



计算机研究与发展

(Jisuanji Yanjiu Yu Fazhan)

第 56 卷 第 10 期 2019 年 10 月

目 次

密码学与智能安全研究专题

前 言 曹珍富 徐秋亮 张玉清 董晓蕾 (2027)

综 述

推荐系统的隐私保护研究进展 周 俊 董晓蕾 曹珍富 (2033)

机器学习系统的隐私和安全性问题综述 何英哲 胡兴波 何锦雯 孟国柱 陈 恺 (2049)

机器学习模型可解释性方法、应用与安全性研究综述 纪守领 李进锋 杜天宇 李 博 (2071)

安全漏洞自动利用综述 赵尚儒 李学俊 方 越 余媛萍 黄伟豪 陈 恺 苏璞睿 张玉清 (2097)

从演化密码到量子人工智能密码综述 王宝楠 胡 风 张焕国 王 潮 (2112)

人工智能系统安全与隐私风险 陈宇飞 沈 超 王 睿 李 琦 王 聪 纪守领 李 康 管晓宏 (2135)

智能密码算法

隐藏访问策略的高效 CP-ABE 方案 王 悦 樊 凯 (2151)

支持属性撤销的可追踪外包属性加密方案 高嘉昕 孙加萌 秦 静 (2160)

云环境下支持可更新加密的分布式数据编码存储方案 严新成 陈 越 巴 阳 贾洪勇 朱 或 (2170)

一种基于分支条件混淆的代码加密技术 耿 普 祝跃飞 (2183)

基于语义扩展的多关键词可搜索加密算法 徐光伟 史春红 王文涛 潘 乔 李 锋 (2193)

基于高性能密码实现的大数据安全方案 杨国强 丁杭超 邹 静 蒋 瀚 陈彦琴 (2207)

物联网中 MIBS 轻量级密码的唯密文故障分析
..... 李 玮 曹 珊 谷大武 李嘉耀 汪梦林 蔡天培 石秀金 (2216)

智能隐私保护

后量子的智能电表隐私保护方案 田杨童 张 煌 谢少浩 张方国 (2229)

基于数据纵向分布的隐私保护逻辑回归 宋 蕾 马春光 段广晗 袁 琪 (2243)

基于卷积神经网络的 JPEG 图像隐写分析参照图像生成方法 任魏翔 翟黎明 王丽娜 嘉 炬 (2250)

一种基于软件定义安全和云取证趋势分析的云取证方法
..... 刘雪花 丁丽萍 刘文懋 郑 涛 李彦峰 吴敬征 (2262)

一种安全高效的无人驾驶车辆地图更新方案 赖成喆 张 敏 郑 东 (2277)

物联网中基于智能合约的访问控制方法 杜瑞忠 刘 妍 田俊峰 (2287)

编者专栏

《计算机研究与发展》征订启事 (2111)

2017 年《计算机研究与发展》高被引论文 TOP10 (2192)

《计算机研究与发展》编委会 (封底)

学术活动

2020 年“数据驱动网络”专题(正刊)征文通知 (2150)

责任编辑:齐 蓉

JOURNAL OF COMPUTER RESEARCH AND DEVELOPMENT

Vol. 56 No. 10 October 2019

CONTENTS

Special Issue on Cryptography and Intelligent Security

Preface Cao Zhenfu, et al. (2027)

Survey

Research Advances on Privacy Preserving in Recommender Systems Zhou Jun, et al. (2033)

Privacy and Security Issues in Machine Learning Systems: A Survey He Yingzhe, et al. (2049)

Survey on Techniques, Applications and Security of Machine Learning Interpretability
..... Ji Shouling, et al. (2071)

A Survey on Automated Exploit Generation Zhao Shangru, et al. (2097)

From Evolutionary Cryptography to Quantum Artificial Intelligent Cryptography
..... Wang Baonan, et al. (2112)

Security and Privacy Risks in Artificial Intelligence Systems Chen Yufei, et al. (2135)

Intelligent Cryptographic Algorithms

Effective CP-ABE with Hidden Access Policy Wang Yue, et al. (2151)

Traceable Outsourcing Attribute-Based Encryption with Attribute Revocation
..... Gao Jiaxin, et al. (2160)

Distributed Data Encoding Storage Scheme Supporting Updatable Encryption in Cloud
..... Yan Xincheng, et al. (2170)

A Code Encrypt Technique Based on Branch Condition Obfuscation Geng Pu, et al. (2183)

Multi-Keyword Searchable Encryption Algorithm Based on Semantic Extension
..... Xu Guangwei, et al. (2193)

A Big Data Security Scheme Based on High-Performance Cryptography Implementation
..... Yang Guoqiang, et al. (2207)

Ciphertext-Only Fault Analysis of the MIBS Lightweight Cryptosystem in the Internet of Things
..... Li Wei, et al. (2216)

Intelligent Privacy Preserving

Post-Quantum Privacy Preserving Smart Metering System Tian Yangtong, et al. (2229)

Privacy-Preserving Logistic Regression on Vertically Partitioned Data Song Lei, et al. (2243)

Reference Image Generation Algorithm for JPEG Image Steganalysis Based on Convolutional Neural Net-
work Ren Weixiang, et al. (2250)

A Cloud Forensics Method Based on SDS and Cloud Forensics Trend Analysis
..... Liu Xuehua, et al. (2262)

A Secure and Efficient Map Update Scheme for Autonomous Vehicles Lai Chengzhe, et al. (2277)

An Access Control Method Using Smart Contract for Internet of Things
..... Du Ruizhong, et al. (2287)

~~~~~  
Editorial Columns ..... (2111,2192,back cover)

Academic Activities ..... (2150)