

# 电子与信息学报

DIANZI YU XINXI XUEBAO

第 45 卷 第 3 期

2023 年 3 月

## 目 次

### “隐私数据安全共享与处理”专题

- ( $\epsilon, \delta$ )-本地差分隐私模型下的均值估计机制 ..... 张 跃, 朱友文, 周玉倩, 袁家斌 (765)
- 基于混合隐私的区块链高效模型协同训练共享方案 .....  
..... 张 翠, 杨 辉, 王寒凝, 王 江, 曾创展, 李荣宽 (775)
- 基于联邦学习的本地化差分隐私机制研究 .....  
..... 任一支, 刘容轲, 王 冬, 袁理锋, 申延召, 吴国华, 王秋华, 杨昌天 (784)
- 对八阵图算法的不可能差分密码分析和线性密码分析 ..... 卫宏儒, 朱一凡 (793)
- 支持预览的版权图像共享 ..... 肖祥立, 叶 茜, 张玉书, 温文斌, 张新鹏 (800)
- 具有隐私保护的细粒度智能家居远程数据安全更新方案 .....  
..... 张应辉, 陈博文, 曹 进, 郭 瑞, 郑 东 (810)
- 基于雾计算的智能电表用户虚拟环隐私保护方案 ..... 夏卓群, 张一超, 谷 科, 周楷鑫, 李 雄 (819)
- 基于内积谓词的属性基隐私保护加密方案 ..... 张志强, 朱友文, 王 箭, 张玉书 (828)
- 基于新型公平盲签名和属性基加密的食用农产品溯源方案 ..... 张学旺, 林金朝, 黎志鸿, 姚亚宁 (836)
- 移动社交网络中基于属性加密的隐私保护方案 ..... 牛淑芬, 戈 鹏, 宋 蜜, 宿 云 (847)
- 云计算与区块链平台的遥感影像安全检索方案 .....  
..... 欧阳雪, 徐彦彦, 毛养素, 刘运祺, 王志恒, 闫悦菁 (856)
- 基于联盟链的身份环签密方案 ..... 俞惠芳, 吕芝蕊 (865)
- 一种基于合同理论的可激励联邦学习模型 ..... 王 鑫, 李美庆, 王黎明, 余 芸, 杨 漾, 孙凌云 (874)
- 医疗社交网络中基于云计算的属性基签密方案 .....  
..... 牛淑芬, 周思玮, 吕锐曦, 闫 森, 张美玲, 王彩芬 (884)
- 基于相似度聚类的可信联邦安全聚合算法 ..... 蔡红云, 张 宇, 王诗云, 赵 傲, 张美玲 (894)
- ### 密码学与信息安全
- 基于云模型的基本概率赋值生成方法及应用 .....  
..... 国 强, 文伟璐, 王亚妮, 戚连刚, Kaliuzhny Mykola (905)
- II型Z-优化二元互补序列对的构造 ..... 林金朝, 周银萍, 李国军, 叶昌荣, 曾凡鑫 (913)
- 基于多项式基的Camellia算法S盒硬件优化 ..... 李艳俊, 张伟国, 葛耀东, 王 克 (921)
- 电磁驱动下一类混合神经元模型的动力学响应与图像加密应用 ..... 安新磊, 熊 丽, 乔 帅 (929)
- ### 图像与智能信息处理
- 基于改进模糊置信规则的意图识别方法 ..... 王海滨, 关 欣, 衣 晓, 李双明 (941)
- 基于知识图谱的城市轨道交通突发事件演化结果预测 ..... 朱广宇, 张 萌, 裔 扬 (949)
- 优化参考图谱发育指征的CHN智能骨龄评估方法研究 .....  
..... 毛科技, 武坤秀, 陆 伟, 陈立建, 毛家发 (958)
- ### 雷达、水声、导航与阵列信号处理
- 基于概率假设密度滤波和动力学方程约束的空间群目标数量和位置分辨 .....  
..... 修建娟, 董 凯, 徐从安 (968)

