Jahresbericht 2002/2003 des Lehrstuhls

„Theoretische Konzepte und neue Anwendungen der Informatik“

(Univ.-Prof. Dr. sc. Christoph Meinel)

Fachbereich IV – Informatik
Universität Trier
D-54286 Trier, Germany

Vorwort

Der vorliegende Bericht gibt Auskunft über die Aktivitäten am Lehrstuhls "Theoretische Konzepte und neue Anwendungen der Informatik" der Universität Trier in den Jahren 2002/2003. Weitere Details finden Sie auf unseren Homepages

`http://www.informatik.uni-trier.de/TI`

`http://www.telematik-institut.org/`

und können dem letzten Jahresbericht des Instituts für Telematik von 2002 entnommen werden. Die Mitarbeiter des Lehrstuhls und ich hoffen auf Ihr Interesse an unserer Arbeit und würden uns über Kontakte und Anstöße zu möglichen Kooperationsprojekten in Forschung und Lehre sehr freuen.

Christoph Meinel — Trier, im Frühjahr 2004

Inhaltsverzeichnis

1 Personelle Zusammensetzung

- **Professor**
  Prof. Dr. sc. nat. Christoph Meinel

- **Wissenschaftliche Mitarbeiter**
  Dipl. Inform. Mohammed Ghasemzadeh
  Dipl. Inform. Volker Klotz
  Dr. rer. nat. Rustam Mubarakzjanov (bis 31.08.2002)
  Dr. rer. nat. Harald Sack (bis 30.06.2002)
  Dipl. Inform. Volker Schillings
  Dipl. Inform. Gennadij Umanskij

- **Sekretärin**
  Agnes Jacoby

- **Stipendiaten**
  Dipl.-Inform. Tongbo Chen
  Dipl.-Inform. Ji Hu
  Dipl.-Inform. Wang Long
  Dipl.-Inform. Wanjun Huang
  Dipl.-Inform. Chunyian Jiang
  Dipl.-Inform. Feng Cheng

- **Praktikanten**
  Tatsiana Borzdova, Belarussion State University, (Russland)
  (01.07.2002-30.09.2002)
  Vladimir Trpkovski, Sts. Cyril and Methodius, (Mazedonien)
  (01.07.2002-01.09.2002)
  Lital Shestowitz, Technion-Israel Institute of Technology,
  (Israel) (01.08.2003 - 30.11.2003)
  Oliver Zofic, University of Maribor, (Slowenien)
  (01.07.2002 - 31.08.2003)

- **Wissenschaftliche Hilfskräfte**

  Dipl. Inform. Christian Stangier (bis 30.09.2002)
  Michael Bahra (bis 31.07.2002)
  Marc Kalle (bis 31.07.2002)
  Michael Ströher (bis 31.07.2002)
  Marco Weber (bis 31.08.2002)
  Natalia Efrosinina (bis 30.09.2002)
  Jan Kalland (01.12.2002 - 28.02.2003)
  Hanh Quyen Nguyen (01.11.2002 - 28.02.2003)
  Thomas Scherer (15.11.2002 - 31.07.2003)
  Sebastian Schneider (01.12.2002 - 28.02.2003)
  Benjamin Boelter (01.12.2002 - 30.04.2003)
  Martin Mitev (15.11.2002 - 15.02.2003)
  Daniel Fischer (01.12.2002 - 31.05.2003)
  Markus Lauer (01.03.2002 - 28.02.2003)

2 Mit dem Lehrstuhl personell verbundene Einrichtungen

2.1 Zentrum für Wissenschaftliches Elektronisches Publizieren - WEP

Das Zentrum für Wissenschaftliches Elektronisches Publizieren an der Universität Trier ist eine fachübergreifende Einrichtung, die als Informationsbasis und Koordinationszentrum für alle universitären Aktivitäten auf dem Gebiet des wissenschaftlichen elektronischen Publizierens dienen soll.

Unter anderem stehen dabei die Erprobung und die Evaluation neuer Möglichkeiten wissenschaftlicher Kommunikation durch Rechnernetze und weltweit verfügbare Informationssysteme im Vordergrund. Darüber hinaus stellen die Förderung des interdisziplinären Erfahrungsaustausches, sowie die Initiierung von Projekten auf dem Gebiet des wissenschaftlichen elektronischen Publizierens einen weiteren Aufgabenschwerpunkt dar. Das WEP soll dabei interessierte Stellen in Wirtschaft und Gesellschaft beraten und dadurch die Zusammenarbeit mit außeruniversitären Kooperationspartnern fördern.

Aufgaben des WEP:

- Initiierung, Verwaltung und Betrieb von online-Journalen
- Zugang zu fachspezifischen online-Recherche-Systemen
- Verwaltung von Bibliographiedatenbeständen
- Unterstützung bei der Konzeption von Internet-Präsenzen
- Hypertext- und Multimedia-Anwendungen
- Organisation von universitären Kolloquien

Das Zentrum für Wissenschaftliches Elektronisches Publizieren steht unter der Leitung von Univ.-Prof. Dr. sc. Christoph Meinel (Direktor), die Geschäftsführung lag in den Händen von Dr. rer. nat. Harald Sack.
Weitere Informationen können im WWW gefunden werden unter der URL

`http://www.wep.uni-trier.de/`

2.2 Institut für Telematik e.V. (bis 2002)

Das eigenständige Institut für Telematik in Trier e.V. war bis zu seiner Auflösung 2002 befasst mit den vielfältigen, neuen Potentialen, die sich aus der Verschmelzung von Telekommunikation und Informatik ergeben. Durch die Verknüpfung von Computern, Mobilfunk und Internet werden Möglichkeiten geschaffen, über stationäre und mobile Geräte aller Art jederzeit effizient auf die in den weltweiten Computer-Netzwerken vorhandenen Informationen zuzugreifen, mit diesen sicher umzugehen und sie intelligent zu nutzen. Das Institut betrieb Hightech-Forschung, um unserer Wirtschaft einen wichtigen Entwicklungs-Vorsprung zu geben und bildete hochqualifizierte IT-Nachwuchskräfte aus, die Deutschland so dringend braucht. Abläufe in Wirtschaft, Verwaltung, Verkehr und Gesundheitswesen konnten durch die Ergebnisse seiner praxisorientierten Arbeit wesentlich rationeller gestaltet werden. Dabei wurde danach gestrebt, die Anwendungen so einfach und nutzerfreundich wie möglich zu machen.

Internet/Intranet, Sicherheit der Datenkommunikation in offenen Netzen, Telemedizin, Elektronisches Publizieren, Systementwurf und -analyse, das waren die Forschungs- und Entwicklungsfelder des Institutes. Das Institut agierte so auf der Bugwelle neuester technologischer Entwicklungen und schuf Pilotlösungen für die tägliche Praxis.

Auftraggeber des Institutes waren sowohl weltbekannte Großunternehmen wie Siemens oder die Dresdner Bank als auch kleine und mittelständische Firmen, Krankenhäuser, Finanzdienstleister und Verwaltungen in Rheinland-Pfalz, Baden-Württemberg und Luxemburg.

Nach fünf Jahren Arbeit weist die wissenschaftliche Bilanz des Institutes für Telematik zwei Patente (ein weiteres beantragt), vier Promotionen (3 weitere kurz vor Abschluss) und über 90 Fachbeiträge zu internationalen Konferenzen auf - eine Leistung, die auch international zu hoher Reputation führte.

2002, das fünfte Jahr des Bestehens des Institutes ist nun überraschenderweise sein letztes. Nicht fehlende Erfolge der wissenschaftlichen Tätigkeit sind dafür der Grund. Immerhin konnte ein drittes Patent zur sicheren Verwahrung elektronischer Dokumente angemeldet und eine Reihe von neuesten Forschungsergebnissen auf internationalen Wissenschaftstagungen vorgestellt werden. Auch gaben unsere Symposien "Digitales Bezahlen" und "Sichere Telemedizin" Aufschluss über wichtige jüngste Entwicklungen. Das Institut konnte sogar bei der europaweiten Ausschreibung eines Registers für die neue Internet Top level Domain ".eu" als einziger deutscher Kandidat antreten. Auch das große Interesse der Medien belegt die hohe Relevanz der Aktivitäten. So gab es sowohl eine Reihe von Fernsehbeiträgen in ARD, ZDF und 3sat über unsere Arbeit als auch eine Vielzahl von Berichten in der Fach- und Publikums-Presse. Die Schwierigkeiten ergaben sich aus der stetig schlechter werdenden Wirtschaftslage und der verringerten Neigung von Unternehmen, Forschungs- und Entwicklungaufträge zu erteilen. So konnten 2002 "lediglich" Aufträge im Wert von etwa 500.000 EURO eingeworben werden. Zusammen mit den vom Land Rheinland-Pfalz bereitgestellten Fördermitteln hat dies nicht für einen ausgeglichenen Haushalt ausgereicht. Im Umfeld der ebenfalls schwierigen Finanzlage des Landes und fehlender Zusagen über weitere Förderung sah sich der Trägerverein des Instituts deshalb genötigt, am 08. Januar 2003 die Liquidation des Instituts zu beschließen. Trotz Auflösung des Instituts arbeitet eine kleine Forschungsgruppe weiter auf dem Gebiet der Telematik. Informationen hierzu können auf der Website

`http://www.telematik-institut.org/`

abgerufen werden.

3 Aktivitäten in der Lehre: Vorlesungen, Übungen und Seminare

Sommersemester 2002

Automatentheorie und formale Sprachen (2 SWS)
Vorlesung: Christoph Meinel
Übung: Rustam Mubarakzjanov

Die Vorlesung gibt eine kompakte Einführung in das Gebiet der Automatentheorie und formalen Sprachen, das sowohl für die theoretische Informatik (Berechenbarkeitstheorie, Komplexitätstheorie, formale Systeme und Semantik) als auch für die praktische Informatik (Programmiersprachen, Syntaxanalyse, Compilerbau usw.) von grundlegender Bedeutung ist. Formale Sprachen sind Mengen von Wörtern über einem vorgegebenen Alphabet, für die es ein Regelsystem gibt, nach dem alle Wörter dieser Menge generiert werden können (und nur diese). Die Chomsky-Hierarchie teilt die Menge der formalen Sprachen ein in vier Klassen: Die regulären Sprachen, die kontextfreien Sprachen, die kontextsensitiven Sprachen, und schließlich sonstige formale Sprachen. Wir folgen dieser Einteilung und arbeiten für jede dieser vier Klassen die wichtigsten Eigenschaften und Darstellungen heraus.

Informationssicherheit im Internet (auch als Teleteaching) (4 SWS)
Vorlesung: Christoph Meinel
Übung: Volker Schillings

In der Vorlesung werden Fragen rund um den sehr aktuellen Themenkreis der Informationssicherheit im Internet behandelt. In einem ersten Abschnitt der Vorlesung geht es um Werkzeuge und Algorithmen aus der Kryptografie. Vorgestellt werden Konzepte und Verfahren aus der symmetrischen Kryptografie, wie z.B. DES und AES, als auch aus der asymmetrischen Kryptografie, z.B. Diffie-Hellman-Algorithmus und RSA. In einem zweiten Abschnitt geht es um Public-Key-Infrastukturen (PKI), ihre Aufgaben, Komponenten und Funktionsweise. In einem dritten Abschnitt der Vorlesung werden wichtige Sicherheitsprotokolle für das Internet besprochen, z.B. Verschlüsselung digitaler Signaturen und Schlüsselaustausch. Der letzte Abschnitt der Vorlesung ist der Vorstellung von Krypto-Standards im Internet gewidmet, wie z.B. IPSec, SSL, HTTPs. Die Vorlesung wurde mit Hilfe der tele-TASK-Technik aufgezeichnet und online ins Internet übertragen.

