



ISSN 1001-2400

CN 61-1076/TN

CODEN XDKXEP

XI'AN DIANZI KEJI DAXUE XUEBAO

西安电子科技大学学报

JOURNAL OF XIDIAN UNIVERSITY

★ 2020中国高校百佳科技期刊

★ 2020年陕西省高校科技名刊

2022



第49卷 第1期
Vol.49 No.1

目 次

隐私计算与数据安全专题

支持属性和代理重加密的区块链数据共享方案
..... 李雪莲, 张夏川, 高军涛, 向登梅 (1)

差分隐私下的权重社交网络隐私保护
..... 徐 花, 田有亮 (17)

一种支持属性撤销的 top- k 多关键词密文检索方案
..... 王凯文, 王树兰, 王海燕, 丁 勇 (26)

一种支持动态可验证的密文检索方案
..... 杜瑞忠, 王 一, 田俊峰 (35)

无双线性对的高效云存储数据审计方案
..... 杨海滨, 李瑞峰, 易铮阁, 钮 可, 杨晓元 (47)

支持灵活访问控制的多关键字搜索加密方案
..... 闫玺玺, 赵 强, 汤永利, 李莹莹, 李静然 (55)

融合语义信息的时空关联位置隐私保护方法
..... 左开中, 刘 蕊, 赵 俊, 谌章义, 陈付龙 (67)

密码累加器研究进展及应用
..... 苗美霞, 武盼汝, 王贇玲 (78)

面向 ECDSA 的低复杂度多标量乘算法设计
..... 黄 海, 那 宁, 刘志伟, 于 斌, 赵石磊 (92)

有限域上一类完全置换单项式的构造
..... 黄萌濛, 伍高飞 (102)

白盒 SM4 的中间值平均差分分析
..... 张跃宇, 徐 东, 蔡志强, 陈 杰 (111)

针对 Fruit v2 和 Fruit-80 的差分错误攻击
..... 乔青蓝, 董丽华 (121)

信息与通信工程

- 一种类 Raptor 多速率 QC-LDPC 码的代数构造方法
..... 李华安, 白宝明, 徐恒舟, 陈 超 (134)
- 偏好感知的边云协同群智感知参与者选择策略
..... 王汝言, 刘 佳, 何 鹏, 崔亚平 (142)
- 移动边缘计算场景下基于免疫优化的任务卸载
..... 朱思峰, 孙恩林, 柴争义 (152)
- 应用 MCDM 的弹性光网络频谱碎片整理算法
..... 王鲸鱼, 冉金志, 王 平 (161)
- 序贯压缩感知下的海洋监测数据在线重构方法
..... 刘 歌, 芮国胜, 田文飏, 田润澜, 王晓峰 (173)
- 阵列误差下的近场源 PCA-BP 参数估计算法
..... 王 乐, 赵佩瑶, 王兰美, 王桂宝 (181)
- 局部特征值解的无条件稳定 FDTD 高效实施方案
..... 赵斯晗, 魏 兵, 何欣波 (188)
- 一种宽范围、高精度的带宽自适应式四相 DLL
..... 杨 雪, 刘 飞, 霍宗亮 (194)
- 毫米波 MIMO 的 DNN 混合预编码梯度优化方法
..... 王 勇, 王喜媛, 任泽洋 (202)

计算机科学与技术 & 人工智能

- 一种非线性变换的自适应透射率去雾算法
..... 孙景荣, 谢林昌, 杜梦欣, 罗丽燕 (208)
- 一种门控卷积生成对抗网络的图像修复算法
..... 高 杰, 霍智勇 (216)
- 无监督孪生函数映射网络的模型对应关系计算
..... 杨 军, 王幸幸, 芦有鹏 (225)
- 一种基于边界感知的遥感影像建筑物提取方法
..... 张 艳, 王翔宇, 张众维, 孙叶美, 刘树东 (236)

Contents

Special Issue on Privacy Computing and Data Security

Blockchain data sharing scheme supporting attribute and proxy re-encryption
 *LI Xuelian, ZHANG Xiachuan, GAO Juntao, XIANG Dengmei* (1)

Protection of privacy of the weighted social network under differential privacy
 *XU Hua, TIAN Youliang* (17)

Top- k multi-keyword ciphertext retrieval scheme supporting attribute revocation
 *WANG Kaiwen, WANG Shulan, WANG Haiyan, DING Yong* (26)

Support dynamic and verifiable scheme for ciphertext retrieval
 *DU Ruizhong, WANG Yi, TIAN Junfeng* (35)

Efficient cloud storage data auditing scheme without bilinear pairing
 *YANG Haibin, LI Rui feng, YI Zhengge, NIU Ke, YANG Xiaoyuan* (47)

Multi-keyword search encryption scheme supporting flexible access control
 *YAN Xixi, ZHAO Qiang, TANG Yongli, LI Yingying, LI Jingran* (55)

Method for the protection of spatiotemporal correlation location privacy with semantic information
 *ZUO Kaizhong, LIU Rui, ZHAO Jun, CHEN Zhangyi, CHEN Fulong* (67)

Research progress and applications of cryptographic accumulators
 *MIAO Meixia, WU Panru, WANG Yunling* (78)

Low computation-complexity multi-scalar multiplication algorithm for the ECDSA
 *HUANG Hai, NA Ning, LIU Zhiwei, YU Bin, ZHAO Shilei* (92)

