

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Marina Gavrilova Osvaldo Gervasi
Vipin Kumar C.J. Kenneth Tan
David Taniar Antonio Laganà
Youngsong Mun Hyunseung Choo (Eds.)

Computational Science and Its Applications – ICCSA 2006

International Conference
Glasgow, UK, May 8-11, 2006
Proceedings, Part III

 Springer

Volume Editors

Marina Gavrilova
University of Calgary, Canada
E-mail: marina@cpsc.ucalgary.ca

Osvaldo Gervasi
University of Perugia, Italy
E-mail: ogervasi@computer.org

Vipin Kumar
University of Minnesota, Minneapolis, USA
E-mail: kumar@cs.umn.edu

C.J. Kenneth Tan
OptimaNumerics Ltd., Belfast, UK
E-mail: cjtan@optimanumerics.com

David Taniar
Monash University, Clayton, Australia
E-mail: david.taniar@infotech.monash.edu.au

Antonio Laganà
University of Perugia, Italy
E-mail: lag@unipg.it

Youngsong Mun
SoongSil University, Seoul, Korea
E-mail: mun@computing.soongsil.ac.kr

Hyunseung Choo
Sungkyunkwan University, Suwon, Korea
E-mail: choo@ece.skku.ac.kr

Library of Congress Control Number: 2006925086

CR Subject Classification (1998): F, D, G, H, I, J, C.2-3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-34075-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-34075-1 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11751595 06/3142 5 4 3 2 1 0

Preface

This five-volume set was compiled following the 2006 International Conference on Computational Science and its Applications, ICCSA 2006, held in Glasgow, UK, during May 8–11, 2006. It represents the outstanding collection of almost 664 refereed papers selected from over 2,450 submissions to ICCSA 2006.

Computational science has firmly established itself as a vital part of many scientific investigations, affecting researchers and practitioners in areas ranging from applications such as aerospace and automotive, to emerging technologies such as bioinformatics and nanotechnologies, to core disciplines such as mathematics, physics, and chemistry. Due to the sheer size of many challenges in computational science, the use of supercomputing, parallel processing, and sophisticated algorithms is inevitable and becomes a part of fundamental theoretical research as well as endeavors in emerging fields. Together, these far-reaching scientific areas contributed to shaping this conference in the realms of state-of-the-art computational science research and applications, encompassing the facilitating theoretical foundations and the innovative applications of such results in other areas.

The topics of the refereed papers span all the traditional as well as emerging computational science realms, and are structured according to the five major conference themes:

- Computational Methods, Algorithms and Applications
- High-Performance Technical Computing and Networks
- Advanced and Emerging Applications
- Geometric Modeling, Graphics and Visualization
- Information Systems and Information Technologies

Moreover, submissions from 31 workshops and technical sessions in areas such as information security, mobile communication, grid computing, modeling, optimization, computational geometry, virtual reality, symbolic computations, molecular structures, Web systems and intelligence, spatial analysis, bioinformatics and geocomputations, are included in this publication. The continuous support of computational science researchers has helped ICCSA to become a firmly established forum in the area of scientific computing.

We recognize the contribution of the International Steering Committee and sincerely thank the International Program Committee for their tremendous support in putting this conference together, the near 800 referees for their diligent work, and the IEE European Chapter for their generous assistance in hosting the event.

We also thank our sponsors for their continuous support without which this conference would not be possible.

Finally, we thank all authors for their submissions and all invited speakers and conference attendants for making the ICCSA Conference truly one of the premium events on the scientific community scene, facilitating exchange of ideas, fostering new collaborations, and shaping the future of computational science.

May 2006

Marina L. Gavrilova
Oswaldo Gervasi

on behalf of the co-editors
Vipin Kumar
Chih Jeng Kenneth Tan
David Taniar
Antonio Laganà
Youngsong Mun
Hyunseung Choo

Organization

ICCSA 2006 was organized by the Institute of Electrical Engineers (IEE)(UK), the University of Perugia (Italy), Calgary University (Canada) and Minnesota University (USA).

Conference Chairs

Vipin Kumar (University of Minnesota, Minneapolis, USA), Honorary Chair
Marina L. Gavrilova (University of Calgary, Calgary, Canada), Conference
Co-chair, Scientific
Osvaldo Gervasi (University of Perugia, Perugia, Italy), Conference Co-chair,
Program

Steering Committee

Vipin Kumar (University of Minnesota, USA)
Marina L. Gavrilova (University of Calgary, Canada)
Osvaldo Gervasi (University of Perugia, Perugia, Italy)
C. J. Kenneth Tan (OptimaNumerics, UK)
Alexander V. Bogdanov (Institute for High Performance Computing
and Data Bases, Russia)
Hyunseung Choo (Sungkyunkwan University, Korea)
Andres Iglesias (University of Cantabria, Spain)
Antonio Laganà (University of Perugia, Italy)
Heow-Pueh Lee (Institute of High Performance Computing, Singapore)
Youngsong Mun (Soongsil University, Korea)
David Taniar (Monash University, Australia)