Elektronisches Publizieren (4 SWS)
Praktikum: Christoph Meinel, Volker Schillings, Gennadij Umanskij

Mit der zunehmenden Verbreitung von Computern und Computernetzen zum Zweck des Information Retrieval wird auch der Teilbereich des Electronic Publishing - d.h. der elektronischen Verfügbarmachung von Informationen von einem Anbieter für möglichst viele Interessenten mit geringem Aufwand an dezidierter Hardware - weiterentwickelt. Sowohl in der Professur Meinel als auch am Institut für Telematik, Trier, werden theoretische wie praktische Arbeiten besonders im Hinblick auf Internet-gestützte Dienste durchgeführt, die in einem gewissen Maß auch als Modell für andere Formen des Electronic Publishing (wie Verbreitung von Information auf maschinellen Datenträgern) dienen können.

Im Rahmen dieser Zielsetzung wurden eine Reihe von Software-Praktika durchgeführt.

IT-Sicherheit (4 SWS)
Praktikum: Christoph Meinel, Volker Schillings, Gennadi Umanski

Spezifizierung und Realisierung eines Virtual Privat Networks (VPNs). Im ersten Teil des Praktikums sollen bestehende Systeme untersucht und ihre Schwachstellen und Angriffspunkte systematisch ausgearbeitet werden (Funknetzwerke vs. Kabelnetzwerk). Im zweiten Teil des Praktikums soll ein VPN aufgebaut werden. Patch-Workflow. Das Ziel des Praktikums ist die Untersuchung von Realisierungen des automatischen (Sicherheits-) Updates von Betriebssystemen und sonstigen Programmen. Die Unterschiede sollen ausgearbeitet und auf Schwachstellen eingegangen werden. Im zweiten Teil des Praktikums soll eine Methodik ausgearbeitet und umgesetzt werden, welche das Einspielen von (Sicherheits-) Patches für Umgebungen mit heterogenen Betriebssystemen automatisiert. IDS (Intrusion detection system) ist ein Systems zum automtischen Erkennen von Computerattacken. Im Praktikum sollen verschiedene Möglichkeiten eines solchen Systems untersucht und ein IDS realisiert, getetstet und die Ergebnisse ausgewertet werden.
Tigerteam: Das Tigerteam ist eine Gruppe von Spezialisten, welche versuchen Sicherheitslücken in Computersystemen aufzuspüren, um unerlaubten Zugriff auf die Systeme zu erlangen. Ziel des Praktikums ist die systematische Bereitstellung entsprechender Werkzeuge und Angriffsszenarien. Visualisierung von Verschlüsselungsalgorithmen wie DES oder AES (die Algorithmen sollen durch programmierte Flashanimationen visualisiert werden).

Theoretische Informatik (2 SWS)
Forschungsseminar: Christoph Meinel

Seminar am Lehrstuhl Meinel (2 SWS)
Christoph Meinel

Informatik-Kolloquium
Dieter Baum, Christoph Meinel, Bernd Walter, Helmut Seidl, Peter Sturm, Stephan Näher

Oberseminar-Informatik
Dieter Baum, Christoph Meinel, Bernd Walter, Helmut Seidl, Peter Sturm, Stephan Näher

Wintersemester 2002/2003

Diskrete Strukturen und Logik I (4 SWS)
Vorlesung: Christoph Meinel
Übung: Volker Klotz

Die Grundstudiumsvorlesung "Diskrete Strukturen und Logik" führt ein in die für das Informatikstudium im Hauptfach bzw. im Nebenfach grundlegenden Begriffe und Methoden der diskreten Mathematik und der mathematischen Logik. Die Vorlesung ist in die drei Komplexe *Grundlagen*, *Techniken* und *Diskrete Strukturen* gegliedert und behandelt folgende Themenkomplexe:

1. *Grundlagen*: Aussagenlogik; Mengen und Mengenoperationen; Relationen und Funktionen; Folgen und Summen; Algorithmen
2. *Techniken*: Mathematisches Schließen; Zählen
3. *Wichtige diskrete Strukturen*: Boolesche Algebren; Aussagen-und Prädikatenlogik, Graphen und Bäume; Endliche Gruppen.

Internet Security - Weaknesses and Targets (Teleteaching) (4 SWS)
Vorlesung: Christoph Meinel
Übung: Volker Schillings

In this lecture questions are treated around Internet architecture and Internet-Security. Chapter 1 gives an introduction into risk analysis and computer crime.
In Chapter 2, the function mode and architecture of Internet and Intranets is discussed in detail (Internet Protocols-, TCP, Addressing and DNS, Internet Protocol

Next Generation - IPv6, Internet Services - WWW, Email, News, FTP, Telnet, Directory Services - LDAP, Multimedia). Then, in Part 3 of the lecture, based on a well-funded understanding of the TCP/IP-protocol weak points and targets of Internet and Intranets are discussed like: Human Factor - Social Hacking, Collecting System Information, Account - and Password Attacks, Attacks on the IP-, TCP-, UDP-,- and Application Level, Design- and Programming Errors, Weaknesses in UNIX/Linux and in Windows NT/2000, Attacks on Web-Server.
The lecture is presented in English. It is also online transferred into the Internet by means of the tele-TASK-Technique. Due to an agreement with the computer science department of the Beijing University of Technology (China), this lecture is part of the curriculum of computer science students from this University, too.

Elektronisches Publizieren (4 SWS)
Praktikum: Christoph Meinel, Volker Schillings, Gennadi Umanski
siehe Sommersemester 2002

IT-Sicherheit (4 SWS)
Praktikum: Christoph Meinel, Volker Schillings, Gennadi Umanski
siehe Sommersemester 2002

Forschungsseminar Theoretische Informatik (2 SWS)
Christoph Meinel

Seminar am Lehrstuhl Meinel (2 SWS)
Christoph Meinel

Informatik-Kolloquium
Dieter Baum, Christoph Meinel, Bernd Walter, Helmut Seidl,
Peter Sturm, Stephan Näher

Oberseminar-Informatik
Dieter Baum, Christoph Meinel, Bernd Walter, Helmut Seidl,
Peter Sturm, Stephan Näher

Sommersemester 2003 (Forschungsfreisemester)

Informationssicherheit im WWW (nur als Teleteaching) (2 SWS)
Vorlesung: Christoph Meinel
siehe Sommersemester 2002

Neue Webtechnologien (2 SWS)
Seminar: Volker Klotz und Volker Schillings

Die Themen gliedern sich in zwei große Unterpunkte: Semantik im World Wide Web und Personalifizierung von Softwareagenten: Vorgestellt werden aktuelle Entwicklungen zur inhaltlichen Erschließung von Informationsquellen im Internet. Topic Maps, semantische Modelle vernetzter Informationsressourcen unter Verwendung von XML bzw. HyTime, bieten alle notwendigen Modellierungskonstrukte, um Dokumente im Internet zu klassifizieren und ein assoziatives, semantisches Netzwerk über diese zu legen. Weiterhin werden Themen wie Semantic Web, Ontologien und semistrukturierte Daten behandelt werden.
Im Bereich Personalifizierung von Softwareagenten werden wir uns mit verschiedenen Web-Anwendungen und Diensten auseinandersetzen, in denen eine Personalifizierung zu besseren Resultaten und einem verbesserten Angebot führen kann.

Softwarepraktikum (4 SWS)
Praktikum: Christoph Meinel, Volker Schillings, Gennadi Umanski

Am Lehrstuhl Prof. Meinel wird im Sommersemester 2003 ein Softwarepraktikum für Grund- und Hauptstudium angeboten. Grundlage hierzu ist die Programmiersprache PHP in Verbindung mit mySQL. Dem Praktikum vorangestellt wird eine Einführung in HTML/PHP/CSS und PHP. Das Praktikum wird sich dann anschließend mit der Entwicklung eine Opensource Lernplattform beschäftigen. Hierbei werden Teilaufgaben an Gruppen der Größe von 2 bis 3 Personen vergeben. Die Aufgabenstellung muß gelöst und gut dokumentiert werden.

IT-Sicherheit (4 SWS)
Praktikum: Christoph Meinel, Volker Schillings, Gennadi Umanski
siehe Sommersemester 2002

Elektronisches Publizieren (4 SWS)
Praktikum: Christoph Meinel, Volker Schillings, Gennadi Umanski
siehe Sommersemester 2002

Forschungsseminar Theoretische Informatik (2 SWS)
Christoph Meinel

Seminar am Lehrstuhl Meinel (2 SWS)
Christoph Meinel

Informatik-Kolloquium
Dieter Baum, Christoph Meinel, Bernd Walter, Peter Sturm, Stephan Näher

Oberseminar-Informatik
Dieter Baum, Christoph Meinel, Bernd Walter, Peter Sturm, Stephan Näher

Wintersemester 2003/2004

Diskrete Strukturen und Logik I (4 SWS)
Vorlesung: Christoph Meinel
Übung: Volker Klotz
siehe Wintersemester 2002/2003

Komplexitätstheorie (auch als Teleteaching) (4 SWS)
Vorlesung: Christoph Meinel
Übung: Volker Klotz

Ziel der Komplexitätstheorie ist die Quantifizierung von Computerressourcen (Zeit, Speicherplatz, Hardwareaufwand ...), die zur algorithmischen Lösung konkreter Probleme bzw. von Problemklassen benötigt werden. In der Vorlesung, die sich an Studenten des Informatik- bzw. Mathematikhauptstudiums wendet und Kernvorlesung für den Bereich der theoretischen Informatik ist, sollen schwerpunktmäßig die folgenden Themenkomplexe behandelt werden:

- Komplexitätsklassen und ihre Beziehungen
- Reduktionskonzepte
- NP-vollständige Probleme
- Randomisierte Berechnungen
- Approximationstheorie

Internet Security I - Internet Technology (Teleteaching) (2 SWS)
Vorlesung: Christoph Meinel
Übung: Volker Schillings

The lecture course „Internet Security I“ gives a detailed introduction into Internet Technology. It explains the function mode and architecture of Internets and Intranets and discusses important Internet protocols like IP, TCP, UDP, ICMP, as well as Internet addressing and DNS. Moreover, the Internet Protocol Next Generation - IPv6 - will be introduced. Furthermore important Internet services like WWW, email, ftp, telnet, rsh and more will be treated. Encryptions standards like IPSec show possibilities for informatiosecurity. New techniques like LDAP and Multimedia applications will complete this lecture about Internet Technology. The lecture course provides the basic understanding for a discussion of security weaknesses of Internet and Intranets and possible targets for attacks over the Internet which will be treated in the lecture course „Internet Security II - Weaknesses and Target“.

