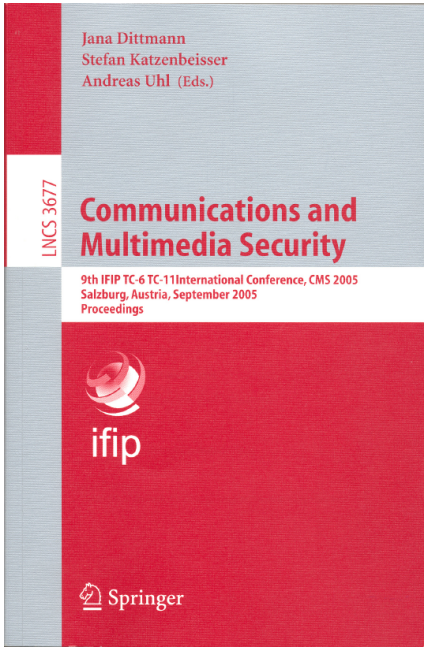
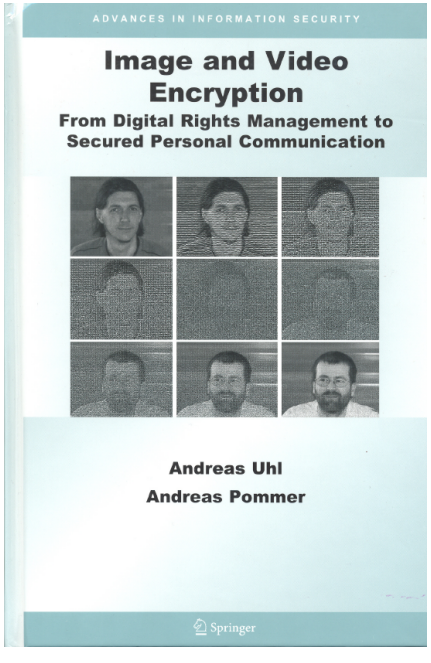
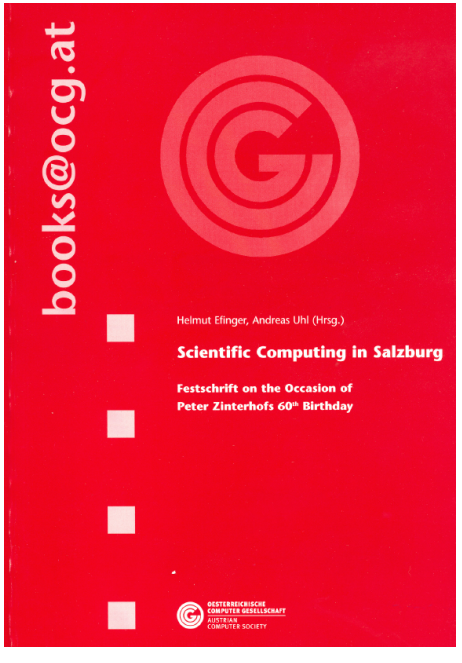
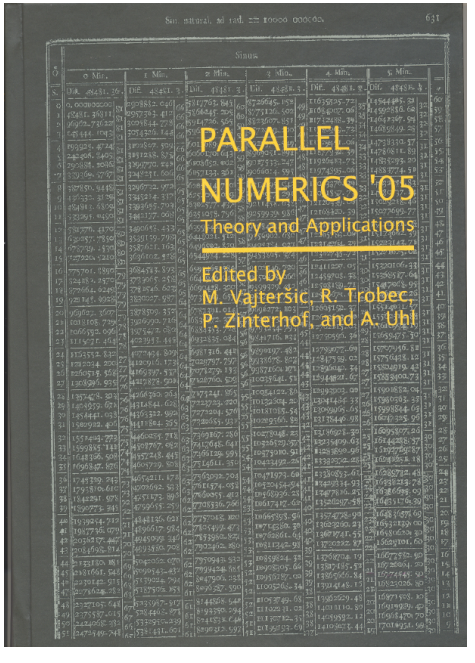




