



ISSN 1000-1239  
CODEN JYYFEY

# CRAD

Journal of Computer Research and Development

# 计算机研究与发展

第57卷 第10期 2020年10月  
Vol.57 No.10 Oct.2020

# CRAD

# CRAD

# CRAD

# CRAD

主办 中国科学院计算技术研究所 中国计算机学会 出版 科学出版社

 中国计算机学会会刊

计算机研究与发展

第五十七卷

第十期

二〇二〇年十月

科学出版社





# 计算机研究与发展

(Jisuanji Yanjiu Yu Fazhan)

第 57 卷 第 10 期 2020 年 10 月

## 目 次

### 密码学与数据隐私保护研究专题

前 言 ..... 曹珍富 徐秋亮 张玉清 董晓蕾 (2009)

### 综 述

量子计算与量子密码的原理及研究进展综述 ..... 王永利 徐秋亮 (2015)

边缘计算隐私保护研究进展 ..... 周 俊 沈华杰 林中允 曹珍富 董晓蕾 (2027)

网络安全威胁情报共享与交换研究综述 ..... 林 玥 刘 鹏 王 鹤 王文杰 张玉清 (2052)

机器学习的安全问题及隐私保护 ..... 魏立斐 陈聪聪 张 蕾 李梦思 陈玉娇 王 勤 (2066)

### 密码算法与协议

基于模格的密钥封装方案的比较分析与优化 ..... 王 洋 沈诗羽 赵运磊 王明强 (2086)

一种增强的多用户前向安全动态对称可搜索加密方案 ..... 卢冰洁 周 俊 曹珍富 (2104)

循环安全的同态加密方案 ..... 赵秀凤 付 雨 宋巍涛 (2117)

无配对公钥认证可搜索加密方案 ..... 杨宁滨 周 权 许舒美 (2125)

移动互联网环境下轻量级 SM2 两方协同签名 ..... 冯 琦 何德彪 罗 敏 李 莉 (2136)

一种基于混沌系统的 ZUC 动态 S 盒构造及应用方案 .....

..... 韩妍妍 何彦茹 刘培鹤 张 铎 王志强 何文才 (2147)

后量子前向安全的可组合认证密钥交换方案 ..... 陈 明 (2158)

工业物联网中服务器辅助且可验证的属性基签名方案 ..... 张应辉 贺江勇 郭 瑞 郑 东 (2177)

### 隐私保护

安全的常数轮多用户  $k$ -均值聚类计算协议 ..... 秦 红 王 皓 魏晓超 郑志华 (2188)

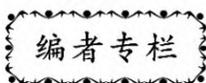
基于随机映射技术的声纹识别模板保护 ..... 丁 勇 李佳慧 唐士杰 王会勇 (2201)

抗位置隐私泄露的物联网频谱共享激励机制 ..... 冯景瑜 杨锦雯 张瑞通 张文波 (2209)

面向集合计算的隐私保护统计协议 ..... 宋祥福 盖 敏 赵圣楠 蒋 瀚 (2221)

ACT:可审计的机密交易方案 ..... 姜轶涵 李 勇 朱 岩 (2232)

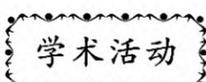
基于秘密分享和梯度选择的高效安全联邦学习 ..... 董 业 侯 炜 陈小军 曾 帅 (2241)



2018 年《计算机研究与发展》高被引论文 TOP10 ..... (2146)

《计算机研究与发展》征订启事 ..... (2176)

《计算机研究与发展》编委会 ..... (封底)



2021 年“人工智能安全与隐私保护技术”专题(正刊)征文通知 ..... (2200)

责任编辑:侯丽珊

# JOURNAL OF COMPUTER RESEARCH AND DEVELOPMENT

Vol. 57 No. 10 October 2020

## CONTENTS

### Special Issue on Cryptography and Privacy Preserving

Preface ..... *Cao Zhenfu, et al.* (2009)

### Survey

Principle and Research Progress of Quantum Computation and Quantum Cryptography .....  
..... *Wang Yongli, et al.* (2015)

Research Advances on Privacy Preserving in Edge Computing ..... *Zhou Jun, et al.* (2027)

Overview of Threat Intelligence Sharing and Exchange in Cybersecurity ..... *Lin Yue, et al.* (2052)

Security Issues and Privacy Preserving in Machine Learning ..... *Wei Lifei, et al.* (2066)

### Cryptography Algorithm and Protocol

Comparisons and Optimizations of Key Encapsulation Mechanisms Based on Module Lattices ...  
..... *Wang Yang, et al.* (2086)

A Multi-User Forward Secure Dynamic Symmetric Searchable Encryption with Enhanced Security  
..... *Lu Bingjie, et al.* (2104)

Circular Secure Homomorphic Encryption Scheme ..... *Zhao Xiufeng, et al.* (2117)

Public-Key Authenticated Encryption with Keyword Search Without Pairings .....  
..... *Yang Ningbin, et al.* (2125)

Efficient Two-Party SM2 Signing Protocol for Mobile Internet ..... *Feng Qi, et al.* (2136)

A Dynamic S-Box Construction and Application Scheme of ZUC Based on Chaotic System .....  
..... *Han Yanyan, et al.* (2147)

A Composable Authentication Key Exchange Scheme with Post-Quantum Forward Secrecy .....  
..... *Chen Ming* (2158)

Server-Aided and Verifiable Attribute-Based Signature for Industrial Internet of Things .....  
..... *Zhang Yinghui, et al.* (2177)

### Privacy Perserving

Secure Constant-Round Multi-User  $k$ -Means Clustering Protocol ..... *Qin Hong, et al.* (2188)

