

# 电子与信息学报

DIANZI YU XINXI XUEBAO

第 41 卷 第 8 期

2019 年 8 月

## 目 次

### 论 文

- 基于容错学习的属性基加密方案的具体安全性分析 ..... 赵 建, 高海英, 胡 斌 (1779)
- 一种可证安全的PKI和IBC双向匿名异构签密方案的改进 .....  
..... 曹素珍, 郎晓丽, 刘祥震, 张玉磊, 王彩芬 (1787)
- 基于 f-mOPE 的数据库密文检索方案 ..... 周艺华, 吉 文, 杨宇光 (1793)
- 基于 Lowe 分类法的 5G 网络 EAP-AKA' 协议安全性分析.....  
..... 刘彩霞, 胡鑫鑫, 刘树新, 游 伟, 赵 宇 (1800)
- 基于授权的多服务器可搜索密文策略属性基加密方案 .....  
..... 张玉磊, 刘文静, 刘祥震, 张永洁, 王彩芬 (1808)
- 一种匿名可撤销的比特币混淆方案 ..... 李雪莲, 王海玉, 高军涛, 李 伟 (1815)
- 无证书公钥密码体制→传统公钥基础设施异构环境下部分盲签密方案 .....  
..... 王彩芬, 许钦百, 刘 超, 成玉丹, 赵 冰 (1823)
- 破损压缩文件的修复还原 ..... 王 刚, 彭 华, 唐永旺 (1831)
- 基于属性攻击图的网络动态威胁分析技术研究.....  
..... 杨英杰, 冷 强, 常德显, 潘瑞莹, 胡 浩 (1838)
- 基于正交混淆的多硬件 IP 核安全防护设计 .....  
..... 张跃军, 王佳伟, 潘 钊, 张晓伟, 汪鹏君 (1847)
- 大整数乘法器的 FPGA 设计与实现 ..... 谢 星, 黄新明, 孙 玲, 韩赛飞 (1855)
- 基于自适应随机线性网络编码的优先级调度方案 ..... 王 练, 张 贺, 张 昭, 张勋杨 (1861)
- 软件定义网络中面向时延和负载的多控制器放置策略 .....  
..... 史久根, 谢熠君, 孙 立, 郭 胜, 刘雅丽 (1869)
- 基于多目标优化的无线传感器网络移动充电及数据收集算法.....  
..... 吕增威, 魏振春, 韩江洪, 孙仁浩, 夏成凯 (1877)
- 软件定义时分波分复用无源光网络中基于带宽预测的资源分配策略 .....  
..... 熊 余, 杨娅娅, 张振振, 蒋 婧 (1885)
- 一种支持硬件加速的虚拟网络功能部署模型 ..... 胡宇翔, 范宏伟, 兰巨龙, 段 通 (1893)
- 两用户非正交多址接入的最优时延均衡和功率控制方法..... 黄 盛 (1902)
- 基于非正交多址接入中继通信系统的功率优化 ..... 黄容兰, 刘 云, 李啟尚, 唐 文 (1909)
- 基于 Hilbert 信号空间的未知干扰自适应识别方法 .....  
..... 黄国策, 王桂胜, 任清华, 董淑福, 高维廷, 魏 帅 (1916)
- 基于 Toeplitz 协方差矩阵重构的互质阵列 DOA 估计方法.....  
..... 孙 兵, 阮怀林, 吴晨曦, 钟 华 (1924)
- 基于对数行列式散度与对称对数行列式散度的高频地波雷达目标检测器.....  
..... 叶 磊, 王 勇, 杨 强, 邓维波 (1931)