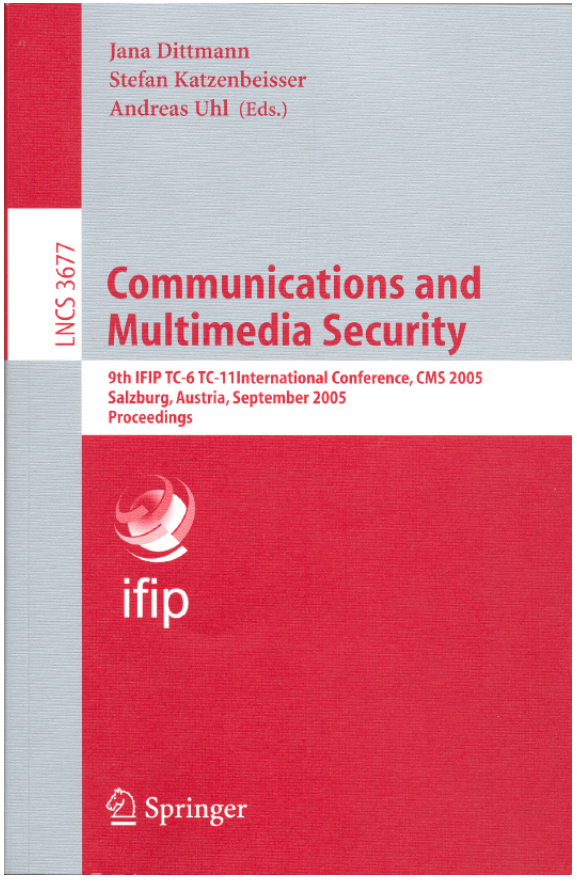




new_books @

Scientific Computing

Proceedings Communications and Multimedia Security (CMS 2005), J. Dittmann, S. Katzenbeisser, A. Uhl (Eds.)



This book constitutes the refereed proceedings of the 9th IFIP TC-6 TC-11 International Conference on Communications and Multimedia Security, CMS 2005, held in Salzburg, Austria in September 2005.
The 28 revised full papers and 13 two-page abstracts were carefully reviewed and selected from 143 submissions. The papers are organized in topical sections on applied cryptography, DRM and e-commerce, media encryption, multimedia security, privacy, biometrics and access control, network security, mobile security, and XML security.

Table of Contents

Applied Cryptography

Fast Contract Signing with Batch Oblivious Transfer
L'ubica Staneková, Martin Stanek 1

An Instruction Set Extension for Fast and Memory-Efficient AES Implementation
Stefan Tillich, Johann Großschädl, Alexander Szekely 11

Self-Healing Key Distribution Schemes with Sponsorization
Germán Sáez 22

DRM & E-Commerce

Effective Protection Against Phishing and Web Spoofing
Rolf Oppliger, Sebastian Gajek 32

Identity Based DRM: Personal Entertainment Domain
Paul Koster, Frank Kamperman, Peter Lenoir, Koen Vrielink 42

Rights and Trust in Multimedia Information Management
Jaime Delgado, Víctor Torres, Silvia Llorente, Eva Rodríguez 55

Signature Amortization Using Multiple Connected Chains
Qusai Abuein, Susumu Shibusawa 65

Media Encryption

A Key Embedded Video Codec for Secure Video Multicast
Hao Yin, Chuang Lin, Feng Qiu, Xiaowen Chu, Geyong Min 77

Puzzle – A Novel Video Encryption Algorithm
Fuwen Liu, Hartmut Koenig 88

Selective Image Encryption Using JBIG
Roman Pfarrhofer, Andreas Uhl 98

Multimedia Security

On Reversibility of Random Binning Techniques: Multimedia Perspectives
Sviatoslav Voloshynovskiy, Oleksiy Koval, Emre Topak, José Emilio Vila-Forcén, Pedro Comesaña Alfaro, Thierry Pun 108

A Graph–Theoretic Approach to Steganography
Stefan Hetzl, Petra Mutzel 119

Non-Interactive Watermark Detection for a Correlation-Based Watermarking Scheme
André Adelsbach, Markus Rohe, Ahmad-Reza Sadeghi 129

Privacy

Video Surveillance: A Distributed Approach to Protect Privacy
Martin Schaffer, Peter Schartner 140