New class of complete permutation monomials over finite fields
 *HUANG Mengmeng, WU Gao fei* (102)

Analysis of the mean difference of intermediate-values in a white box SM4
 *ZHANG Yueyu, XU Dong, CAI Zhiqiang, CHEN Jie* (111)

A differential fault attack of fruit v2 and fruit 80
 *QIAO Qinglan, DONG Lihua* (121)

Information and Communications Engineering

Algebraic method for constructing Raptor-like multi-rate QC-LDPC codes
 *LI Hua'an, BAI Baoming, XU Hengzhou, CHEN Chao* (134)

Preference aware participant selection strategy for edge-cloud collaborative crowdsensing	WANG Ruyan, LIU Jia, HE Peng, CUI Yaping	(142)
Noveltask offloading solutions based on immune optimization immobile edge computing	ZHU Si feng, SUN Enlin, CHAI Zhengyi	(152)
Research on the spectrum defragmentation algorithm for the elastic optical network based on MCDM	WANG Jingyu, RAN Jinzhi, WANG Ping	(161)
Method for online reconstruction of marine monitoring data with sequential compressed sensing	LIU Ge, RUI Guosheng, TIAN Wenbiao, TIAN Runlan, WANG Xiaofeng	(173)
Parameter estimation of the near-field source using the PCA-BPalgorithm with the array error	WANG Le, ZHAO Peiyao, WANG Lanmei, WANG Guibao	(181)
Efficient implementation of unconditionally stable FDTD with the local eigenvalue solution	ZHAO Sihan, WEI Bing, HE Xinbo	(188)
Wide-range and high-accuracy four-phase DLL with the adaptive-bandwidth scheme	YANG Xue, LIU Fei, HUO Zongliang	(194)
Algorithm for gradient optimization of hybrid precoding based on DNN in the millimeter wave MIMO system	WANG Yong, WANG Xiyuan, REN Zeyang	(202)

Computer Science and Technology & Artificial Intelligence

Adaptive transmittance dehazing algorithm based on non-linear transformation	SUN Jingrong, XIE Linchang, DU Mengxin, LUO Liyan	(208)
Algorithmfor image inpainting in generative adversarial networks based on gated convolution	GAO Jie, HUO Zhiyong	(216)
Shape correspondence calculation using the unsupervised siamese functional maps network	YANG Jun, WANG Xingxing, LU Youpeng	(225)
Boundary-aware network for building extraction from remote sensing images	ZHANG Yan, WANG Xiangyu, ZHANG Zhongwei, SUN Yemei, LIU Shudong	(236)

中国无线电电子学、电信技术类核心期刊

本刊被国内外多家著名检索刊物或数据库固定收录

- ❖ 美国《工程索引》(Ei)(Compendex 数据库)
- ❖ 英国《科学文摘》(SA)(Inspec 数据库)
- ❖ 荷兰《文摘与引文数据库》(Scopus 数据库)
- ❖ 日本《科学技术文献速报》(CBST)
- ❖ 俄罗斯《文摘杂志》(PЖ)
- ❖ 美国《剑桥科学文摘》(CSA)
- ❖ 《中文核心期刊要目总览》(第一~八版)
- ❖ 中国科技论文统计源期刊(中国科技核心期刊)
- ❖ 中国科学引文数据库(CSCD)
- ❖ 中国知网(CNKI)
- ❖ 万方数据资源系统
- ❖ 中文期刊数据库(维普)
- ❖ 中国学术期刊文摘数据库
- ❖ 电子科技文摘
- ❖ 中国科技论文在线
- ❖ 中国数学文摘
- ❖ 超星期刊域出版平台

**JOURNAL OF
XIDIAN UNIVERSITY**

(Bimonthly)

(Started in Jun. 1955)

Vol. 49 No. 1 Feb. 2022

西安电子科技大学学报

Xi'an Dianzi Keji Daxue Xuebao

(双月刊)

(1955年6月创刊)

第49卷 第1期

Sponsored by	Xidian University
Editor-in-Chief	LIAO Guisheng
Edited by	Editorial Department of Journal of Xidian University
Printed by	Culture Communication Branch, Xi'an Changda Culture Development Co., Ltd.
Distributed by	China International Book Trading Corporation (P.O. Box 399, Beijing, China)
Address	P.O. Box 349, 2 South Taibai Road, Xi'an 710071, China
Tel	+86-29-88202853
E-mail	xuebao@mail.xidian.edu.cn
Website	http://journal.xidian.edu.cn/xdxb

主管单位	中华人民共和国教育部
主办单位	西安电子科技大学
主编	廖桂生
编辑出版	西安电子科技大学学报编辑部
印刷	西安长大文化发展有限公司文化传播分公司
发行范围	国内外公开发行
国内发行	西安电子科技大学学报编辑部
国外总发行	中国国际图书贸易总公司(北京399信箱)
订购	西安电子科技大学学报编辑部
出版日期	2022-02-20
通信地址	西安市太白南路2号349信箱
邮政编码	710071
电话	(029)88202853
电子邮箱	xuebao@mail.xidian.edu.cn
网址	http://journal.xidian.edu.cn/xdxb

ISSN 1001-2400
CN 61-1076/TN

国外代号: BM4116
定 价: 20.00 元

ISSN 1001-2400



9 771001 240221