Theoretische Informatik

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

Ergebnisse

Automatentheorie und 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 Minimierung für endliche Automaten auf unendlichen Wörtern. Im Jahr 2005 ist es der Arbeitsgruppe gelungen, einen entscheidenden Fortschritt zu erzielen. Wir wissen nun, wie man aus der Formulierung einer Spezifikation in linearer temporaler Logik mit meist verträglichem Aufwand einen entsprechenden Automaten konstruieren kann. Basis dieses Verfahrens ist einerseits die von uns entwickelte Simulationstheorie, andererseits eine geschickte Art, bekannte Algorithmen *on the fly* anzuwenden.

Synthese verteilter Systeme. Immer wieder zeigt es sich, dass Entwickler von verteilten Algorithmen oder verteilten Systemen das *Wissen* der beteiligten Agenten in den Mittelpunkt ihrer Entwurfsüberlegungen stellen. Typische Aussagen sind etwa: „Wenn Agent A nicht weiß, ob er eine aktuelle Kopie der Speicherstelle x besitzt, bezieht er eine gültige Kopie von x über das Netzwerk." Seit einigen Jahren wird deshalb die Idee verfolgt, bei der Spezifikation verteilter Systeme Formalismen zu benutzen, die explizit über das Wissen der beteiligten Agenten sprechen können. Eine wichtige Frage ist dann die, ob Spezifikationen in diesem Formalismus automatisch in verteilte Systeme umgesetzt werden können, was auch lange Zeit vermutet wurde. Der Arbeitsgruppe gelang es, im Jahr 2005 zu beweisen, dass diese Vermutung nicht wahr ist: Selbst bei sehr eingeschränkten Rahmenbedingungen lassen sich verteilte Systeme, die in *Logic of Knowledge* spezifiziert sind, nicht automatisch entwickeln.

Kryptographische Protokolle. Die Arbeitsgruppe hat sich im Jahr 2005 zum einen mit der Analyse kryptographischer Protokolle und zum anderen mit der simulationsbasierten Sicherheit für den modularen Entwurf kryptographischer Protokolle beschäftigt. Bei der Analyse kryptographischer Protokolle konzentrierte sich die Arbeit auf solche Protokolle, deren Sicherheitseigenschaften komplexer, typischerweise spieltheoretischer Natur sind. Hierzu zählen insbesondere optimistische Vertragsabschlussprotokolle, bei denen die Vertragsparteien in der Regel ohne Vermittlung durch eine dritte Partei (Notar) einen Vertrag abschließen. Es hat sich in den vergangenen Jahren herausgestellt, dass derartige Protokolle besonders im Hinblick auf Fragen der Fairness schwierig zu entwerfen und auf ihre Sicherheit hin zu überprüfen sind. Die Arbeitsgruppe hat im Jahr 2005 deshalb das erste vollautomatische Analyseverfahren für Vertragsabschlussprotokolle entwickelt und aufgezeigt, welche Grenzen der automatischen Analyse von Vertragsabschlussprotokollen gesetzt sind.

Im Bereich der simulationsbasierten Sicherheit werden in der Literatur zahlreiche Sicherheitsbegriffe und Modelle vorgeschlagen, ohne jedoch deren Beziehungen zu klären. Dies ist nicht nur aus theoretischer Sicht sehr unbefriedigend, sondern verhindert auch die Übertragung von Resultaten zwischen den verschiedenen Begriffen und Modellen. Der Arbeitsgruppe ist es gelungen, die Beziehungen der Sicherheitsbegriffe bzgl. bestimmter modellspezifischer Merkmale fast vollständig zu klären. Desweiteren wurde ein auf einer Prozessalgebra basierendes Modell zur simulationsbasierten Sicherheit entwickelt. Für dieses Modell wurden allgemeine Kompositionstheoreme bewiesen, die den modularen Entwurf kryptographischer Protokolle ermöglichen.

Personal

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

Wissenschaftliche Mitarbeiter:

Dipl.-Inf. C. Fritz Verifikation	01.01.-31.12.2005	DFG
Dr. R. Küsters Kryptographische Protokolle	01.01.-31.12.2005	CAU
Dipl.-Inf. D. Kähler Verifikation kryptographischer Protokolle	01.01.-31.12.2005	CAU
Dr. E. Valkema	01.01.-31.12.2005	CAU

Vorlesungen, Seminare und Praktika

Winter 2004/2005

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

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

Automaten und formale Sprachen, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
R. Küsters, Th. Wilke (+ C. Fritz)

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

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

Sommer 2005

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

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

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

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

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

Algorithmische Zahlentheorie und Kryptographie, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke

Hacker-Praktikum, 4 Std. Praktikum/Woche,
H. Kreft, Th. Wilke

Modallogik, 2 Std. Vorlesung/Woche,
Th. