

计 算 机 学 报

(JISUANJI XUEBAO)

第 41 卷 第 5 期 2018 年 5 月

目 次

区块链与电子支付安全

区块链技术:架构及进展	邵奇峰 金澈清 张 召 钱卫宁 周傲英 (969)
轻量级比特币交易溯源机制	高 峰 毛洪亮 吴 震 沈 蒙 祝烈煌 李艳东 (989)
许可链多中心动态共识机制	闵新平 李庆忠 孔兰菊 张世栋 郑永清 肖宗水 (1005)
一种高效安全的去中心化数据共享模型	
.....	董祥千 郭 兵 沈 艳 段旭良 申云成 张 洪 (1021)
基于 PSO 优化的移动位置隐私保护算法	李 婕 白志宏 于瑞云 崔亚盟 王兴伟 (1037)
适用于移动互联网的门限群签名方案	陈立全 朱 政 王慕阳 孙晓燕 (1052)
基于新“0”测试参数的理想格上多线性映射	古春生 景征骏 史培中 于志敏 (1068)
基于网络攻击面自适应转换的移动目标防御技术	
.....	雷 程 马多贵 张红旗 杨英杰 王利明 (1109)
保密替换及其在保密科学计算中的应用	杨晓艺 李顺东 亢 佳 (1132)
基于双管道结构的在线加密方案	睦 晗 吴文玲 张立廷 (1143)
无线网络中基于共享密钥的轻量级匿名认证协议	钟 成 李兴华 宋园园 马建峰 (1157)
多个字符排序的安全多方计算	李顺东 亢 佳 杨晓艺 窦家维 刘 新 (1172)

CHINESE JOURNAL OF COMPUTERS

Vol.41 No.5 May 2018

CONTENTS

Blockchain and ePayment Security

Blockchain: Architecture and Research Progress	SHAO Qi-Feng et al. (969)
Lightweight Transaction Tracing Technology for Bitcoin	GAO Feng et al. (989)
Permissioned Blockchain Dynamic Consensus Mechanism Based Multi-Centers	
.....	MIN Xin-Ping et al. (1005)
An Efficient and Secure Decentralizing Data Sharing Model	DONG Xiang-Qian et al. (1021)
Mobile Location Privacy Protection Algorithm Based on PSO Optimization	LI Jie et al. (1037)
A Threshold Group Signature Scheme for Mobile Internet Application	CHEN Li-Quan et al. (1052)
New Zero-Test Parameter Based Multilinear Maps from Ideal Lattices	GU Chun-Sheng et al. (1068)
Moving Target Defense Technique Based on Network Attack Surface Self-Adaptive Mutation	
.....	LEI Cheng et al. (1109)
Private Substitution and Its Applications in Private Scientific Computation	
.....	YANG Xiao-Yi et al. (1132)
Double-Pipeline Online Encryption	SUI Han et al. (1143)
A Lightweight Anonymous Authentication Protocol Based on Shared Key in Wireless Networks	
.....	ZHONG Cheng et al. (1157)
Secure Multiparty Characters Sorting	LI Shun-Dong et al. (1172)