



• ISSN 0254-4164

• CODEN JIXUDT

计算机学报

CHINESE JOURNAL OF COMPUTERS

第36卷 Vol.36

第6期 No.6



2013.6

• 中国计算机学会 中国科学院计算技术研究所 主办

• 科学出版社 出版

CHINESE JOURNAL OF COMPUTERS

Vol.36 No.6 June 2013

CONTENTS

Big Data

Network Big Data: Present and Future WANG Yuan-Zhuo et al. (1125)

Information Security

Biclique Analysis on the Reduced-Round PRESENT GONG Zheng et al. (1139)

Improved Public Key Encryption Scheme Secure Against Adaptive Chosen-Ciphertext Attacks
..... CHEN Min-Rong et al. (1149)

Key Pre-Distribution Scheme for Wireless Sensor Network against LU Attack
..... ZHONG Xiao-Rui et al. (1155)

Detection of QIM Steganography in Low Bit-Rate Speech Codec Based on Statistical Models and SVM
..... LI Song-Bin et al. (1168)

Cryptanalysis of Extended Multivariate Public Key Cryptosystem NIE Xu-Yun et al. (1177)

Research on Hamming Weight-Based Algebraic Side-Channel Attacks on SMS4
..... LIU Hui-Ying et al. (1183)

A Privacy and Integrity Preserving Range Query Protocol in Two-Tiered Sensor Networks
..... LI Rui et al. (1194)

An Approach for Resolving Inconsistency Conflicts in Access Control Policies
..... LI Rui-Xuan et al. (1210)

Computer Theory

A Quasi-physical Algorithm Based on Coarse and Fine Adjustment for Solving Circles Packing Problem
with Constraints of Equilibrium HE Kun et al. (1224)

Equivalent Characterizations of Fuzzy Büchi Automata HAN Zhao-Wei et al. (1235)

Constructing a Reliability Dominating Set of a New Family of Networks LI Feng et al. (1246)

C2E: An EPCCL Compiler with Good Performance LIU Da-You et al. (1254)

k-Choice Nets and Expressiveness of the Pi Calculus LI Xiang-Ning et al. (1261)

Computer Architecture

A Regression-Based Prediction Model for TPC-C Performance of High-End Fault-Tolerant Computers
..... LIU Di et al. (1267)

Data Parallelism Optimization for the CGRA Loop Pipelining Mapping YANG Zi-Yu et al. (1280)

S-RAID 5: An Energy-Saving RAID for Sequential Access Based Applications
..... LI Yuan-Zhang et al. (1290)

Software Engineering

Evaluating the Prediction Performance of Different Kernel Functions in Kernel Based Software
Reliability Models LOU Jun-Gang et al. (1303)

Behavioral Model Based Requirements Visualization Method LI Lin et al. (1312)

An Effective Error Recovery Method for GLR Parsers XU Fu et al. (1325)

《计算机学报》编辑委员会

The Editorial Board of Chinese Journal of Computers

主 编 Editor-in-Chief 孙凝晖 SUN Ning-Hui

副主编 Associate Editors-in-Chief

陈熙霖 CHEN Xi-Lin 冯登国 FENG Deng-Guo 金 芝 JIN Zhi
林 闯 LIN Chuang 周傲英 ZHOU Ao-Ying

委 员 Members

陈贵海 CHEN Gui-Hai	陈克非 CHEN Ke-Fei	程学旗 CHENG Xue-Qi	范玉顺 FAN Yu-Shun
方滨兴 FANG Bin-Xing	傅育熙 FU Yu-Xi	高 文 GAO Wen	韩燕波 HAN Yan-Bo
何新贵 HE Xin-Gui	胡事民 HU Shi-Min	华庆一 HUA Qing-Yi	怀进鹏 HUAI Jin-Peng
黄继武 HUANG Ji-Wu	蒋昌俊 JIANG Chang-Jun	蒋巍川 JIANG Yi-Chuan	焦李成 JIAO Li-Cheng
金 海 JIN Hai	李德毅 LI De-Yi	李 刚 LI Gang	李国杰 LI Guo-Jie
李建中 LI Jian-Zhong	李克秋 LI Ke-Qiu	李 未 LI Wei	李晓明 LI Xiao-Ming
李忠诚 LI Zhong-Cheng	林惠民 LIN Hui-Min	刘大有 LIU Da-You	刘云浩 LIU Yun-Hao
刘志勇 LIU Zhi-Yong	卢汉清 LU Han-Qing	卢锡城 LU Xi-Cheng	陆汝钤 LU Ru-Qian
吕 建 LU Jian	罗军舟 LUO Jun-Zhou	马建峰 MA Jian-Feng	梅 宏 MEI Hong
孟 丹 MENG Dan	孟祥旭 MENG Xiang-Xu	闵革勇 MIN Ge-Yong	闵应骅 MIN Ying-Hua
钮心忻 NIU Xin-Xin	欧阳丹彤 OUYANG Dan-Tong	潘启敬 PAN Qi-Jing	潘云鹤 PAN Yun-He
潘志庚 PAN Zhi-Geng	彭群生 PENG Qun-Sheng	钱德沛 QIAN De-Pei	瞿裕忠 QU Yu-Zhong
沈向洋 SHEN Xiang-Yang	沈绪榜 SHEN Xu-Bang	史忠植 SHI Zhong-Zhi	舒继武 SHU Ji-Wu
苏金树 SU Jin-Shu	孙钟秀 SUN Zhong-Xiu	谭铁牛 TAN Tie-Niu	唐志敏 TANG Zhi-Min
田 捷 TIAN Jie	王国胤 WANG Guo-Yin	王怀民 WANG Huai-Min	王 戟 WANG Ji
王 珏 WANG Jue	王 珊 WANG Shan	王兴伟 WANG Xing-Wei	吴建平 WU Jian-Ping
肖建国 XIAO Jian-Guo	许 进 XU Jin	杨学军 YANG Xue-Jun	杨义先 YANG Yi-Xian
于 戈 YU Ge	于 剑 YU Jian	查红彬 ZHA Hong-Bin	张 钹 ZHANG Bo
张长水 ZHANG Chang-Shui	张大鹏 ZHANG Da-Peng	张 健 ZHANG Jian	张尧学 ZHANG Yao-Xue
赵沁平 ZHAO Qin-Ping	周立柱 ZHOU Li-Zhu	周兴社 ZHOU Xing-She	朱传琪 ZHU Chuan-Qi
祝跃飞 ZHU Yue-Fei			

