schemes, and then has proved the digital multi-signature scheme based on lattice is especially efficient and secure to multi-signature generation.

Key words： lattice; multi-signature; simultaneous signature; sequential signature

作者简介：
彭春燕 女，（1980-），博士研究生，副教授.研究方向为无线网络与安全研究.E-mail:7456911@qq.com.
杜秀娟 女，（1970-），教授，博士生导师.研究方向为水下通信协议、无线网络安全.