



2013 年全国百强科技期刊



2015 年全国百强科技期刊



中国精品科技期刊



中国计算机学会会刊

软件学报

(Ruanjian Xuebao)

第 36 卷第 10 期

2025 年 10 月

目次

抗量子密码与区块链应用专题

抗量子密码与区块链应用专题前言	翁 健 祝烈煌 赵运磊 (4403)
半均匀 LWE 问题的紧致归约	王 洋 王明强 (4405)
SM3-OTS: 基于国密算法 SM3 的紧凑型后量子一次签名方案	杨亚涛 殷方锐 陈亮宇 潘 登 (4417)
基于 Kyber 公钥加密的高效认证密钥交换协议	米瑞琪 江浩东 张振峰 (4430)
具有用户自主链接及验证者条件撤销的格基群签名	陈 颖 何德彪 彭 聪 罗 敏 (4444)
基于 FPGA 的格基数字签名算法硬件优化	胡 跃 赵旭阳 王 威 袁 谦 郑婕妤 杨亚芳 (4461)
抗量子的高效区块链认证存储方案	张 川 任旭豪 邓昊天 王亚杰 李春海 吴 桐 王励成 (4483)
基于多父链辅助工作量证明共识机制的后量子区块链系统	王御天 贾舒瑞 陈铭希 董怡帆 杨亚芳 (4507)

理论计算机科学

正则图上对称双态自旋系统相关的细密度二分定理	刘 莹 (4525)
------------------------------	------------

算法设计与分析

基于两种新标量表示的安全高效标量乘算法	程 石 胡 志 陶 铮 (4542)
---------------------------	--------------------

系统软件与软件工程

SZZ 误标变更对移动 APP 即时缺陷预测性能和解释的影响	李志强 马 睿 张洪宇 荆晓远 任 杰 刘金会 (4558)
基于抽象语法树变异的漏洞样本生成方法	郑 炜 李云帆 桂 奎 吴潇雪 陈 翔 邓沛然 (4590)

面向联盟链的智能合约行为可信验证机制 张建标 康 双 张兆乾 刘德田 (4612)

基于代码控制流图的庞氏骗局合约检测 黄 静 王梦晓 韩红桂 (4628)

干扰惰性序列的连续决策模型模糊测试 吴泊逾 王凯锐 王亚文 王俊杰 (4645)

模式识别与人工智能

面向二分类问题的直觉模糊深度随机配置网络 丁世飞 朱姜兰 张成龙 郭丽丽 张 健 (4660)

结合大语言模型和领域知识库的证券规则规约方法 李靓果 薛志一 陈小红 张 民 陈良育 李萍萍 姜婷婷 (4671)

扩散模型期望最大化的离线强化学习方法 刘 全 颜 洁 乌 兰 (4695)

中文对抗攻击下的 ChatGPT 鲁棒性评估 张云婷 叶 麟 李柏松 张宏莉 (4710)

面向集值数据的孪生支持函数机 梁志贞 闵玉寒 丁世飞 (4735)

针对 LLM 对话属性情感理解的多代理一致性反思 刘一丁 王晶晶 罗佳敏 周国栋 (4753)

BIVM: 类脑计算编译框架及其原型研究 杨 乐 刘晓义 李广力 渠 鹏 崔慧敏 张悠慧 (4768)

计算机网络与信息安全

基于双边拍卖的多基站移动边缘计算资源分配方法 汪建洲 付晓东 丁家满 李 杰 (4792)

基于视觉特征解耦的无数据依赖模型窃取攻击方法 张锦弘 刘仁阳 韦廷楚 董云云 周 维 (4812)

FBS-uBlock: 灵活的 uBlock 算法比特切片优化方法 龚子睿 郭 华 陈 晨 张宇轩 陈俊鑫 关振宇 (4827)

计算机图形学与计算机辅助设计

隐式多尺度对齐与交互的文本-图像行人重识别方法 孙 锐 杜 云 陈 龙 张旭东 (4846)

基于图像变换的双阈值对抗样本检测 刘 会 文福举 杜红琴 王敬华 赵 波 (4864)

计算机体系结构

用于二值神经网络的加宽和收缩机制 韩 凯 刘传建 吴恩华 (4880)

《软件学报》投稿指南 (封三)

Contents

SPECIAL TOPIC ON POST-QUANTUM CRYPTOGRAPHY AND BLOCKCHAIN APPLICATIONS

- 4403 Preface
WENG Jian, ZHU Lie-Huang, ZHAO Yun-Lei
- 4405 Tighter Reductions of LWE Problems with Semi-uniform Seeds
WANG Yang, WANG Ming-Qiang
- 4417 SM3-OTS: Compact Post Quantum One-time Signature Scheme Based on Chinese Cryptographic Algorithm SM3
YANG Ya-Tao, YIN Fang-Rui, CHEN Liang-Yu, PAN Deng
- 4430 Efficient Authenticated Key Exchange Protocol Based on Kyber Public-key Encryption
MI Rui-Qi, JIANG Hao-Dong, ZHANG Zhen-Feng
- 4444 Lattice-based Group Signatures with User-controlled Linkability and Verifier Conditional Revocation
CHEN Ying, HE De-Biao, PENG Cong, LUO Min
- 4461 Hardware Optimization of Lattice-based Digital Signature Algorithm Based on FPGA
HU Yue, ZHAO Xu-Yang, WANG Wei, YUAN Qian, ZHENG Jie-Yu, YANG Ya-Fang
- 4483 Quantum-resistant and Efficient Blockchain Authentication Storage Scheme
ZHANG Chuan, REN Xu-Hao, DENG Hao-Tian, WANG Ya-Jie, LI Chun-Hai, WU Tong, WANG Li-Cheng
- 4507 Post-quantum Blockchain System Based on Multi-parent Chain Auxiliary Proof-of-work Consensus Mechanism
WANG Yu-Tian, JIA Shu-Rui, CHEN Ming-Xi, DONG Yi-Fan, YANG Ya-Fang

