

软件学报 *Software* *Journal of*

中国科学院软件研究所 主办
科学出版社 出版
中国计算机学会 会刊

Sponsored by Institute of Software, The Chinese Academy of Sciences

Published by Science Press

A Publication of the China Computer Federation



Editorial Board of *Journal of Software*

EDITOR-IN-CHIEF

FENG Yu-lin(冯玉琳) *Institute of Software, The Chinese Academy of Sciences (CAS), China*

ASSOCIATE EDITORS-IN-CHIEF

XU Jia-fu(徐家福) *Nanjing University, China*

LU Ru-qian(陆汝铃) *Institute of Mathematics, The Chinese Academy of Sciences (CAS), China*

JU Yu-lan(鞠玉兰, 专职) *Institute of Software, The Chinese Academy of Sciences (CAS), China*

MEMBERS (in alphabetic order)

Björner, Dines

Technical University of Denmark, Denmark

CHEN Huo-wang(陈火旺)

National Univ. of Defense Technology, China

Chin, Francis Yuk-Lun

University of Hong Kong, Hong Kong, China

Clarke, Edmund M.

Carnegie Mellon University, USA

DAI Guo-zhong(戴国忠)

Institute of Software, CAS, China

DONG Yun-mei(董隰美)

Institute of Software, CAS, China

GAO Wen(高文)

Institute of Computing Technology, CAS, China

HE Xin-gui(何新贵)

Beijing System Engineering Institute, China

Krieg-Brückner, Bernd

Universität Bremen, Germany

LI Guo-jie(李国杰)

National Research Center for Intelligent Computing Systems, CAS, China

LI Jian-zhong(李建中)

Harbin Institute of Technology, China

LI Shi-xian(李师贤)

Zhongshan University, China

LI Wei(李未)

Beijing University of Aeronautics and Astronautics, China

LIN Hui-min(林惠民)

Institute of Software, CAS, China

LIU Chun-nian(刘椿年)

Beijing University of Industry, China

LIU Da-you(刘大有)

Jilin University, China

LIU Ji-ren(刘积仁)

Northeastern University, China

LU Wei-ming(陆维明)

Institute of Mathematics, CAS, China

LUO Xiao-pei(罗晓沛)

Graduate School of University of Science and Technology of China, China

MA Song-de(马颂德)

Institute of Automation, CAS, China

Motiwalla, Juzar

Institute of Systems Science, National University of Singapore, Singapore

PENG Qun-sheng(彭群生)

Zhejiang University, China

SHAO Wei-zhong(邵维忠)

Beijing University, China

SHI Chun-yi(石纯一)

Tsinghua University, China

SHI Bai-le(施伯乐)

Fudan University, China

SUN Yong-qiang(孙永强)

Shanghai Jiaotong University, China

SUN Zhong-xiu(孙钟秀)

Nanjing University, China

TANG Ze-sheng(唐泽圣)

Tsinghua University, China

TANG Zhi-song(唐稚松)

(Tang C. S.)
Institute of Software, CAS, China

WANG Ding-xing(王鼎兴)

Tsinghua University, China

WANG Shan(王珊)

People's University of China, China

WANG Xuan(王选)

Beijing University, China

WEI Dao-zheng(魏道政)

Institute of Computing Technology, CAS, China

XIE Li(谢立)

Nanjing University, China

XU Kong-shi(许孔时)

Institute of Software, CAS, China

XU Zhuo-qun(许卓群)

Beijing University, China

YANG Fu-qing(杨芙清)

Beijing University, China

Yao, Andrew C.

Princeton University, USA

Yeh, Raymond T.

International Software System Inc., USA

ZHANG Bo(张钹)

Tsinghua University, China

ZHENG Nan-ning(郑南宁)

Xi'an Jiaotong University, China

ZHONG Xi-chang(钟锡昌)

Software Engineering Center, CAS, China

ZHOU Chao-chen(周巢尘)

UNU/IIST, Macau, China

ZHOU Long-xiang(周龙襄)

Institute of Mathematics, CAS, China

ZHOU Xi-ling(周锡龄)

Beijing Information Technology Institute, China

ZHU San-yuan(朱三元)

Shanghai Development Center for Computer Software Technology, China



中国科学院科学出版基金资助出版

软件学报

(Ruanjian Xuebao)



