

ISSN 2095-7025
CN 10-1195/TN

密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

第3卷 第2期 Vol.3 No.2

2016年4月



主办



中国密码学会

北京信息科学技术研究院



中国科学技术出版社

目次

弱规则单向函数及其应用 郁 昱, 李祥学 (101)

一种保护隐私集合并集外包计算协议 孙茂华, 宫 哲 (114)

一种加密硬盘的身份鉴别和密钥保护方案 谷双双, 夏鲁宁, 贾世杰 (126)

两轮次的可否认的群密钥协商协议 陈 勇, 何明星, 曾晟珂, 李 虓 (137)

一类扩展广义 Feistel 结构抵抗差分 and 线性密码分析能力评估 殷 勳, 王念平 (147)

更高效的指纹生物特征加密 高 莹, 郑长春, 张 凯, 陈 洁 (157)

一种隐私保护的智能电网多级用户电量聚合控制方案 沈 华, 张明武 (171)

Q_Value 检测: 一种新的随机数统计检测方法 庄 家, 马 原, 朱双怡, 林璟镛, 荆继武 (192)

基于 DPA 对 Gauss 形式 CRT-RSA 的选择明文攻击
..... 李增局, 史汝辉, 王建新, 李 超, 李海滨, 石新凌 (202)

第四届密码学与云计算安全国际研讨会征文通知 (156)

“中国密码学会 2016 年青年论坛”通知 (191)

《密码学报》投稿指南 (封三)

CONTENTS

Weakly Regular One-way Functions and Their Applications YU Yu, LI Xiang-Xue (101)

A Privacy-preserving Outsourcing Set Union ProtocolSUN Mao-Hua, GONG Zhe (114)

A Program of Authentication and Key Protection for Hard Disk Encryption
.....GU Shuang-Shuang, XIA Lu-Ning, JIA Shi-Jie (126)

Two-round Deniable Group Key Agreement Protocol
.....CHEN Yong, HE Ming-Xing, ZENG Sheng-Ke, LI Xiao (137)

Security Evaluation for an Extended Generalized Feistel Structure against Differential and Linear
Cryptanalysis YIN Qing, WANG Nian-Ping (147)

More Efficient Fingerprint Biometric Encryption
.....GAO Ying, ZHENG Chang-Chun, ZHANG Kai, CHEN Jie (157)

A Privacy-preserving Multilevel Users' Electricity Consumption Aggregation and Control Scheme in
Smart Grids SHEN Hua, ZHANG Ming-Wu (171)

Q_Value Test: A New Method on Randomness Statistical Test
.....ZHUANG Jia, MA Yuan, ZHU Shuang-Yi, LIN Jing-Qiang, JING Ji-Wu (192)

DPA-based Adaptive Chosen-message Attack on CRT-RSA
..... LI Zeng-Ju, SHI Ru-Hui, WANG Jian-Xin, LI Chao, LI Hai-Bin, SHI Xin-Ling (202)

密码学报

Mima Xuebao

(双月刊, 2014年创刊)
第3卷 第2期 2016年4月

Journal of Cryptologic Research (Bimonthly)

(Started in 2014)

Vol.3 No.2 Apr. 2016

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
北京信息科学技术研究院
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 Beijing Academy of Information
Science & Technology (BAIST) 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