一种 W 波段无人机微型 SAR 系统 .....	丁满来, 丁赤飏, 唐 跃, 王雪梅, 温智磊, 曲佳萌	(1939)
S 波段高分辨宽幅 SAR 辐射定标及误差分析方法 .....	刘亚波, 刘 霖, 童智勇, 喻忠军	(1946)
空间目标的短时三维几何重构方法 .....		
.....	徐 丹, 符吉祥, 孙光才, 邢孟道, 苏 涛, 保 铮	(1952)
探月卫星同波束干涉测量技术应用研究 .....	韩松涛, 陈 明, 李翠兰, 路伟涛	(1960)
矢量 GNSS 接收机自主完好性监控性能研究 .....	邹晓军, 廉保旺	(1966)
基于双层多参数加权类分数阶傅里叶变换的双极化卫星安全传输方案.....		
.....	达新宇, 王浩波, 罗章凯, 胡 航, 倪 磊, 潘 钰	(1974)
基于样本质量估计的空间正则化自适应相关滤波视觉跟踪.....		
.....	侯志强, 王 帅, 廖秀峰, 余旺盛, 王姣尧, 陈传华	(1983)
基于改进深度卷积神经网络的纸币识别研究 .....	盖 杉, 鲍中运	(1992)
一种基于树增强朴素贝叶斯的分类器学习方法 .....	陈 曦, 张 坤	(2001)
一种基于邻接表的极大频繁项集挖掘算法 .....	殷 茗, 王文杰, 张焯宇, 姜继娇	(2009)
基于改进的自适应差分演化算法的二维 Otsu 多阈值图像分割 .....	罗 钧, 杨永松, 侍宝玉	(2017)
基于非局部低秩和加权全变分的图像压缩感知重构算法 .....		
.....	赵 辉, 张 静, 张 乐, 刘莹莉, 张天骐	(2025)

# JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

Vol.41 No.8 Aug. 2019

## CONTENTS

### Papers

- Analysis Method for Concrete Security of Attribute-based Encryption Based on Learning With Errors ..... ZHAO Jian, GAO Haiying, HU Bin (1779)
- Improvement of a Provably Secure Mutual and Anonymous Heterogeneous Signcryption Scheme Between PKI and IBC ..... CAO Suzhen, LANG Xiaoli, LIU Xiangzhen, ZHANG Yulei, WANG Caifen (1787)
- Database Ciphertext Retrieval Scheme Based On f-mOPE ..... ZHOU Yihua, JI Wen, YANG Yuguang (1793)
- Security Analysis of 5G Network EAP-AKA' Protocol Based on Lowe's Taxonomy ..... LIU Caixia, HU Xinxin, LIU Shuxin, YOU Wei, ZHAO Yu (1800)
- Searchable Multi-server CP-ABE Scheme Based on Authorization ..... ZHANG Yulei, LIU Wenjing, LIU Xiangzhen, ZHANG Yongjie, WANG Caifen (1808)
- Anonymous Revocation Scheme for Bitcoin Confusion. .... LI Xuelian, WANG Haiyu, GAO Juntao, LI Wei (1815)
- Partial Blind Signcryption Scheme in CLPKC-to-TPKI Heterogeneous Environment. .... WANG Caifen, XU Qinbai, LIU Chao, CHENG Yudan, ZHAO Bing (1823)
- Repair and Restoration of Corrupted Compressed Files ..... WANG Gang, PENG Hua, TANG Yongwang (1831)
- Research on Network Dynamic Threat Analysis Technology Based on Attribute Attack Graph ..... YANG Yingjie, LENG Qiang, CHANG Dexian, PAN Ruixuan, HU Hao (1838)
- Hardware Security for Multi IPs Protection Based on Orthogonal Obfuscation. .... ZHANG Yuejun, WANG Jiawei, PAN Zhao, ZHANG Xiaowei, WANG Pengjun (1847)
- FPGA Design and Implementation of Large Integer Multiplier ..... XIE Xing, HUANG Xinming, SUN Ling, HAN Saifei (1855)
- A Priority Scheduling Scheme Based on Adaptive Random Linear Network Coding. .... WANG Lian, ZHANG He, ZHANG Zhao, ZHANG Xunyang (1861)
- Multi-controller Placement Strategy Based on Latency and Load in Software Defined Network. .... SHI Jiugen, XIE Yijun, SUN Li, GUO Sheng, LIU Yali (1869)
- A Mobile Charging and Data Collecting Algorithm Based on Multi-objective Optimization. .... LÜ Zengwei, WEI Zhenchun, HAN Jianghong, SUN Renhao, XIA Chengkai (1877)
- Resource Allocation Based on Bandwidth Prediction in Software-defined Time and Wavelength Division Multiplexed Passive Optical Network. .... XIONG Yu, YANG Yaya, ZHANG Zhenzhen, JIANG Jing (1885)
- A Model for Virtualized Network Function Placement with Hardware Acceleration Support. .... HU Yuxiang, FAN Hongwei, LAN Julong, DUAN Tong (1893)
- Optimal Delay Equilibrium and Power Control Method for Two-user Non-orthogonal Multiple Access ..... HUANG Sheng (1902)
- Power Allocation Optimization of Cooperative Relaying Systems Using Non-orthogonal Multiple Access ..... HUANG Ronglan, LIU Yun, LI Qishang, TANG Wen (1909)
- Adaptive Recognition Method for Unknown Interference Based on Hilbert Signal Space. .... HUANG Guoce, WANG Guisheng, REN Qinghua, DONG Shufu, GAO Weiting, WEI Shuai (1916)
- Direction of Arrival Estimation with Coprime Array Based on Toeplitz Covariance Matrix Reconstruction. .... SUN Bing, RUAN Huailin, WU Chenxi, ZHONG Hua (1924)

