

电子与信息学报

DIANZI YU XINXI XUEBAO

第 42 卷 第 2 期

2020 年 2 月

目 次

抗量子攻击密码技术专题	专题主编:冯登国院士
后量子对称密码的研究现状与发展趋势	睦 晗, 吴文玲 (287)
改进的Type-1型广义Feistel结构的量子攻击及其在分组密码CAST-256上的应用	倪博煜, 董晓阳 (295)
基于相干态光场的连续变量测量设备无关Cluster态量子通信	王 宇, 苏 琦 (307)
格上本地验证者撤销属性基群签名的零知识证明.....	张彦华, 胡子濮, 刘西蒙, 张启坤, 贾惠文 (315)
基于列表译码方法在查询访问模型下含错学习问题的分析	王明强, 庄金成 (322)
关于非对称含错学习问题的困难性研究	张 江, 范淑琴 (327)
FatSeal: 一种基于格的高效签名算法	谢天元, 李昊宇, 朱熠铭, 潘彦斌, 刘 珍, 杨照民 (333)
基于量子不经意密钥传输的量子匿名认证密钥交换协议	魏春艳, 蔡晓秋, 王天银, 苏 琦, 秦素娟, 高 飞, 温巧燕 (341)
论 文	
一种适用于工业控制系统的加密传输方案	屠袁飞, 苏清健, 杨 庚 (348)
基于随机位置选择和矩阵编码的语音信息隐藏方法	吴志军, 李常亮, 李 荣 (355)
一种新的图像超像素分割方法	廖 苗, 李 阳, 赵于前, 刘毅志 (364)
基于深度卷积神经网络的多元医学信号多级上下文自编码器	袁 野, 贾克斌, 刘鹏宇 (371)
基于多模态生成对抗网络和三元组损失的说话人识别	陈 莹, 陈湟康 (379)
用于表示级特征融合与分类的相关熵融合极限学习机	吴 超, 李雅倩, 张亚茹, 刘 彬 (386)
基于双向参考集矩阵度量学习的行人再识别	陈 莹, 许潇月 (394)
基于张量分解的卫星遥测缺失数据预测算法	马 友, 贾树泽, 赵现纲, 冯小虎, 范存群, 朱爱军 (403)
一种全数字前馈式时间交织模数转换器时间误差后台校准算法	邓红辉, 闫 辉, 肖 瑞, 陈红梅 (410)
一种基于天牛须算法的新型超宽带功分器研究.....	李 杰, 阎跃鹏, 梁晓新, 万 晶, 王魁松 (418)
一种新型的高阶时域有限差分方法	许 杰, 徐 珂, 黄志祥 (425)
基于集成固有尺度分解的 IFF 辐射源个体识别算法	张 玉, 李天琪, 张 进, 唐 波 (430)
自适应时频同步压缩算法研究	李 林, 王 林, 韩红霞, 姬红兵, 江 莉 (438)
一种适用于小样本的迭代多重信号分类算法	王 娟, 王 彤, 吴建新 (445)
雷达间歇辐射对测向交叉定位性能的影响分析	王亚涛, 曾小东, 周龙建 (452)
基于高超声速平台前斜视多通道 SAR-GMTI 杂波抑制方法	王 宇, 曹运合, 齐 晨, 韩玖胜, 刘玉涛 (458)
基于价值优化的相控阵雷达任务调度算法	杨善超, 田康生, 刘仁争, 郑玉军 (465)
一种基于短合成孔径的双星干涉精确定位方法	孙光才, 王裕旗, 高昭昭, 江 帆, 邢孟道, 保 铮 (472)
异构网络中基于能效优化的 D2D 资源分配机制	张达敏, 张绘娟, 闫 威, 陈忠云, 辛梓芸 (480)

Chernoff 加权分类器框架在运动想象脑-机接口中的应用.....	谭平, 刘利枚, 郭璠, 周开军	(488)
超密集组网下一种基于干扰增量降低的分簇算法	梁彦霞, 姜静, 孙长印, 刘欣, 谢永斌	(495)
一种新的基于虚拟队列的无线多播网络编码调度策略	张瑞, 占友, 钱权	(503)
基于 SideLink 的 LTE-V2X 联合切换方案设计.....	申滨, 周晓勇, 徐浪, 黄晓舸	(511)
大规模 MIMO 系统上行链路时间-空间结构信道估计算法	路新华, MANCHÓN Carles Navarro, 王忠勇, 张传宗	(519)
基于能效的 NOMA 蜂窝车联网动态资源分配算法	唐伦, 肖娇, 赵国繁, 杨友超, 陈前斌	(526)
基于快速贝叶斯匹配追踪优化的海上稀疏信道估计方法	张颖, 姚雨丰	(534)

JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

Vol.42 No.2 Feb. 2020

CONTENTS

Special Topic on Cryptography against Quantum Attack <i>Leading Editor: FENG Dengguo</i>	
Research Status and Development Trend of Post-quantum Symmetric Cryptography	
..... SUI Han, WU Wenling	(287)
Improved Quantum Attack on Type-1 Generalized Feistel Schemes and Its Application to CAST-256	
..... NI Boyu, DONG Xiaoyang	(295)
Continuous Variable Measurement-Device-Independent Cluster State Quantum Communication Based on Coherent State	
..... WANG Yu, SU Qi	(307)
Zero-knowledge Proofs for Attribute-Based Group Signatures with Verifier-local Revocation Over Lattices	
..... ZHANG Yanhua, HU Yupu, LIU Ximeng, ZHANG Qikun, JIA Huiwen	(315)
Analysis of Learning With Errors in Query Access Model: A List Decoding Approach	
..... WANG Mingqiang, ZHUANG Jincheng	(322)
On the Hardness of the Asymmetric Learning With Errors Problem	
..... ZHANG Jiang, FAN Shuqin	(327)
FatSeal: An Efficient Lattice-based Signature Algorithm	
..... XIE Tianyuan, LI Haoyu, ZHU Yiming, PAN Yanbin, LIU Zhen, YANG Zhaomin	(333)
Quantum Anonymous Authenticated Key Exchange Protocol Based on Quantum Oblivious Key Transfer	
..... WEI Chunyan, CAI Xiaoqiu, WANG Tianyin, SU Qi, QIN Sujuan, GAO Fei, WEN Qiaoyan	(341)
Papers	
An Encryption Transmission Scheme for Industrial Control System	
..... TU Yuanfei, SU Qingjian, YANG Geng	(348)
Speech Information Hiding Method Based on Random Position Selection and Matrix Coding	
..... WU Zhijun, LI Changliang, LI Rong	(355)
A New Method for Image Superpixel Segmentation	
..... LIAO Miao, LI Yang, ZHAO Yuqian, LIU Yizhi	(364)
Multi-context Autoencoders for Multivariate Medical Signals Based on Deep Convolutional Neural Networks	
..... YUAN Ye, JIA Kebin, LIU Pengyu	(371)
Speaker Recognition Based on Multimodal Generative Adversarial Nets with Triplet-loss	
..... CHEN Ying, CHEN Huanggang	(379)
Correntropy-based Fusion Extreme Learning Machine for Representation Level Feature Fusion and Classification	
..... WU Chao, LI Yaqian, ZHANG Yaru, LIU Bin	(386)
Matrix Metric Learning for Person Re-identification Based on Bidirectional Reference Set	
..... CHEN Ying, XU Xiaoyue	(394)
Missing Telemetry Data Prediction Algorithm via Tensor Factorization	
..... MA You, JIA Shuze, ZHAO Xiangang, FENG Xiaohu, FAN Cunqun, ZHU Aijun	(403)
Fully Digital Feedforward Background Calibration of Time Skew for Sub-Sampling Time-interleaved Analog-to-digital Converter	
..... DENG Honghui, YAN Hui, XIAO Rui, CHEN Hongmei	(410)
Research on the Novel Ultra-wideband Power Divider Based on Beetle Antennae Search Algorithm	
..... LI Jie, YAN Yuepeng, LIANG Xiaoxin, WAN Jing, WANG Kuisong	(418)
A New High Order Finite Difference Time Domain Method	
..... XU Jie, XU Ke, HUANG Zhixiang	(425)
Individual Recognition Algorithm of IFF Radiation Sources Based on Ensemble Intrinsic Time-scale Decomposition	
..... ZHANG Yu, LI Tianqi, ZHANG Jin, TANG Bo	(430)
Research on the Adaptive Synchrosqueezing Algorithm	
..... LI Lin, WANG Lin, HAN Hongxia, JI Hongbing, JIANG Li	(438)
Iterative Multiple Signal Classification Algorithm with Small Sample Size	
..... WANG Juan, WANG Tong, WU Jianxin	(445)

(To be continued on inside back cover)

(Continued)

Analysis for Effect of Radar Intermittent Radiation on the Performance of Cross Location	(452)
..... WANG Yatao, ZENG Xiaodong, ZHOU Longjian	
Multi-channel SAR-GMTI Clutter Suppression Method Based on Hypersonic Platform Forward Squint	(458)
..... WANG Yu, CAO Yunhe, QI Chen, HAN Jiusheng, LIU Yutao	
Scheduling Algorithm Based on Value Optimization for Phased Array Radar	(465)
..... YANG Shanchao, TIAN Kangsheng, LIU Renzheng, ZHENG Yujun	
A Dual Satellite Interferometric Precise Localization Method Based on Short Synthetic Aperture	(472)
..... SUN Guangcai, WANG Yuqi, GAO Zhaozhao, JIANG Fan, XING Mengdao, BAO Zheng	
D2D Resource Allocation Mechanism Based on Energy Efficiency Optimization in Heterogeneous Networks	(480)
..... ZHANG Damin, ZHANG Huijuan, YAN Wei, CHEN Zhongyun, XIN Ziyun	
Applying Chernoff Weighted Classification Frame Method to Motor Imagery Brain Computer Interface	(488)
..... TAN Ping, LIU Limei, GUO Fan, ZHOU Kaijun	
A Cluster Algorithm Based on Interference Increment Reduction in Ultra-Dense Network	(495)
..... LIANG Yanxia, JIANG Jing, SUN Changyin, LIU Xin, XIE Yongbin	
New Coding Scheduling Strategy Based on Virtual Queue in Wireless Multicast Network	(503)
..... ZHANG Rui, ZHAN You, QIAN Quan	
A SideLink-assisted Joint Handover Scheme for Long Term Evolution -Vehicle to Everything System	(511)
..... SHEN Bin, ZHOU Xiaoyong, XU Lang, HUANG Xiaoge	
Channel Estimation Algorithm Using Temporal-spatial Structure for Up-link of Massive MIMO Systems	(519)
..... LU Xinhua, MANCHÓN Carles Navarro, WANG Zhongyong, ZHANG Chuanzong	
Energy Efficiency Based Dynamic Resource Allocation Algorithm for Cellular Vehicular Based on Non-Orthogonal Multiple Access	(526)
..... TANG Lun, XIAO Jiao, ZHAO Guofan, YANG Youchao, CHEN Qianbin	
Channel Estimation Algorithm of Maritime Sparse Channel Based on Fast Bayesian Matching Pursuit Optimization	(534)
..... ZHANG Ying, YAO Yufeng	