电子与信息学报 2007 29 (1): 185-188 ISSN: 1009-5896 CN: 11-4494/TN

论文

一种新的基于Lucas序列的公钥密码体制

王衍波, 张凯泽, 王开华, 端木庆峰, 雷凤宇

解放军理工大学通信工程学院 南京 210007

收稿日期 2005-6-8 修回日期 2005-11-30 网络版发布日期 2008-1-9 接受日期

摘要
该文分析了LUC公钥密码体制，提出了基于Lucas序列的新的公钥密码体制LUC-RSA，LUC-Rabin，其安全性比LUC，RSA强，数据吞吐率大于LUC。

关键词 公钥密码体制 RSA LUC

分类号 TN918

A New Public-Key Cryptosystems on Lucas Sequence

Wang Yan-bo, Zhang Kai-ze, Wang Kai-hua, Duanmu Qing-feng, Lei Feng-yu

Institute of Communications Engineering, PLA Univ. of Sci. & Tech., Nanjing 210007, China

Abstract
LUC public-key cryptosystem is analyzed, two new public-key cryptosystems on Lucas sequence LUC-RSA, LUC-Rabin are presented, their security are stonger than LUC, RSA, and the rate of throughput of the data are greater than LUC.

Key words Public-key cryptosystem RSA LUC

DOI:

通讯作者

作者个人主页 王衍波; 张凯泽; 王开华; 端木庆峰; 雷凤宇