低信噪比下离散频率编码波形脉冲信号联合积累检测算法 .....	魏 嵩, 张 磊, 马 岩, 钟卫军	(977)
基于空间与光谱注意力的光学图像和SAR图像特征融合分类方法 .....	姜 文, 潘 洁, 朱金彪, 岳昔娟	(987)
针对eLORAN系统窄带干扰的权函数陷波算法 .....	刘时尧, 华 宇, 张首刚	(996)
基于变分贝叶斯双尺度自适应时变噪声容积卡尔曼滤波的同步定位与建图算法 .....	李帅永, 谢现乐, 毛文平, 杨雪梅, 聂嘉炜	(1006)
基于改进盖尔-沙普利算法的自动识别系统与双频地波雷达断裂航迹关联 .....	张 晖, 曾显普, 高 亮	(1015)
<b>无线通信与物联网</b>		
一种适用于战术通信环境的车对车信道模型 .....	林 鑫, 刘爱军, 梁小虎, 韩 晨	(1023)
扩容型正交抑噪多级差分混沌移位键控通信系统 .....	张 刚, 王 磊, 蒋忠均	(1032)
一种融合噪声网络的深度强化学习通信干扰资源分配算法 .....	彭 翔, 许 华, 蒋 磊, 饶 宁, 宋佰霖	(1043)
基于加权二部图及贪婪策略的蜂窝网络D2D通信资源分配 .....	申 滨, 孙万平, 张 楠, 崔太平	(1055)
基于信息年龄的工业无线传感器网络混合数据调度方法 .....	王 恒, 余 蕾, 谢 鑫	(1065)
基于集成深度神经网络流量预测的动态网络切片迁移算法 .....	唐 伦, 周鑫隆, 吴 婷, 王 恺, 陈前斌	(1074)
捕获效应对LTE授权辅助接入网络的影响 .....	裴二荣, 陈新虎, 张 泰, 邓炳光, 孙远欣	(1083)
车载边缘计算中多任务部分卸载方案研究 .....	王 练, 闫润搏, 徐 静	(1094)
小样本图像处理方法赋能的宽带频谱感知 .....	周 金, 李玉芝, 李 斌	(1102)
<b>电路与系统设计</b>		
基于VMD和DAIPSO-GPR解决容量再生现象的锂离子电池寿命预测研究 .....	刘金凤, 陈浩玮, HERBERTHo-Ching Iu	(1111)
<b>综述评论</b>		
水下无线传感器网络安全研究综述 .....	苏毅珊, 张贺贺, 张 瑞, 马素雅, 范 榕, 付晓梅, 金志刚	(1121)
云环境下对称可搜索加密研究综述 .....	黄一才, 李森森, 郁 滨	(1134)

# JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

Vol.45 No.3 March 2023

## CONTENTS

### Special Topic on Secure Sharing and Processing of Private Data

Mean Estimation Mechanisms under $(\epsilon, \delta)$ -Local Differential Privacy .....	ZHANG Yue, ZHU Youwen, ZHOU Yuqian, YUAN Jiabin	(765)
Efficient Model Collaborative Training and Sharing Scheme of Blockchain Based on Hybrid Privacy .....	ZHANG Cui, YANG Hui, WANG Hanning, WANG Jiang, ZENG Chuangzhan, LI Rongkuan	(775)
A Study of Local Differential Privacy Mechanisms Based on Federated Learning .....	REN Yizhi, LIU Rongke, WANG Dong, YUAN Lifeng, SHEN Yanzhao, WU Guohua, WANG Qihua, YANG Changtian	(784)
Impossible Differential Cryptanalysis and Linear Cryptanalysis for Eight-Sided Fortress Algorithm .....	WEI Hongru, ZHU Yifan	(793)
Preview-supported Copyright Image Sharing .....	XIAO Xiangli, YE Xi, ZHANG Yushu, WEN Wenying, ZHANG Xinpeng	(800)
Fine-grained Remote Data Security Update Scheme for Smart Home with Privacy Protection .....	ZHANG Yinghui, CHEN Bowen, CAO Jin, GUO Rui, ZHENG Dong	(810)
Virtual Ring Privacy Preserving Scheme Based on Fog Computing for Smart Meter System .....	XIA Zhuoqun, ZHANG Yichao, GU Ke, ZHOU Kaixin, LI Xiong	(819)
Attribute Based Privacy Protection Encryption Scheme Based on Inner Product Predicate .....	ZHANG Zhiqiang, ZHU Youwen, WANG Jian, ZHANG Yushu	(828)
Traceability Scheme of Edible Agricultural Products Based on Novel Fair Blind Signature and Attribute-based Encryption .....	ZHANG Xuewang, LIN Jinzhao, LI Zhihong, YAO Yaning	(836)
A Privacy Protection Scheme Based on Attribute Encryption in Mobile Social Networks .....	NIU Shufen, GE Peng, SONG Mi, SU Yun	(847)
Secure Remote Sensing Image Retrieval Scheme Based on Cloud Computing and Blockchain Platforms .....	OUYANG Xue, XU Yanyan, MAO Yangsu, LIU Yunqi, WANG Zhiheng, YAN Yuejing	(856)
Identity Ring SignCryption Based on Consortium Blockchain .....	YU Huifang, LÜ Zhirui	(865)
An Incentivized Federated Learning Model Based on Contract Theory .....	WANG Xin, LI Meiqing, WANG Liming, YU Yun, YANG Yang, SUN Lingyun	(874)
Attribute-Base Signcryption Scheme Based on Cloud Computing in Mobile Medical Social Network .....	NIU Shufen, ZHOU Siwei, LU Ruixi, YAN Sen, ZHANG Meiling, WANG Caifen	(884)
Trusted Federated Secure Aggregation via Similarity Clustering .....	CAI Hongyun, ZHANG Yu, WANG Shiyun, ZHAO Ao, ZHANG Meiling	(894)
<b>Cryption and Information Security</b>		
Basic Probability Assignment Generation Method and Application Based on Cloud Model .....	GUO Qiang, WEN Weilu, WANG Yani, QI Liangang, Kaliuzhny Mykola	(905)
Construction of Type II Z-Optimal Binary Complementary Sequence Pairs .....	LIN Jinzhao, ZHOU Yinping, LI Guojun, YE Changrong, ZENG Fanxin	(913)
Hardware Optimization of S-box of Camellia Algorithm Based on Polynomial Basis .....	LI Yanjun, ZHANG Weiguo, GE Yaodong, WANG Ke	(921)
Dynamic Response of a Class of Hybrid Neuron Model by Electromagnetic Induction and Application of Image Encryption .....	AN Xinlei, XIONG Li, QIAO Shuai	(929)