Workshop Organizers

Applied Cryptography and Information Security (ACIS 2006)

Sherman S.M. Chow (New York University, USA)
Joseph K. Liu (University of Bristol, UK)
Patrick Tsang (Dartmouth College, USA)
Duncan S Wong (City University of Hong Kong, Hong Kong)

Approaches or Methods of Security Engineering (AMSE 2006)

Haeng Kon Kim (Catholic University of Daegu, Korea)
Tai-hoon Kim (Korea Information Security Agency, Korea)

Authentication, Authorization and Accounting (AAA 2006)
Haeng Kon Kim (Catholic University of Daegu, Korea)

Computational Geometry and Applications (CGA 2006)
Marina Gavrilova (University of Calgary, Calgary, Canada)

Data Storage Devices and Systems (DSDS 2006)
Yeonseung Ryu (Myongji University, Korea)
Junho Shim (Sookmyong Womens University, Korea)
Youjip Won (Hanyang University, Korea)
Yongik Eom (Seongkyunkwan University, Korea)

Embedded System for Ubiquitous Computing (ESUC 2006)
Tei-Wei Kuo (National Taiwan University, Taiwan)
Jiman Hong (Kwangwoon University, Korea)

4th Technical Session on Computer Graphics (TSCG 2006)
Andres Iglesias (University of Cantabria, Spain)
Deok-Soo Kim (Hanyang University, Korea)

GeoComputation (GC 2006)
Yong Xue (London Metropolitan University, UK)

Image Processing and Computer Vision (IPCV 2006)
Jiawan Zhang (Tianjin University, China)

**Intelligent Services and the Synchronization in Mobile
Multimedia Networks (ISS 2006)**
Dong Chun Lee (Howon University, Korea)
Kuinam J Kim (Kyonggi University, Korea)

**Integrated Analysis and Intelligent Design Technology
(IAIDT 2006)**
Jae-Woo Lee (Konkuk University, Korea)

Information Systems Information Technologies (ISIT 2006)
Youngsong Mun (Soongsil University, Korea)

Information Engineering and Applications in Ubiquitous Computing Environments (IEAUCE 2006)

Sangkyun Kim (Yonsei University, Korea)

Hong Joo Lee (Dankook University, Korea)

Internet Communications Security (WICS 2006)

Sierra-Camara José Maria (University Carlos III of Madrid, Spain)

Mobile Communications (MC 2006)

Hyunseung Choo (Sungkyunkwan University, Korea)

Modelling Complex Systems (MCS 2006)

John Burns (Dublin University, Ireland)

Ruili Wang (Massey University, New Zealand)

Modelling of Location Management in Mobile Information Systems (MLM 2006)

Dong Chun Lee (Howon University, Korea)

Numerical Integration and Applications (NIA 2006)

Elise de Doncker (Western Michigan University, USA)

Specific Aspects of Computational Physics and Wavelet Analysis for Modelling Suddenly-Emerging Phenomena in Nonlinear Physics, and Nonlinear Applied Mathematics (PULSES 2006)

Carlo Cattani (University of Salerno, Italy)

Cristian Toma (Titu Maiorescu University, Romania)

Structures and Molecular Processes (SMP 2006)

Antonio Laganà (University of Perugia, Perugia, Italy)

Optimization: Theories and Applications (OTA 2006)

Dong-Ho Lee (Hanyang University, Korea)

Deok-Soo Kim (Hanyang University, Korea)

Ertugrul Karsak (Galatasaray University, Turkey)

Parallel and Distributed Computing (PDC 2006)

Jiawan Zhang (Tianjin University, China)

Pattern Recognition and Ubiquitous Computing (PRUC 2006)

Jinok Kim (Daegu Haany University, Korea)

Security Issues on Grid/Distributed Computing Systems (SIGDCS 2006)

Tai-Hoon Kim (Korea Information Security Agency, Korea)

Technologies and Techniques for Distributed Data Mining (TTDDM 2006)

Mark Baker (Portsmouth University, UK)

Bob Nichol (Portsmouth University, UK)

Ubiquitous Web Systems and Intelligence (UWSI 2006)

David Taniar (Monash University, Australia)

Eric Pardede (La Trobe University, Australia)

Ubiquitous Application and Security Service (UASS 2006)

Yeong-Deok Kim (Woosong University, Korea)

Visual Computing and Multimedia (VCM 2006)

Abel J. P. Gomes (University Beira Interior, Portugal)

Virtual Reality in Scientific Applications and Learning (VRSAL 2006)

Oswaldo Gervasi (University of Perugia, Italy)

Antonio Riganelli (University of Perugia, Italy)

Web-Based Learning (WBL 2006)

Woochun Jun Seoul (National University of Education, Korea)

