

ISSN 2095-7025
CN 10-1195/TN

密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

创刊号

第1卷 第1期 Vol.1 No.1
2014年2月



主办



中国密码学会

中国科学技术出版社

目 次

属性密码学研究.....	冯登国, 陈 成 (1)
格密码学研究.....	王小云, 刘明洁 (13)
Lai-Massey 结构的轮安全性.....	睦 晗, 吴文玲, 张立廷 (28)
椭圆曲线离散对数的不动点.....	杜育松, 张方国 (41)
针对轻量化掩码方案的功耗分析方法.....	唐 明, 王 欣, 李延斌, 向 潇, 邱镇龙, 张焕国 (51)
具有良好密码学性质的布尔函数的级联构造.....	吴保峰, 林东岱 (64)
非线性反馈移位寄存器序列子簇的研究进展.....	田 甜, 戚文峰 (72)
马尔可夫密码理论在实际密钥变换算法下的适用性.....	薛伟佳, 王清泉, 来学嘉 (83)
对一种纵向重用型 AES 掩码的能量分析攻击.....	王 安, 于艳艳, 陈 曼, 王小妹, 张国双 (91)
基于彩虹表的时间-存储折中攻击改进算法.....	郑中翔, 吉庆兵, 于红波 (100)
中国密码学会 2014 年会征文通知.....	(12)
《密码学报》投稿指南.....	(封三)

CONTENTS

Research on Attribute-based Cryptography FENG Deng-Guo, CHEN Cheng (1)

Survey of Lattice-based Cryptography WANG Xiao-Yun, LIU Ming-Jie (13)

Round Security of Lai-Massey Structure SUI Han, WU Wen-Ling, ZHANG Li-Ting (28)

Fixed Points for Elliptic Curve Discrete Logarithms DU Yu-Song, ZHANG Fang-Guo (41)

Power Analysis on Lightweight Mask Scheme
.....TANG Ming, WANG Xin, LI Yan-Bin, XIANG Xiao, QIU Zhen-Long, ZHANG Huan-Guo (51)

Constructing Boolean Functions with Good Cryptographic Properties by Concatenation
..... WU Bao-Feng, LIN Dong-Dai (64)

Survey on Sub-families of NFSR Sequences TIAN Tian, QI Wen-Feng (72)

Applicability of Markov-cipher Theory on Actual Key Schedules
..... XUE Wei-Jia, WANG Qing-Quan, LAI Xue-Jia (83)

Power Analysis Attacks on AES with Vertically-reused Masks
..... WANG An, YU Yan-Yan, CHEN Man, WANG Xiao-Mei, ZHANG Guo-Shuang (91)

Faster Cryptanalytic Time-memory Trade-off Using Rainbow Table
..... ZHENG Zhong-Xiang, JI Qing-Bing, YU Hong-Bo (100)

密码学报

Mima Xuebao
(双月刊, 2014年创刊)
第1卷 第1期 2014年2月

Journal of Cryptologic Research

(Bimonthly)
(Started in 2014)
Vol.1 No.1 Feb. 2014

编辑 《密码学报》编辑部
(北京市海淀区永翔北路9号 邮编100878)
电话: 86-10-81033105
传真: 86-10-81033101
E-mail: jcr@cacrnet.org.cn
<http://www.jcr.cacrnet.org.cn>

主编 裴定一
主办单位 中国密码学会 中国科学技术出版社
主管单位 中国科学技术协会
出版 中国科学技术出版社
印刷 北京科信印刷有限公司
发行 《密码学报》编辑部

Edited by Editorial Board of Journal of Cryptologic Research
(No. 9, North Yongxiang Road, Haidian District,
Beijing 100878, P. R. China)
Tel: 86-10-81033105
Fax: 86-10-81033101
E-mail: jcr@cacrnet.org.cn
<http://www.jcr.cacrnet.org.cn>

Editor-in-Chief PEI Ding-Yi
Sponsored by Chinese Association for Cryptologic
Research (CACR) and China Science and Technology Press
Supervised by China Association for Science and
Technology (CAST)
Published by China Science and Technology Press
Printed by Beijing Kexin Printing Co., Ltd.

ISSN 2095-7025
CN 10-1195/TN

公开发行

定价:60.00元