

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(周龙骧)

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 8 期

2000 年 8 月

目 次

“软件新技术和新工具专辑”序	杨芙清 (995)
基于 XYZ/RE 的多媒体同步器自动构造方法	赵 琛 唐稚松 马华东 (996)
形式规约语言中函数运算的优化	张荣华 董樞美 (1003)
面向本体的需求分析	陆汝铃 金 芝 陈 刚 (1009)
基于移动 Agent 技术的构件软件框架研究	吕 建 张 鸣 廖 宇 陶先平 (1018)
可视化体系结构描述语言 XYZ/ADL	骆华俊 唐稚松 郑建丹 (1024)
基于产生式集划分的上下文无关语言句子生成	王泓皓 董樞美 (1030)
基于事件约束的分布式程序正确性测试	顾 庆 陈道蓄 于 勤 谢 立 孙钟秀 (1035)
一种从面向对象 Z 规约到代码的精细化演算方法	王云峰 庞 军 查 鸣 杨朝晖 郑国梁 (1041)
基于主动连接件的软件体系结构及其描述方法	张家晨 冯 铁 陈 伟 金淳兆 (1047)
一个面向分布式程序的测试系统框架	顾 庆 陈道蓄 韩 杰 谢 立 孙钟秀 (1053)
Mogent 系统的通信机制	陶先平 冯新宇 李 新 张冠群 吕 建 (1060)
基于重写技术的程序开发与验证	孙永强 陆朝俊 邵志清 (1066)
基于程序窗口推理的精细化演算	王云峰 李必信 庞 军 查 鸣 郑国梁 (1071)
基于框架和角色模型的软件体系结构规约	冯 铁 张家晨 陈 伟 金淳兆 (1078)
基于虚拟机的并行体绘制	邓俊辉 唐泽圣 (1087)
前馈网络的一种超线性收敛 BP 学习算法	梁久祯 何新贵 黄德双 (1094)
基于 DAG 图解-重构的机群系统静态调度算法	周佳祥 郑纬民 (1097)
Internet 上集成服务到区分服务的映射	郭国强 张尧学 (1105)
基于遗传算法的二叉树画树算法	黄竞伟 康立山 陈毓屏 (1112)
BDI Agent 解释器的研究和改进	路 军 王亚东 王晓龙 (1118)
用于口型识别的实时唇定位方法	姚鸿勋 高 文 李静梅 吕雅娟 王 瑞 (1126)
部分密钥托管的监听体制	蒋绍权 张玉峰 (1133)
全国第 3 次程序设计语言发展与教学学术会议征文通知	(1029)
第 3 届国际多模态接口会议(The Third International Conference on Multimodal Interfaces)征文通知	(1034)
书讯	(1040)
第 9 届全国多媒体技术学术会议征文通知	(1077)
2001 年全国开放式分布与并行计算学术会议征文通知	(1117)
敬告作者	(1132)

“软件新技术和新工具专辑”序

Foreword for the Special Issue on New Software Technology and Tools

“青鸟工程”是国家重点支持的大型软件工程项目。在经历了“六五”、“七五”、“八五”和“九五”攻关的历史阶段之后,已经积累了许多成果,为我国大型软件开发环境的应用和普及奠定了基础,并且已在不少实际应用领域取得了效果。20年来,我们以国家需要为动力,先后推出了青鸟I型、II型和III型3套软件开发平台,连续上了3个台阶。与此同时,我们清醒地看到,国际上软件工程技术的发展是很快的。青鸟工程必须在技术上体现自己的先进性,不仅与国际先进技术同步,而且还要有自己的创新,才能保持旺盛的生命力。因此,我们从“八五”攻关开始,在每一期攻关项目中都设置一个“软件新技术和新工具”专题,对这个专题的研究目标和内容不提任何特定要求,而只是要求该专题的各承担单位在软件新技术和新工具方面努力作出具有国际先进水平的创新,同时为青鸟技术和型号的下一步发展提供技术后备。10年的经验表明,我们的这个做法是成功的。

本专辑(第996页~1086页)刊登了青鸟“软件新技术和新工具”专题“九五”攻关第2期的部分成果,一共14篇文章。从这些文章中,读者不难看出该专题覆盖的范围是相当广的。从软件工程中生命周期的观点来看,它们覆盖了需求分析、规约获取、体系设计、代码生成和优化、程序测试、程序正确性验证等各个阶段。从新技术的特点来看,它们覆盖了多媒体、可视化、形式规约、分布式、本体论、移动Agent等多个领域。其中所涉及的理论问题包括可编程时态逻辑、上下文无关文法上的递归函数、同步理论、函数优化、重写方法等等。其中不仅有对国际新技术的跟踪和创新,也有我国独创技术的进一步开拓。在本刊上发表,既可以与国内外的计算机科学工作者交流,又可以作为向国家和有关课题下达及组织部门的一种汇报。愿“软件新技术和新工具”的研究在开拓创新的道路上不断前进。

杨芙清

北京大学计算机科学技术系教授、博士生导师、中国科学院院士

2000年6月15日

了来自托管代理的欺骗,故欺骗者只可能是用户.

致谢 作者衷心感谢导师戴宗铎教授的热忱关心与支持.

参考文献

- 1 Burmester M, Desmedt Y, Seberry J. Equitable key escrow with limited time span (or how to enforce time expiration cryptographically). In: Pei Ding-yi ed. *Advances in Cryptology-Asiacrypt'98*. LNCS 1514, New York: Springer-Verlag, 1998. 380~391
- 2 Bellare M, Goldwasser S. Verifiable Key escrow. In: *Proceedings of the 4th Annual Conference on Computer and Communications Security*. New York: ACM Press, 1997
- 3 Diffie, Hellman W M E. New direction in cryptography. *IEEE Transactions on Information Theory*, 1976, IT-22(6):644~654
- 4 Elgamal T. A subexponential-time algorithm for computing discrete algorithms over $GF(q^2)$. *IEEE Transactions on Information Theory*, 1985, IT-31(4):473~481

Partial Key Escrow Monitoring Scheme

JIANG Shao-quan ZHANG Yu-feng

(State Key Laboratory of Information Security Graduate School University of Science and Technology of China Beijing 100039)

Abstract During (partial) key escrow, monitoring is a vital phase. So how to monitor a user safely and efficiently is a very important problem. According to the known monitoring schemes, after a user is monitored, his secret key is known. It is unfair to an honest user. In this paper, the authors propose a monitoring scheme of a typical partial key escrow scheme. In this scheme, the escrowed key of a user is not compromised even if the user has been monitored for many times.

Key words Monitor scheme, trustee, law enforce agency, secret key, security.

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:4628M

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 8 期 2000 年 8 月

Journal of Software

(monthly)

(Started in 1990)

Vol. 11 No. 8 Aug. 2000

32

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 100717)

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 100717, 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)

ISSN1000-9825
CN11-2560/TP

国内邮发代号:82-367
国外发行代号:4628M

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