



计算机研究与发展

(Jisuanji Yanjiu Yu Fazhan)

第 55 卷 第 10 期 2018 年 10 月

目 次

分布式安全与区块链技术研究专题

前 言 曹珍富 徐秋亮 张玉清 董晓蕾 (2095)

综 述

区块链可扩展性研究:问题与方法 潘 晨 刘志强 刘 振 龙 宇 (2099)

智能家居安全综述 王基策 李意莲 贾 岩 周 威 王宇成 王 鹤 张玉清 (2111)

分布式安全计算与密码算法

一个高效安全三方带通配符模式匹配协议 魏晓超 郑志华 王 皓 (2125)

基于用户定义安全条件的可验证重复数据删除方法 刘红燕 咸鹤群 鲁秀青 侯瑞涛 高 原 (2134)

双服务器模型下支持相关度排序的多关键字密文搜索方案 李宇溪 周福才 徐 剑 徐紫枫 (2149)

标准模型下格上基于身份的门限解密方案 吴立强 杨晓元 张敏情 (2164)

LBlock 轻量级密码算法的唯一密文故障分析
..... 李 玮 吴益鑫 谷大武 曹 珊 廖林峰 孙 莉 刘 亚 刘志强 (2174)

区块链与数字货币

基于聚合签名与加密交易的全匿名区块链 王子钰 刘建伟 张宗洋 喻 辉 (2185)

基于区块链的云数据删除验证协议 刘忆宁 周元健 蓝如师 唐春明 (2199)

基于沙普利值计算的区块链中 PoS 共识机制的改进 刘怡然 柯俊明 蒋 瀚 宋祥福 (2208)

基于区块链的可监管数字货币模型 张健毅 王志强 徐治理 欧阳雅菲 杨 涛 (2219)

基于区块链和同态加密的电子健康记录隐私保护方案 徐文玉 吴 磊 阎允雪 (2233)

基于共识机制的 LEO 低轨卫星网络区域合作认证协议 魏松杰 李 帅 莫 冰 王佳贺 (2244)

分布式系统安全

面向 SDN 的脆弱性扩散形式化建模与扩散因素分析 王 健 赵国生 赵中楠 李 可 (2256)

基于独立分量技术的类 GIFT 算法 S 盒逆向分析 马向亮 李 冰 习 伟 陈 华 陈财森 (2269)

一种基于隐藏事件触发机制的内存取证方法 崔超远 李勇钢 乌 云 王励成 (2278)

人工智能

基于位置的社会化网络推荐技术研究进展 焦 旭 肖迎元 郑文广 朱 珂 (2291)

考虑投资者朋友关系和预期效用的 P2P 借贷个性化投资推荐方法
..... 万常选 游运 江腾蛟 刘喜平 廖国琼 刘德喜 (2307)

一种小样本数据的特征选择方法 许 行 张 凯 王文剑 (2321)

软件技术

程序状态条件合并中变量隐式关联分析方法 郭 曦 王 盼 (2331)



2016 年《计算机研究与发展》高被引论文 TOP10 (2198)

《计算机研究与发展》征订启事 (2330)

《计算机研究与发展》编委会 (封底)

CONTENTS

Distributed Security and Blockchain Technology

Preface *Cao Zhenfu, et al.* (2095)

Survey

Research on Scalability of Blockchain Technology: Problems and Methods *Pan Chen, et al.* (2099)

Survey of Smart Home Security *Wang Jice, et al.* (2111)

Distributed Security Computing and Cryptography Algorithm

An Efficient and Secure Three-Party Wildcard Pattern Matching Protocol
..... *Wei Xiaochao, et al.* (2125)

Verifiable Secure Data Deduplication Based on User-Defined Security Requirements
..... *Liu Hongyan, et al.* (2134)

Multiple-Keyword Encrypted Search with Relevance Ranking on Dual-Server Model
..... *Li Yuxi, et al.* (2149)

Identity-Based Threshold Decryption Scheme from Lattices under the Standard Model
..... *Wu Liqiang, et al.* (2164)

Ciphertext-Only Fault Analysis of the LBlock Lightweight Cipher *Li Wei, et al.* (2174)

Blockchain and Digital Currency

Full Anonymous Blockchain Based on Aggregate Signature and Confidential Transaction
..... *Wang Ziyu, et al.* (2185)

Blockchain-Based Verification Scheme for Deletion Operation in Cloud *Liu Yining, et al.* (2199)

Improvement of the PoS Consensus Mechanism in Blockchain Based on Shapley Value
..... *Liu Yiran, et al.* (2208)

A Regulatable Digital Currency Model Based on Blockchain *Zhang Jianyi, et al.* (2219)

Privacy-Preserving Scheme of Electronic Health Records Based on Blockchain and Homomorphic
Encryption *Xu Wenyu, et al.* (2233)

Regional Cooperative Authentication Protocol for LEO Satellite Networks Based on Consensus
Mechanism *Wei Songjie, et al.* (2244)

Distributed System Security

Formal Modeling and Factor Analysis for Vulnerability Propagation Oriented to SDN
..... *Wang Jian, et al.* (2256)

Reverse-Analysis of S-Box for GIFT-Like Algorithms Based on Independent Component Analysis
Technology *Ma Xiangliang, et al.* (2269)

A Memory Forensic Method Based on Hidden Event Trigger Mechanism
..... *Cui Chaoyuan, et al.* (2278)

Artificial Intelligence

Research Progress of Recommendation Technology in Location-Based Social Networks
..... *Jiao Xu, et al.* (2291)

Personalized Investment Recommendation in P2P Lending Considering Friend Relationships and
Expected Utilities of Investors *Wan Changxuan, et al.* (2307)

A Feature Selection Method for Small Samples *Xu Hang, et al.* (2321)

Software Technology

Variable Dependent Relation Analysis in Program State Condition Merging *Guo Xi, et al.* (2331)

~~~~~  
Editorial Columns ..... (2198, 2330, back cover)