

GI, the Gesellschaft für Informatik, publishes this series in order

- to make available to a broad public recent findings in informatics (i.e. computer science and information systems)
- to document conferences that are organized in cooperation with GI and
- to publish the annual GI Award dissertation.

Broken down into the fields of “Seminars”, “Proceedings” and “Dissertations”, current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: <http://www.gi-ev.de/service/publikationen/lni/>

ISBN 978-3-88579-410-3

This book gives an overview of outstanding dissertations in computer science of the year 2005. Every year, the Gesellschaft für Informatik (GI), together with the Swiss Informatics Society (SI), the Austrian Computer Society (OCG) and the German Chapter of the ACM (GChACM), awards an excellent dissertation that represents an important improvement in Informatics. The award-winner is chosen in a careful selection procedure from dissertations proposed by Austrian, Swiss and German universities, where each university can make at most one suggestion per year. The series “Ausgezeichnete Informatikdissertationen” presents these outstanding dissertations to the informatics community, as well as to the public in order to support knowledge transfer from universities to industry and society (in German).



GI-Edition

Lecture Notes in Informatics

Dorothea Wagner et al. (Hrsg.)

Ausgezeichnete Informatikdissertationen 2005

GI-Dissertationspreis 2005

D-6

Dissertations



Ausgezeichnete Informatikdissertationen 2005

Im Auftrag der GI herausgegeben durch
den Nominierungsausschuss

Abraham Bernstein, Universität Zürich
Thomas Dreier, Universität Karlsruhe (TH)
Steffen Hölldobler, Technische Universität Dresden
Günter Hotz, Universität des Saarlandes
Klaus-Peter Löhr, Freie Universität Berlin
Paul Molitor, Martin-Luther-Universität Halle-Wittenberg
Gustaf Neumann, Wirtschaftsuniversität Wien
Rüdiger Reischuk, Universität zu Lübeck
Dietmar Saupe, Universität Konstanz
Myra Spiliopoulou, Otto-von-Guericke-Universität Magdeburg
Dorothea Wagner (Vorsitzende), Universität Karlsruhe (TH)

Gesellschaft für Informatik 2006

Lecture Notes in Informatics (LNI) - Dissertations

Series of the German Informatics society (GI)

Volume D-6

ISBN 3-88579-330-X

ISSN 978-3-88579-410-3

Dissertations Editorial Board

Prof. Dr. Dorothea Wagner (Chair),
Universität Karlsruhe (TH)
Institut für Theoretische Informatik
76128 Karlsruhe

Abraham Bernstein, Universität Zürich
Thomas Dreier, Universität Karlsruhe (TH)
Steffen Hölldobler, Technische Universität Dresden
Günter Hotz, Universität des Saarlandes
Klaus-Peter Lühr, Freie Universität Berlin
Paul Molitor, Martin-Luther-Universität Halle-Wittenberg
Gustaf Neumann, Wirtschaftsuniversität Wien
Rüdiger Reischuk, Universität zu Lübeck
Dietmar Saupe, Universität Konstanz
Myra Spiliopoulou, Otto-von-Guericke-Universität Magdeburg
Dorothea Wagner (Vorsitzende), Universität Karlsruhe (TH)

Series Editorial Board

Heinrich C. Mayr, Universität Klagenfurt, Austria (Chairman, mayr@ifit.uni-klu.ac.at)
Jörg Becker, Universität Münster, Germany
Ulrich Furbach, Universität Koblenz, Germany
Axel Lehmann, Universität der Bundeswehr München, Germany
Peter Liggesmeyer, TU Kaiserslautern und Fraunhofer IESE, Germany
Ernst W. Mayr, Technische Universität München, Germany
Heinrich Müller, Universität Dortmund, Germany
Heinrich Reiner mann, Hochschule für Verwaltungswissenschaften Speyer, Germany
Karl-Heinz Rödiger, Universität Bremen, Germany
Sigrid Schubert, Universität Siegen, Germany

Seminars

Reinhard Wilhelm, Universität des Saarlandes, Germany

© Gesellschaft für Informatik, Bonn 2006

printed by Köllen Druck+Verlag GmbH, Bonn

Vorwort

Die Gesellschaft für Informatik e.V. (GI) vergibt gemeinsam mit der Schweizer Informatik Gesellschaft (SI), der Österreichischen Computergesellschaft (OCG) und dem German Chapter of the ACM (GChACM) jährlich einen Preis für eine hervorragende Dissertation im Bereich der Informatik. Hierzu zählen nicht nur Arbeiten, die einen Fortschritt für die Informatik bedeuten, sondern auch Arbeiten aus dem Bereich der Anwendungen in anderen Disziplinen und Arbeiten, die die Wechselwirkungen zwischen Informatik und Gesellschaft untersuchen. Die Auswahl dieser Dissertation stützt sich auf die von den Universitäten und Hochschulen für diesen Preis vorgeschlagenen Dissertationen. Jede dieser Hochschulen kann jedes Jahr nur eine Dissertation vorschlagen. Somit sind die zum Auswahlverfahren der GI vorgeschlagenen Kandidatinnen und Kandidaten bereits „Preisträger“ ihrer Hochschule.

