电子与信息学报 2008 30 (6): 1450-1452 ISSN: 1009-5896 CN: 11-4494/TN

论文

一种新的等价于大整数分解的公钥密码体制研究

姜正涛①, 张京良②, 王育民②

①北京航空航天大学计算机学院 北京 100083;②西安电子科技大学综合业务网国家重点实验室 西安 710071

收稿日期 2006-11-20 修回日期 2007-6-4 网络版发布日期 2008-8-28 接受日期

摘要
在弱的安全假设下构造可证明安全的密码体制原型可以有效提高密码体制的安全性, 该文对用Lucas序列构造公钥密码体制做进一步研究, 给出一种新的可证明安全的密码体制原型, 该密码体制的加、解密效率比现有的LUC密码体制效率高, 并证明它的安全性等价于分解RSA模数, 最后给出该体制在签名方面的应用, 伪造签名等价于分解RSA模数。

关键词 公钥加密体制 Lucas序列 Lucas二次（非）剩余 整数分解 签名

分类号 TN918

Research on a New Public Key Cryptosystem as Secure as Integer Factorization

Jiang Zheng-tao①, Zhang Jing-liang②, Wang Yu-min②

①School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100083, China; ②National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China

Abstract
Constructing provably secure cryptographic primitives under weak assumptions can improve the security of cryptographic schemes efficiently. Further research on the construction of public-key cryptosystem is provided, and a new public-key encryption primitive is investigated. This scheme is more efficient than that of existing LUC cryptosystems. More over, the proposed scheme is provable secure and its security is proved to be equivalent to the factorization of RSA modulus. At last, an application in signature is suggested; forgery of signature is also equivalent to the factorization of RSA modulus.

Key words Public-key encryption scheme Lucas sequence Lucas (non)quadratic residue Integer factorization Signature

DOI:

通讯作者

作者个人主页 姜正涛①; 张京良②; 王育民②