中国计算机学会会刊

第 11 卷第 10 期

2000 年 10 月

目 次

关于极小泄露证明协议的注记(英文)	蒋绍权	冯登国	卿斯汉 (1283)
并行密码体制的构造			卿斯汉 (1286)
截断差分-线性密码分析	贺也平	吴文玲	卿斯汉 (1294)
满足若干密码学性质的 S-盒的构造		刘晓晨	冯登国 (1299)
一种椭圆曲线签名方案与基于身份的签名协议	杨君辉	戴宗铎	杨栋毅 刘宏伟 (1303)
关于“停走”生成器输出序列的中心极限定理		黄晓英	李世取 (1307)
基于 Agent 的分布式入侵检测系统模型	马恒太	蒋建春	陈伟锋 卿斯汉 (1312)
强制访问控制在基于角色的安全系统中的实现	李立新	陈伟民	黄尚廉 (1320)
几个门限群签名方案的弱点		王贵林	卿斯汉 (1326)
新型 Rabin 签名方案	邱卫东	陈克非	白英彩 (1333)
一种新型的非否认协议			卿斯汉 (1338)
防欺诈的二方共享 RSA 密钥	王 宏	肖 鸿	肖国镇 (1344)
Needham-Schroeder 公钥协议的模型检测分析	张玉清	王 磊	肖国镇 吴建平 (1348)
Agent-BDI 逻辑		胡山立	石纯一 (1353)
联机手写中文速记符的自动识别	陈小革	俞铁城	戴汝为 (1361)
平面 NURBS 曲线及其 Offset 的双圆弧逼近		汪国平	孙家广 (1368)
基于服务质量水平的带宽分层自适应		万俊伟	卢锡城 (1375)
A-ADL: 一种多智能体系统体系结构描述语言	马俊涛	傅韶勇	刘积仁 (1382)
ORDBMS 中动态模式修改的研究		李红燕	李战怀 (1390)
基于印刷字符模糊结构分析的字符预分类方法	卢 达	谢铭培	浦 炜 (1397)
基于空间网格表面距离的插值曲面	尹宝才	孔德慧	吴思宁 (1405)
支持 OO 查询物理优化的二维字典签名方法		吴燕萍	施润身 (1412)
磺化过程 PLC 控制系统中模拟量的控制方法	李文兵		裴伟东 (1420)
敬告作者			(1325)
2001 年中国智能自动化会议(CIAC'2001)征文通知			(1332)
第 1 届中国 Rough 集与软计算学术研讨会(CRSSC'2001)征文通知			(1337)
2001 年全国开放式分布与并行计算学术会议征文通知			(1360)
第 1 届中国虚拟现实与可视化学术会议(CCVRV'01)征文通知			(1419)
全国第 3 次程序设计语言发展与教学学术会议征文通知			(1424)
征稿简则			(封 3)

征 稿 简 则

一、《软件学报》是中国科学院软件研究所主办的学术性刊物,创刊于1990年,主要报道计算机软件各领域的学术论文;尤其注重刊登能反映计算机软件发展方向的综述性文章;具有创造性的研究报告和研究简报;软件新理论、新方法、新技术介绍。为了促进学术、科研信息的交流,欢迎有兴趣者踊跃投稿。

二、本刊刊登内容:数理逻辑、自动机及其在计算机科学中的应用,可计算理论,算法复杂性理论、网论,算法设计与分析,思维科学,计算语言学,形式语言和语义理论,程序设计逻辑,软件开发形式技术,软件自动生成,人工智能,专家系统,知识工程,定理机器证明,自动翻译,计算机辅助软件工程、程序设计语言,操作系统,数据库,计算机网络,分布式系统,CAD/CAM/CAT/CAE,图形、图像、汉字、语言等信息处理,计算机辅助教学、软件新技术的应用开发等。

三、来稿要求和注意事项

1. 来稿要求论点明确,数据可靠,论证合理、层次分明,文字精炼。

2. 各类文稿具体要求如下:

学术论文:具有重大创新,有新的观点、见解,可推动或丰富该课题领域的研究与发展。

综 述:针对计算机科学技术的新兴或活跃领域,对国内外发展状况及趋势的全面、系统的综合评述。

短 文:具有创造性的见解或包含新见解,但不要求是完整的工作;与已有工作相比,有较大改进和提高。

技术报告:具有重大或较大的实用、推广价值,技术上先进、内容完整的研究报告。

简 报:技术上先进,对具有一定的实用或推广价值的研究成果(包括阶段成果)的扼要报道。

通 讯:有关本刊已发表文章的问题讨论或简短表达的新思想以及对学科发展的建议等。

3. 投稿需计算机打印稿一式3份,文章需要有200字左右的中文摘要和英文摘要,中、英文摘要均应包括题目、作者姓名、单位名称、摘要和关键词。

4. 来稿务必做到清稿定稿,文中的插图要精绘,图中的文字应书写清楚,注明图序、图题和图注。

5. 在文章中被引用的参考文献才能被列入文献表中,文献编号以在文中出现的先后为序,书写格式如下:

