



# 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)

工业互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)

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)

### 编者专栏

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)

### 学术活动

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

## 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)