THEORETICAL COMPUTER SCIENCE

- 4525 Fine-grained Dichotomies for Symmetric 2-spin System on Regular Graphs
LIU Ying

ALGORITHM DESIGN AND ANALYSIS

- 4542 Safe and Efficient Scalar Multiplication Algorithms Based on Two New Scalar Representations
CHENG Shi, HU Zhi, TAO Zheng

SYSTEM SOFTWARE AND SOFTWARE ENGINEERING

- 4558 Impact of Mislabeled Changes by SZZ on Performance and Interpretation of Just-in-time Defect Prediction for Mobile APP
LI Zhi-Qiang, MA Rui, ZHANG Hong-Yu, JING Xiao-Yuan, REN Jie, LIU Jin-Hui
- 4590 Vulnerability Sample Generation Method Based on Abstract Syntax Tree Variation
ZHENG Wei, LI Yun-Fan, GUI Kui, WU Xiao-Xue, CHEN Xiang, DENG Pei-Ran
- 4612 Trusted Verification Mechanism of Smart Contract Behaviour for Consortium Blockchain
ZHANG Jian-Biao, KANG Shuang, ZHANG Zhao-Qian, LIU De-Tian
- 4628 Ponzi Scheme Contract Detection Based on Code Control Flow Graph
HUANG Jing, WANG Meng-Xiao, HAN Hong-Gui
- 4645 Fuzz Testing for Sequential Decision-making Model with Intervening Inert Sequences
WU Bo-Yu, WANG Kai-Rui, WANG Ya-Wen, WANG Jun-Jie

PATTERN RECOGNITION AND ARTIFICIAL INTELLIGENCE

- 4660 Intuitionistic Fuzzy Deep Stochastic Configuration Network for Solving Binary Classification Problems
DING Shi-Fei, ZHU Jiang-Lan, ZHANG Cheng-Long, GUO Li-Li, ZHANG Jian
- 4671 Specification Method of Securities Rules Integrating Large Language Models and Domain Knowledge Base
LI Liang-Guo, XUE Zhi-Yi, CHEN Xiao-Hong, ZHANG Min, CHEN Liang-Yu, LI Ping-Ping, JIANG Ting-Ting
- 4695 Offline Reinforcement Learning Method with Diffusion Model and Expectation Maximization
LIU Quan, YAN Jie, WU Lan
- 4710 Robustness Evaluation of ChatGPT Against Chinese Adversarial Attacks
ZHANG Yun-Ting, YE Lin, LI Bai-Song, ZHANG Hong-Li
- 4735 Twin Support Function Machine for Set-valued Data
LIANG Zhi-Zhen, MIN Yu-Han, DING Shi-Fei
- 4753 Multi-agent Consistency Reflection for LLM-grounded Conversational Aspect Sentiment Understanding
LIU Yi-Ding, WANG Jing-Jing, LUO Jia-Min, ZHOU Guo-Dong
- 4768 BIVM: Compilation Framework for Brain-inspired Computing and Prototype Research
YANG Le, LIU Xiao-Yi, LI Guang-Li, QU Peng, CUI Hui-Min, ZHANG You-Hui

COMPUTER NETWORKS AND INFORMATION SECURITY

- 4792 Mobile Edge Computing Resource Allocation Algorithm Under Multi-base Station Based on Double Auction
WANG Jian-Zhou, FU Xiao-Dong, DING Jia-Man, LI Jie
- 4812 Data-free Model Stealing Attack Method Based on Visual Feature Decoupling
ZHANG Jin-Hong, LIU Ren-Yang, WEI Ting-Chu, DONG Yun-Yun, ZHOU Wei
- 4827 FBS-uBlock: Flexible Bit Slicing Optimization Method of uBlock Algorithm
GONG Zi-Rui, GUO Hua, CHEN Chen, ZHANG Yu-Xuan, CHEN Jun-Xin, GUAN Zhen-Yu

COMPUTER GRAPHICS AND COMPUTER AIDED DESIGN

- 4846 Implicit Multi-scale Alignment and Interaction for Text-image Person Re-identification Method
SUN Rui, DU Yun, CHEN Long, ZHANG Xu-Dong
- 4864 Dual-threshold Adversarial Example Detection Based on Image Transformation
LIU Hui, WEN Fu-Ju, DU Hong-Qin, WANG Jing-Hua, ZHAO Bo

COMPUTER ARCHITECTURE

- 4880 Widening and Squeezing Mechanism for Binary Neural Network
HAN Kai, LIU Chuan-Jian, WU En-Hua