Program Committee

Jemal Abawajy (Deakin University, Australia)
Kenny Adamson (EZ-DSP, UK)
Srinivas Aluru (Iowa State University, USA)
Mir Atiqullah (Saint Louis University, USA)
Frank Baetke (Hewlett Packard, USA)
Mark Baker (Portsmouth University, UK)
Young-Cheol Bang (Korea Polytechnic University, Korea)
David Bell (Queen's University of Belfast, UK)
Stefania Bertazzon (University of Calgary, Canada)
Sergei Bepamyatnikh (Duke University, USA)
J. A. Rod Blais (University of Calgary, Canada)
Alexander V. Bogdanov (Institute for High Performance Computing
and Data Bases, Russia)
Peter Brezany (University of Vienna, Austria)
Herve Bronnimann (Polytechnic University, NY, USA)
John Brooke (University of Manchester, UK)
Martin Buecker (Aachen University, Germany)
Rajkumar Buyya (University of Melbourne, Australia)
Jose Sierra-Camara (University Carlos III of Madrid, Spain)
Shyi-Ming Chen (National Taiwan University of Science and Technology,
Taiwan)
YoungSik Choi (University of Missouri, USA)
Hyunseung Choo (Sungkyunkwan University, Korea)
Bastien Chopard (University of Geneva, Switzerland)
Min Young Chung (Sungkyunkwan University, Korea)
Yiannis Cotronis (University of Athens, Greece)
Danny Crookes (Queen's University of Belfast, UK)
Jose C. Cunha (New University of Lisbon, Portugal)
Brian J. d'Auriol (University of Texas at El Paso, USA)
Alexander Degtyarev (Institute for High Performance Computing
and Data Bases, Russia)
Frederic Desprez (INRIA, France)
Tom Dhaene (University of Antwerp, Belgium)
Beniamino Di Martino (Second University of Naples, Italy)
Hassan Diab (American University of Beirut, Lebanon)
Ivan Dimov (Bulgarian Academy of Sciences, Bulgaria)
Iain Duff (Rutherford Appleton Laboratory, UK and CERFACS, France)
Thom Dunning (NCSA and University of Illinois, USA)
Fabrizio Gagliardi (Microsoft, USA)
Marina L. Gavrilova (University of Calgary, Canada)
Michael Gerndt (Technical University of Munich, Germany)
Osvaldo Gervasi (University of Perugia, Italy)
Bob Gingold (Australian National University, Australia)
James Glimm (SUNY Stony Brook, USA)

Christopher Gold (Hong Kong Polytechnic University, Hong Kong)
Yuriy Gorbachev (Institute of High Performance Computing
and Information Systems, Russia)
Andrzej Goscinski (Deakin University, Australia)
Jin Hai (Huazhong University of Science and Technology, China)
Ladislav Hluchy (Slovak Academy of Science, Slovakia)
Xiaohua Hu (Drexel University, USA)
Eui-Nam John Huh (Seoul Women's University, Korea)
Shen Hong (Japan Advanced Institute of Science and Technology, Japan)
Paul Hovland (Argonne National Laboratory, USA)
Andres Iglesias (University of Cantabria, Spain)
Peter K. Jimack (University of Leeds, UK)
In-Jae Jeong (Hanyang University, Korea)
Chris Johnson (University of Utah, USA)
Benjoe A. Juliano (California State University at Chico, USA)
Peter Kacsuk (MTA SZTAKI Research Institute, Hungary)
Kyung Wo Kang (KAIST, Korea)
Carl Kesselman (USC/ Information Sciences Institute, USA)
Daniel Kidger (Quadrics, UK)
Haeng Kon Kim (Catholic University of Daegu, Korea)
Jin Suk Kim (KAIST, Korea)
Tai-Hoon Kim (Korea Information Security Agency, Korea)
Yoonhee Kim (Syracuse University, USA)
Mike Kirby (University of Utah, USA)
Dieter Kranzmueller (Johannes Kepler University Linz, Austria)
Deok-Soo Kim (Hanyang University, Korea)
Vipin Kumar (University of Minnesota, USA)
Domenico Laforenza (Italian National Research Council, Italy)
Antonio Laganà (University of Perugia, Italy)
Joseph Landman (Scalable Informatics LLC, USA)
Francis Lau (The University of Hong Kong, Hong Kong)
Bong Hwan Lee (Texas A&M University, USA)
Dong Chun Lee (Howon University, Korea)
Dong-Ho Lee (Institute of High Performance Computing, Singapore)
Sang Yoon Lee (Georgia Institute of Technology, USA)
Tae-Jin Lee (Sungkyunkwan University, Korea)
Bogdan Lesyng (ICM Warszawa, Poland)
Zhongze Li (Chinese Academy of Sciences, China)
Laurence Liew (Scalable Systems Pte, Singapore)
David Lombard (Intel Corporation, USA)
Emilio Luque (University Autònoma of Barcelona, Spain)
Michael Mascagni (Florida State University, USA)
Graham Megson (University of Reading, UK)
John G. Michopoulos (US Naval Research Laboratory, USA)
Edward Moreno (Euripides Foundation of Marilia, Brazil)