计算机学报
(月刊, 1978年创刊)

第 36 卷 第 6 期 总第 366 期 2013 年 6 月

Chinese Journal of Computers
(Monthly, Started in 1978)

Vol. 36 No. 6 Series No. 366 June 2013

主 管 中国科学院
主 办 中国计算机学会
 中国科学院计算技术研究所
编 辑 《计算机学报》编辑委员会
 中国科学院计算技术研究所
 邮政编码 100190, 北京 2704 信箱
 E-mail: cjc@ict.ac.cn
 http://cjc.ict.ac.cn

主 编 孙凝晖
出 版 科 学 出 版 社
印 刷 装 订 北京中科印刷有限公司
总 发 行 处 科 学 出 版 社
 北京东黄城根北街 16 号
 邮政编码 100717

国外总发行 中国国际图书贸易总公司
 (中国 国际书店)
 北 京 399 信 箱

Supervised by Chinese Academy of Sciences
Sponsored by China Computer Federation,
Institute of Computing Technology, CAS
Edited by Editorial Board of Chinese
Journal of Computers
P. O. Box 2704, Beijing 100190, China

Editor-in-Chief: SUN Ning-Hui
Published by Science Press
Printed by Beijing Zhongke Printing Limited Company
Distributed by Science Press
16 Donghuangchenggen North Street, Beijing
100717, China
Foreign: Guoji Shudian
P. O. Box 399, Beijing 100044, China

国内统一连续出版物号: CN 11-1826/TP

订 购 处: 全国各邮电局

定 价: 56.00 元

国内邮发代号: 2-833

国外发行代号: M 206

国内 外 公 开 发 行

ISSN 0254-4164



计 算 机 学 报

(JISUANJI XUEBAO)

第 36 卷 第 6 期 2013 年 6 月

目 次

大数据

网络大数据:现状与展望 王元卓 靳小龙 程学旗 (1125)

信息安全

缩减轮数 PRESENT 算法的 Biclique 分析 龚 征 刘树生 温雅敏 唐韶华 (1139)

改进的选择密文安全公钥加密方案 陈泯融 张 席 何 凯 关超文 刘 丹 (1149)

一种抗 LU 攻击的传感器网络密钥预分配方案 钟晓睿 马春光 (1155)

基于统计模型及SVM的低速率语音编码QIM隐写检测 李松斌 黄永峰 卢记仓 (1168)

多变量公钥密码扩展方案的安全性分析 聂旭云 徐赵虎 廖永建 钟 婷 (1177)

基于汉明重的 SMS4 密码代数旁路攻击研究

..... 刘会英 赵新杰 王 韬 郭世泽 张 帆 冀可可 (1183)

两层传感器网络中隐私与完整性保护的 范围查询协议 李 睿 林亚平 易叶青 胡玉鹏 (1194)

一种访问控制策略非一致性冲突消解方法 李瑞轩 鲁剑锋 李添翼 辜希武 唐 卓 (1210)

计算机理论

基于粗精调技术的求解带平衡约束圆形 Packing 问题的拟物算法

..... 何 琨 莫旦增 许如初 黄文奇 (1224)

模糊 Büchi 自动机的等价刻画 韩召伟 李永明 (1235)

构建一类新网络簇的可靠性控制集 李 峰 赵海兴 徐宗本 (1246)

C2E:一个高性能的 EPCCL 编译器 刘大有 赖 永 林 海 (1254)

k -选择网和 Π 演算的表达能 力 李向宁 郝克刚 郭小群 (1261)

计算机体系结构

基于回归模型的高端容错计算机 TPC-C 性能估算研究 刘 迪 翟季冬 陈文光 (1267)

面向 CGRA 循环流水映射的数据并行优化 杨子煜 严 明 王大伟 李思昆 (1280)

S-RAID 5:一种适用于顺序数据访问的节能磁盘阵列

..... 李元章 孙志卓 马忠梅 郑 军 谭毓安 (1290)

软件工程

软件可靠性预测中不同核函数的预测能力评估 楼俊钢 蒋云良 申 情 江建慧 (1303)

基于行为模型的需求可视化研究 李 琳 毋国庆 黄 勃 万 黎 吴 昊 (1312)

一种有效的 GLR 分析器错误恢复方法 许 福 刘 辉 孙 俏 陈志泊 王春玲 (1325)