Template Protection of Speaker Recognition Based on Random Mapping Technology .....  
..... *Ding Yong, et al.* (2201)

A Spectrum Sharing Incentive Scheme Against Location Privacy Leakage in IoT Networks .....  
..... *Feng Jingyu, et al.* (2209)

Privacy-Preserving Statistics Protocol for Set-Based Computation ..... *Song Xiangfu, et al.* (2221)

ACT: Auditable Confidential Transaction Scheme ..... *Jiang Yihan, et al.* (2232)

Efficient and Secure Federated Learning Based on Secret Sharing and Gradients Selection .....  
..... *Dong Ye, et al.* (2241)

~~~~~  
Editorial Columns ..... (2146,2176,back cover)

Academic Activities ..... (2200)

# 《计算机研究与发展》第八届编委会

主 编 徐志伟 中国科学院计算技术研究所

副 主 编 石统一 清华大学

赵沁平 北京航空航天大学

史忠植 中国科学院计算技术研究所

郑纬民 清华大学

吕 建 南京大学

领域编委 刘志勇(体系结构) 中国科学院计算技术研究所

林 闯(网络技术) 清华大学

孟小峰(软件技术) 中国人民大学

曹珍富(信息安全) 华东师范大学

郑庆华(应用技术) 西安交通大学

周志华(人工智能) 南京大学

## 编 委

安 虹 中国科学技术大学

曹军威 清华大学

曹子宁 北京航空航天大学

陈恩红 中国科学技术大学

陈国良 中国科学技术大学

陈左宁 江南计算技术研究所

崔 莉 中国科学院计算技术研究所

窦 勇 国防科技大学

方滨兴 北京邮电大学

冯 丹 华中科技大学

冯志勇 天津大学

过敏意 上海交通大学

侯丽珊 中国科学院计算技术研究所

黄河燕 北京理工大学

黄 华 北京理工大学

黄刘生 中国科学技术大学苏州研究院

金澈清 华东师范大学

金 海 华中科技大学

李华伟 中国科学院计算技术研究所

李建中 哈尔滨工业大学

李仁发 湖南大学

李晓明 北京大学

李宣东 南京大学

梁吉业 山西大学

廖士中 天津大学

林东岱 中国科学院信息工程研究所

刘国华 东华大学

罗军舟 东南大学

马华东 北京邮电大学

梅 宏 军事科学院

孟祥旭 山东大学

苗夺谦 同济大学

欧阳彤彤 吉林大学

彭宇新 北京大学

钱德沛 北京航空航天大学

秦志光 电子科技大学

任丰原 清华大学

舒继武 清华大学

苏开乐 暨南大学

孙茂松 清华大学

孙晓明 中国科学院计算技术研究所

陶建华 中国科学院自动化研究所

王晓阳 复旦大学

王兴伟 东北大学

王意洁 国防科技大学

王永吉 中国科学院软件研究所

吴 威 北京航空航天大学

徐秋亮 山东大学

薛 锐 中国科学院信息工程研究所

薛向阳 复旦大学

杨学军 军事科学院

于 戈 东北大学

于 剑 北京交通大学

于 炯 新疆大学

詹乃军 中国科学院软件研究所

张 路 北京大学

张 伟 烟台大学

张悠慧 清华大学

张玉清 中国科学院大学

章 毅 四川大学

周傲英 华东师范大学

周 昆 浙江大学

计算机研究与发展

Jisuanji Yanjiu yu Fazhan

(月刊, 1958年创刊)

第57卷 第10期 2020年10月

主 管 中国科学院

主 办 中国科学院计算技术研究所

中国计算机学会

主 编 徐志伟

编辑部主任 侯丽珊

编 辑 《计算机研究与发展》编辑部

中国科学院计算技术研究所

地址: 北京中关村科学院南路6号

邮政编码: 100190

电话: +86(10)62620696(兼传真)

+86(10)62600350

E-mail: crad@ict.ac.cn

http://crad.ict.ac.cn

出 版 科学出版社

地址: 北京东黄城根北街16号

邮政编码: 100717

印刷装订 艺堂印刷(天津)有限公司

国内总发行 北京报刊发行局

订 购 处 全国各邮电局

国外总发行 中国国际图书贸易总公司

北京399信箱

邮政编码: 100044

**Journal of Computer  
Research and Development**  
(Monthly, Started in 1958)  
Vol.57 No.10 Oct.2020

Supervised by Chinese Academy of Sciences

Sponsored by Institute of Computing Technology,  
Chinese Academy of Sciences  
China Computer Federation

Editor-in-Chief Xu Zhiwei

Director Hou Lishan

Edited by Editorial Office of *Journal of  
Computer Research and Development*

Institute of Computing Technology,  
Chinese Academy of Sciences

Add: 6 Kexueyuan South Road,

Zhongguancun, Beijing

100190, China

Tel: +86(10) 62620696 (also Fax)

+86(10) 62600350

E-mail: crad@ict.ac.cn

http://crad.ict.ac.cn

Published by Science Press

Add: 16 Donghuangchenggen North  
Street, Beijing 100717, China

Printed by Yitang Printing(Tianjin) Co.Ltd

Distributed by Beijing Bureau for Distribution of  
Newspapers and Journals

Domestic All Local Post Offices in China

Foreign China International Book

Trading Corporation

P.O.Box 399, Beijing 100044, China

CN 11-1777 / TP

国内邮发代号: 2-654

定价: 78.00元

国外发行代号: M603

万方数据

国内外公开发行人

ISSN 1000-1239



10>

9 771000 123204