



QK1836313

软件学报 *Software*

Journal of *Software*

主办



中国科学院软件研究所



中国计算机学会

出版



科学出版社





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 29 卷第 7 期

2018 年 7 月

目次

面向隐私保护的新技术与密码算法专题

面向隐私保护的新技术与密码算法专题前言	薛锐 彭长根 黄欣沂 刘吉强 禹勇 (1827)
同态加密技术及其在云计算隐私保护中的应用	李宗育 桂小林 顾迎捷 李雪松 戴慧璐 张学军 (1830)
基于用户分布感知的移动 P2P 快速位置匿名算法	许明艳 赵华 季新生 申涓 (1852)
面向工业物联网环境下后门隐私泄露感知方法	沙乐天 肖甫 陈伟 孙晶 王汝传 (1863)
格上基于身份哈希证明系统的新型构造	来齐齐 杨波 陈原 韩露露 白健 (1880)
基于字符串排序的高效保密数据库查询	李顺东 亢佳 杨晓艺 窦家维 (1893)
基于离线密钥分发的加密数据重复删除方法	张曙光 咸鹤群 王雅哲 刘红燕 侯瑞涛 (1909)
基于恶意读写器发现的 RFID 空口入侵检测技术	黄伟庆 丁昶 崔越 王思叶 张艳芳 赵博白 诸邵忆 毛锐 陈超 (1922)
对三个多服务器环境下匿名认证协议的分析	汪定 李文婷 王平 (1937)
公平理性委托计算协议	尹鑫 田有亮 王海龙 (1953)
面向云数据的隐私度量研究进展	熊金波 王敏荣 田有亮 马蓉 姚志强 林铭炜 (1963)
本地化差分隐私研究综述	叶青青 孟小峰 朱敏杰 霍峥 (1981)
高效且可验证的多授权机构属性基加密方案	仲红 崔杰 朱文龙 许艳 (2006)

模式识别与人工智能

时空数据语义理解:技术与应用	姚迪 张超 黄建辉 陈越新 毕经平 (2018)
特征驱动的关键词提取算法综述	常耀成 张宇翔 王红 万怀宇 肖春景 (2046)
深度神经网络训练中梯度不稳定现象研究综述	陈建廷 向阳 (2071)

计算机网络与信息安全

区块链技术及其在信息安全领域的研究进展	刘教迪 杜学绘 王娜 李少卓 (2092)
分布式云的研究进展综述	张晓丽 杨家海 孙晓晴 吴建平 (2116)

计算机图形学与计算机辅助设计

CT 投影采样策略对重建质量影响综述	杨富强 张定华 黄魁东 高宗照 廖金明 (2133)
--------------------------	----------------------------

操作系统

实时多核嵌入式系统研究综述	陈刚 关楠 吕鸣松 王义 (2152)
---------------------	---------------------

《软件学报》投稿指南 (封三)

期刊基本参数: CN11-2560/TP*1990*m*16*352*zh+en*P*¥70*2018*20*2018-07

Contents

SPECIAL TOPIC ON PRIVACY PRESERVING ORIENTED NEW TECHNOLOGIES AND CRYPTOGRAPHIC ALGORITHMS

- 1827 Preface
XUE Rui, PENG Chang-Gen, HUANG Xin-Yi, LIU Ji-Qiang, YU Yong
- 1830 Survey on Homomorphic Encryption Algorithm and Its Application in the Privacy-Preserving for Cloud Computing
LI Zong-Yu, GUI Xiao-Lin, GU Ying-Jie, LI Xue-Song, DAI Hui-Jun, ZHANG Xue-Jun
- 1852 Distribution-Perceptive-Based Spatial Cloaking Algorithm for Location Privacy in Mobile Peer-to-Peer Environments
XU Ming-Yan, ZHAO Hua, JI Xin-Sheng, SHEN Juan
- 1863 Leakage Perception Method for Backdoor Privacy in Industry Internet of Things Environment
SHA Le-Tian, XIAO Fu, CHEN Wei, SUN Jing, WANG Ru-Chuan
- 1880 Novel Construction of Identity-Based Hash Proof System Based on Lattices
LAI Qi-Qi, YANG Bo, CHEN Yuan, HAN Lu-Lu, BAI Jian
- 1893 String Sorting Based Efficient Secure Database Query
LI Shun-Dong, KANG Jia, YANG Xiao-Yi, DOU Jia-Wei
- 1909 Secure Encrypted Data Deduplication Method Based on Offline Key Distribution
ZHANG Shu-Guang, XIAN He-Qun, WANG Ya-Zhe, LIU Hong-Yan, HOU Rui-Tao
- 1922 RFID Air Interface Intrusion Detection Technology Based on Malicious Reader Finding
HUANG Wei-Qing, DING Chang, CUI Yue, WANG Si-Ye, ZHANG Yan-Fang, ZHAO Bo-Bai, ZHU Shao-Yi, MAO Rui, CHEN Chao
- 1937 Cryptanalysis of Three Anonymous Authentication Schemes for Multi-Server Environment
WANG Ding, LI Wen-Ting, WANG Ping
- 1953 Fair and Rational Delegation Computation Protocol
YIN Xin, TIAN You-Liang, WANG Hai-Long
- 1963 Research Progress on Privacy Measurement for Cloud Data
XIONG Jin-Bo, WANG Min-Shen, TIAN You-Liang, MA Rong, YAO Zhi-Qiang, LIN Ming-Wei
- 1981 Survey on Local Differential Privacy
YE Qing-Qing, MENG Xiao-Feng, ZHU Min-Jie, HUO Zheng
- 2006 Efficient and Verifiable Multi-Authority Attribute Based Encryption Scheme
ZHONG Hong, CUI Jie, ZHU Wen-Long, XU Yan