Youngsong Mun (Soongsil University, Korea)
Jiri Nedoma (Academy of Sciences of the Czech Republic, Czech Republic)
Genri Norman (Russian Academy of Sciences, Russia)
Stephan Olariu (Old Dominion University, USA)
Salvatore Orlando (University of Venice, Italy)
Robert Panoff (Shodor Education Foundation, USA)
Marcin Paprzycki (Oklahoma State University, USA)
Gyung-Leen Park (University of Texas, USA)
Ron Perrott (Queen's University of Belfast, UK)
Dimitri Plemenos (University of Limoges, France)
Richard Ramaroson (ONERA, France)
Rosemary Renaut (Arizona State University, USA)
Reneé S. Renner (California State University at Chico, USA)
Paul Roe (Queensland University of Technology, Australia)
Alexey S. Rodionov (Russian Academy of Sciences, Russia)
Heather J. Ruskin (Dublin City University, Ireland)
Ole Saastad (Scali, Norway)
Muhammad Sarfraz (King Fahd University of Petroleum and Minerals,
Saudi Arabia)
Edward Seidel (Louisiana State University, USA and Albert-Einstein-Institut,
Potsdam, Germany)
Jie Shen (University of Michigan, USA)
Dale Shires (US Army Research Laboratory, USA)
Vaclav Skala (University of West Bohemia, Czech Republic)
Burton Smith (Cray, USA)
Masha Sosonkina (Ames Laboratory, USA)
Alexei Sourin (Nanyang Technological University, Singapore)
Elena Stankova (Institute for High Performance Computing and Data Bases,
Russia)
Gunther Stuer (University of Antwerp, Belgium)
Kokichi Sugihara (University of Tokyo, Japan)
Boleslaw Szymanski (Rensselaer Polytechnic Institute, USA)
Ryszard Tadeusiewicz (AGH University of Science and Technology, Poland)
C.J. Kenneth Tan (OptimaNumerics, UK and Queen's University
of Belfast, UK)
David Taniar (Monash University, Australia)
John Taylor (Streamline Computing, UK)
Ruppa K. Thulasiram (University of Manitoba, Canada)
Pavel Tvrdik (Czech Technical University, Czech Republic)
Putchong Uthayopas (Kasetsart University, Thailand)
Mario Valle (Swiss National Supercomputing Centre, Switzerland)
Marco Vanneschi (University of Pisa, Italy)
Piero Giorgio Verdini (University of Pisa and Istituto Nazionale di Fisica
Nucleare, Italy)
Jesus Vigo-Aguar (University of Salamanca, Spain)

Jens Volkert (University of Linz, Austria)
Koichi Wada (University of Tsukuba, Japan)
Stephen Wismath (University of Lethbridge, Canada)
Kevin Wadleigh (Hewlett Packard, USA)
Jerzy Wasniewski (Technical University of Denmark, Denmark)
Paul Watson (University of Newcastle Upon Tyne, UK)
Jan Weglarz (Poznan University of Technology, Poland)
Tim Wilkens (Advanced Micro Devices, USA)
Roman Wyrzykowski (Technical University of Czestochowa, Poland)
Jinchao Xu (Pennsylvania State University, USA)
Chee Yap (New York University, USA)
Osman Yasar (SUNY at Brockport, USA)
George Yee (National Research Council and Carleton University, Canada)
Yong Xue (Chinese Academy of Sciences, China)
Igor Zacharov (SGI Europe, Switzerland)
Xiaodong Zhang (College of William and Mary, USA)
Aledander Zhmakin (SoftImpact, Russia)
Krzysztof Zielinski (ICS UST / CYFRONET, Poland)
Albert Zomaya (University of Sydney, Australia)

Sponsoring Organizations

Institute of Electrical Engineers (IEE), UK
University of Perugia, Italy
University of Calgary, Canada
University of Minnesota, USA
Queen's University of Belfast, UK
The European Research Consortium for Informatics and Mathematics (ERCIM)
The 6th European Framework Project "Distributed European Infrastructure
for Supercomputing Applications" (DEISA)
OptimaNumerics, UK
INTEL
AMD

Table of Contents – Part III

Workshop on Approaches or Methods of Security Engineering (AMSE 2006, Sess. A)