(To be continued on inside back cover)

(Continued)

### **Image and Intelligent Information Processing**

- An Intention Recognition Method Based on Fuzzy Belief-Rule-Base ..... WANG Haibin, GUAN Xin, YI Xiao, LI Shuangming (941)
- Prediction of Evolution Results of Urban Rail Transit Emergencies Based on Knowledge Graph ..... ZHU Guangyu, ZHANG Meng, YI Yang (949)
- A Study of the CHN Intelligent Bone Age Assessment Method with Reference to Atlas Developmental Indications ..... MAO Keji, WU Kunxiu, LU Wei, CHEN Lijian, MAO Jiufa (958)

### **Radar, Sonar, Navigation and Array Signal Processing**

- Number and Position Estimation Algorithm of Space Group Targets Based on Probability Hypothesis Density Filter and Dynamic Model ..... XIU Jianjuan, DONG Kai, XU Cong'an (968)
- Robust Joint Accumulation and Detection for Discrete Frequency Coded Waveform Signals at Low Signal-to-Noise Ratio ..... WEI Song, ZHANG Lei, MA Yan, ZHONG Weijun (977)
- Feature Fusion Classification for Optical Image and SAR Image Based on Spatial-spectral Attention ..... JIANG Wen, PAN Jie, ZHU Jinbiao, YUE Xijuan (987)
- Weight-Function Notch Filter Algorithm for Narrow-band Interference in eLORAN System ..... LIU Shiyao, HUA Yu, ZHANG Shougang (996)
- Simultaneous Localization And Mapping Based on Variational Bayses Double-Scale Adaptive time-varying noise Cubature Kalman Filter ..... LI Shuaiyong, XIE Xianle, MAO Wenping, YANG Xuemei, NIE Jiawei (1006)
- Track Segment Association of Automatic Identification System and Dual-frequency High-Frequency Surface Wave Radar Based on Improved Gale-Shapley Algorithm ..... ZHANG Hui, ZENG Xianpu, GAO Liang (1015)

### **Wireless Communication and Internet of Things**

- A Vehicle-to-Vehicle Channel Model for Tactical Communication Environments ..... LIN Xin, LIU Aijun, LIANG Xiaohu, HAN Chen (1023)
- Expanded Capacity Orthogonal Noise Suppression Multi-level Differential Chaotic Shift Keying Communication System ..... ZHANG Gang, WANG Lei, JIANG Zhongjun (1032)
- A Deep Reinforcement Learning Communication Jamming Resource Allocation Algorithm Fused with Noise Network ..... PENG Xiang, XU Hua, JIANG Lei, RAO Ning, SONG Bailin (1043)
- Resource Allocation Based on Weighted Bipartite Graph and Greedy Strategy for D2D Communication in Cellular Networks ..... SHEN Bin, SUN Wanping, ZHANG Nan, CUI Taiping (1055)
- Hybrid Data Scheduling Method for Industrial Wireless Sensor Networks Based on Age of Information ..... WANG Heng, YU Lei, XIE Xin (1065)
- Dynamic Network Slice Migration Algorithm Based on Ensemble Deep Neural Network Traffic Prediction ..... TANG Lun, ZHOU Xinlong, WU Ting, WANG Kai, CHEN Qianbin (1074)
- Impact of Capture Effect on LTE-Licensed Assisted Access Networks ..... PEI Errong, CHEN Xinhui, ZHANG Tai, DENG Bingguang, SUN Yuanxin (1083)
- Research on Multi-task Partial Offloading Scheme in Vehicular Edge Computing ..... WANG Lian, YAN Runbo, XU Jing (1094)
- Image Processing-Driven Spectrum Sensing with Small Training Samples ..... ZHOU Jin, LI Yuzhi, LI Bin (1102)

### **Circuit and System Design**

- Li-ion Batteries Life Prediction Based on Variational Modal Decomposition and DAIPSO-GPR to Solve the Capacity Regeneration Phenomenon ..... LIU Jinfeng, CHEN Haowei, HERBERT Ho-Ching Lu (1111)

### **Overviews**

- Review of Security for Underwater Wireless Sensor Networks ..... SU Yishan, ZHANG Hehe, ZHANG Rui, MA Suyu, FAN Rong, FU Xiaomei, JIN Zhigang (1121)
- A Survey of Symmetric Searchable Encryption in Cloud Environment ..... HUANG Yicai, LI Sensen, YU Bin (1134)