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

电子与信息学报 » 2010, Vol. 32 » Issue (10) :2400-2403 DOI: 10.3724/SP.J.1146.2009.01491

论文

格上基于盆景树模型的环签名

王凤和[①②] 胡予濮[①] 王春晓[③]*

[①](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)
[②](泰山学院数学与系统科学学院 泰安 271021)
[③](山东建筑大学理学院 济南 250101)

A Lattice-based Ring Signature Scheme from Bonsai Trees

Wang Feng-he[①②] Hu Yu-pu[①] Wang Chun-xiao[③]*

[①](Key Laboratory of Computer Networks & Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)
[②](Dept. of Mathematics, Taishan Collage., Taian 271021, China)
[③](Dept. of Mathematic and physics. Shandong Jianzhu University, Jinan 250101, China)

摘要 | 参考文献 | 相关文章

Download: PDF (258KB) HTML 1KB Export: BibTeX or EndNote (RIS) Supporting Info

摘 要 基于格上SIS(Short Integral Solution)问题的困难性假设，在盆景树模型下，利用盆景树签名构造了一个格上的环签名。环签名的安全性是基于格上SIS问题的困难性。方案实现了签名者身份的完全匿名性，在标准模型下(无随机预言机)证明环签名方案满足存在性不可伪造。

关键词： 密码学 环签名 格 盆景树 基向量

Abstract： Under the hard assumption of SIS (Short Integral Solution), a lattice-based ring signature scheme in bonsai tree model is proposed, which based on the bonsai tree signature scheme. Security of proposed ring signature is based on the hardness of SIS. The privacy of signer is guaranteed in proposed ring signature. This ring signature is also unforgeability, which is proved in the standard model (without random oracle).

Keywords： Cryptography Ring signature Lattice Bonsai trees Basis vectors

Received 2009-11-20;

本文基金:

国家自然科学基金(60970119，60803149)和国家973计划项目(2007CB311201)资助课题

通讯作者: 王凤和 Email: fenghe2166@163.com

Service
把本文推荐给朋友
加入我的书架
加入引用管理器
Email Alert
RSS
作者相关文章
王凤和
胡予濮
王春晓

引用本文:
王凤和, 胡予濮, 王春晓.格上基于盆景树模型的环签名[J] 电子与信息学报, 2010,V32(10): 2400-2403

Wang Feng-He, Hu Yu-Pu, Wang Chun-Xiao.A Lattice-based Ring Signature Scheme from Bonsai Trees[J] , 2010,V32(10): 2400-2403

链接本文:
http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2009.01491 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I10/2400