图书:[编号]作者姓名(姓在前,名在后,下同),书名,出版地:出版者,出版年,起止页码

期刊:[编号]作者姓名,文章题目,刊物名称,出版年,卷号(期号);起止页码

会议论文:[编号]作者姓名,论文题目,见:编者,论文集全名,出版地:出版者,出版年,起止页码

6. 为联系顺畅,请详细提供联系人的通讯地址、邮编、E-mail地址和联系电话。

7. 在收到作者投稿后,本刊及时返回给作者收稿回执。

8. 作者投稿后,自收到收稿回执之日起若6个月无消息,则可改投他刊。

9. 录用稿件将按收到修改稿的时间排序安排发表,来稿一经刊发,将酌致稿酬,并赠送样刊及单行本。

10. 不拟刊登稿件,本刊均有详细的审查意见返回给作者,但原稿恕不退还,请自留底稿。

11. 来稿应未正式发表且不存在一稿多投的情况,一旦发现违反上述规定者,将通知其所在单位或其导师。

12. 为帮助广大作者尽快地把其优秀研究成果发表在本刊上,本刊在1999年第8期第896页上的敬告作者中列举了一些在审稿过程中经常遇到的问题,建议作者在投稿之前,请阅读此栏目。

13. 稿件在排版后,校样将寄给作者校对,除录入排版错误外,文字一般不宜再作改动,为保证按时出版,请在指定日期内将校样返回,本刊可对来稿文字进行删改,但对实质性内容的修改,需征求作者同意。

14. 除印刷版外,本刊还有光盘版和网络版等电子版本,凡不同意将自己的文章以光盘版和网络版形式发表的作者,请在来稿时声明,否则视为同意将文稿的印刷版、光盘版和网络版版权转让给本刊编辑部。

15. 本刊欢迎国外或国际合作研究的英文稿件,对于此类稿件,本刊有优惠政策,投稿要求与中文稿件相同,并应附有中文题目、作者及单位、中文详细摘要及关键词。

16. 本刊欢迎作者通过E-mail投稿,投稿时请注意以下问题:① 请用Word或LaTex软件编辑稿件;② 请使用Attach功能传送,当文件过大时,请首先进行压缩(Winzip);③ 在传送稿件之前,请务必检查文件是否染有病毒,如有病毒,本刊拒绝接受投稿;④ 本刊在收到作者从网上投稿后的两三天之内,将从网上告诉作者收稿情况,在没有收到本刊的信息之前,可来E-mail询问,但不要反复传送稿件。

通讯地址:100080 北京 8718 信箱 中科院软件所《软件学报》编辑部

联系电话:(010)62562563 E-mail:jos@ns.ict.ac.cn

<http://www.ios.ac.cn/xuebao/sy.html>

欢迎订阅《软件学报》

《软件学报》由中国科学院软件研究所主办,科学出版社出版,是中国计算机学会会刊。《软件学报》及时反映我国计算机软件研究的学术水平和应用成果,是计算机软件工程、技术及应用人员最好的参考书。《软件学报》被美国工程信息公司 Ei Page One 数据库和 Ei Compendex 数据库、英国科学文摘(SA)、中国科学引文数据库等国内外多家检索机构收录,成为展示我国软件科技成果的一个重要的国际窗口。

《软件学报》在 2001 年将由原来的 144 页增版至 160 页,但价格不变,定价仍然为 20.00 元。

国内邮发代号:82-367 国外发行代号:M4628

欢迎读者到当地邮局订阅,也随时欢迎大家提出宝贵意见和建议,并踊跃投稿,为推动计算机事业的发展共同做出努力。

软件学报

Ruanjian Xuebao

(月刊,1990 年创刊)

第 11 卷 第 10 期 2000 年 10 月

Journal of Software

(monthly)

(Started in 1990)

Vol. 11 No. 10 Oct. 2000

编辑 《软件学报》编辑委员会
(北京海淀区中关村 邮编 100080)
北京 8718 信箱 中国科学院软件研究所
电话:(010)62562563
E-mail: jos@ns.ict.ac.cn
<http://www.ios.ac.cn/xuebao/sy.html>

主编 冯玉琳
主办单位 中国科学院软件研究所
出版 科学出版社
(北京东黄城根北街 16 号 邮编 100071)

印刷 北京林业大学印刷厂
总发行处 北京报刊发行局
订购处 全国各地邮局
国外总发行 中国国际图书贸易总公司
(北京 399 信箱 邮编 100044)

Edited by
Editorial Board of Journal of Software
(P. O. Box 8718, Beijing 100080, China)
E-mail: jos@ns.ict.ac.cn
<http://www.ios.ac.cn/xuebao/sy.html>

Editor-in-Chief: FENG Yu-lin
Sponsored by Institute of Software
The Chinese Academy of Sciences
Published by Science Press
(16 Donghuangchenggen North Street,
Beijing 100071, China)

Printed by Printing Factory of Beijing Forestry Univ.
Distributed by Beijing Bureau for Distribution of
Newspapers and Journals
Domestic All Local Post Offices in China
Foreign China International Book Trading
Corporation
(P. O. Box 399, Beijing 100044, China)

ISSN 1000-9825
CN 11-2560/TP

国内邮发代号:82-367
国外发行代号:M4628

广告经营许可证号:京东工商广字第 0706 号

定价:20.00 元

国内外公开发行人