Schaltkreisentwurf und Verifikation (2 SWS)
Proseminar: Volker Klotz

Längst schon sind digitale Schaltkreise zu einem allgegenwärtigen und unverzichtbaren Bestandteil unseres täglichen Lebens geworden. Dabei wächst die Komplexität der Schaltkreise kontinuierlich von Jahr zu Jahr; nach dem Gesetz von Moore verdoppelt sie sich in ein bis zwei Jahren. Dies hat zur Folge, dass der Entwurf von (optimierten) Schaltkreisen immer schwieriger wird, wie auch die mithin lebenswichtige Aufgabe, die Korrektheit von Schaltkreisen zu garantieren. Im Proseminar setzen wir uns mit den Fragen des Schaltkreisentwurfs auseinander als auch mit der Verifikation von Schaltungen (Erreichbarkeitsanalyse, Symbolic Model Checking).

Elektronisches Publizieren (4 SWS)
Praktikum: Christoph Meinel, Gennadi Umanski, Volker Schillings
siehe Sommersemester 2003

IT-Sicherheit (4 SWS)
Praktikum: Christoph Meinel, Gennadi Umanski, Volker Schillings
siehe Sommersemester 2003

4 Dissertationen und Habilitationen

4.1 Dissertationen

Dipl.-Inform. Harald Sack

“Improving the Power of Ordered Binary Decision Diagrams by Integrating Parity Nodes“
Dissertationsschrift, Universität Trier, 2002

Gutachter:

- Prof. Dr. Stefan Waack, Universität Göttingen
- Prof. Dr. Christoph Meinel, Universität Trier
- Prof. Dr. Stefan Näher, Universität Trier

Datum des Dissertationsvortrages: 11.01.2002

Abstract: Hardware bugs can be extremely expensive, financially. Because microprocessors and integrated circuits have become omnipresent in our daily live and also because of their continously growing complexity, research is driven towards methods and tools that are supposed to provide higher reliability of hardware designs and their implementations. Over the last decade Ordered Binary Decision Diagrams (OBDDs) have been well proven to serve as a data structure for the representation of combinatorial or sequential circuits. Their conciseness and their efficient algorithmic properties are responsible for their huge success in formal verification. But, due to Shannon’s counting argument, OBDDs can not always guarantee the concise representation of a given design. In this thesis, Parity Ordered Binary Decision Diagrams (Parity-OBDDs) are presented, which are a true extension of OBDDs. In addition to the regular branching nodes of an OBDD, functional nodes representing a parity operation (Parity-nodes) are integrated into the data structure, thus resulting in Parity-OBDDs. Parity-OBDDs are more powerful than OBDDs are, but, they are no longer a canonical representation. Besides theoretical aspects of Parity-OBDDs, algorithms for their efficient manipulation are the main focus of this thesis. Furthermore, an analysis on the factors that influence the Parity-OBDD representation size gives way for the development of heuristic algorithms for their minimization. The results of these analyses as well as the efficiency of the data structure are also supported by experiments. Finally, the algorithmic concept of Parity-OBDDs is extended to Mod-p-Decision Diagrams (Mod-p-DDs) for the representation of functions that are defined over an arbitrary finite domain.

Dipl.-Inform. Christian Stangier

"High-level Methods for OBDD-based Sequential Verification"
Dissertationsschrift, Universität Trier, 2002

Gutachter:

- Prof. Dr. Dieter Baum, Universität Trier
- Prof. Dr. Christoph Meinel, Universität Trier
- Prof. Dr. Helmut Seidl, Universität Trier

Datum des Dissertationsvortrages: 29.11.2002

Abstract: Today, usage of complex circuit designs in computers, in multimedia applications and communication devices is widespread and still increasing. At the same time, due to Moore's Law we do not expect to see an end in the growth of the complexity of digital circuits.

The decreasing ability of common validation techniques – like simulation – to assure correctness of a circuit design enlarges the need for formal verification techniques. Formal verification delivers a mathematical proof that a given implementation of a design fulfills its specification. One of the basic and during the last years widely used data structure in formal verification are the so called *Ordered Binary Decision Diagrams* (OBDDs) introduced by R. Bryant in 1986.

The topic of this thesis is integration of structural high-level information in the OBDD-based formal verification of sequential systems. This work consist of three major parts, covering different layers of formal verification applications:

1. At the application layer, an assertion checking methodology, integrated in the verification flow of the high-level design and verification tool Protocol Compiler is presented.

2. At the algorithmic layer, new approaches for partitioning of transition relations of complex finite state machines, that significantly improve the performance of OBDD-based sequential verification are introduced.

3. Finally, at the data structure level, dynamic variable reordering techniques that drastically reduce the time required for reordering without a trade-off in OBDD-size are described.

Overall, this work demonstrates how a tighter integration of applications by using structural information can significantly improve the efficiency of formal verification applications in an industrial setting.

5 Kurzbeschreibung der Forschungsbereiche

Die Forschungsarbeiten am Lehrstuhl für Theoretische Konzepte und neue Anwendungen der Informatik konzentrierten sich im genannten Zeitraum auf die folgenden drei Schwerpunkte:

- *Internet-Research und Sicherheit*
- *BDD-basierte Datenstrukturen*
- *Komplexität von Berechnungen*

Die erzielten Forschungsergebnisse wurden auf ausgewiesenen internationalen Tagungen vorgestellt und in den einschlägigen wissenschaftlichen Journalen veröffentlicht bzw. zur Veröffentlichung eingereicht. Sie sind darüber hinaus in Form von Forschungsberichten und Softwaretools weitgehend über World Wide Web

URL: http://www.informatik.uni-trier/∼meinel/

bzw.

URL: http://www.informatik.uni-trier/TI/

abrufbar.

5.1 Internet-Research und Sicherheit

Im Forschungsschwerpunkt **Internet-Research und Sicherheit** haben wir uns mit telematischen Anwendungen in den Bereichen Elektronisches Publizieren, Teleteaching/E-Learning und Telemedizin befasst, wobei sich in allen Bereichen immer wieder Fragen der Sicherheit in den Vordergrund geschoben haben. Viele der Themen aus diesem Bereich wurden im Auftrag von Wirtschaft und Gesellschaft am Institut für Telematik e.V. bzw. in Zusammenarbeit mit dem Institut für Telematik bearbeitet. Am Lehrstuhl haben wir uns schwerpunktmäßig mit dem Thema Elektronisches Publizieren und Teleteaching befasst.

Im Forschungsschwerpunkt **Elektronisches Publizieren und Teleteaching** wird an der Erschließung der Möglichkeiten der neuen elektronischen Kommunikationsmedien, allen voran des Internets, gearbeitet. Anders als der traditionelle Weg der Publikation ermöglicht das Elektronische Publizieren die Verfügbarmachung von Dokumenten weitgehend unabhängig vom bestehenden Verlagswesen. Dabei ist unter „Verfügbarmachung“ weniger die Bereitstellung für einen gezielten Abruf *dieses Dokuments* zu verstehen als vielmehr die Schaffung von Möglichkeiten, das Dokument anhand von Thema, Stichworten, Zitatketten etc. aufzufinden. Für die Erstellung der Dokumente wiederum sind die besonderen Möglichkeiten, die die verwendeten *neuen Medien* bieten, von besonderem Interesse. Speziell in den *Web-Seiten* des *WWW* kommen im Vergleich zu papierbasierten Publikationen multimediale Funktionalitäten wie *Hyperlinks,* bewegte Bilder, Töne etc. hinzu. Folgende Projekte wurden im Berichtszeitraum bearbeitet:

1.) Herausgabe und Weiterentwicklung des *"Electronic Colloquium on Computational Complexity" (ECCC).* In diesem internationalen elektronischen Forschungsarchiv, das im WWW unter der URL

`http://www.eccc.uni-trier.de/eccc/`

zu erreichen ist, veröffentlichen die Forscher auf dem Gebiet der *Computational Complexity* ihre aktuellen Forschungsergebnisse. Die Erfahrungen mit diesem bereits seit 1994 erfolgreich betriebenen Projekt wurden wissenschaftlich aufbereitet und unter anderem auf der Konferenz SIGDOC '98 vorgestellt. Das vorhandene Archiv wird zusätzlich seit 2000 jährlich in Form einer CDROM publiziert.

2.) Ein weiteres Projekt *OBDD Heuristics Online (OHO)*, das die Forschungsschwerpunkte elektronisches Publizieren und BDD-basierte Datenstrukturen miteinander verbindet, sucht einen neuralgischen Punkt bei der BDD-Forschung zu überwinden, nämlich den, daß die Hersteller von integrierten Schaltkreisen nur äußerst ungern Schaltkreisentwürfe, die Stand der Technik sind, nach außen geben — die Entwerfer von Algorithmen und Datenstrukturen benötigen aber genau solche Entwürfe als *Benchmarks,* um die Anwendbarkeit ihrer Neuerungen beurteilen zu können. Bei OHO werden nun Implementationen dieser Neuerungen einerseits und Benchmarks andererseits auf einem zentralen Server zusammengeführt mit einem WWW-Interface für die Einspeisung der Benchmarks. Auf diese Weise müssen die Benchmarks nicht mehr uneingeschränkt veröffentlicht, sondern nur noch bei Bedarf an eine einzelne vertrauenswürdige Stelle übermittelt werden.

3.) Ein weiteres Projekt beschäftigt sich mit der Visualisierung komplexer Algorithmen und Strukturen. Die Visualisierung soll dazu dienen, sowohl Studenten als auch Praktikern das Verständnis und das Begreifen der visualisierten Sachverhalte zu erleichtern. Neben der Visualisierung von Kommunikationsabläufen im Intra- und

Internet, die mit Hilfe von Studenten in die Tat umgesetzt worden sind, wurde in dem Projekt *visBDD* der Versuch unternommen, den komplexen OBDD-Synthese-Algorithmus in geeigneter Form graphisch und in multimedialer Form umzusetzen.

4.) Der Bereich *Teleteaching*, zu dem bereits auch das bereits angesprochene Projekt *visBDD*, sowie die bereits realisierten Visualisierungen zählen, gewann im Wintersemester 2001 große Aufmerksamkeit, als erstmals mit Hilfe eines neuentwickelten praxistauglichen Systems tele-TASK

`http://www.tele-task.de/`

eine Informatikvorlesung sowohl live online, als auch später in archivierter Form über das Internet angeboten werden konnte. Neben einem Videobild des Dozenten wurde das Tafelbild in hoher Qualität sowie natürlich der Ton übertragen. Die Bemühungen in diesem Bereich zielten darauf ab, eine technisch möglichst einfache Umgebung für alle Beteiligten zu schaffen, die sie ohne große Mühe in die Lage versetzten, das Teleteaching-Angebot zu nutzen, sowie eine Reduktion der notwendigen Bandbreite herbeizuführen.

5.) Der Lehrstuhl hat eine WWW-Portalsite

`http://www.bdd-portal.org/`

aufgebaut, die ein aktuelles Link-Archiv über Forscher, Forschungsgruppen, Publikationen, sowie Programmpakete und einen Konferenzkalender aus allen Bereichen der BDD-Forschung unterhält.

