

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4期 Vol.7 No.4

2020年8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

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 4 期
2020 年 8 月

目 次

一种高效的无证书认证密钥交换协议 曾润智, 王立斌 (421)

基于 XOR 门加密的抗控制流攻击方法 余云飞, 张跃军, 汪鹏君, 李 刚 (430)

一种基于 Rule30+ 细胞自动机的流密码设计方法 郭晓威, 郭亚军 (439)

对 SM4 算法的改进差分故障攻击 金雨璇, 杨宏志, 王相宾, 袁庆军 (453)

ARIA 算法的一个新不可能差分路径及相应攻击 欧海文, 王湘南, 李艳俊, 雷亚超 (465)

利用 K-Means LSH 加速求解格中的最短向量问题 金悦祺, 胡红钢 (473)

最大最小值的保密计算 杨颜璟, 李顺东, 杜润萌 (483)

基于安全经络图元诱因治疗的数学模型分析 汤 卫, 陈玉玲, 杨义先, 钮心忻 (498)

基于 ECDLP 的工作量证明方案设计 刘志杰, 张方国, 田海博 (511)



人工智能与密码专栏 专栏责任编辑: 李 晖

人工智能与密码专栏序言(中英文) 李 晖 (522)

面向加密数据的安全图像分类模型研究综述 孙隆隆, 李 辉, 于诗文, 王迎雪 (525)

基于机器学习的公平数据交易 赵艳琦, 于 斌, 李慧琳, 陈若楠, 禹 勇 (541)

基于改进残差网络和数据增强技术的能量分析攻击研究
..... 王 恺, 严迎建, 郭朋飞, 朱春生, 蔡爵嵩 (551)

学术评论 (封三)

CONTENTS

An Efficient Certificateless Authenticated Key Exchange Protocol
..... ZENG Run-Zhi, WANG Li-Bin (421)

Defending Control Flow Attack Based on XOR-gate Encryption
..... YU Yun-Fei, ZHANG Yue-Jun, WANG Peng-Jun, LI Gang (430)

An Efficient Stream Cipher Design Based on Rule30+ Cellular Automaton
..... GUO Xiao-Wei, GUO Ya-Jun (439)

Improved Differential Fault Attack for SM4 Cipher
..... JIN Yu-Xuan, YANG Hong-Zhi, WANG Xiang-Bin, YUAN Qing-Jun (453)

A New Impossible Difference Path and Corresponding Attack for ARIA Algorithm
..... OU Hai-Wen, WANG Xiang-Nan, LI Yan-Jun, LEI Ya-Chao (465)

Using K-Means LSH to Speed up Solving the Shortest Vector Problem
..... JIN Yue-Qi, HU Hong-Gang (473)

Private Maximum and Minimum Computation
..... YANG Yan-Jing, LI Shun-Dong, DU Run-Meng (483)

Mathematical Model Analysis Based on Safe Meridian Diagram Element Inducement Therapy ...
..... TANG Wei, CHEN Yu-Ling, YANG Yi-Xian, NIU Xin-Xin (498)

Design of PoW Based on ECDLP LIU Zhi-Jie, ZHANG Fang-Guo, TIAN Hai-Bo (511)

////////////////////////////////////

Special Column: Artificial Intelligence and Cryptography **LI Hui**

Preface of Artificial Intelligence and Cryptography Column LI Hui (522)

A Survey on Encrypted Image Recognition Models
..... SUN Long-Long, LI Hui, YU Shi-Wen, WANG Ying-Xue (525)

Fair Data Trading Based on Machine Learning
..... ZHAO Yan-Qi, YU Bin, LI Hui-Lin, CHEN Ruo-Nan, YU Yong (541)

Research on Power Analysis Attack Based on Improved Residual Network and Data Augmentation Tech-
nology WANG Kai, YAN Ying-Jian, GUO Peng-Fei, ZHU Chun-Sheng, CAI Jue-Song (551)