A Security Requirement Management Database Based on ISO/IEC 15408 <i>Shoichi Morimoto, Daisuke Horie, Jingde Cheng</i>	1
Development of Committee Neural Network for Computer Access Security System <i>A. Sermet Anagun</i>	11
C-TOBI-Based Pitch Accent Prediction Using Maximum-Entropy Model <i>Byeongchang Kim, Gary Geunbae Lee</i>	21
Design and Fabrication of Security and Home Automation System <i>Eung Soo Kim, Min Sung Kim</i>	31
PGNIDS(Pattern-Graph Based Network Intrusion Detection System) Design <i>Byung-kwan Lee, Seung-hae Yang, Dong-Hyuck Kwon, Dai-Youn Kim</i>	38
Experiments and Hardware Countermeasures on Power Analysis Attacks <i>ManKi Ahn, HoonJae Lee</i>	48
Information System Modeling for Analysis of Propagation Effects and Levels of Damage <i>InJung Kim, YoonJung Chung, YoungGyo Lee, Eul Gyu Im, Dongho Won</i>	54
A Belt-Zone Method for Decreasing Control Messages in Ad Hoc Networks <i>Youngrag Kim, JaeYoun Jung, Seunghwan Lee, Chonggun Kim</i>	64
A VLSM Address Management Method for Variable IP Subnetting <i>SeongKwon Cheon, DongXue Jin, ChongGun Kim</i>	73
SDSEM: Software Development Success Evolution Model <i>Haeng-Kon Kim, Sang-Yong Byun</i>	84

A Robust Routing Protocol by a Substitute Local Path in Ad Hoc Networks <i>Mary Wu, SangJoon Jung, Seunghwan Lee, Chonggun Kim</i>	93
Power Efficient Wireless LAN Using 16-State Trellis-Coded Modulation for Infrared Communications <i>Hae Geun Kim</i>	104
The Design and Implementation of Real-Time Environment Monitoring Systems Based on Wireless Sensor Networks <i>Kyung-Hoon Jung, Seok-Cheol Lee, Hyun-Suk Hwang, Chang-Soo Kim</i>	115
Ontology-Based Information Search in the Real World Using Web Services <i>Hyun-Suk Hwang, Kyoo-Seok Park, Chang-Soo Kim</i>	125
An Active Node Set Maintenance Scheme for Distributed Sensor Networks <i>Tae-Young Byun, Minsu Kim, Sungho Hwang, Sung-Eok Jeon</i>	134
Intelligent Information Search Mechanism Using Filtering and NFC Based on Multi-agents in the Distributed Environment <i>Subong Yi, Bobby D. Gerardo, Young-Seok Lee, Jaewan Lee</i>	144
Network Anomaly Behavior Detection Using an Adaptive Multiplex Detector <i>Misun Kim, Minsoo Kim, JaeHyun Seo</i>	154
Applying Product Line to the Embedded Systems <i>Haeng-Kon Kim</i>	163
Enhanced Fuzzy Single Layer Learning Algorithm Using Automatic Tuning of Threshold <i>Kwang-Baek Kim, Byung-Kwan Lee, Soon-Ho Kim</i>	172
Optimization of Location Management in the Distributed Location-Based Services Using Collaborative Agents <i>Romeo Mark A. Mateo, Jaewan Lee, Hyunho Yang</i>	178
Design of H.264/AVC-Based Software Decoder for Mobile Phone <i>Hyung-Su Jeon, Hye-Min Noh, Cheol-Jung Yoo, Ok-Bae Chang</i>	188
Transforming a Legacy System into Components <i>Haeng-Kon Kim, Youn-Ky Chung</i>	198

Pseudorandom Number Generator Using Optimal Normal Basis <i>Injoo Jang, Hyeong Seon Yoo</i>	206
Efficient Nonce-Based Authentication Scheme Using Token-Update <i>Wenbo Shi, Hyeong Seon Yoo</i>	213
An Efficient Management of Network Traffic Performance Using Framework-Based Performance Management Tool <i>Seong-Man Choi, Cheol-Jung Yoo, Ok-Bae Chang</i>	222
A Prediction Method of Network Traffic Using Time Series Models <i>Sangjoon Jung, Chonggun Kim, Younky Chung</i>	234
An Obstacle Avoidance Method for Chaotic Robots Using Angular Degree Limitations <i>Youngchul Bae, MalRey Lee, Thomas M. Gatton</i>	244
Intersection Simulation System Based on Traffic Flow Control Framework <i>Chang-Sun Shin, Dong-In Ahn, Hyun Yoe, Su-Chong Joo</i>	251
A HIICA(Highly-Improved Intra CA) Design for M-Commerce <i>Byung-kwan Lee, Chang-min Kim, Dae-won Shin, Seung-hae Yang</i>	261
Highly Reliable Synchronous Stream Cipher System for Link Encryption <i>HoonJae Lee</i>	269
Recognition of Concrete Surface Cracks Using ART2-Based Radial Basis Function Neural Network <i>Kwang-Baek Kim, Hwang-Kyu Yang, Sang-Ho Ahn</i>	279
Hybrid Image Mosaic Construction Using the Hierarchical Method <i>Oh-Hyung Kang, Ji-Hyun Lee, Yang-Won Rhee</i>	287
Workshop on Applied Cryptography and Information Security (ACIS 2006)	
Public Key Encryption with Keyword Search Based on K-Resilient IBE <i>Dalia Khader</i>	298
A Generic Construction of Secure Signatures Without Random Oracles <i>Jin Li, Yuen-Yan Chan, Yanming Wang</i>	309