Privacy-Preserving Electronic Health Records
Liesje Demuynck, Bart De Decker 150

Using XACML for Privacy Control in SAML-Based Identity Federations
Wolfgang Hommel 160

Biometrics & Access Control

Verifier-Tuple as a Classifier for Biometric Handwriting Authentication - Combination of Syntax and Semantics
Andrea Oermann, Jana Dittmann, Claus Vielhauer 170

Decentralised Access Control in 802.11 Networks
Marco Domenico Aime, Antonio Lioy, Gianluca Ramunno 180

Multimodal Biometrics for Voice and Handwriting
Claus Vielhauer, Tobias Scheidat 191

Network Security

Compact Stimulation Mechanism for Routing Discovery Protocols in Civilian Ad-Hoc Networks
Huafei Zhu, Feng Bao, Tieyan Li 200

Polymorphic Code Detection with GA Optimized Markov Models
Udo Payer, Stefan Kraxberger 210

A Secure Context Management for QoS-Aware Vertical Handovers in 4G Networks
Minsoo Lee, Sehyun Park 220

Mobile Security

Security Analysis of the Secure Authentication Protocol by Means of Coloured Petri Nets
Wiebke Dresp 230

Assessment of Palm OS Susceptibility to Malicious Code Threats
Tom Goovaerts, Bart De Win, Bart De Decker, Wouter Joosen 240

Implementation of Credit-Control Authorization with Embedded Mobile IPv6 Authentication
HyunGon Kim, ByeongKyun Oh 250

Work in Progress Track

Biometrics: Different Approaches for Using Gaussian Mixture Models in Handwriting
Sascha Schimke, Athanasios Valsamakis, Claus Vielhauer, Yannis Stylianou 261

INVUS: INtelligent VUlnerability Scanner
Turker Akyuz, Ibrahim Sogukpinar 264

Personal Rights Management – Enabling Privacy Rights in Digital Online Content
Mina Deng, Lothar Fritsch, Klaus Kursawe 266

Flexible Traitor Tracing for Anonymous Attacks
Hongxia Jin, Jeffery Lotspiech 269

Efficient Key Distribution for Closed Meetings in the Internet
Fuwen Liu, Hartmut Koenig 271

Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics
Taras Holotyak, Jessica Fridrich, Sviatoslav Voloshynovskiy 273

Applying LR Cube Analysis to JSteg Detection
Kwangsoo Lee, Changho Jung, Sangjin Lee, HyungJun Kim, Jongin Lim 275

Digital Signatures Based on Invertible Watermarks for Video Authentication
Enrico Hauer, Jana Dittmann, Martin Steinebach 277

A Theoretical Framework for Data-Hiding in Digital and Printed Text Documents
Renato Villán, Sviatoslav Voloshynovskiy, Frédéric Deguillaume, Yuriy Rytsar, Oleksiy Koval, Emre Topak, Ernesto Rivera, Thierry Pun 280

Semantically Extended Digital Watermarking Model for Multimedia Content
Huajian Liu, Lucilla Croce Ferri, Martin Steinebach 282

An Architecture for Secure Policy Enforcement in E-Government Services Deployment
Nikolaos Oikonomidis, Sergiu Tcaciuc, Christoph Ruland 284

Some Critical Aspects of the PKIX TSP
Cristian Marinescu, Nicolae Tapus 286

Motivations for a Theoretical Approach to WYSIWYS
Antonio Lioy, Gianluca Ramunno, Marco Domenico Aime, Massimiliano Pala 289