Für den Dissertationspreis 2005 wurden 24 Dissertationen vorgeschlagen, welche vom Nominierungsausschuss, der sich aus Vertretern des Beirats der Universitätsprofessoren der GI zusammensetzt, sorgfältig begutachtet und diskutiert wurden. Im Rahmen eines Kolloquiums, das nach vielen Jahren erstmals wieder im Internationalen Begegnungs- und Forschungszentrum für Informatik Schloss Dagstuhl stattfand, wurden die vorgeschlagenen Arbeiten von den Nominierten vorgestellt. Erfreulicherweise konnten fast alle Kandidaten trotz zum Teil weiter Anreise teilnehmen. Wie jedes Jahr war für die Mitglieder des Nominierungsausschusses das persönliche Zusammentreffen mit den Nominierten das „Highlight“ der Auswahlarbeit. Das wissenschaftlich hohe Niveau der Vorträge, die regen Diskussionen und die angenehme Atmosphäre in Schloss Dagstuhl wurde von allen Teilnehmerinnen und Teilnehmern des Kolloquiums sehr begrüßt.

Dem Nominierungsausschuss fiel es schwer, unter allen nominierten Dissertationen eine einzelne auszuwählen, um sie mit dem Preis besonders zu würdigen. Mit der Präsentation aller vorgeschlagenen Dissertationen in diesem Band wird die Ungerechtigkeit, eine aus mehreren ebenbürtigen Dissertationen hervorzuheben, etwas ausgeglichen. Dieser Band soll zudem einen Beitrag zum Wissenstransfer innerhalb der Informatik und von den Universitäten in die Bereiche Technik, Wirtschaft und Gesellschaft leisten.

Die beteiligten Gesellschaften zeichnen Herrn Dr. rer. nat. Renato Renner, der an der ETH Zürich promovierte, für seine hervorragende Dissertation „Security of Quantum Key Distribution“ mit dem Dissertationspreis 2005 aus.

Die Quantenkryptographie liefert sichere geheime Schlüssel, die auch durch einen beliebig mächtigen Angreifer nicht gebrochen werden können. Damit bietet sie eine zukunfts-trächtige Alternative zu den derzeit eingesetzten Verfahren, für die eine langfristige Sicherheit nicht garantiert werden kann.

Wie Renato Renner in seiner Dissertation zeigt, griffen die bisherigen Sicherheitsbeweise der Quantenkryptographie allerdings nicht weit genug. Es genügt nicht zu zeigen, dass der Angreifer den Schlüssel nicht kennt, sondern der Schlüssel sollte auch in einer beliebigen Anwendung sicher verwendet werden können. Ein wesentlicher Beitrag der Dissertation

besteht in dem Nachweis, dass diese universelle Verwendbarkeit von Quantenschlüsselaustauschprotokollen tatsächlich erreicht werden kann. Dazu wird zunächst die Sicherheit gegen eine eingeschränkte Klasse von Angriffen, sogenannte kollektive Angriffe, bewiesen und dann gefolgert, dass dies schon die Sicherheit gegen allgemeine Angriffe impliziert. Letztgenanntes war ein bekanntes offenes Problem.

Für den Sicherheitsbeweis hat Renato Renner neue Entropiemaße eingeführt und eine quantenmechanische Verallgemeinerung des Darstellungssatzes von de Finetti für endliche Systeme entwickelt. Diese Ergebnisse haben bereits jetzt die Arbeit anderer Wissenschaftler entscheidend beeinflusst.

Mit dieser Preisverleihung würdigen die beteiligten Gesellschaften - die Gesellschaft für Informatik e.V. (GI), die Schweizer Informatik Gesellschaft (SI), die Österreichische Computergesellschaft (OCG) und das German Chapter of the ACM (GChACM) - eine Arbeit, die bahnbrechende Erkenntnisse in der Quantenkryptographie liefert und damit von höchstem Interesse für die Informatik ist.

Ein besonderer Dank gilt dem Nominierungsausschuss, der sehr effizient und konstruktiv zusammengearbeitet hat. Bei Frau Lilian Beckert möchte ich mich für die Unterstützung bei der Entgegennahme der vorgeschlagenen Dissertationen und bei Herrn Robert Görke für die Zusammenstellung und Anpassung der Beiträge an das Format der GI-Edition Lecture Notes in Informatics (LNI) bedanken. Für die finanzielle Unterstützung des Nominationskolloquiums sei den beteiligten Gesellschaften gedankt. Die Gastfreundschaft und die hervorragende Bewirtung in Dagstuhl trugen zum Erfolg des Kolloquiums bei, wofür ich mich an dieser Stelle ebenfalls herzlich bedanke.

Dorothea Wagner, Karlsruhe im September 2006

**Kandidaten für den
GI-Dissertationspreis 2005**

Dr. Mohamed Ibrahim Abouelhoda	Universität Ulm
Dr. Mario Botsch	RWTH Aachen
Dr. Thomas Gärtner	Rheinische Friedrich-Wilhelms-Uni Bonn
Dr. Brijnesh Johannes Jain	TU Berlin
Dr. Wolfgang Kapferer	Leopold-Franzens-Universität Innsbruck
Dr. Marc Lettrari	Carl von Ossietzky-Universität Oldenburg
Dr. Bodo Manthey	Universität Lübeck
Dr. Stefan Milius	TU Braunschweig
Dr. Roland Müller	FU Berlin
Dr. André Neubauer	TU Wien
Dr. Thomas Neumann	Universität Mannheim
Dr. Christian Panse	Uni Konstanz
Dr. Niels Pinkwart	Uni Duisburg-Essen
Dr. Renato Renner	ETH Zürich
Dr. Ing. Felix Ritter	Otto-von-Guericke-Universität Magdeburg
Dr. Andrey Rybalchenko	Universität des Saarlandes
Dr. Ingo Schellhammer	Universität Hamburg
Dr. Till Schümmer	FernUniversität Hagen
Dr. Niels Schütze	TU Dresden
Dr. Holger Spakowski	Heinrich-Heine-Universität Düsseldorf
Dr. Mirko Streckenbach	Universität Passau
Dr. Ing. Volkmar Uhlig	Universität Karlsruhe
Dr. Oliver Waldhorst	Universität Dortmund
Dr. Arne Wiebalck	Ruprecht-Karls-Universität Heidelberg

Nominierungsausschuss für den GI-Dissertationspreis 2005

Prof. Dr. Abraham Bernstein	Universität Zürich
Prof. Dr. Thomas Dreier	Universität Karlsruhe
Prof. Dr. Steffen Hölldobler	TU Dresden
Prof. Dr. Dr. h.c. mult. Günter Hotz	Universität des Saarlandes
Prof. Dr. Ing. Klaus-Peter Löhr	Freie Universität Berlin
Prof. Dr. Paul Molitor	Martin-Luther-Universität Halle-Wittenberg
Prof. Dr. Gustaf Neumann	Wirtschaftsuniversität Wien
Prof. Dr. Rüdiger Reischuk	Universität zu Lübeck
Prof. Dr. Dietmar Saupe	Universität Konstanz
Prof. Dr. Myra Spiliopoulou	Otto-von-Guericke-Universität Magdeburg
Prof. Dr. Dorothea Wagner (Vorsitzende)	Universität Karlsruhe (TH)



Inhaltsverzeichnis

Mohamed Ibrahim Abouelhoda	
Algorithmen und Softwarewerkzeuge für Vergleichende Genomanalyse	9
Mario Botsch	
High Quality Surface Generation and Efficient Multiresolution Editing Based on Triangle Meshes	19
Thomas Gärtner	
Kernfunktionen für Strukturierte Daten	29
Brijnesh Johannes Jain	
Structural Neuronal Learning Machines	39
Wolfgang Kapferer	
Metal Enrichment of the Intra-Cluster Medium Galactic Winds Starbursts and Galaxy Interactions	49
Bodo Manthey	
Approximability of Cycle Covers and Smoothed Analysis of Binary Search Trees	57
Stefan Milius	
Koalgebren Monaden und Semantik	67
Roland Müller	
Knowledge Sharing and Trading on Electronic Marketplaces	77
André Neubauer	
Virtuelle Endoskopie fuer Praeoperative Planung und Training von Endona- saler Transsphenoidaler Hypophysenchirurgie	85
Thomas Neumann	
Effiziente Generierung und Ausfuehrung von DAG-strukturierten Anfrage- graphen	95
Christian Panse	
Kartogramme zur Visualisierung Geographie-Bezogener Daten	105
Niels Pinkwart	
Graphbasierte Modelle als Kollaborationsmedien	115

Renato Renner	
Security of Quantum Key Distribution	125
Felix Ritter	
Interaktives Illustrieren von Informationsräumen: Räumliche und funktionale Zusammenhänge spielerisch begreifen	135
Andrey Rybalchenko	
Temporale Verifikation mit Transitionsinvarianten	141
Ingo Schellhammer	
TriX Strukturbasierte virtuelle Suche in Wirkstoffdatenbanken in sublinearer Zeit	151
Till Schümmer	
Ein Patternorientierter Ansatz fuer die Endbenutzerzentrierte Entwicklung Kooperativer Systeme	161
Niels Schütze	
Neue Methoden zur Steuerung der Wassergabe mit Neuronalen Netzen in der Bewässerungslandwirtschaft	171
Holger Spakowski	
Completeness for Parallel Access to NP and Counting Class Separation	181
Mirko Streckenbach	
KABA Ein System zur Refaktorisierung von Java-Programmen	191
Volkmar Uhlig	
Skalierbarkeit Mikrokernbasierter Systeme	201
Oliver Waldhorst	
Design and Quantitative Analysis of Protocols for Epidemic Information Dissemination in Mobile Ad Hoc Networks	211
Arne Wiebalck	
ClusterRAID Architektur und Prototyp eines Verteilten Fehlertoleranten Massenspeichersystems fuer Cluster	221