A Separation Between Selective and Full-Identity Security Notions for Identity-Based Encryption <i>David Galindo</i>	318
Traceable Signature: Better Efficiency and Beyond <i>He Ge, Stephen R. Tate</i>	327
On the TYS Signature Scheme <i>Marc Joye, Hung-Mei Lin</i>	338
Efficient Partially Blind Signatures with Provable Security <i>Qianhong Wu, Willy Susilo, Yi Mu, Fanguo Zhang</i>	345
A Framework for Robust Group Key Agreement <i>Jens-Matthias Bohli</i>	355
BGN Authentication and Its Extension to Convey Message Commitments <i>Yuen-Yan Chan, Jin Li</i>	365
New Security Problem in RFID Systems “Tag Killing” <i>Dong-Guk Han, Tsuyoshi Takagi, Ho Won Kim, Kyo Il Chung</i>	375
A Model for Security Vulnerability Pattern <i>Hyungwoo Kang, Kibom Kim, Soonjwa Hong, Dong Hoon Lee</i>	385
A New Timestamping Scheme Based on Skip Lists <i>Kaouthar Blibech, Alban Gabillon</i>	395
A Semi-fragile Watermarking Scheme Based on SVD and VQ Techniques <i>Hsien-Chu Wu, Chuan-Po Yeh, Chwei-Shyong Tsai</i>	406
New Constructions of Universal Hash Functions Based on Function Sums <i>Khoongming Khoo, Swee-Huay Heng</i>	416
Analysis of Fast Blockcipher-Based Hash Functions <i>Martin Stanek</i>	426
Application of LFSRs for Parallel Sequence Generation in Cryptologic Algorithms <i>Sourav Mukhopadhyay, Palash Sarkar</i>	436
Provable Security for an RC6-like Structure and a MISTY-FO-like Structure Against Differential Cryptanalysis <i>Changhoon Lee, Jongsung Kim, Jaechul Sung, Seokhie Hong, Sangjin Lee</i>	446

Design and Implementation of an FPGA-Based 1.452-Gbps Non-pipelined AES Architecture <i>Ignacio Algreto-Badillo, Claudia Feregrino-Urbe, René Cumplido . . .</i>	456
--	-----

Workshop on Internet Communications Security (WICS 2006)

Security Weaknesses in Two Proxy Signature Schemes <i>Jiqiang Lu</i>	466
A Proposal of Extension of FMS-Based Mechanism to Find Attack Paths <i>Byung-Ryong Kim, Ki-Chang Kim</i>	476
Comparative Analysis of IPv6 VPN Transition in NEMO Environments <i>Hyung-Jin Lim, Dong-Young Lee, Tai-Myoung Chung</i>	486
A Short-Lived Key Selection Approach to Authenticate Data Origin of Multimedia Stream <i>Namhi Kang, Younghan Kim</i>	497
Weakest Link Attack on Single Sign-On and Its Case in SAML V2.0 Web SSO <i>Yuen-Yan Chan</i>	507
An Inter-domain Key Agreement Protocol Using Weak Passwords <i>Youngsook Lee, Junghyun Nam, Dongho Won</i>	517
A Practical Solution for Distribution Rights Protection in Multicast Environments <i>Josep Pegueroles, Marcel Fernández, Francisco Rico-Novella, Miguel Soriano</i>	527
Audit-Based Access Control in Nomadic Wireless Environments <i>Francesco Palmieri, Ugo Fiore</i>	537

Workshop on Optimization: Theories and Applications (OTA 2006)

Cost – Time Trade Off Models Application to Crashing Flow Shop Scheduling Problems <i>Morteza Bagherpour, Siamak Noori, S. Jafar Sadjadi</i>	546
--	-----

The ASALB Problem with Processing Alternatives Involving Different Tasks: Definition, Formalization and Resolution <i>Liliana Capacho, Rafael Pastor</i>	554
Satisfying Constraints for Locating Export Containers in Port Container Terminals <i>Kap Hwan Kim, Jong-Sool Lee</i>	564
A Price Discrimination Modeling Using Geometric Programming <i>Seyed J. Sadjadi, M. Ziaee</i>	574
Hybrid Evolutionary Algorithms for the Rectilinear Steiner Tree Problem Using Fitness Estimation <i>Byounghak Yang</i>	581
Data Reduction for Instance-Based Learning Using Entropy-Based Partitioning <i>Seung-Hyun Son, Jae-Yearn Kim</i>	590
Coordinated Inventory Models with Compensation Policy in a Three Level Supply Chain <i>Jeong Hun Lee, Il Kyeong Moon</i>	600
Using Constraint Satisfaction Approach to Solve the Capacity Allocation Problem for Photolithography Area <i>Shu-Hsing Chung, Chun-Ying Huang, Amy Hsin-I Lee</i>	610
Scheduling an R&D Project with Quality-Dependent Time Slots <i>Mario Vanhoucke</i>	621
The Bottleneck Tree Alignment Problems <i>Yen Hung Chen, Chuan Yi Tang</i>	631
Performance Study of a Genetic Algorithm for Sequencing in Mixed Model Non-permutation Flowshops Using Constrained Buffers <i>Gerrit Färber, Anna M. Coves Moreno</i>	638
Optimizing Relative Weights of Alternatives with Fuzzy Comparative Judgment <i>Chung-Hsing Yeh, Yu-Hern Chang</i>	649
Model and Solution for the Multilevel Production-Inventory System Before Ironmaking in Shanghai Baoshan Iron and Steel Complex <i>Guoli Liu, Lixin Tang</i>	659