Special Session: XML Security

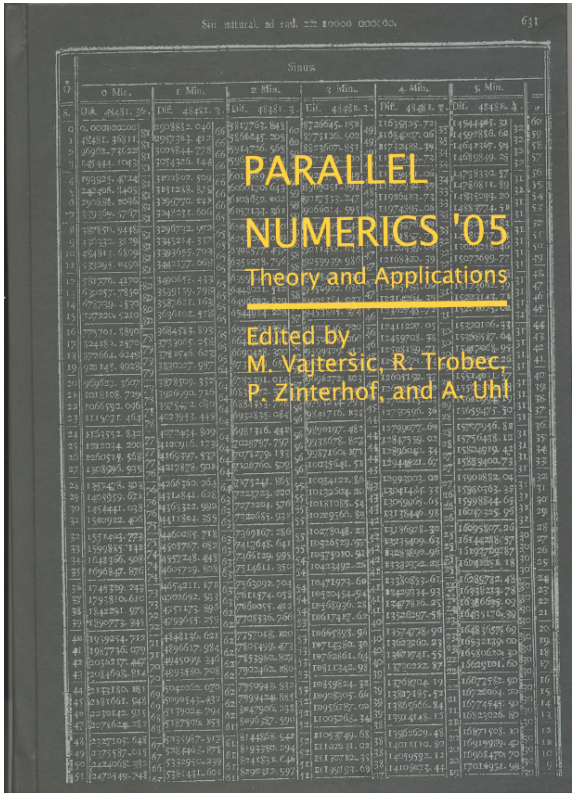
Secure XMaiL or How to Get Rid of Legacy Code in Secure E-Mail Applications
Lars Ewers, Wolfgang Kubbilun, Lijun Liao, Jörg Schwenk 291

Integrating XML Linked Time-Stamps in OASIS Digital Signature Services
Ana Isabel González-Tablas, Karel Wouters 301

Trustworthy Verification and Visualisation of Multiple XML-Signatures
Wolfgang Kubbilun, Sebastian Gajek, Michael Psarros, Jörg Schwenk 311

Experience XML Security – The XML-Security Plug-In for Eclipse
Dominik Schadow 321

Proceedings Parallel Numerics 2005 (ParNum 2005), R. Trobec, M. Vajtersic, P. Zinterhof, A. Uhl (Eds.)



Proceedings des Workshops "Parallel Numerics" der im April 2005 in Portoroz abgehalten wurde und wesentlich vom FB Scientific Computing mitorganisiert wurde. Diese Workshopreihe gibt es seit 1994 und sie wurde gegründet anlässlich eines Grossprojekts (PACT) der Zentraleuropaeischen Initiative CEI zum Thema Parallelverarbeitung. Frühere Workshops wurden abgehalten in Smolenice (Slovakei), Sorrento (Italien), Gozd Martuljek (Slovenien), Zakopane (Poland), Salzburg, Bratislava (Slovakei) und Bled (Slovenien).

Table of Contents

Abstracts of Invited Talks

S. G. Akl:
The Myth of Universal Computation 5

Z. Drmač:
New Jacobi–Type Algorithm for Computing the SVD 7

D. Janežič:
Large-Scale Molecular Dynamics Simulations on Parallel Clusters 9

U. Rüde:
Experiences with Large Scale Numerical Simulation 11

Matrix Algebra

G. Okša, M. Vajteršic:
Preconditioned Parallel Block–Jacobi SVD Algorithm 15

P. Arbenz, M. Bečka, R. Geus, U. Hetmaniuk, T. Mengotti:
Parallel Maxwell Eigensolver Using Trilinos Software Framework 25

