Theoretische Informatik

Die Arbeitsgruppe forscht auf den Gebieten Logik in der Informatik, Automaten und formale Sprachen, automatische Verifikation und kryptographische Protokolle.

Ergebnisse

Automaten auf unendlichen Objekten und unendliche Spiele, automatische Verifikation.

Ein weit verbreiteter Ansatz zur automatischen Verifikation besteht darin, zunächst sowohl das betrachtete System als auch die zu verifizierende Eigenschaft in Form von endlichen Automaten zu repräsentieren und für die eigentliche Verifikation dann automatenbasierte Algorithmen zu nutzen. Um hinsichtlich der Effizienz gute Ergebnisse zu erzielen, ist es notwendig, die beteiligten Automaten möglichst klein zu wählen. Seit Jahren arbeitet die Arbeitsgruppe deshalb an einer Theorie der Verkleinerung endlicher Automaten auf unendlichen Wörtern. Im Jahr 2006 ist es der Arbeitsgruppe gelungen, einen entscheidenden Fortschritt zu erzielen. Wir wissen nun, wie man alternierende Automaten, die auf unendlichen Wörtern arbeiten und unendliche Spiele unter Zuhilfenahme von *Simulationsrelationen* gut verkleinern kann. Dazu haben wir einerseits eine entsprechende Simulationstheorie aufgebaut andererseits aber auch geeignete Algorithmen entwickelt und implementiert.

Analyse kryptographischer Protokolle

Die Arbeitsgruppe konzentriert sich unter anderem auf die Analyse solcher kryptographischer Protokolle, deren Sicherheitseigenschaften komplexer Natur sind. Hierzu zählen insbesondere optimistische Vertragsabschlussprotokolle, bei denen die Vertragsparteien in der Regel ohne Vermittlung durch eine dritte Partei (Notar) einen Vertrag abschließen. Die Arbeitsgruppe hat im Jahr 2006 die weltweit erste präzise Definition von *Missbrauchsfreiheit* für Vertragsabschlussprotokolle gegeben und für konkrete Protokolle untersucht, ob sie dieser Definition genügen.

Dass ein kryptographisches Protokoll sicher ist, kann nach allgemeiner Auffassung nur durch komplexitätstheoretische Überlegungen nachgewiesen werden. Diese sind im Einzelfall jedoch sehr kompliziert, wenn kein geeigneter theoretischer Unterbau zur Verfügung steht. Es gibt deutliche Anzeichen, dass ein *simulationsbasierter Sicherheitsbegriff* im Zentrum eines solchen Unterbaus stehen wird, die Wissenschaft ist aber noch weit entfernt von einer ausgereiften Theorie. Mit mehreren Arbeiten hat die Arbeitsgruppe die aktuellen Forschungen in diesem Gebiet vorangetrieben, insbesondere mit Vorschlägen dazu, wie der in diesem Zusammenhang besonders kritische Begriff der zeitlichen Ressourcen behandelt werden muss.

Bei der formalen Analyse kryptographischer Protokolle stellte die Modellierung von Hashfunktionen – ein wichtiger kryptographischer Grundbaustein – bislang ein Problem dar. Gemeinsam mit Wissenschaftlern aus Frankreich hat die Arbeitsgruppe im Jahr 2006 einen neuen Vorschlag für die Modellierung von Hashfunktionen machen können, der den bislang diskutierten Vorschlägen überlegen ist.

Personal

Leiter/-innen: Prof. Dr. Th. Wilke; Sekretariat: M. Krause (50%)
Technisches Personal: T. Hess (50%)

Wissenschaftliche Mitarbeiter/-innen:

Dipl.-Inf. S.-P. Brandt Wissensrepräsentation	01.08.-30.11.2006	EU
Dipl.-Inf. C. Fritz Verifikation	01.01.-28.02.2006	DFG

Dr. R. Küsters	01.01.-31.07.2006	CAU
Kryptographische Protokolle		
Dipl.-Inf. D. Kähler	01.01.-31.12.2006	CAU
Verifikation kryptographischer Protokolle		
MSc. B. Sertkaya	15.08.-31.12.2006	EU
Wissensrepräsentation		
Dr. T. Truderung	01.03.-31.12.2006	DFG
Kryptoprotokolle		
Dr. E. Valkema	01.01.-31.12.2006	CAU

Vorlesungen, Seminare und Praktika

Winter 2005/2006

Kryptographie, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke (+ R. Küsters)

Informatik für Nebenfächler, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
E. Valkema (+ D. Kähler)

Automaten, Logiken, Spiele, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
D. Kähler, Th. Wilke (+ D. Kähler)

Verlustfreie Datenkompression, 2 (+ 1) Std. Vorlesung (+ Übungen)/Woche,
R. Küsters

Theoretische Informatik, 1 Std. Oberseminar/Woche,
Th. Wilke

(t,i)-Café, 1 Std. Arbeitsgemeinschaft/Woche,
C. Fritz, D. Kähler, R. Küsters, Th. Wilke

Sommer 2006

Informatik II für Ingenieure, 3 (+ 1) Std. Vorlesung (+ Übungen)/Woche,
E. Valkema (+ D. Kähler)

Informatik II für Ingenieure, 2 Std. Praktische Übungen/Woche,
D. Kähler

Secure Communications, 2 (+ 1) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke (+ R. Küsters)

(t,i)-Café, 1 Std. Arbeitsgemeinschaft/Woche,
D. Kähler, R. Küsters, Th. Wilke

Informatik IV - Theoretische Grundlagen der Informatik, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke (+ D. Kähler)

Kryptographie, 2 Std. Seminar/Woche,
R. Küsters

Theoretische Informatik, 2 Std. Oberseminar/Woche,
Th. Wilke

Winter 2006/2007

Kryptographie, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke (+ D. Kähler)

