

Scopus 数据库收录期刊

中国科学引文数据库核心期刊 (CSCD)

中国科技核心期刊 (CSTPCD)

ISSN 2095-7025

CN 10-1195/TN

# 密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

第7卷 第3期 Vol.7 No.3

2020年6月

密码应用安全专刊



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

Scopus 数据库收录期刊  
中国科学引文数据库核心期刊(CSCD)  
中国科技核心期刊(CSTPCD)

密码学报  
(Mima Xuebao)

第 7 卷第 3 期  
2020 年 6 月

目 次

密码应用安全专刊	专刊责任编辑: 刘建伟, 林璟铨, 黄欣沂, 汪 定
密码应用安全专刊序言(中英文).....	刘建伟, 林璟铨, 黄欣沂, 汪 定 (285)
密码应用安全技术研究及软件密码模块检测的讨论.....	郑昉昱, 林璟铨, 魏 荣, 王琼霄 (290)
倍点运算的白盒化实现及应用.....	潘文伦, 张立廷 (311)
大规模监视下安全性定义再分析.....	李 耕, 刘建伟, 张宗洋 (326)
一种 NoisyRounds 保护的白盒 AES 实现及其差分故障分析.....	..... 孙 涛, 唐国俊, 吴昕锴, 毛振宁, 龚 征 (342)
SM4 算法的一种新型白盒实现.....	姚 思, 陈 杰 (358)
车联网中支持动态操作的密钥协商协议.....	周天祺, 杨惠杰, 沈 剑 (375)
无证书签名方案的分析及改进.....	张振超, 刘亚丽, 殷新春, 黄可可 (389)
基于区块链技术的密钥生命周期演示设计.....	刘天野, 张艳硕, 石 钰, 朱倩倩 (404)
学术评论.....	(封三)

CONTENTS

Special Issue: Security Applications of Cryptography

LIU Jian-Wei, LIN Jing-Qiang, HUANG Xin-Yi, WANG Ding

Preface of Special Issue on Security Applications of Cryptography .....  
..... LIU Jian-Wei, LIN Jing-Qiang, HUANG Xin-Yi, WANG Ding (285)

Research Progresses on Security Applications of Cryptography and Discussions on Validation of Software  
Cryptographic Modules ..... ZHENG Fang-Yu, LIN Jing-Qiang, WEI Rong, WANG Qiong-Xiao (290)

White-box Implementation of Multiple Point Operation and Its Applications .....  
..... PAN Wen-Lun, ZHANG Li-Ting (311)

Security Definition Against Mass Surveillance, Revisited.....  
..... LI Geng, LIU Jian-Wei, ZHANG Zong-Yang (326)

A NoisyRounds-based White-box AES Implementation and Corresponding Differential Fault Analysis..  
..... SUN Tao, TANG Guo-Jun, WU Xin-Kai, MAO Zhen-Ning, GONG Zheng (342)

A New Method for White-box Implementation of SM4 Algorithm ..... YAO Si, CHEN Jie (358)

Key Agreement Protocol with Dynamic Property for VANETs.....  
..... ZHOU Tian-Qi, YANG Hui-Jie, SHEN Jian (375)

Analysis and Improvement of Certificateless Signature Schemes.....  
.....ZHANG Zhen-Chao, LIU Ya-Li, YIN Xin-Chun, HUANG Ke-Ke (389)

On the Design of Key Life Cycle Demonstration Based on Blockchain Technology .....  
.....LIU Tian-Ye, ZHANG Yan-Shuo, SHI Yu, ZHU Qian-Qian (404)