Differential Equations

P. Purcz:
Theoretical Estimates of the Speed-up of One Parallel Algorithm 37

V. Horak, P. Gruber:
Parallel Numerical Solution of 2-D Heat Equation 47

M. Šterk, B. Robič, R. Trobec:
Mesh Free Method Applied to Diffusion Equation 57

Integration

P. Zinterhof, C. Amstler:
On the Covariance of Sequences in General Spaces 69

B. Hechenleitner, K. Entacher:
Selection of Good Lattice Points Utilizing a Cluster 81

Optimization and Classification

X. Liu, O. Sýkora:
Algorithms for the Shortest Common Superstring Problem 97

K. F. Doerner, R. F. Hartl, M. Lucka:
A Parallel Version of the D-Ant Algorithm for the VRP 109

G. Topić, T. Šmuc, Z. Šojat, K. Skala:
Reimplementation of the Random Forest Algorithm 119

Multimedia

F. Tischler, A. Uhl:
Limitations of Cluster Computing 129

R. Kutil, P. Eder, M. Watzl:
SIMD Parallelization of Common Wavelet Filters 141

A. Lutsyk, O. Lutsyk, O. Pelenskyy:
Parallel Image Processing on Configurable Computing Architecture 151

Systems and Simulation

S. G. Akl:
The Myth of Universal Computation 167

R. Trummer, P. Zinterhof, R. Trobec:
A High-Performance Data-Dependent Hardware Divider 193

I. Rozman, R. Trobec, M. Šterk:
Tuning Communication in Gigabit Ethernet Cluster 207

N. Pavković, K. Skala, V. Vidić, Z. Šojat:
Bioinformatics Application Oriented IT Deployment Model 217

D. Janežič, U. Borštnik:
Large-Scale Molecular Dynamics Simulations on Parallel Clusters 223

Author Index 233

ParNum 2005: Papers

- Professor Akl aus Kingston hat bewiesen, dass ein universaler Rechner ein Mythos ist. Er hat drei Konterbeispiele präsentiert, die auf der Turing-Maschine nicht lösbar sind. Für die Berechnung solcher Aufgaben bräuchte man einen Rechner der eine unendliche Anzahl von Operationen in einem Schritt ausführen kann. So eine Leistung ist aber unvorstellbar.

- Z.Drmac hat die neuesten Verfahren fuer die Berechnung von SVD (Singular Value Decomposition) vorgestellt. Dieses Verfahren hat eine breite Anwendung (z.B. in der Bildverarbeitung).

- Frau Janezic hat gezeigt wie man die Berechnungen mit komplexen Molekülstrukturen auf dem parallelen Multiprozessor Cluster durchführen kann.

- Für Data-Mining in komplexen Datenbanken werden in letzter Zeit algebraische Oksa und Vajtersic haben solche Methoden effektiv parallelisiert und auf dem Salzburger Hochleistungscluster Gaisberg auch ausprobiert.

ParNum 2005: Papers

- Die Studierenden V.Horak und P.Gruber aus Salzburg haben sich mit der Lösung der zweidimensionalen Wärmegleichung beschäftigt. Die Experimente wurden auf den modernen Rechenclustern durchgeführt.

- Der Beitrag von Zinterhof und Amstler beschäftigt sich mit der Kovarianz von Sequenzen.

- Die Arbeit von Hechenleitner und Entacher über Good Lattice Points findet ihre Anwendung u.a. in der Finanzmathematik.

- Für das Shortest Common Superstring Problem (es handelt sich um das sogenannte NP-Problem) haben Liu und Sykora aus Lougborough parallele genetische Algorithmen angewendet.

ParNum 2005: Papers

- Eine interessante Arbeit wurde aus Wien eingereicht. Die Autoren aus dem Institut fuer Scientific Computing dortiger Universität haben die Technik D-Ant (Analog zu Ameisen-Kolonien) fuer die Lösung des Vehicle Routing Problems verwendet. Dabei haben sie einen hohen Grad an Parallelitaet erreicht.
- In der Arbeit von Tischler und Uhl über kommunikations-intensive Multimedia Applikationen wurden Limits bei der Benutzung von Rechenclustern festgestellt. Ein Vergleich zu sogenannten Shared Memory Architectures wird gemacht.
- Kutil, Eder und Watzl (ein Team aus Salzburg) haben die SIMD (Single Instruction Multiple Data)-Erweiterung von CPUs für Wavelet Filterung effektiv ausgenutzt. Sie erzielen dabei eine deutliche Beschleunigung von Algorithmen die auf dieser Transformation basieren (z.B. die des JPEG2000-Standard).
- Einen Entwurf einer parallelen Architektur fuer Image Processing haben die Autoren aus Lviv in der Ukraine ausgearbeitet. Diese Architektur kann eine Real-Time Bearbeitung wichtiger Operationen (z.B. Segmentation und Filtering) erreichen.

ParNum 2005: Papers

- Die nächste Arbeit beschäftigt sich mit der Thematik Hardware-Divider. Es wird gezeigt, wie man bei der Division durch Verbesserungen eine 600%ige Beschleunigung erreichen kann.

- Das Autoren-Trio aus dem Jozef Stefan Institut in Ljubljana beschreibt, wie man die Kommunikation in einem Ethernet-Cluster wesentlich verbessern kann.

