



• ISSN 0254-4164

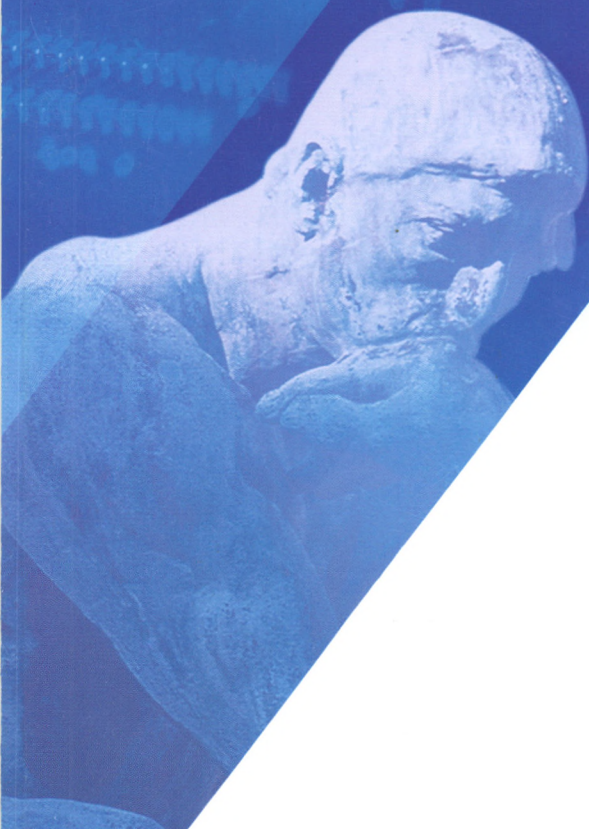
• CODEN JIXUDT

计算机学报

CHINESE JOURNAL OF COMPUTERS

第39卷 Vol.39

第3期 No.3



2016.3

• 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

CHINESE JOURNAL OF COMPUTERS

Vol.39 No.3 March 2016

CONTENTS

Information Security

- (3, n)-Visual Secret Sharing Scheme with Unexpanded Shares HOU Young-Chang et al. (441)
- Password Vulnerability Assessment and Recovery Based on Rules Mined from Large-Scale Real Data
..... LIU Gong-Shen et al. (454)
- Study on the ASCA Resistance of Block Ciphers LI Yan-Bin et al. (468)
- A Single Query Forgery Attack on Raviyoyla v1 YAO Yuan et al. (478)
- An Efficient Leakage-Resilient and CCA2-Secure PKE System ZHANG Ming-Wu et al. (492)
- Median Filtering Forensics Based on Multi-Directional Difference of Filtering Residuals
..... PENG An-Jie et al. (503)
- Cryptanalysis of HKKS Key Exchange Protocols LIU Jin-Hui et al. (516)
- Survey on Malicious Webpage Detection Research SHA Hong-Zhou et al. (529)
- Provably Secure and Efficient Certificateless Generalized Signcryption Scheme
..... ZHOU Yan-Wei et al. (543)
- KCapISO: A HybridHP-Based Capability Isolation Method of Loaded Modules on Monolithic Kernel
Operating System QIAN Zhen-Jiang et al. (552)
- CCA Secure PKE with Auxiliary Input WANG Zhi-Wei et al. (562)
- A Novel Reversible Image Watermarking Algorithm in Homomorphic Encrypted Domain
..... XIANG Shi-Jun et al. (571)
- The Vulnerabilities and Solutions of Third-Party Login Services in Android System
..... DONG Chao et al. (582)

Privacy Protection

- Privacy Preservation in Mobile Participatory Sensing ZENG Ju-Ru et al. (595)
- A Privacy Protection Model Base on Game Theory ZHANG Yi-Xuan et al. (615)
- Safe Region Scheme for Privacy-Preserving Continuous Nearest Neighbor Query on Road Networks
..... NI Wei-Wei et al. (628)

计 算 机 学 报

(JISUANJI XUEBAO)

第 39 卷 第 3 期 2016 年 3 月

目 次

信息安全

- 没有形变的 $(3, n)$ -视觉秘密分享方案 侯永昌 官振宇 蔡志丰 王道顺 (441)
- 基于真实数据挖掘的口令脆弱性评估及恢复 刘功申 邱卫东 孟 魁 李建华 (454)
- 分组密码抗 ASCA 安全性研究 李延斌 唐 明 郭志鹏 王龙龙 胡晓波 张焕国 (468)
- 对 Raviyoyla v1 的实际伪造攻击 姚 远 张 斌 吴文玲 (478)
- 高效弹性泄漏下 CCA2 安全公钥加密体制 张明武 陈泌文 何德彪 杨 波 (492)
- 基于滤波残差多方向差分的中值滤波取证技术 彭安杰 康显桂 (503)
- HKKS 密钥交换协议分析 刘金会 张焕国 贾建卫 王后珍 毛少武 吴万青 (516)
- 恶意网页识别研究综述 沙泓州 刘庆云 柳厅文 周 舟 郭 莉 方滨兴 (529)
- 可证安全的高效无证书广义签密方案 周彦伟 杨 波 张文政 (543)
- KCapISO: 一种基于 HybridHP 的宏内核操作系统载入模块权能隔离方案
..... 钱振江 刘永俊 汤 力 姚宇峰 黄 皓 (552)
- 抗辅助输入 CCA 安全的 PKE 构造 王志伟 李道丰 张 伟 陈 伟 (562)
- 一种同态加密域图像可逆水印算法 项世军 罗欣荣 石书协 (571)
- Android 系统中第三方登录漏洞与解决方案 董 超 杨 超 马建峰 张俊伟 (582)

隐私保护

- 参与式感知隐私保护技术 曾菊儒 陈 红 彭 辉 吴 垚 李翠平 王 珊 (595)
- 一个基于博弈理论的隐私保护模型 张伊璇 何泾沙 赵 斌 朱娜斐 (615)
- 面向路网隐私保护连续近邻查询的安全区域构建 倪巍伟 马中希 陈 萧 (628)

《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 | 蒋焜川 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 钺 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39卷 第3期 总第399期 2016年3月

Chinese Journal of Computers
(Monthly, Started in 1978)

Vol. 39 No. 3 Series No. 399 March 2016

| | |
|---|---|
| <p>主 管 中国科学院</p> <p>主 办 中国计算机学会 中国科学院计算技术研究所</p> <p>主 编 孙凝晖</p> <p>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</p> <p>编辑部主任 李 刚</p> <p>出 版 科 学 出 版 社</p> <p>印刷装订 北京科信印刷有限公司</p> <p>总发行处 科 学 出 版 社 北京东黄城根北街16号 邮政编码 100717</p> <p>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</p> <p>数字出版 CNKI http://www.cnki.net</p> | <p>Supervised by Chinese Academy of Sciences Sponsored by China Computer Federation, Institute of Computing Technology, CAS Editor-in-Chief: SUN Ning-Hui</p> <p>Edited by Editorial Board of Chinese Journal of Computers P. O. Box 2704, Beijing 100190, China</p> <p>Director: LI Gang Published by Science Press Printed by Beijing Kexin Printing Co., Ltd. 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 http://www.cnki.net</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: 58.00 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



9 770254 416162