PATTERN RECOGNITION AND ARTIFICIAL INTELLIGENCE

- 2018 Semantic Understanding of Spatio-Temporal Data: Technology & Application
YAO Di, ZHANG Chao, HUANG Jian-Hui, CHEN Yue-Xin, BI Jing-Ping
- 2046 Features Oriented Survey of State-of-the-Art Keyphrase Extraction Algorithms
CHANG Yao-Cheng, ZHANG Yu-Xiang, WANG Hong, WAN Huai-Yu, XIAO Chun-Jing
- 2071 Survey of Unstable Gradients in Deep Neural Network Training
CHEN Jian-Ting, XIANG Yang

COMPUTER NETWORKS AND INFORMATION SECURITY

- 2092 Research Progress of Blockchain Technology and Its Application in Information Security
LIU Ao-Di, DU Xue-Hui, WANG Na, LI Shao-Zhuo
- 2116 Survey of Geo-Distributed Cloud Research Progress
ZHANG Xiao-Li, YANG Jia-Hai, SUN Xiao-Qing, WU Jian-Ping

COMPUTER GRAPHICS AND COMPUTER AIDED DESIGN

- 2133 Review of the Effect of Computed Tomography Projection Sampling Strategy on Reconstruction Quality
YANG Fu-Qiang, ZHANG Ding-Hua, HUANG Kui-Dong, GAO Zong-Zhao, LIAO Jin-Ming

OPERATING SYSTEM

- 2152 State-of-the-Art Survey of Real-Time Multicore System
CHEN Gang, GUAN Nan, LÜ Ming-Song, WANG Yi

《软件学报》2017 年已出版专刊

发表期数	专刊/题名称	特约编辑
2017 年第 3 期	大数据管理技术	崔斌, 马帅
2017 年第 4 期	程序设计语言和系统前沿	冯新宇, 陈海波
2017 年第 5 期	形式化方法与应用	董威, 赵建华, 吕鸣松
2017 年第 6 期	大数据时代软件工程研究	刘璘, 周明辉, 尹刚
2017 年第 8 期	分布式云存储: 理论、技术、系统	黄宇, 吴维刚, 赵军平
2017 年第 9 期	信息系统安全	李舟军, 李瑞轩, 陈驰
2017 年第 11 期	复杂环境下的机器学习研究专刊	胡清华, 张道强, 张长水

登录软件学报网站: <http://www.jos.org.cn> 免费下载专刊全文.

软件学报
Ruanjian Xuebao
(月刊, 1990 年创刊)

Journal of Software
(monthly)
(Started in 1990)

第 29 卷 第 7 期 2018 年 7 月

Vol.29 No.7 Jul. 2018

主管单位 中国科学院
主办单位 中国科学院软件研究所 中国计算机学会
主 编 赵 琛
编 辑 《软件学报》编辑部
(北京 8718 信箱 邮编 100190)
电话: 010-62562563, E-mail: jos@iscas.ac.cn
<http://www.jos.org.cn>

编辑部主任 方 梅
出 版 科 学 出 版 社
(北京东黄城根北街 16 号 邮编 100717)
印 刷 北京宝昌彩色印刷有限公司
总发行处 中国邮政集团公司北京市报刊发行局
订 购 处 全国各地邮局
国外总发行 中国国际图书贸易总公司
(北京 399 信箱 邮编 100044)

Sponsored by the Chinese Academy of Sciences
Published by Institute of Software, The Chinese Academy of Sciences (ISCAS) and China Computer Federation
Editor-in-Chief: ZHAO Chen
Edited by Editorial Board of Journal of Software
(P.O.Box 8718, Beijing 100190, P.R.China)
Tel: 8610-62562563, E-mail: jos@iscas.ac.cn
<http://www.jos.org.cn>

Distributed by Science Press (16 Donghuangchenggen North Street, Beijing 100717, China)
Printed by Beijing Baochang Color Printing Co., Ltd
Generally Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestically Distributed by All Local Post Offices in China
Overseas Distributed by China International Book Trading Corporation (P.O.Box 399, Beijing 100044, China)

ISSN 1000-9825
CN 11-2560/TP

国内邮发代号: 82-367
国外发行代号: M4628

©2018 ISCAS (版权所有)

定价: 70.00 元



公 开 发 行