- Die letzte Arbeit im Band kommt vom Rudjer Boskovic Institut in Zagreb. Hier wird eine effektive Auslastung der vorhandenen Rechner vorgeschlagen, um eine komplexe Aufgabe aus der Bioinformatik lösen zu koennen.

Image and Video Encryption, A. Uhl, A. Pommer

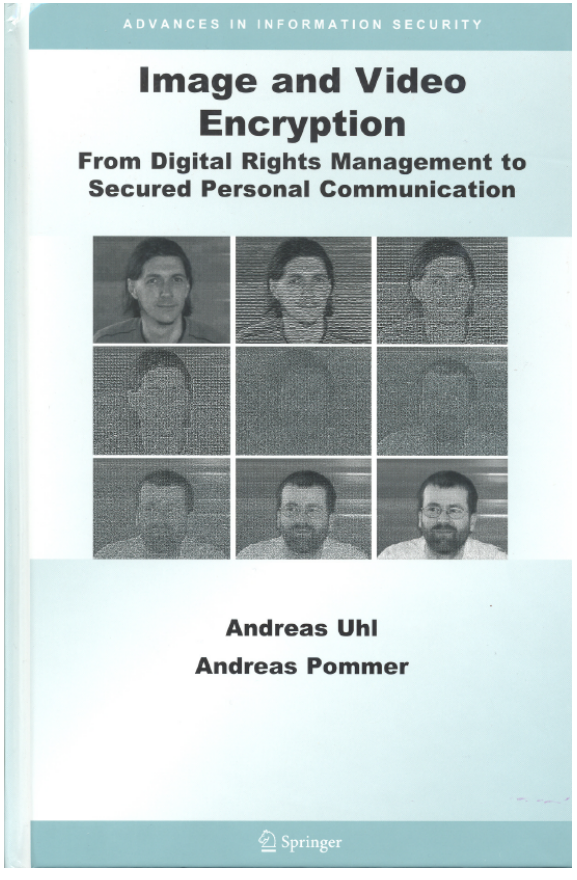


Image and Video Encryption provides a unified overview of techniques for encryption of images and video data. This ranges from commercial applications like DVD or DVB to more research oriented topics and recently published material. This volume introduces different techniques from unified viewpoint, then evaluates these techniques with respect to their respective properties (e.g., security, speed.....).
The authors experimentally compare different approaches proposed in the literature and include an extensive bibliography of corresponding published material.

Contents

Dedication v
List of Figures ix
List of Tables xiii
Preface xv
Acknowledgments xvii

1. INTRODUCTION 1

2. VISUAL DATA FORMATS 11
   1 Image and Video Data 11
   2 DCT-based Systems 12
   3 Wavelet-based Systems 14
   4 Further Techniques 18

3. CRYPTOGRAPHY PRIMER 21
   1 Introduction, Terminology 21
   2 Secret key vs. Public key Cryptography 22
   3 Block Ciphers 23
   4 Stream Ciphers 27
   5 Hybrid Algorithms, some Applications 28
   6 Cryptanalysis Overview 29
   7 Further Information 30

4. APPLICATION SCENARIOS FOR THE ENCRYPTION OF VISUAL DATA 31
   1 Security provided by Infrastructure or Application 31
   2 Full Encryption vs. Selective Encryption 32
   3 Interplay between Compression and Encryption 37

5. IMAGE AND VIDEO ENCRYPTION 45
   1 DCT-based Techniques 47
   2 Wavelet-based Techniques 82
   3 Further Techniques 115
   4 Transparent Encryption 127
   5 Commercial Applications and Standards 129

