● ISSN 0254-4164
● CODEN JIXUDT

计算机学报

CHINESE JOURNAL OF COMPUTERS

第42卷 Vol.42 第5期 No.5

2019.5

● 中国计算机学会 中国科学院计算技术研究所 主办
● 科学出版社 出版

计 算 机 学 报

(JISUANJI XUEBAO)

第 42 卷 第 5 期 2019 年 5 月

目 次

网络空间安全

基于软件指令定位的新型高阶侧信道分析方法 …… 郭志鹏 唐 明 胡晓波 李煜光 彭国军 张焕国 (929)

基于区块链的分布式 K 匿名位置隐私保护方案 …… 刘 海 李兴华 雒 彬 王运帷 任彦冰 马建峰 丁红发 (942)

车载自组网中基于信任管理的安全组播协议设计 …… 夏 辉 张三顺 孙运传 肖 甫 李 晔 成秀珍 (961)

格基环签名的车联网隐私保护 …… 崔永泉 曹 玲 张小宇 曾功贤 (980)

硬件木马:关键问题研究进展及新动向 …… 黄 钊 王 泉 杨鹏飞 (993)

USB HID 攻击检测技术研究 …… 姜建国 常子敬 吕志强 张 宁 (1018)

区间位置关系的保密判定 …… 窦家维 王文丽 李顺东 (1031)

数字货币的匿名性研究 …… 付 烁 徐海霞 李佩丽 马添军 (1045)

基于密文策略的流程加密研究 …… 邓宇乔 杨 波 唐春明 宋 歌 温雅敏 (1063)

无人机信息安全研究综述 …… 何道敬 杜 晓 乔银荣 朱耀康 樊 强 罗 旺 (1076)

网络直播平台主播地理位置泄露漏洞的分析与利用 …… 乐洪舟 张玉清 (1095)

基于二元 BKF 统计建模的双树复数小波域数字水印检测算法 …… 王向阳 李 丽 李海芳 牛盼盼 王思淼 杨红颖 (1112)

有限域 F_{p^n} 上与逆函数仿射等价的密码函数计数问题 …… 袁 峰 江继军 杨 旸 欧海文 王敏娟 (1126)

一种抵御中间人攻击的可信网络连接协议 …… 赵 波 向 程 张焕国 (1137)

科学与工程论坛

基于离散优化的哈希编码学习方法 …… 刘昊淼 王瑞平 山世光 陈熙霖 (1149)

CHINESE JOURNAL OF COMPUTERS

Vol.42 No.5 May 2019

CONTENTS

Cyberspace Security

Instruction-Location-Based Analysis Against Software Implementation of Higher-Order Masking ··· GUO Zhi-Peng et al. (929)

Distributed K-Anonymity Location Privacy Protection Scheme Based on Blockchain ··· LIU Hai et al. (942)

Design of Trust-Based Secure Multicast Routing Protocol in VANETs ··· XIA Hui et al. (961)

Ring Signature Based on Lattice and VANET Privacy Preservation ··· CUI Yong-Quan et al. (980)

Hardware Trojan: Research Progress and New Trends on Key Problems ··· HUANG Zhao et al. (993)

Research on USB HID Attack Detection Technology ··· JIANG Jian-Guo et al. (1018)

Privately Determining Interval Location Relation ··· DOU Jia-Wei et al. (1031)

A Survey on Anonymity of Digital Currency ··· FU Shuo et al. (1045)

Research of Ciphertext Policy Process-Based Encryption ··· DENG Yu-Qiao et al. (1063)

A Survey on Cyber Security of Unmanned Aerial Vehicles ··· HE Dao-Jing et al. (1076)

Vulnerability Analysis and Exploitation of Location Privacy Leakage in Webcasting Platforms ··· YUE Hong-Zhou et al. (1095)

A Blind Watermark Decoder in DT CWT Domain using Multivariate Bessel K Form Distribution ··· WANG Xiang-Yang et al. (1112)

Enumeration of Cryptographic Functions Affine Equivalent to the Inverse Function Over F_{p^n} ··· YUAN Feng et al. (1126)

A Trusted Network Connect Protocol for Resisting Man-in-the-Middle Attack ··· ZHAO Bo et al. (1137)

Science and Engineering Forum

Learning to Hash with Discrete Optimization ··· LIU Hao-Miao et al. (1149)

计 算 机 学 报	Chinese Journal of Computers
（月刊，1978 年创刊）	（Monthly，Started in 1978）
第 42 卷　第 5 期　总第 437 期　2019 年 5 月	Vol. 42　No. 5　Series No. 437　May　2019
主　管　中国科学院	Supervised by Chinese Academy of Sciences
主　办　中国计算机学会 中国科学院计算技术研究所	Sponsored by China Computer Federation, Institute of Computing Technology, CAS
主　编　孙凝晖	Editor-in-Chief: SUN Ning-Hui
编　辑　《计算机学报》编辑委员会 中国科学院计算技术研究所 邮政编码 100190，北京 2704 信箱 E-mail: cjc@ict.ac.cn http://cjc.ict.ac.cn	Edited by Editorial Board of Chinese Journal of Computers P. O. Box 2704, Beijing 100190, China
编辑部主任　李　刚	Director: LI Gang
出　版　科学出版社	Published by Science Press
印刷装订　北京科信印刷有限公司	Printed by Beijing Kexin Printing Co., Ltd.
总发行处　科学出版社 北京东黄城根北街 16 号 邮政编码 100717	Distributed by Science Press 16 Donghuangchenggen North Street, Beijing 100717, China
国外总发行　中国国际图书贸易总公司 （中国国际书店） 北京 399 信箱	Foreign: Guoji Shudian P. O. Box 399, Beijing 100044, China
数字出版　CNKI　http://www.cnki.net	Online Published by CNKI　http://www.cnki.net

国内统一连续出版物号：CN 11-1826/TP

订 购 处：全国各邮电局

定　　价：73.00 元

国内邮发代号：2-833

国外发行代号：M 206

国内外公开发行

ISSN 0254-4164