



QK1919483

• 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 王思森 杨红颖 (1112)
- 有限域  $F_p$  上与逆函数仿射等价的密码函数计数问题 .....  
..... 袁 峰 江继军 杨 畅 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 ..... 刘昊森 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》编辑委员会

## The Editorial Board of Chinese Journal of Computers

**主 编** Editor-in-Chief 孙凝晖 SUN Ning-Hui

**副主编** Associate Editors-in-Chief

陈熙霖 CHEN Xi-Lin 冯登国 FENG Deng-Guo 金 芝 JIN Zhi

林 闯 LIN Chuang 周傲英 ZHOU Ao-Ying

**委 员** Members

陈贵海 CHEN Gui-Hai	陈克非 CHEN Ke-Fei	程学旗 CHENG Xue-Qi	范玉顺 FAN Yu-Shun
方滨兴 FANG Bin-Xing	傅育熙 FU Yu-Xi	高 文 GAO Wen	韩燕波 HAN Yan-Bo
何新贵 HE Xin-Gui	胡事民 HU Shi-Min	华庆一 HUA Qing-Yi	怀进鹏 HUAI Jin-Peng
黄继武 HUANG Ji-Wu	蒋昌俊 JIANG Chang-Jun	蒋焱川 JIANG Yi-Chuan	焦李成 JIAO Li-Cheng
金 海 JIN Hai	李德毅 LI De-Yi	李 刚 LI Gang	李国杰 LI Guo-Jie
李建中 LI Jian-Zhong	李克秋 LI Ke-Qiu	李 未 LI Wei	李晓明 LI Xiao-Ming
李忠诚 LI Zhong-Cheng	林惠民 LIN Hui-Min	刘大有 LIU Da-You	刘云浩 LIU Yun-Hao
刘志勇 LIU Zhi-Yong	卢汉清 LU Han-Qing	卢锡城 LU Xi-Cheng	陆汝钤 LU Ru-Qian
吕 建 LV Jian	罗军舟 LUO Jun-Zhou	马建峰 MA Jian-Feng	梅 宏 MEI Hong
孟 丹 MENG Dan	孟祥旭 MENG Xiang-Xu	闵革勇 MIN Ge-Yong	钮心忻 NIU Xin-Xin
欧阳丹彤 OUYANG Dan-Tong	潘启敬 PAN Qi-Jing	潘云鹤 PAN Yun-He	潘志庚 PAN Zhi-Geng
彭群生 PENG Qun-Sheng	钱德沛 QIAN De-Pei	瞿裕忠 QU Yu-Zhong	沈向洋 SHEN Xiang-Yang
沈绪榜 SHEN Xu-Bang	史忠植 SHI Zhong-Zhi	舒继武 SHU Ji-Wu	苏金树 SU Jin-Shu
谭铁牛 TAN Tie-Niu	唐志敏 TANG Zhi-Min	田 捷 TIAN Jie	王国胤 WANG Guo-Yin
王怀民 WANG Huai-Min	王 戟 WANG Ji	王 珊 WANG Shan	王兴伟 WANG Xing-Wei
吴建平 WU Jian-Ping	肖建国 XIAO Jian-Guo	许 进 XU Jin	杨学军 YANG Xue-Jun
杨义先 YANG Yi-Xian	于 戈 YU Ge	于 剑 YU Jian	查红彬 ZHA Hong-Bin
张 钹 ZHANG Bo	张长水 ZHANG Chang-Shui	张大鹏 ZHANG Da-Peng	张 健 ZHANG Jian
张尧学 ZHANG Yao-Xue	赵沁平 ZHAO Qin-Ping	周立柱 ZHOU Li-Zhu	周兴社 ZHOU Xing-She
朱传琪 ZHU Chuan-Qi	祝跃飞 ZHU Yue-Fei		

### 计 算 机 学 报

(月刊, 1978年创刊)

第42卷 第5期 总第437期 2019年5月

### Chinese Journal of Computers

(Monthly, Started in 1978)

Vol. 42 No. 5 Series No. 437 May 2019

<p><b>主 管</b> 中国科学院</p> <p><b>主 办</b> 中国计算机学会 中国科学院计算技术研究所</p> <p><b>主 编</b> 孙凝晖</p> <p><b>编 辑</b> 《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</p> <p><b>编辑部主任</b> 李 刚</p> <p><b>出 版</b> 科 学 出 版 社</p> <p><b>印 刷 装 订</b> 北京科信印刷有限公司</p> <p><b>总 发 行 处</b> 科 学 出 版 社 北京东黄城根北街16号 邮政编码 100717</p> <p><b>国外总发行</b> 中国国际图书贸易总公司 (中国 国际书店) 北京 399 信箱</p> <p><b>数字出版</b> CNKI <a href="http://www.cnki.net">http://www.cnki.net</a></p>	<p>Supervised by Chinese Academy of Sciences</p> <p>Sponsored by China Computer Federation, Institute of Computing Technology, CAS</p> <p>Editor-in-Chief: SUN Ning-Hui</p> <p>Edited by Editorial Board of Chinese Journal of Computers</p> <p>P. O. Box 2704, Beijing 100190, China</p> <p>Director: LI Gang</p> <p>Published by Science Press</p> <p>Printed by Beijing Kexin Printing Co., Ltd.</p> <p>Distributed by Science Press 16 Donghuangchenggen North Street, Beijing 100717, China</p> <p>Foreign: Guoji Shudian P. O. Box 399, Beijing 100044, China</p> <p>Online Published by CNKI <a href="http://www.cnki.net">http://www.cnki.net</a></p>
--	---

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