(To be continued on inside back cover)

(Continued)

- High Frequency Surface Wave Radar Detector Based on Log-determinant Divergence and Symmetrized  
Log-determinant Divergence ..... *YE Lei, WANG Yong, YANG Qiang, DENG Weibo* (1931)
- A W Band Mini-SAR System for Unmanned Aerial Vehicle .....  
..... *DING Manlai, DING Chibiao, TANG Li, WANG Xuemei, WEN Zhilei, QU Jiameng* (1939)
- A Radiometric Calibration and Error Analysis Method for HWRS SAR in S-band.....  
..... *LIU Yabo, LIU Lin, TONG Zhiyong, YU Zhongjun* (1946)
- A Short Time 3D Geometry Reconstruction Method of Space Targets .....  
..... *XU Dan, FU Jixiang, SUN Guangcai, XING Mengdao, SU Tao, BAO Zheng* (1952)
- Research on Application of Same-beam Interferometry in China Lunar Exploration .....  
..... *HAN Songtao, CHEN Ming, LI Cuilan, LU Weitao* (1960)
- Research on Autonomous Integrity Monitoring Performance of Vector GNSS Receiver .....  
..... *ZOU Xiaojun, LIAN Baowango* (1966)
- Dual-polarization Satellite Security Transmission Scheme Based on Double Layer Multi-Parameter Weighted-type  
FRactional Fourier Transform ..... *DA Xinyu, WANG Haobo, LUO Zhangkai, HU Hang, NI Lei, PAN Yu* (1974)
- Adaptive Regularized Correlation Filters for Visual Tracking Based on Sample Quality Estimation .....  
..... *HOU Zhiqiang, WANG Shuai, LIAO Xiufeng, YU Wangsheng, WANG Jiaoyao, CHEN Chuanhua* (1983)
- Banknote Recognition Research Based on Improved Deep Convolutional Neural Network .....  
..... *GAI Shan, BAO Zhongyun* (1992)
- A Classifier Learning Method Based on Tree-Augmented Naïve Bayes..... *CHEN Xi, ZHANG Kun* (2001)
- A Maximal Frequent Itemsets Mining Algorithm Based on Adjacency Table.....  
..... *YIN Ming, WANG Wenjie, ZHANG Xuanyu, JIANG Jijiao* (2009)
- Multi-threshold Image Segmentation of 2D Otsu Based on Improved Adaptive Differential Evolution Algorithm .....  
..... *LUO Jun, YANG Yongsong, SHI Baoyu* (2017)
- Compressed Sensing Image Restoration Based on Non-local Low Rank and Weighted Total Variation .....  
..... *ZHAO Hui, ZHANG Jing, ZHANG Le, LIU Yingli, ZHANG Tianqi* (2025)