6.) Das im November 1997 eröffnete *Zentrum für Wissenschaftliches Elektronisches Publizieren (WEP)*

`http://www.wep.uni-trier.de/`

veranstaltete eine Reihe von Gastorträgen und Kolloquien und ist beratend an fächerübergreifenden Projekten, wie z.B. mit der Germanistik, der Linguistik oder der Politikwissenschaft beteiligt. Die Aktivitäten des WEP wurden im März 2001 mit großem Erfolg auf der CeBit 2001 vorgestellt, auf der das WEP als Aussteller präsent war.

5.2 BDD-basierte Datenstrukturen

Im Forschungsschwerpunkt **BDD-basierte Datenstrukturen für boolesche Funktionen** wurden Datenstrukturen für die Repräsentation und Bearbeitung von booleschen (also 0-1-wertigen) Funktionen entworfen und analysiert. Der vielgestaltige praktische Einsatz dieser Datenstrukturen z.B. in CAD-Systemen zum Schaltkreisentwurf oder in Tools zur Verifikation von sequentiellen Systemen, elektronischen Schaltkreisen oder Kommunikationsprotokollen machte Bemühungen zur Optimierung und Kompaktifizierung solcher Strukturen zu einem sehr lohnenden Forschungsziel. Im einzelnen lassen sich die in diesem Forschungsschwerpunkt behandelten Fragestellungen folgendermaßen zusammenfassen:

1.) Der einzige Weg, die BDD-Größe zu verringern, liegt in der Bestimmung einer geeigneteren Variablenordnung. Als wirkungsvollste Methode hat sich hierzu das dynamische Umordnen der Variablen erwiesen. Problematisch ist dabei lediglich das oftmals sehr schlechte und für den praktischen Einsatz nicht darstellbare Zeitverhalten. Daher wurde intensiv an Techniken zur Beschleunigung des dynamischen Umordnens gearbeitet. Die entwickelten Methoden und Heuristiken basieren jeweils auf der Auswertung struktureller oder semantischer Informationen.

Die Heuristiken wurden erfolgreich in der *kombinatorischen Verifikation* eingesetzt. Um auch einen Einsatz auf den sehr anspruchsvollen Gebieten der *Erreichbarkeitsanalyse* und des *symbolisches Model Checking* zu ermöglichen wurden die Heuristiken an die speziellen Erfordernisse dieser Gebiete angepasst und erweitert.

2.) Eine weitere Steigerung der Effizienz der BDD-Datenstrukturen stellt die Erweiterung durch Relaxation von Strukturrestriktionen zum Beispiel und Einbringung zusätzlicher Funktionalelemente dar. In Free-BDDs kann auf jedem Berechnungspfad von der Wurzel zur Senke eine andere Ordnung der Eingabevariablen vorliegen. $\oplus$-OBDDs hingegen stellen eine Erweiterung der OBDD-Datenstruktur hinsichtlich der Funktionalität der einzelnen Knoten innerhalb des Entscheidungsdiagrammes dar. Zusätzlich zu den bekannten Entscheidungsknoten werden Operatorknoten eingeführt, die im Falle von $\oplus$-OBDDs die Parität der beiden Vorgängerknoten berechnen und in vielen Fällen eine kompaktere Darstellung ermöglichen. Am Lehrstuhl wurden Programmbibliotheken zur effizienten Manipulation von Free-BDDs und $\oplus$-OBDDs entwickelt und gepflegt.

3.) Nach Anwendung einer geeigneten linearen Transformation auf den Definitionsbereich einer Booleschen Funktion kann diese oft sehr viel kompakter als OBDD dargestellt werden, als dies ohne Transformation möglich wäre. Von besonderem Interesse bei dieser Herangehensweise ist, daß der grundlegende Vorteil der guten algorithmischen Handhabbarkeit von OBDDs nicht verloren geht. Bestehende BDD-Programmpakete wurden hinsichtlich dieser Funktionalität erweitert und finden nun

Einsatz in der formalen Verifikation.

4.) Der praktische Umgang mit BDDs zeigt, daß für die jeweils darzustellenden Funktionen oft sehr stark unterschiedliche Variablenordnungen geeignet sind. Es wurde deshalb ein Programmpaket zur Synthese von BDDs entwickelt, das OBDDs mit unterschiedlichen Variablenordnungen bearbeiten kann. Erklärtes Ziel ist es, Heuristiken zu entwerfen, die - jeweils im Kontext einer Anwendung in der formalen Verifikation - gut geeignete gemeinsame Variablenordnungen ermitteln.

5.) Der Kern jeglicher formaler sequentieller Verifikation ist die Berechnung der erreichbaren Zustände. Problematisch bei der OBDD-basierten Erreichbarkeitsanalyse ist die Repräsentation der Transitionsrelation, die meistens partitioniert wird. Nur eine gute Partitionierung erlaubt eine effiziente Berechnung. Es wurden Heuristiken entwickelt, die die Qualität der Partitionierung erheblich verbessern und so die Analyse von industriellen Protokollen vereinfachen bzw. erst ermöglichen.

6.) Wenn formale Verifikation in einem industriellen Umfeld nicht angewendet wird, liegt das oft daran, daß sie nicht in den Entwicklungszyklus passt, am Lehrstuhl wurde eine Methodik entwickelt, die die formale Verifikation von Protokollen in den Entwicklungszyklus integriert. Die daraus resultierenden gestiegenen Anforderungen an die BDD-Technologie werden ebenfalls untersucht.

5.3 Komplexität von Berechnungen

Im Forschungsschwerpunkt **Komplexität von Berechnungen** ging es um zentrale Fragestellungen aus dem Kernbereich der Forschung in der theoretischen Informatik, nämlich um die Charakterisierung des Ressourcenbedarfs – insbesondere des Ressourcenmindestbedarfs – für konkrete Berechnungen. Im einzelnen waren die in diesem Forschungsschwerpunkt angesiedelten Arbeiten vornehmlich der Untersuchung folgender Fragestellungen gewidmet:

1.) Untersuchung der *Schaltkreiskomplexität*. Hier wurden Ressourcenbedarfsgrenzen (sogenannte untere und obere Schranken) für die Berechnung konkreter Probleme durch Schaltkreise und verwandte Berechnungsmodelle untersucht. Es wurden:

- Zusammenhänge zwischen Booleschen und algebraischen Berechnungen untersucht und Komplexitätsklassen durch algebraische Probleme charakterisiert;
- untere Schranken für zahlentheoretische Probleme mit Fourier-analytischen Methoden nachgewiesen;
- untere Schranken für die mittlere Sensitivität zahlentheoretischer Funktionen nachgewiesen und untere Schranken für Entscheidungsbäume und Formeln abgeleitet;

- ein einfaches *kombinatorisches* Untere-Schranken-*Kriterium* für monotone Schaltkreise gefunden und damit ein vor 15 Jahren von A. Razborov gestelltes Problem gelöst;
- ein Entropie-Ansatz zur Ableitung unterer Schranken für Verzweigungsprogramme gefunden. Dies hat exponentielle untere Schranken sogenannter "gentle programs" geliefert, wo alle bisher bekannte Methoden versagt haben.

2.) Untersuchung der *Kommunikationskomplexität*. Es konnte gezeigt werden, daß arithmetische Varianten von verteilten Berechnungen die üblichen nichtdeterministischen Varianten approximieren können, obwohl im Sinne der Simulierbarkeit arithmetische und Boolesche Kommunikationskomplexität unvergleichbar sind. Dieses Resultat konnte noch erweitert werden auf alternierende Kommunikationskomplexität.

3.) Untersuchung der *Instanzen-Komplexität*. Es wurde ein Begriff angegeben, mit dem "harte Instanzen" – d.h. Instanzen, die ein Problem zu schwierig für Berechnungen unter bestimmten Ressourcenbeschränkungen machen – bestimmt werden können. Dieser Begriff basiert auf dem Vergleich von Instanzen- und Kolmogoroff-Komplexität. Daraus ergeben sich Charakterisierungen der Klassen der semi-entscheidbaren, entscheidbaren und effizient entscheidbaren Probleme.

4.) Untersuchung der *Komplexität Markoff'scher Entscheidungsprozesse*. Abhängig von verschiedenen Parametern betreffend die Sichtbarkeit, Darstellung und Steuerungsmöglichkeit wurden Markoff'sche Entscheidungsprozesse bezüglich ihrer strukturellen Komplexität untersucht. Dabei ergaben sich Vollständigkeitsresultate für bekannte Komplexitätsklassen wie NL, P, NP und PSPACE, aber auch für interessante Zählklassen wie PL, PP, P^{PP} und $\mathrm{NP}^{\mathrm{PP}}$. Darüberhinaus wird die Approximierbarkeit der Probleme betrachtet.

6 Drittmittelprojekte am Lehrstuhl

Linear-Algebraische Berechnungsmodelle für Boolesche Funktionen und ihre Anwendung

Förderer: Deutsche Forschungsgemeinschaft – DFG
Förderzeitraum: 1999 - 2004

Über die zahlreichen, vornehmlich durch die Wirtschaft finanzierten Drittmittelprojekte, die am Institut für Telematik bearbeitet werden, wird an anderer Stelle berichtet, z.B. im Tätigkeitsbericht des TI.

7 Bücher und Buchbeiträge

7.1 Bücher

Christoph Meinel, Martin Mundhenk
Mathematische Grundlagen der Informatik
Mathematisches Denken und Beweisen - Eine Einführung
2. Auflage, B.G. Teubner (Stuttgart, Leipzig), 2002, ISBN 3-519-02949-9

Abstract: Konzepte und Anwendungen der Informatik durchdringen in immer stärkerem Maße alle Bereiche der Wirtschaft und Gesellschaft; ohne ihr Grundverständnis ist deshalb ein erfolgreiches Wirken dort zunehmend unmöglich. Das daraus resultierende große Interesse auch bei Nichtinformatikern an der Informatik und ihren intellektuellen Grundlagen macht eine Einführung auch in die mathematischen Grundlagen der Informatik immer dringlicher, eine Einführung, die auch ohne eine traditionell vorausgesetzte mathematische Grundausbildung auskommt und trotzdem sachkundig in die für die Informatik typischen und grundlegenden mathematischen Denkweisen und Formalisierungen einführt. Das vorliegene Buch hat sich diese Aufgabe zum Ziel gestellt. Es führt den interessierten Leser ein in das für die Informatik typische Vorgehen, zunächst noch vage Ideen und KonzepteCh. Meinel, L. Gollan Numerous Articles of IT-Security and Digital Signatures In: Die Deutsche Bibliothek - CIP-Einheitsaufnahme - Lexikon Electronic Business , Th. Schildhauer, Oldenburg Wissenschaftsverlag GmbH, München, 2003 schrittweise zu formalisieren und damit einer Bearbeitung durch den Computer

Christoph Meinel, Harald Sack
WWW–Kommunikation, Internetworking, Web-Technologien
Springer-Verlag, Berlin, Heidelberg, New York, 2004, ISBN 3-540-44276-6

Abstract: Dieses Handbuch bietet für alle Nutzer und Entwickler des World Wide Web einen fundierten Einblick in dessen Aufbau und Funktionsweise. Die Autoren stellen die Internet-Technologie ausführlich dar und geben einen umfassenden Überblick über die relevanten Teilbereiche des WWWW. Neben den allgemeinen theoretischen und praktischen Grundlagen der Netzwerktechnik und einer Darstellung der TCP/IP-Protokolle werden auch die vielfältigen Medientypen und deren Kodierung im WWW erläutert. Darauf aufbauend wird auf spezielle Web-Technologien im WWW wie HTTP, HTML, CSS, XML/XSL aber auch Skriptsprachen und CGI-Programmierung eingegangen. Dabei werden die allgemeinverständlich angelegten Kapitel punktuell durch relevante Schwerpunktthemen technischer Natur ergänzt und vertieft. Zahlreiche Abbildungen sowie Index und Glossar zu jedem Kapitel erhöhen den praktischen Nutzen des Handbuchs.