Theoretische Informatik, 1 Std. Oberseminar/Woche,
Th. Wilke

Informatik für Nebenfächler, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
E. Valkema

Drittmittel

Deutsche Forschungsgemeinschaft (DFG), *Minimierung von Automaten mit Anwendungen in der Verifikation nichtterminierender Systeme*, 01.03.2004-28.02.2006 (125000 EUR)
EU-Programm IST: Network of Excellence (NoE), *Semantic Interoperability and Datamining in Biomedicine*, 01.01.2004-30.06.2007 (97000 EUR)
Deutsche Forschungsgemeinschaft (DFG), *Automatische Analyse kryptographischer Protokolle mit komplexen Nachrichtenformaten*, 01.03.2006-27.02.2008 (125000 EUR)

Weitere Zusammenarbeiten, Technologietransfers und Konsultationen

Die Arbeitsgruppe unterhielt unter anderem rege Kontakte zu Arbeitsgruppen in Aachen (Prof. Dr. Erich Grädel, Prof. Dr. Dr. hc. Wolfgang Thomas), Dresden (Prof. Dr. Franz Baader) und Saarbrücken (Prof. Dr. Michael Backes) sowie Arbeitsgruppen in Edinburgh (Dr. Kousha Etessami), am LORIA, Nancy (Dr. Veronique Cortier, Dr. Michael Rusinowitch), an der Stanford University (Prof. John Mitchell), am IBM Research Lab, New York (Dr. Ran Canetti), in Sydney (Prof. Ron van der Meyden) und in Szeged (Prof. Zoltan Esik).

Diplom- und Master-Arbeiten

T. Krieger, *Entwicklung, Analyse und Implementierung eines sicheren Zugangskontrollmechanismus ohne Passworttabelle*, 13.12.2006

Dissertationen / Habilitationen

C. Fritz, *Simulation-Based Simplification of omega-Automata*, 10.02.2006

Veröffentlichungen

erschienen im Jahre 2006

R. Küsters, *Simulation-based security with inexhaustible interactive Turing machines*, CSFW, 309 - 320 (2006)
M. Backes, M. Dürmuth, D. Hofheinz, R. Küsters, *Conditional reactive simulatability*, ESORICS, 424 - 443 (2006)
V. Cortier, S. Kremer, R. Küsters, B. Warinschi, *Computationally sound symbolic secrecy in the presence of hash functions*, FSTTCS, 176 - 187 (2006)
M. Benedikt, B. Kuipers, C. Löding, J. van den Bussche, Th. Wilke, *A characterization of first-order topological properties of planar spatial data*, JACM, **53(2)**, 273 - 305 (2006)
C. Fritz, Th. Wilke, *Simulation relations for alternating parity automata and parity games*, DLT, 59 - 70 (2006)
D. Kähler, R. Küsters, Th. Wilke, *A Dolev-Yao-based definition of abuse-free protocols*, ICALP, 95 - 106 (2006)

Präsentationen

Th. Wilke, *Simulation Relations for Alternating Parity Automata and Parity Games,* DLT, Santa Barbara, USA, 26.-29.06.2006

R. Küsters, *Simulation-based Security with Inexhaustible Interactive Turing Machines,* CSFW, Venedig, Italien, 05.-07.07.2006

R. Küsters, *A Dolev-Yao-based Definition of Abuse-free Protocols,* ICALP, Venedig, Italien, 10.-14.07.2006

Th. Wilke, *Tree Automata and Tree Transducers for Analyzing Recursive Cryptographic,* Workshop on Tree Automata, Bonn, Deutschland, 07.-09.06.2006

Th. Wilke, *Logics, Automata, and Finite Semigroups,* Workshop on Finite and Algorithmic Model Theory, Durham, England, 09.-13.01.2006

R. Küsters, *Constraint Solving for Contract-Signing Protocols,* Seminar am MPI, Saarbrücken, 22.-22.03.2006

R. Küsters, *Computationally Sound Automatic Analysis of Security Protocols,* 4. Kryptotag der, Bochum, 11.-11.05.2006

R. Küsters, *Security Requirements and Analysis of Contract-Signing Protocols,* Security Seminar, Zürich, Schweiz, 25.-25.06.2006

R. Küsters, *Simulation-Based Security with Inexhaustible Interactive Turing Machines,* Seminar, Hawthorne, NY, USA, 07.-07.08.2006

R. Küsters, *A Dolev-Yao-based definition of Abuse-free Protocols,* Short Presentation at LICS, Seattle, WA, USA, 15.-15.08.2006

Andere Aktivitäten und Ereignisse

R. Küsters war Mitglied des Programmkomitees der folgenden internationalen Konferenzen und Workshops: DL 2006, FCC 2006, AAAI 2006, S&P 2006.

R. Küsters war einer der Vorsitzenden des Programmkomitees von FCS-ARSPA 2006.

Th. Wilke war Associate Editor der Zeitschrift Formal Methods in System Design und Member of the Editorial Board der Zeitschrift Fundamenta Informaticae.

Th. Wilke war Mitglied des Programmkomitees der folgenden internationalen Konferenzen: FOSSACS, LICS.

Th. Wilke war stellvertretender Sprecher des Fachbereiches Grundlagen der Informatik der GI und des Fachausschusses Theoretische Informatik sowie Mitglied des Leitungsgremiums der Fachgruppe Logik in der Informatik.

Im Rahmen der Öffentlichkeitsarbeit beteiligte sich die Arbeitsgruppe am Girls' Day 2006, einem Schnupperstudium Informatik für Schülerinnen, der b + m-Software-Challenge und dem Enrichment-Programm des Ministeriums für Bildung und Frauen.