A Coordination Algorithm for Deciding Order-Up-To Level of a Serial Supply Chain in an Uncertain Environment <i>Kung-Jeng Wang, Wen-Hai Chih, Ken Hwang</i>	668
Optimization of Performance of Genetic Algorithm for 0-1 Knapsack Problems Using Taguchi Method <i>A.S. Anagun, T. Sarac</i>	678
Truck Dock Assignment Problem with Time Windows and Capacity Constraint in Transshipment Network Through Crossdocks <i>Andrew Lim, Hong Ma, Zhaowei Miao</i>	688
An Entropy Based Group Setup Strategy for PCB Assembly <i>In-Jae Jeong</i>	698
Cross-Facility Production and Transportation Planning Problem with Perishable Inventory <i>Sandra Duni Ekşioğlu, Mingzhou Jin</i>	708
A Unified Framework for the Analysis of M/G/1 Queue Controlled by Workload <i>Ho Woo Lee, Se Won Lee, Won Ju Seo, Sahng Hoon Cheon, Jongwoo Jeon</i>	718
Tabu Search Heuristics for Parallel Machine Scheduling with Sequence-Dependent Setup and Ready Times <i>Sang-Il Kim, Hyun-Seon Choi, Dong-Ho Lee</i>	728
The Maximum Integer Multiterminal Flow Problem <i>Cédric Bentz</i>	738
Routing with Early Ordering for Just-In-Time Manufacturing Systems <i>Mingzhou Jin, Kai Liu, Burak Eksioğlu</i>	748
A Variant of the Constant Step Rule for Approximate Subgradient Methods over Nonlinear Networks <i>Eugenio Mijangos</i>	757
On the Optimal Buffer Allocation of an FMS with Finite In-Process Buffers <i>Soo-Tae Kwon</i>	767
Optimization Problems in the Simulation of Multifactor Portfolio Credit Risk <i>Wanmo Kang, Kyungsik Lee</i>	777

Two-Server Network Disconnection Problem <i>Byung-Cheon Choi, Sung-Pil Hong</i>	785
One-Sided Monge TSP Is NP-Hard <i>Vladimir Deineko, Alexander Tiskin</i>	793
On Direct Methods for Lexicographic Min-Max Optimization <i>Włodzimierz Ogryczak, Tomasz Śliwiński</i>	802
Multivariate Convex Approximation and Least-Norm Convex Data-Smoothing <i>Alex Y.D. Siem, Dick den Hertog, Aswin L. Hoffmann</i>	812
Linear Convergence of Tatônnement in a Bertrand Oligopoly <i>Guillermo Gallego, Woonghee Tim Huh, Wanmo Kang, Robert Phillips</i>	822
Design for Using Purpose of Assembly-Group <i>Hak-Soo Mok, Chang-Hyo Han, Chan-Hyoung Lim, John-Hee Hong, Jong-Rae Cho</i>	832
A Conditional Gaussian Martingale Algorithm for Global Optimization <i>Manuel L. Esquivel</i>	841
Finding the Number of Clusters Minimizing Energy Consumption of Wireless Sensor Networks <i>Hyunsoo Kim, Hee Yong Youn</i>	852
A Two-Echelon Deteriorating Production-Inventory Newsboy Model with Imperfect Production Process <i>Hui-Ming Wee, Chun-Jen Chung</i>	862
Mathematical Modeling and Tabu Search Heuristic for the Traveling Tournament Problem <i>Jin Ho Lee, Young Hoon Lee, Yun Ho Lee</i>	875
An Integrated Production-Inventory Model for Deteriorating Items with Imperfect Quality and Shortage Backordering Considerations <i>H.M. Wee, Jonas C.P. Yu, K.J. Wang</i>	885
A Clustering Algorithm Using the Ordered Weight Sum of Self-Organizing Feature Maps <i>Jong-Sub Lee, Maing-Kyu Kang</i>	898