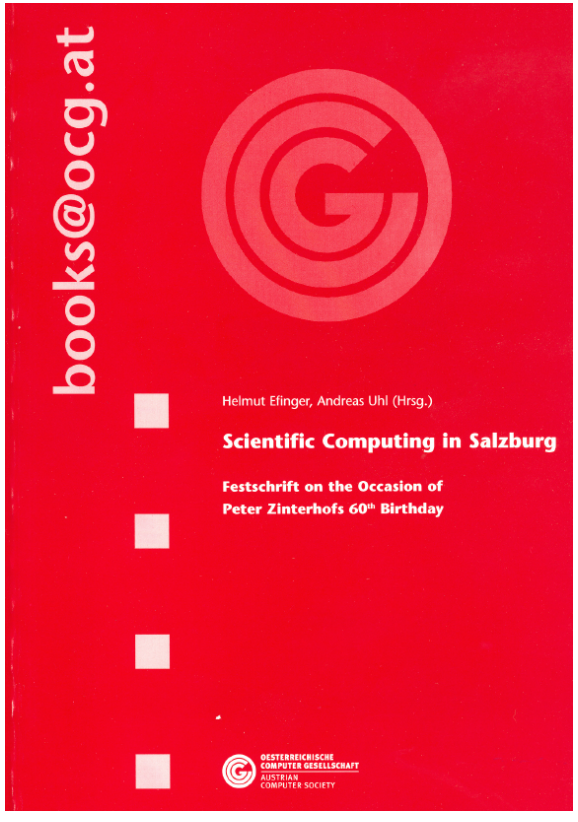
6. CONCLUSIONS 135

Appendices 137
A Copyrighted sections 137
B Test Images and Videos 139
   1 Cover Page 139
   2 Test Images 139
   3 Sequence 1 — Bowing 141
   4 Sequence 2 — Surf Side 141
   5 Sequence 3 — Coast Guard 141
   6 Sequence 4 — Akiyo 142
   7 Sequence 5 — Calendar 142
C Authors' Biographies 143

References 145

Index 159

Scientific Computing in Salzburg, H. Efinger, A. Uhl (Eds.)



Die Festschrift "Scientific Computing in Salzburg" wurde anlässlich des 60. Geburtstags von Prof. Peter Zinterhof herausgegeben. Das Buch zeigt das Gebiet Scientific Computing in seiner ganzen Breite, von Grundlagenthemen in den Bereichen Mathematik, Logik und Physik bis hin zu Anwendungen in den Ingeneurwissenschaften wie z.B. Datenkodierung und -übertragung. Durch die Auswahl der Beiträge (Vorträge des Scientific Computing Minisymposiums im Oktober 2004 in Salzburg und Beiträge von Salzburger Wissenschaftlern) wird die besondere Ausprägung dieses Fachgebiets in Salzburg und die besondere Rolle von Peter Zinterhof bei dessen Prägung gezeigt.

TABLE OF CONTENTS

Preface 7

Invited Talks

On some Systems with Incomplete Information 11
Claudia Lidia Badea

Remarks on the weighted sum-of-digits function 27
Gerhard Lacher, Friedrich Pillichshammer

Faster Computers and Algorithms in Scientific Computing 37
Roman Trobec

The Initiative AUSTRIAN GRID 45
Jens Volkert

Contributions from the Department

Reproducing Kernel Hilbert Spaces and their Application to high dimensional Integration 59
Clemens Amstler

A New Class of Erasure Codes and its Application to Scalable Multicast Content Delivery 69
Wolfgang Brauneis, Hilmar Linder

Efficiency of IPv6 Encapsulation with ULE/DVB 81
Bernhard Collini-Nocker, Hilmar Linder, Andreas Maier, Peter Maurutschek, Wolfram Stering, Klaus Würflinger

Algebraic Properties of Rules of Frege-Hilbert Calculi 87
Elmar Eder

A Nonlinear Unitary Framework For Quantum State Reduction: a phenomenological approach 97
Helmut J. Efinger

Split Queue Time Warp and a Flexible Distributed Simulation System 105
Helge Hagenauer, Werner Pohlmann

Alluvion - A Language for Computer Arithmetic Algorithms 113
Rade Kutil

A Taxonomy of Artifical Neural Systems Evolution 121
Helmut A. Mayer

Parallel SVD Computations on Supercomputer Cluster 137
G.Oksa, M.Vajtersic

A Web-based Tool for MPEG Encryption Experiments 147
Andreas Pommer, Andreas Uhl

Further Salzburg Contributions

A Parallel Search for Korobov Lattice Rules 163
Karl Entacher, Bernhard Hechenleitner

Shift Nets and Salzburg Tables: Power Computing in Number-Theoretical Numerics 175
W.Ch. Schmid, R. Schürer