7.2 Buchbeiträge

Christoph Meinel, Harald Sack, Arno Wagner
WWW.BDD-Portal.ORG: An Experimentation Platform for Binary Decision Diagram Algorithms
In: Experimental Algorithmics, R. Fleischer, E. Meineche Schmidt, B. Moret
LNCS 2547, Springer Verlag, Berlin, Heidelberg, New York, pp. 127-137, 2002

Christoph Meinel, Christian Stangier
Algorithms and Heuristics in VLSI Design
In: Experimental Algorithmics, R. Fleischer, E. Meineche Schmidt, B. Moret,
LNCS 2547, Springer Verlag, Berlin, Heidelberg, New York, pp. 139-159, 2002

Ch. Meinel, L. Gollan
Numerous Articles of IT-Security and Digital Signatures
In: Die Deutsche Bibliothek - CIP-Einheitsaufnahme - Lexikon Electronic Business,
Th. Schildhauer, Oldenburg Wissenschaftsverlag GmbH, München, 2003

8 Herausgeberschaft

8.1 Proceedingsbände

Christoph Meinel, M. Bittner, U. Sandl, I. Münch (Eds)
eSecurity, Net-Security & Trusted eCommerce
Proceedings Online 2002 - Congress IV
Online-Verlag, ISBN 3-89077-222-6, 2002

Christoph Meinel, Frank Rudolf (Eds)
Digitales Geld
Proceedings Trierer Symposium Digitales Geld, Trier, Germany, 2002,
Institut für Telematik, ISSN 1433-8106, 2002

Christoph Meinel, Ulf Birkel, Frank Rudolf (Eds)
Sichere Telemedizin
Proceedings Trierer Symposium Sichere Telemedizin, Trier, Germany, 2002,
Institut für Telematik, ISSN 1433-8106, 2002

T. Becker, Ch. Meinel
Sicherheit: Der entscheidende Erfolgsfaktor für eCommerce und mCommerce Proceedings Online 2003 - Congress IV
ONLINE-Verlag, ISBN 3-89077-222-6, 2003

Ch. Meinel, H. Sack
Representations and Methodology of Future Computing Technologies
Proceedings of International Symposium RM 2003,
University of Trier, Germany 2003

8.2 Web-Sites

„ECCC.uni-trier.de“

Seit Ende 1994 wird am Lehrstuhl „Theoretische Konzepte und neue Anwendungen der Informatik” das „Electronic Colloquium on Computational Complexity — ECCC” herausgegeben.

„www.tele-task.de“

Eine WWW-Portalseite mit einem reichen Teleteaching-Angebot an Vorlesungsaufzeichnungen, Konferenzmitschnitten, Kolloquiumsvorträgen usw.

„www.bdd-portal.org“

Eine WWW-Portalsite mit umfassendendem Informationsangebot und Link-Archiv zu allen Themengebieten rund um die Datenstruktur OBDD. Zusätzlich wird eine standardisierte Testumgebung für BDD-Experimente mit dem System *OHO* bereitgestellt.

„www.informatik.uni-trier.de/GI/FG-014/"

Regelmäßig werden von Christoph Meinel, dem Sprecher der GI-Fachgruppe 0.1.4 „Komplexität", Jochen Bern (bis zum 31.09.2000) und Rustam Mubarakzjanov (ab 01.10.2000) aktualisierte WWW–Seiten mit Informationen zu Konferenzen, Theorietagen, Graduiertenkollegs, Sommerschulen, Stellenangeboten etc. für die Mitglieder der Fachgruppe „Komplexität der deutschen Gesellschaft für Informatik (GI)" veröffentlicht.

9 Veröffentlichungen

9.1 Veröffentlichungen in Zeitschriften

Ch. Meinel, L. Gollan
Der elektronische Personalausweis? - Elektronische Signaturen und staatliche Verantwortung
JurPc - Internet-Zeitschrift für Rechtsinformatik, Web-Dok.223/2002, Abs. 1-15, 2002

M. Schmitt, J. Hu, Ch. Meinel
A Tutoring System for IT Security Education
Journal of Information Warfare, Vol. 2, Isse 3, 79-85, 2003

V. Schillings, Ch. Meinel
tele-TASK - Teleteaching - Anywhere Solution Kit
Information Wissenschaft u. Praxis (DGI), Heft 1/2003, pp. 21-26, 2003

9.2 Veröffentlichungen in Tagungsbänden

Christoph Meinel, Harald Sack, Volker Schillings
Course Management in the Twinkle of an Eye
In Proc: SIGUCCS 2002, Providence, Rhode Island, USA, pp. 281-283, 2002

Abstract: In this paper we describe a course management system for university lectures and lab courses, called LCMS. Started as a simple registration tool for students, signing up for lab courses and examinations, LCMS has been developed into a powerful system, assisting the lecturer and the lab course administrator in the management of entire courses. LCMS tasks are ranging from course registration, student data administration, creation of course webpages, design and administration of exercises and test sheets, up to the design of certificates for successful course participation. For three years in use now, LCMS has become an essential tool for student administration. It is freely available and can easily be adapted to any kind of course management.

Christoph Meinel, Rustam Mubarakzjanov
Nonlinear Sifting of Decision Diagrams
In: Proc. VLSI 2002, Las Vegas, Nevada, USA, pp. 117-127, 2002

Abstract: We propose a new algorithm for the optimization of decision diagrams that combines the efficiency of sifting and the power of transformations. We show that the new algorithm is applicable to large examples, and that in many cases it leads to more compact diagrams when compared to linear sifting algorithm known to be more efficient than simple variable reordering.

Christoph Meinel, Harald Sack, Volker Schillings
VisBDD - A Webbased Visualization Framework for OBDD Algorithms
In: Proc. IWLS 2002, New Orleans, Louisiana, USA, pp. 385-390, 2002

Abstract: This paper presents a web-based visualization framework visBDD, intended for learning and understanding basic algorithms related to Ordered Binary Decision Diagrams (OBDDs). With visBDD the key algorithm for OBDD-synthesis the ITE-algorithm can be explored in depth and step-by-step by the user, while all involved data structures can be made visible at different levels of abstraction. The framework is intended as well as for students as also for professionals, who want to gain more insight into the powerful OBDD data structure that is used in many verification and synthesis tools, for a better understanding of the underlying mechanisms and the problem complexity, without being dependent on reading textbooks.

Christoph Meinel, Christian Stangier
Modular Partitioning and Dynamic Conjunction Scheduling in Image Computation
In: Proc. IWLS 2002, New Orleans, Louisiana, USA, pp. 391-396, 2002

Abstract: Image computation is the core task in any formal verification applications like reachable states computation or model checking. In OBDD-based image computation a partitioned representation of the transition relation is used. The quality of the partitioning and the schedule in which the partitions are processed is crucial for the efficiency of the image computation. In this paper we describe an approach to build a hierarchical modular partitioned transition relation. Based on this partitioning we present a dynamic conjunction scheduling algorithm that improves the flexibility and computational power of the image computation. The concept is proven by symbolic model checking experiments.

Volker Schillings, Christoph Meinel
tele-TASK-Teleteaching Anywhere Solution Kit
In Proc: SIGUCCS 2002, Providence, Rhode Island, USA, pp. 130-133, 2002

Abstract: With the help of the new developed system tele-TASK - Teleteaching Anywhere Solution Kit - [2] [7] a new, drastically simplified entrance technology for on-line lectures is reached. Out of the apartment or the office each PC user with a suitable Internet connection can follow online lessons comfortably. Even an interested layman is able to access the courses. Not only content of teaching are delivered, which are presented to the students in the lecture-room by either a whiteboard or a video beamer, but simultaneously also video and audio of the lecutrer. Navigation bar for accessing different parts in the recorded lecture are included. Tele-TASK supports all usual platforms, differerent net bandwiths, arbitrary presentation programs and needs no special software installations, configurations and no precognition of the end-users. For the first time, the system was deployed for recording, transmission and archiving of the computer science lecture ïnformation security in open networksät the University of Trier in the summer semester 2002. High access numbers are expression of the perfectly problem-free and easy possibilities of using.

Tongbo Chen, Mingchao Ma, Christoph Meinel, Volker Schillings
A Novel Approach to E-Learning Content Creation
In: Proc. m-ICTE 2003, Badajoz, Spain, pp. 410-414, 2003

Abstract: Modern information technologies are transforming the way people learn. E-learning provides new possiblities for personalized learning at home or in the workplace, reduces the need for costly classroom training and enables an optimal

balance between traditional and innovative forms of knowledge transfer. But facts have proven that content creation for online courses are time-consuming and costly. Also most of them are not easy to call up. A simple and efficient solution of content creation for online courses is strongly required. Our new system, tele-TASK [2] - Teleteaching Anywhere Solution Kit, paves the way for these institutions. With the help of the new developed system tele-TASK a new, drastically simplified entrance technology for on-line lectures has been reached. From his apartment or office each PC user with a suitable Internet connection can follow online lessons comfortably. Not only contents of teaching, which are presented to the students in the lecture-room by either a whiteboard or a video beamer are delivered, but also video and audio of the lecturer. For tele-TASK a special hardware (t-Cube) is now available, which permits the creation of Real or Mpeg4 streams in different bandwidth ranges on the fly. Thus an installed standard player can be used.

Feng Cheng, Ch. Meinel, Th. Engel, Gerhard Müllenheim, Jochen Bern, Dominik Thewes
A Complete Solution for Highly Secure Data Exchange: Lock-Keeper and its Advancements
In: Proc. IEEE PDCAT 2003, Chengdu, China, pp. 201-205, 2003

Abstract: The Lock-Keeper is a new network security solution which can provide secure data transfers between two different networks without having to establish a direct physical connection. By means of the Lock-Keeper system, the possibility of direct attacks to the protected network can be eliminated. An actual system, the Single-Gate Lock-Keeper, is used as an example to introduce the Lock-Keeper concept in detail, including its architecture, funtionalities, applications, vulnerabilities and benefits. Based on this system, a new advanced DualGate Lock-Keeper including another “gate” unit is prepared that can provide more efficient and secure data exchange and make extensions of the Lock-Keeper applications possible.

Feng Cheng, Paul Ferring, Christoph Meinel, Gerhard Müllenheim, Jochen Bern
The DualGate Lock-Keeper: A Highly Efficient, Flexible and Applicable Network Security Soulution
In: Proc. SNPD 2003, Lübeck, Germany, pp. 152-159, 2003

Abstract: The idea of data transfer by phyically severed connections has been applied in a simple realization of the Lock-Keeper technology, the SingleGate Lock-Keeper system. By means of it, the possiblity of direct attacks to a protected network can be eliminated entirely and data can be exchanged between two networks through a completely secure and reliable way. As an advanced implementation of this technology, the DualGate Lock-Keeper is proposed by including another new “gate” unit.

