



QK1705490

●ISSN 0254-4164

●CODEN JIXUDT

# 计算机学报

CHINESE JOURNAL OF COMPUTERS

第40卷 Vol.40 第5期 No.5



## 2017.5

● 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

# CHINESE JOURNAL OF COMPUTERS

Vol.40 No.5 May 2017

## CONTENTS

### Cyber Security

Lightweight Privacy-Preserving Framework for Location-Aware Recommender System .....	MA Xin-Di et al. (1017)
Android Driver Vulnerability Discovery Based on Black-Box Genetic Algorithm .....	HE Yuan et al. (1031)
An Adaptive Video Motion Vector Steganography Based on Macroblock Complexity .....	WANG Li-Na et al. (1044)
A Survey on System Security Isolation Technology .....	ZHENG Xian-Yi et al. (1057)
Improved Meet-in-the-Middle Attack of LBlock Cipher .....	ZHENG Ya-Fei et al. (1080)
The Researches on the ASIP of ECC in Embedded Domain .....	XIA Hui et al. (1092)
Universally Composable Gateway-Oriented Password-Authenticated Key Exchange Protocol .....	HU Xue-Xian et al. (1109)
co-Z Montgomery Algorithm on Elliptic Curves Over Finite Fields of Characteristic Three .....	YU Wei et al. (1121)
Secure Multiparty Vector Computation .....	ZHOU Su-Fang et al. (1134)
An Efficient Algorithm to Generate Password Sets Based on Samples .....	HAN Wei-Li et al. (1151)
Selectively Linkable and Convertible Ring Signature Based on RSA Public Key Cryptosystem .....	ZHANG Wen-Fang et al. (1168)
An Improved Two-Party Authenticated Certificateless Key Agreement Protocol .....	ZHOU Yan-Wei et al. (1181)
Improved Multidimensional Zero-Correlation Linear Cryptanalysis and Applications to 23-Round LBlock-s .....	LI Ling-Chen et al. (1192)

### Science and Engineering Forum

Characteristics of Color Images with Watermark Based on the Relationship Between Non-Void Subspaces of Inner Space .....	MA Ling et al. (1203)
An Efficient ISC Offset Parameter Coding Algorithm in Screen Content Coding .....	ZHAO Li-Ping et al. (1218)

# 计 算 机 学 报

(JISUANJI XUEBAO)

第 40 卷 第 5 期 2017 年 5 月

## 目 次

### 网络空间安全

轻量级位置感知推荐系统隐私保护框架 .....	
..... 马鑫迪 李 辉 马建峰 习 宁 姜 奇 高 胜 卢 笛 (1017)	
基于黑盒遗传算法的 Android 驱动漏洞挖掘 .....	何 远 张 玉 清 张 光 华 (1031)
基于宏块复杂度的自适应视频运动矢量隐写算法 .....	王 丽 娜 徐 一 波 翟 黎 明 任 延 珍 (1044)
系统安全隔离技术研究综述 .....	郑 显 义 史 岗 孟 丹 (1057)
LBlock 算法的改进中间相遇攻击 .....	郑 雅 菲 吴 文 玲 (1080)
嵌入式领域 ECC 专用指令处理器的研究 .....	
..... 夏 辉 于 佳 秦 尧 程 相 国 陈 仁 海 潘 振 宽 (1092)	
通用可组合的网关口令认证密钥交换协议 .....	胡 学 先 张 启 慧 张 振 峰 刘 凤 梅 (1109)
特征 3 有限域上椭圆曲线的 co-Z Montgomery 算法 .....	
..... 于 伟 李 宝 王 鲲鹏 李 维 恒 田 松 (1121)	
安全多方向量计算 .....	周 素 芳 窦 家 维 郭 奕 旻 毛 庆 李 顺 东 (1134)
一种基于样本的模拟口令集生成算法 .....	韩 伟 力 袁 琅 李 思 斯 王 晓 阳 (1151)
基于 RSA 公钥密码体制的可选择可转换关联环签名 .....	
..... 张 文 芳 熊 丹 王 小 敏 陈 楨 刘 旭 东 (1168)	
一种改进的无证书两方认证密钥协商协议 .....	周 彦 伟 杨 波 张 文 政 (1181)
多维零相关线性分析模型的改进及在 23 轮 LBlock-s 算法中的应用 .....	
..... 李 灵 琛 吴 文 玲 汪 艳 凤 (1192)	

### 科学与工程论坛

基于内积空间非空子空间变换关系的含水印彩色图像特征分析 .....	马 玲 张 晓 辉 (1203)
屏幕图像压缩中串复制位移参数的高效编码算法 .....	赵 利 平 林 涛 周 开 伦 (1218)



# 《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

方滨兴 FANG Bin-Xing

何新贵 HE Xin-Gui

黄继武 HUANG Ji-Wu

金 海 JIN Hai

李建中 LI Jian-Zhong

李忠诚 LI Zhong-Cheng

刘志勇 LIU Zhi-Yong

吕 建 LV Jian

孟 丹 MENG Dan

欧阳丹彤 OUYANG Dan-Tong

彭群生 PENG Qun-Sheng

沈绪榜 SHEN Xu-Bang

谭铁牛 TAN Tie-Niu

王怀民 WANG Huai-Min

吴建平 WU Jian-Ping

杨义先 YANG Yi-Xian

张 钹 ZHANG Bo

张尧学 ZHANG Yao-Xue

朱传琪 ZHU Chuan-Qi

陈克非 CHEN Ke-Fei

傅育熙 FU Yu-Xi

胡事民 HU Shi-Min

蒋昌俊 JIANG Chang-Jun

李德毅 LI De-Yi

李克秋 LI Ke-Qiu

林惠民 LIN Hui-Min

卢汉清 LU Han-Qing

罗军舟 LUO Jun-Zhou

孟祥旭 MENG Xiang-Xu

潘启敬 PAN Qi-Jing

钱德沛 QIAN De-Pei

史忠植 SHI Zhong-Zhi

唐志敏 TANG Zhi-Min

王 戟 WANG Ji

肖建国 XIAO Jian-Guo

于 戈 YU Ge

张长水 ZHANG Chang-Shui

赵沁平 ZHAO Qin-Ping

祝跃飞 ZHU Yue-Fei

程学旗 CHENG Xue-Qi

高 文 GAO Wen

华庆一 HUA Qing-Yi

蒋焱川 JIANG Yi-Chuan

李 刚 LI Gang

李 未 LI Wei

刘大有 LIU Da-You

卢锡城 LU Xi-Cheng

马建峰 MA Jian-Feng

闵革勇 MIN Ge-Yong

潘云鹤 PAN Yun-He

瞿裕忠 QU Yu-Zhong

舒继武 SHU Ji-Wu

田 捷 TIAN Jie

王 珊 WANG Shan

许 进 XU Jin

于 剑 YU Jian

张大鹏 ZHANG Da-Peng

周立柱 ZHOU Li-Zhu

范玉顺 FAN Yu-Shun

韩燕波 HAN Yan-Bo

怀进鹏 HUAI Jin-Peng

焦李成 JIAO Li-Cheng

李国杰 LI Guo-Jie

李晓明 LI Xiao-Ming

刘云浩 LIU Yun-Hao

陆汝钊 LU Ru-Qian

梅 宏 MEI Hong

钮心忻 NIU Xin-Xin

潘志庚 PAN Zhi-Geng

沈向洋 SHEN Xiang-Yang

苏金树 SU Jin-Shu

王国胤 WANG Guo-Yin

王兴伟 WANG Xing-Wei

杨学军 YANG Xue-Jun

查红彬 ZHA Hong-Bin

张 健 ZHANG Jian

周兴社 ZHOU Xing-She

## 计算机学报

(月刊, 1978年创刊)

第40卷 第5期 总第413期 2017年5月

主 管 中国科学院  
主 办 中国计算机学会  
中国科学院计算技术研究所  
主 编 孙凝晖  
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

编辑部主任 李 刚  
出 版 科 学 出 版 社  
印刷装订 北京科信印刷有限公司  
总发行处 科 学 出 版 社

北京东黄城根北街16号  
邮政编码 100717  
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

数字出版 CNKI <http://www.cnki.net>

## Chinese Journal of Computers

(Monthly, Started in 1978)

Vol. 40 No. 5 Series No. 413 May 2017

Supervised by Chinese Academy of Sciences  
Sponsored by China Computer Federation,  
Institute of Computing Technology, CAS  
Editor-in-Chief: SUN Ning-Hui

Edited by Editorial Board of Chinese  
Journal of Computers  
P. O. Box 2704, Beijing 100190, China

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

Foreign: Guoji Shudian

P. O. Box 399, Beijing 100044, China

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: 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 416179

05>