Global Optimization of the Scenario Generation and Portfolio Selection Problems	
<i>Panos Parpas, Berç Rustem</i>	908
A Generalized Fuzzy Optimization Framework for R&D Project Selection Using Real Options Valuation	
<i>E. Ertugrul Karsak</i>	918
Supply Chain Network Design and Transshipment Hub Location for Third Party Logistics Providers	
<i>Seungwoo Kwon, Kyungdo Park, Chulung Lee, Sung-Shick Kim, Hak-Jin Kim, Zhong Liang</i>	928
A Group Search Optimizer for Neural Network Training	
<i>S. He, Q.H. Wu, J.R. Saunders</i>	934
Application of Two-Stage Stochastic Linear Program for Portfolio Selection Problem	
<i>Kuo-Hwa Chang, Huifen Chen, Ching-Fen Lin</i>	944
General Tracks	
Hierarchical Clustering Algorithm Based on Mobility in Mobile Ad Hoc Networks	
<i>Sulyun Sung, Yuhwa Seo, Yongtae Shin</i>	954
An Alternative Approach to the Standard Enterprise Resource Planning Life Cycle: Enterprise Reference Metamodeling	
<i>Miguel Gutiérrez, Alfonso Durán, Pedro Cocho</i>	964
Static Analysis Based Software Architecture Recovery	
<i>Jiang Guo, Yuehong Liao, Raj Pamula</i>	974
A First Approach to a Data Quality Model for Web Portals	
<i>Angelica Caro, Coral Calero, Ismael Caballero, Mario Piattini</i>	984
Design for Environment-Friendly Product	
<i>Hak-Soo Mok, Jong-Rae Cho, Kwang-Sup Moon</i>	994
Performance of HECC Coprocessors Using Inversion-Free Formulae	
<i>Thomas Wollinger, Guido Bertoni, Luca Breveglieri, Christof Paar</i>	1004
Metrics of Password Management Policy	
<i>Carlos Villarrubia, Eduardo Fernández-Medina, Mario Piattini</i>	1013

Using UML Packages for Designing Secure Data Warehouses <i>Rodolfo Villarroel, Emilio Soler, Eduardo Fernández-Medina, Juan Trujillo, Mario Piattini</i>	1024
Practical Attack on the Shrinking Generator <i>Pino Caballero-Gil, Amparo Fúster-Sabater</i>	1035
A Comparative Study of Proposals for Establishing Security Requirements for the Development of Secure Information Systems <i>Daniel Mellado, Eduardo Fernández-Medina, Mario Piattini</i>	1044
Stochastic Simulation Method for the Term Structure Models with Jump <i>Kisoeb Park, Moonseong Kim, Seki Kim</i>	1054
The Ellipsoidal l_p Norm Obnoxious Facility Location Problem <i>Yu Xia</i>	1064
On the Performance of Recovery Rate Modeling <i>J. Samuel Baixauli, Susana Alvarez</i>	1073
Using Performance Profiles to Evaluate Preconditioners for Iterative Methods <i>Michael Lazzareschi, Tzu-Yi Chen</i>	1081
Multicast ω -Trees Based on Statistical Analysis <i>Moonseong Kim, Young-Cheol Bang, Hyunseung Choo</i>	1090
The Gateways Location and Topology Assignment Problem in Hierarchical Wide Area Networks: Algorithms and Computational Results <i>Przemyslaw Ryba, Andrzej Kasprzak</i>	1100
Developing an Intelligent Supplier Chain System Collaborating with Customer Relationship Management <i>Gye Hang Hong, Sung Ho Ha</i>	1110
The Three-Criteria Servers Replication and Topology Assignment Problem in Wide Area Networks <i>Marcin Markowski, Andrzej Kasprzak</i>	1119
An Efficient Multicast Tree with Delay and Delay Variation Constraints <i>Moonseong Kim, Young-Cheol Bang, Jong S. Yang, Hyunseung Choo</i>	1129
Algorithms on Extended (δ, γ) -Matching <i>Inbok Lee, Raphaël Clifford, Sung-Ryul Kim</i>	1137

SOM and Neural Gas as Graduated Nonconvexity Algorithms <i>Ana I. González, Alicia D’Anjou, M. Teresa García-Sebastian, Manuel Graña</i>	1143
Analysis of Multi-domain Complex Simulation Studies <i>James R. Gattiker, Earl Lawrence, David Higdon</i>	1153
A Fast Method for Detecting Moving Vehicles Using Plane Constraint of Geometric Invariance <i>Dong-Joong Kang, Jong-Eun Ha, Tae-Jung Lho</i>	1163
Robust Fault Matched Optical Flow Detection Using 2D Histogram <i>Jaechoon Chon, Hyongsuk Kim</i>	1172
Iris Recognition: Localization, Segmentation and Feature Extraction Based on Gabor Transform <i>Mohammadreza Noruzi, Mansour Vafadoost, M. Shahram Moin</i>	1180
Optimal Edge Detection Using Perfect Sharpening of Ramp Edges <i>Eun Mi Kim, Cherl Soo Park, Jong Gu Lee</i>	1190
Eye Tracking Using Neural Network and Mean-Shift <i>Eun Yi Kim, Sin Kuk Kang</i>	1200
The Optimal Feature Extraction Procedure for Statistical Pattern Recognition <i>Marek Kurzynski, Edward Puchala</i>	1210
A New Approach for Human Identification Using Gait Recognition <i>Murat Ekinçi</i>	1216
Author Index	1227