Along with this development, not only the Lock-Keeper performance on data transfer, especially the transmit speed, is improved significantly, but also some other new good characteristics appear simultaneously. All these changes make the DualGate Lock-Kepper more efficient, flexible and applicable. Moreover, an architecture and its working principle of the Lock-Keeper Cluster which is built up by two DualGate Lock-Keeper are analyzed in detail in this paper.

Mohammad GhasemZadeh, Christoph Meinel
BDDs, Horn Clauses and Resolution
In: Proc. RM2003, Trier, Germany, pp. 63-38, 2003

Abstract: In this research we present the utilization of BDDs in representing propositional logic programs and implementing the refutation by resulotion deduction method. A logic program is a collection of axioms from which a goal clause can be proven. Axioms are written in a standard form known as Horn clauses. In logic programming, we try to find a collection of axioms and inference steps that imply the goal. The standard and usual method for this kind of inference is r "refutation by resolution". Binary Decision Diagrams, shortly called BDDs, are data structures proposed for representing switching functions. DDs have been found more practical and more efficient in time and space than other switching function representation methods. One may consider a Horn clause as a switching function and represent it as a BDD. In the same way, all the clauses of a propositional logic program and the gaol clause can be representedby menas of a multi-rooted BDD. Because of the characteristics of BDDs we can make the inference in some other methods in addition to the standard method. In this paper, this kind of representation as well as proving the goal in formal linear resolution and Non-linear resolution are investigated.

Wanjun Huang, Uwe Roth, Christoph Meinel
A Flexible Middleware Platform with Piped Workflow
In: Proc. WRSM 2003, Sicily, Italy, pp. 950-959, 2003

Astract: Middleware emerges as an excellent solution for the complicated distributed computing application. But as the appearance of new devices and new applications, the flexibility of traditional middleware system becomes more serious and urgent. In this paper we propose a workflow and computational modules to provide a modular and extensible platform for future applications. The piped workflow provides a very flexible mechanism to organize all computational modules working together. During the running time, all computational modules communicate only with data channel of the piped workflow through with they can keep extremely independent, and the flexible flow control strategy makes the application programmer convenient to arrange all functional components for variable customer requirements.

Chunjan Jiang, Lutz Vorwerk, Christoph Meinel
Concept for DICOM about 3D data interchange
In: Proc. TTC 2003, Tromso, Norway, pp. 40, 2003

Abstract: Digital imaging and communications in medicine abbreviated as DICOM, is the ubiquitous standard in the radiology digital imaging industry for the exchange of image and related information. DICOM defines format and communication standard of 2d image. Many applications and equipments which conform to DICOM have been put into use. DICOM is much helpful for the archiving, retrieving and communicating of the medical image and associated information.

Mingchao Ma, Volker Schillings, Tongbo Chen, Christoph Meinel
T-Cube: A Multimedia Authoring System for eLearning
In: Proc. AACE E-Learn 2003, Phoenix, Arizona, USA, pp. 2289-2296, 2003

Abstract: eLearning has become an alternative approach to the traditional college and university of education. Experiments have shown that producing of the teaching contents for eLearning is a time-consuming and costly job. This paper introduces a programming-free and easy-to-use multimedia authoring system, T-Cube, designed and already been used at the University of Trier for eLearning. As a rich-media authoring system, T-Cube constructs and presents multimedia contents to students with multi-rate for either offline (CD/DVD/download) or online (in real time or on demand) usage. The rich-media teaching contents, including video, audio and screenshot, are recorded and encoded at the classroom and simultaneously published on the Internet. Broadband users can access the lecture in real time as if they were sitting in the classroom. After being compressed and encoded, the teaching contents are also available for narrowband users on demand. Further, the contents on CD/DVD are also available on request. This paper focuses on describing the features, practical experiments and assessments of t-Cube system.

Christoph Meinel, Harald Sack
Variable Reordering for $\oplus$-OBDDs
In: Proc. RM2003, Trier, Germany, pp. 135-144, 2003

Abstract: Ordered Binary Decision Diagrams (OBDDs) have already proved useful in the process of electronic design automation. Due to limitations of the descriptive power of OBDDs more general models of Binary Decision Diagrams have been studied. In this paper, $\oplus$-OBDDs as a true extension of the OBDD data structure are addressed. As for OBDDs, the most important factor influencing the representation size of $\oplus$-OBDDs is the chosen order of the input variables. Adaptive variable reordering heuristics as sifting for OBDDs can be adapted to $\oplus$-OBDDs, while some important restrictions arise from the property of being a non canonical data structure. The viability and the efficiency of the adapted sifting algorithm for $\oplus$-OBDDs is shown by symbloic simulation of standard benchmarks.

Christoph Meinel, Volker Schillings, Vanessa Walser
Overcoming Technical Frustrations in Distance Education: tele-TASK
In: Proc. e-Society 2003, Lisboa, Portugal, pp. 34-41, 2003

Abstract: Modern information technologies are transforming the way people learn. E-learning provides new possibilities or personalized learning at home or in the workplace, reduces the need for costly classroom training, and enables an optimal balance between traditional and innovative forms of knowledge transfer. But facts have proven that content creation for online courses is time-consuming and costly. Also most of them are not easy to call up. A simple and efficient solution of content creation for online courses is strongly required. Our new system, tele-TASK [1]-Teleteaching Anywhere Solution Kit, paves the way for these requirements. With the help of the new developed system tele-TASK a new, drastically simplified entrance technology for on-line lectures has been reached. Not only contents of teaching, which are presented to the students in the lecture-room by either a whiteboard or a video beamer are delivered, but also video and audio of the lecturer. For tele-TASK a special hardware (T-Cube) is now available, which permits the creation o Real or Mpeg4 streams in different bandwith ranges on the fly. Thus a pre-installed standard player can be used.

Christoph Meinel, Ji Hu, Michael Schmitt, Christian Willems
A Tutoring System for IT-Security
In Proc. IFIP WISE 2003, Monterey, California, USA, pp. 51-60, 2003

Abstract: Due to the many vulnerabilities of today‘s computer systems, IT security education has become an important topic. For that reason, a new tutoring system is developed at the Institute for Telematics, Trier, that allows users to gain knowledge about security technologies and tools via a web browser interface. Unlike other systems, this tutoring system does not provide a resticted simulation environment. Instead, guided exercises are performed on a real system (linux). In this papers, the user interface and architecture of the tutoring system as well as some implementation aspects and future enhancements are described.

Xinhua Zhang, Christoph Meinel, A. Dulaunoy
A Security Improved opensst Prototype combining with Smart Card
In: Proc. IEEE ICCNMC 2003, Shanghai, China, pp. 358-361, 2003

Abstract: Open Simple Secure Transaction (OpenSST) protocol aims to be a secure and transaction-orientated protocol for the unsecured network. OpenSST is an open source project, at present a simple prototype based on HTTP protocol has been implemented. In this paper, we give firstly an overview of openSST, and then we describe the basic architecture of this prototype, as well as make an analysis on its security. Then we introduce a security-enhanced model based on this prototype, which utilize the tamper-resistant nature of Smart Card. We will discuss several possible ways of integrating Smart Card into the OpenSST.

Xinhua Zhang, A. Dulaunoy, Christoph Meinel
Enhance opensst Protocol's Security with Smart Card
In: Proc. WWW/Internet 2003, Algarve, Portugal, pp. 565-571, 2003

Abstract: As an open source project, Open Simple Secure Transaction (OpenSST) protocol aims to be a secure and transaction-oriented protocol for the unsecured network. At present a prototype has been implemented. In this paper, we give firstly an overview of OpenSST, and then we describe the key store and authentication mechanism of the prototype, as well as make an analysis on its security. Then we introduce a security-enhanced model based on this prototype, which integrates Smart Card into the OpenSST protocol. This model demonstrates how to use Smart Card to improve the public key authentication process in a secure network protocol.

Torsten Becker, Christoph Meinel
Sicherheit: Der entscheidende Erfolgsfaktor für ECommerce und M-Commerce
In: Proc. ONLINE 2003, Düsseldorf, Germany, pp. C421.03-C421.08, 2003

Abstract: Laut "(N)ONLINER Atlas 2003"sind über 50 Prozent der Deutschen im Jahr 2003 im Internet. Dies ist im Vergleich zum Vorjahr eine Steigerung um 8 der Anteil der Online-Käufer nimmt kontinuierlich zu. Mittlerweile haben unter den Online-Nutzern rund zwei Drittel Erfahrungen mit Online-Käufern und -Buchungen. Das heißt aber auch, dass etwa ein Drittel der Online-Nutzer keine Geschäfte über das Internet abwickeln. Laut einer Studie der Unternehmensberatung Accenture liegt beispielsweise die größte Hemmschwelle der Kunden bei einem Online-Kauf darin, persönliche Daten ungeschützt über das Internet zu übermitteln. Dies führt laut Accenture in Deutschland zu einem jährlichen Umsatzausfall in Milliardenhöhe. Auch Fittkau und Maaß haben in einer Studie ermittelt, dass bei den Anforderungen der Nutzer an Online-Finanzdienstleister die sicherheit der Datenübertragung im Vordergrund steht. Eine Studie von ComCult Research verstärkt dies: "Sicher-

heitsbedenken der Nutzer sind die größte Barriere beim Online-Shopping. Sie werden als Hauptgrund dafür genannt, dass Nicht-Shopper bisher noch keine Erfahrung im Online-Shopping gesammelt haben und das Shopper nicht häufiger online bestellen. Shopper und Nicht-Shopper sind sich einig, dass die sichere Übermittlung der Zahlungsdaten bedenklich ist." Zu den Erfolgsfaktoren im E-Commerce und M-Commerce gehören demnach der konsequente Aufbau von Vertrauen von Datenschutzinformationen und die sichere Datenübermittlung.

9.3 Vorabveröffentlichungen in der Reihe Forschungsberichte Mathematik/Informatik der Universität Trier

Randy Bryant, Christoph Meinel
Ordered Binary Decision Diagrams in Electronic Design Automation
Forschungsbericht Nr. 02-20

Abstract: Ordered Binary Decision Diagrams (OBDDs) play a key role in the automated synthesis and formal verification of digital systems. They are the state-of-the-art data structure for representing switching functions in various branches of electronic design automation. In the following we discuss the properties of this data structure, characterize its algorithmic behaviour, and describe some prominent applications.

Volker Schillings, Christoph Meinel
tele-TASK - Teleteaching Anywhere Solution Kit
Forschungsbericht Nr. 02-21

Abstract: With the help of the new developed system tele-TASK - Teleteaching Anywhere Solution Kit - [2] [7] a new, drastically, simplified entrance technology for on-line lecutres is reached. Out of the apartment or the office each PC user with a suitable Internet connection can follow online lessons comfortably. Even an interesed layman is able to access the courses. Not only content of teaching are delivered, which are presented to the students in the lecutre-room by either a whiteboard or a video beamer, but simultaneously also video and audio of the lecturer. Navigation bar for accessing different parts in the recorded lecture are included. Tele-TASK supports all usual platforms, different net bandwidths, arbitrary presentation programs and needs no special software installations, configurations and no precognition of the end-users. For the first time, the system was deployed for recording, transmission and archiving of the computer science lecture Ïnformation security in open networksät the University of Trier in the summer semester 2002. High access numbers are expression of the perfectly problem-free and easy possibilities of using.

Wei Zhou, Christoph Meinel
Implement Role-Based Access Control With Attribute Certificates
Forschungsbericht Nr. 03-03

Abstract: Nowadays more and more activities are performed over the Internet. But as more people are involved in the transaction circle, security and authorisation control becomes one of the biggest concerns. Hence, we are motivated by the need to manage and to enforce a strong authorisation mechanism in large-scale Web-environment. As well known, Role Based Access Control (RBAC) provides a strong authentication. Privilege Management Infrastructure (PMI) as a new technology can provide strong authorisation. To satisfy mentioned security requirements, we have established a role based access control infrastructure and developed a prototype that uses X.509 public key certificate (PKCs) and X.509 attribute certificates (ACs). Access control is performed by an access control policy that is written in XML, roles and policies are stored in ACs. PKCs and ACs are all stored in a LDAP server. Our prototype includes an access control engine and an administration tool. The access control engine is implemented by a Java servlet. The access control engine provides a service that mediates the data between the users and the database, which also executes the function of authentication and authorisation. The administration tool can create key pair, X.509 PKCs, X.509 ACs, manage users'information and some other functions.

Christoph Meinel, Volker Schillings
tele-TASK - Teletaching praxistauglich für den Universitätsalltag
Forschungsbericht Nr. 03-04

Astract: An der Universität Trier wurde eine neue, drastisch vereinfachte Zugangstechnik für Online-Vorlesungen namens tele-TASK (Teleteaching Anywhere Solution Kit) [2][9] mit Erfolg erprobt. Von der Wohnung oder vom Büro aus kann dadurch jeder PC-Nutzer mit geeignetem Internetanschluss - ob interessierter Laie, Fachspezialist oder eingeschriebener Student- Lehrveranstaltungen komfortabel mitverfolgen. Dabei werden nicht nur die Lehrinhalte übermittelt, welche den Studenten im Hörsaal präsentiert werden, sondern simultan auch Bilder und Ton des Dozenten sowie eine Navigationsleiste. tele-TASK unterstützt alle gängigen Plattformen, verschiedene Netzbandbreiten, beliebige Präsentationsprogramme und benötigt keine Installationen, Konfigurationen und Vorkenntnisse seitns der Endanwender. Integraler Bestandteil des Systems ist der t-Cube. Dieser ist eine integrierte tele-TASK Komplettlösung in Form eines kleinen und transportablen Gerätes. Der t-Cube ist eine Art digitaler Videorekorder, der zwischen Doezentenlaptop und Netzwerk geschaltet wird. Für den Betrieb sind keine Installationen oder Vorkenntnisse von Nöten.

Die Plug'n Play Architektur ermöglicht eine direkte Inbetriebnahme. Im folgenden wird das tele-TASK System und insbesondere die Architektur und Funktionsweise der integrierten t-Cube Lösung vorgestellt. Auf der ACM SIGUCCS Conference 2002 erhielt tele-TASK den Einstein Award für das "außergewöhnlichste und herausragendste" Projekt.

Feng Cheng, Paul Ferring, Christoph Meinel
Lock-Keeper Technology - A New Network Security Solution
Forschungsbericht Nr. 03-05

Abstract: The threats originating from the Internet are ever-increasing and far from being "under control". Modern security is designed to protect the vast range of business communication facilities from external as well as internal intrudes, so-called "hackers". To this effect, various defensive mechanisms have been developed to protect internal data and systems from unauthorized access. This paper will introduce a novel security solution named Lock-Keeper, which can provide data transfer by physically separate connections. By means of the SingleGate Lock-Keeper system, a simple implementation of this idea, the possibility of direct attacks to a protected network can be eliminated entirely and data can be exchanged between two networks through a completely secure and reliable way. As an advanced implementation of this technology, the DualGate Lock-Keeper is proposed by including another new "gate" unit. Along with this development, not only the Lock-Keeper performance on data transfer, expecially the transmit speed, is improved significantly, but also some other new good characteristics appear simultaneously. All these improvements make the DualGate Lock-Keeper more efficient, flexible and applicable. Moreover, an architecture and its working principle of the Lock-Keeper cluster which is built up by the combination of two or more independent Lock-Keeper systems are analyzed in detail. Thanks to this lock concept, the Lock-Keeper can provide higher levels of security and completely prevents specific intruder attacks. A lot of scenarios, which can be protected by the Lock-Keeper, are revealed in this paper.

Michael Schmitt, Christoph Meinel
Design and Implementation of a PHP-based Web Server for the Tele-Lab IT Security
Forschungsbericht Nr. 03-06

Abstract: The Tele-Lab IT Security project aims at specifying and implementing a web-based, intelligent tutoring system that allows computer science students, system administrators, and end users to get familiar with the basics of IT security. It provides a powerful, real-life workint environment in which users can develop and practice solutions for problems of their every-day work with only little support by

the teaching staff. This technical report focuses on the web-browser part of the Tele-Lab. It discusses the design and the implementation of a web framework that is responsible for user administration and for presenting the teaching contents in a user-friendly manner.

9.4 Vorabveröffentlichungen in den Berichten des Instituts für Telematik

Sämtliche Technische Berichte des Instituts für Telematik können über das Institut bezogen oder unter der URL

http://www.telematik-institut.de/publikationen/technische-berichte/index.html

abgerufen werden.

Christoph Meinel, Michael Schmitt
Sicherheitsrisiken und Schwachstellenanalyse von IT-Systemen
TR-Nr. 02-10

Lutz Gollan, Christoph Meinel
Digitale Signaturen in der Verwaltung
TR-Nr. 02-09

Christoph Meinel, Frank Rudolf
Trierer Symposium Sichere Telemedizin, Proceedings
TR-Nr. 02-08

Lutz Vorwerk, Chunyan Jiang, Christoph Meinel
Generieren von diagnostischen 3D-Ojekten aus deformierten 2D-DICOM Bildern
TR-Nr. 02-07

Bernd Dusemund, Christoph Meinel
Patientenreminder
TR-Nr. 02-06

Lutz Gollan, Andreas Heuer, Christoph Meinel, Thomas Engel
Secure E-Document Container
TR-Nr. 02-05

Lutz Gollan, Christoph Meinel
Digitale Signaturen für Kraftfahrzeuge
TR-Nr. 02-04

Volker Schillings , Christoph Meinel
tele-TASK-Teleteaching Anywhere Solution Kit
TR-Nr. 02-03

Christoph Meinel, Frank Rudolf
Trierer Symposium Digitales Geld, Proceedings
TR-Nr. 02-02

Lutz Gollan, Christoph Meinel
Digital Signatures for Automobiles?!
TR-Nr. 02-01

10 Vorträge

10.1 Vorträge außerhalb der Universität Trier

Feng Cheng:

„A Complete Solution for Highly Secure Data Exchange: Lock-Keeper and its Advancements“
PDCAT 2003, Chengdu (China), 27.08.-29.08.2003

Ji Hu:

„A Tutoring System for IT-Security“
WISE 2003, Monterey (USA), 26.06.-28.06.03

Chunyan Jiang:

„Concept for DICOM about 3D Data Interchange"
TTC 2003, Tromso (Norway), 14.-17.09.2003

Mingchao Ma:

„T-Cube: A Multimedia Authoring System for eLearning"
eLearn 2003, Phoenix (Arizona, USA), 07.-11.11.2003

Christoph Meinel:

„Course Management in the Twinkle of an Eye"
SIGUCCS 2002, Providence, 19.11.-24.11.2002

„Leistungsangebote der Telematikforschung in Trier"
Allianz AG, München, 02.10.2002

„Telematic-Technology for Risk-Management"
LuxFinance, Luxembourg, 07.10.2002

„Trierer Forschungsaktivitäten im Bereich Telemedizin"
Charité, Berlin, 05.12.2002

„Telematics - Research and Developments Acitivities in Trier"
EU-Kommission, Brüssel, 27.06.2002

„Telematik - eine junge Disziplin mit grenzenlosen Anwendungen"
Lufthansa Systems, Frankfurt, 09.07.2002

„Digital Signatures in Automobiles?!"
SCI 2002, Orlando, 15.07.-19.07.2002

„Deformation and Construction of 3-D Medicla Image"
ICDIA 2002, Shanghai, 16.08.-22.08.2002

„Sichere E-Mail Systeme"
Boehringer, Ingelheim, 28.03.2002

„Sicherheit in offenen Netzen"
GIBU, Dagstuhl, 25.03.-28.03.2002

„Leistungsangebote der aktuellen Telematikforschung"
DZ-Bank, Luxembourg, 03.04.2002

„Recent Research Efforts in BDD-Technology"
Carnegie-Mellon-University, Pittsburgh, 05.03.-12.03.02

„Telematik - eine junge Disziplin mit grenzenlosen Anwendungen"
ARCOR, Hannover, 26.04.2002

„Telematics - Research and Development Activities in Trier"
SES-Astra, Luxembourg, 02.05.2002

„Entwicklung eines GPS-basierten Fahrtenbuchs für den Palm"
DATEV, Nürnberg, 31.05.2002

„Telemedicine - New Tools for DICOM-Management"
Arab Health, Dubai, 23.01.-27.01.2002

„Public-Key-Infrastrukturen - Der Weg ist nicht das Ziel"
ONLINE 2002, Düsseldorf, 28.01.2002

„Internet-Security - Angriffspunkte und Schwächen"
Security Gipfel, Berlin, 21.02.2002

„tele-TASK - ein innovatives System zur Aufzeichnung und Übertragung von Vorlesungen im Internet"
RWTH Aachen, 16.01.2003

„Concepts and Tools for Internet Security"
Telindus S.A., Luxembourg, 14.02.2003

„Cyberwar"
CHIP-Podiumsdiskussion, Cebit, Hannover, 14.03.2003

„PKI and PMI in Telemedicine - Implementation of the HPC"
La Laguna/Teneriffa, CATAI Winter School, 19.03.2003

„Introduction into Public Key Cryptography"
Beijing University of Technology, 04.04.2003

„New Concepts of Internet Security - the Lock-Keeper Architecture"
Grimstaad/Norwegen, 05.05.2003

„Unsere Forschungsaktivitäten im Bereich Telemedizin"
Mutterhaus Trier, 10.07.2003

„Sicherheit: Der entscheidende Erfolgsfaktor für eCommerce und mCommerce"
Online 2003, Düsseldorf, 24.09.2003

„tele-TASK Teleteaching Anywhere Solution Kit - Anspruch und Praxis"
Campus Innovation, Hamburg, 29.09.2003

„Sicherung mobiler Zugänge"
IT-Security Gipfel, Berlin, 08.10.2003

„tele-TASK Teleteaching Anywhere Solution Kit“
Mediaforum Rheinland-Pfalz, Kaiserslautern, 10.11.2003

„Recent Developments in Web-Content-Management“
FirstThuesDay, Luxembourg

„Digitale Signaturen und Zertifikatsmanagement“
Wirtschaftsministerium, Luxembourg

Rustam Mubarakzjanov:

„On Complexity of Probabilistic Branching Programs“
13th International Conference PProblems of theoretical Cybernetics,
Kazan (Russland), 26.05.-03.06.2002

Harald Sack:

„Das Internet - Technologische Grundlagen und Organisation“
Deutsche Richterakademie Trier „Zivilrecht und Internet“, 29.01.2002

„Improving the Power of OBDDs by Integrating Parity Nodes“
Disputationsvortrag, Universität Trier, 11.01.2002

Volker Schillings:

„VisBDD - A Web-based Visualization framework for OBDD Algorithms“
Int. Workshop on Logic and Synthesis (IWLS 2002), New Orleans, (Louisiana, USA), 04.-07.06.2002

„tele-TASK - Teleteaching Anywhere Solution Kit“
SIGUCCS 2002, Providence, (Rhode Island, USA), 20.- 23.11.2002

Christian Stangier:

„Modular Partitioning and Dynamic Conjunction Scheduling in Image Compuation“
Int. Workshop on Logic and Synthesis (IWLS 2002), New Orleans, (Louisiana, USA), 04.-07.06.2002

„High-Level Methods for OBDD Based Sequential Verification“
Disputationsvortrag, Universität Trier, 29.11.2002

Xinhua Zhang:

„Enhance opnsst Protocol's Security with Smart Card"
WWW/Internet 2003, Algarve (Portugal), 04.-07.11.2003

10.2 Vorträge im Informatik-Kolloquium

28.01.03	**Christoph Meinel - Volker Schillings**: *tele-TASK-Teleteaching Anywhere Solution Kit, Anspruch und Praxis*

10.3 Vorträge im Forschungsseminar

16.12.03	Thomas Scherer: *JCOP - Ein Betriebssystem für Smart Cards*
09.12.03	Volker Klotz: *Transformierte OBDDs - ein Ein- und Ausblick*
25.11.03	Serge Linckels: *CHESt - A new method of teaching?*
18.11.03	Uwe Roth: *Extreme programming, Aspektorientierte Programmierung*
11.11.03	Tongbo Chen: *Several Image-based Techniques*
04.11.03	Mohammad Ghasemzadeh: *BDD Versus Resolution Based SAT Solvers*
28.10.03	Lital Shestowitz: *Praktikum im Sommer 2003, ein Rückblick*
23.10.03	Mingchao Ma: *Building an Ubiqutious Capture and Access System for eLearning*
30.09.03	Xinhua Zhang: *Enhance OpenSST Protocol's Security with Smart Card*
07.10.03	Lutz Vorwerk: *Kontrolle klassifizierter sicherheitskritischer Prozesse telemedizinischer Anwendungen*

30.09.03	Ji Hu: *Design of TeleLab IT Security*
23.09.03	Mingchao Ma: *Metadata and Content Management*
09.09.03	Chunyan Jiang: *Concepts for DICOM about 3D Image Data Interchange*
02.09.03	Torsten Becker: *GPS-unterstütztes Fahrtenbuch für Pocket PCs*
26.08.03	Oliver Zofic: *ECCC - Electronic Colloquium on Computational Complexity - presentation of the system and new updates*
19.08.03	Uwe Roth: *Eine kleine Einführung in XSLT*
12.08.03	Feng Cheng: *A Complete Solutin for Highly Secure Data Exchange: Lock-Keeper and its Advancements*
15.07.03	Long Wang: *Extensions of JDaphne*
08.07.03	Volker Klotz: *Primes is in P.*
01.07.03	Ingo Scholtes: *Erweiterung der DICOM-Management Suite um ein verteiltes objektorientiertes Datenbanksystem mit DICOM-Schnittstelle*
24.06.03	Oliver Zlotowski: *Implementierung eines generischen Observer Pattern in C++*
03.06.03	Michael Schmitt: *Automatische Testgenerierung basierend auf formalen Spezifikationen*
20.05.03	Volker Schillings: *course management-systeme*
13.05.03	Andreas Hau: *Metadatenbasierte Aufbereitung multimedialer tele-TASK-Daten mit Hilfe von RDF*
17.12.02	Mohammad GhasemZadeh: *Logic Programming Using BDDs*
26.11.02	Volker Klotz: *QUIP: ein Beweissystem für nichtmonotone Logiken*
12.11.02	Tong Bo Chen: *Problems, Ideas and Practice in Multimedia*
02.07.02	Natalia Efrosinina: *State encoding in FSM as an optimisation parameter for OBDD-size*
18.06.02	Rustam Mubarakzjanov:

	Nonlinear sifting of decision diagrams
28.05.02	Volker Schillings: *VisBDD - A web-based Visualization Framework for OBDD Algorithms*
14.05.02	Mohammad Ghasemzadeh: *Fibonacci numbers: An O(log(n)algorithm*
05.04.02	Baocai Yin: *Detection and Synthesis of Facial Image*
19.03.02	Mohammad Ghasemzadeh: *an Introduction in my Education, Interests, BSc and MSc Projects*
12.02.02	Harald Sack: *POBDDs for Dummies*
05.02.02	Volker Schillings, Gennadij Umanskij: *Entwicklung für W3C.org*
29.01.02	Christian Stangier: *Non-linear and Dynamic Quantification Scheduling in Image Computation*
15.01.02	Rustam Mubarakzjanov: *BDD-based Cryptanalysis of Keystream Generators*

10.4 Gäste und Gastvorträge

28.05.02	Prof. Dr. Baocai Yin, Beijing Polytechnic University, China *Hair animation in human face synthesis*
04.05.02	HoonSang Jin, University of Colorado at Boulder, USA *Fine Grain Conjunction Scheduling for Symbolic Reachability Analysis*
27.02.02	Prof. Dr. Max Mühlhäuser, TU Darmstadt *Ubiquitous Computing - Herausforderung oder „Hype"?*

11 Mitgliedschaften in Programmkomitees und Aufsichtsräten, Gutachtertätigkeiten

Christoph Meinel:

Veranstaltung von Tagungen und Symposien

- Veranstalter der RM03 conference - 6th international Symposium on Representations and Methology of Future Computer Technologies RM 2003, Trier, 10.-11.03.2003, Trier
- Veranstalter des Trierer Symposiums "Sichere Telemedizin", 14. - 15.November 2002
- Veranstalter des Trierer Symposiums "Digitales Geld", 20. - 21. Juni 2002

Mitglied in Programmkomitees nationaler und internationaler Tagungen

- IEEE/ACM IWLS 2003 - International Workshop on Logic Synthesis, 28.-30.05.2003, Laguna Beach (California, USA)

- MFCS 2003 - 28th International Symposium on Mathematical Foundations of Computer Science, 25.-29.08.2003, Bratislava (Slovak Republic)

- Online 2003 - Symposium IV-: Electronic u. Mobile Security - Aktuelle Problembereiche und Entwicklungstrends, 23.-26.09.2003, Düsseldorf (Germany) Chair

- RM03 - 6th international Symposium on Representations and Methodology of Future Computer Technologies RM2003, Trier, 10.-11.03.2003, Trier

- 5th International Workshop on Boolean Problems, 19. - 20.09.2002, Freiberg (Germany)

- Online' 2002 - Symposium IV-1: Digitale Signaturen und TrustCenter, 28. - 31.01.2002 Düsseldorf (Germany), Chair

- IEEE/ACM/IWLS 2002 - International Workshop on Logic Synthesis, 04.-07.06.2002, New Orleans (Louisiana, USA)

Weitere Funktionen

- Vorstandsvorsitzender und Direktor des Instituts für Telematik, e.V. (bis 2002)
- Sprecher der GI-Fachgruppe 01.1.4 „Komplexität“
- Direktor des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP)
- Mitglied des Aufsichtsrates des IBFI Schloss Dagstuhl
- Visiting Professor at the Luxembourg International Advanced Studies in Information Technology - LIASIT
- Visiting Professor of the Graduate School of the CS Department of the Beijing University of Technology, China

Gutachtertätigkeiten

- RM03
- STACS 2003
- IWLS 2003
- DATE 2003
- MFCS 2003
- IWLS 2002
- MFCS 2002
- STACS 2002
- DATE 2002
- Computational Complexity
- Formal Methode in CAD
- IEEE Transactions on CAD
- IEEE Transactions on Computers
- ACM Reviews
- Zentralblatt für Mathematik
- ToC Transaction on Computings

Volker Klotz:

Gutachtertätigkeiten:

- DATE’ 2003
- MFCS’ 2003
- RM’ 2003

- STACS 2003
- JDA (JournalRM 2003)
- IWLS 2003
- TCAD 2003
- TC 2003

Rustam Mubarakzjanov:

Gutachtertätigkeiten:

- ICCAD' 2002
- IWLS' 2002
- ICALP' 2002
- MFCS' 2002
- Applied Mathematics
- Journal of Computer and System Science

Harald Sack:

Weitere Funktionen

- Geschäftsführer des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP)

Gutachtertätigkeiten

- IWLS' 2002
- STTT - Springer's Int. Journal on Software Tools for Technology Transfer
- ToC - IEEE Transactions on Computing
- TCAD - IEEE Transactions on CAD
- RM' 2003

Volker Schillings:

Gutachtertätigkeiten

- IWLS 2002
- ACM Journal
- RM 2003

Christian Stangier:

Gutachtertätigkeiten

- IWLS' 2002
- TCAD Journal

12 Rechnerausstattung

Derzeit sind insgesamt 25 Pentium II/III/IV -PCs mit etlichen 17″/19″ TFT Monitoren und eine SUN in Betrieb,sowie eine kleinere Anzahl von SUNs als Notfallreserve verfügbar. Die benutzten Betriebssysteme sind SunOS 4.1.3 U1B auf SUN-Seite sowie SuSE Linux 7.1 - 9.0, seltener Windows 2k/XP, meist bi-bootable auf derselben Maschine, für die PCs. Ein Toshiba-Notebook mit Pentium IV unterstützt die Vorführungen in Hörsälen. Als Drucker sind nun zwei HP LaserJet der 4000er Reihe sowie zwei Farbdrucker HP DeskJet 970cxi im Einsatz. Zur Unterstützung von Multimedia-Anwendungen stehen ein Multimedia-PC sowie eine WebCam, ein DVD-Brenner und mehrere Scanner zur Verfügung. Für unsere Tele-Teaching Aktivitäten wurden 2 Shuttle-PC angeschafft, die das on-the-fly Encoding und das Streaming von Lerninhalten übernehmen und das mobiles Teleteaching erst ermöglichen . Auf der Dozenten-Seite läuft das Notebook Gericom WebgineXL mit einem Pentium 4 Prozessor. Die Computer-Präsentation wird von einem SmartBoard unterstützt. Das Bild und der Ton des Dozenten werden mit Hilfe von DV-Camcoder von Panasonic und eines Funk-Mikrophon von AKG in das Teleteaching System eingespeist.

Zur Netzwerkinstallation ist anzumerken, daß die Professur eine modulare Vernetzung auf der Basis von *1000BaseTX Ethernet* (Stern-Struktur) mit *RJ45-Anschlußdosen* aufweist. Ein Funk-LAN Access Point von Cisco unterstützt die Funk-LAN Anbindung der Professur nach der IEEE 802.11b Norm.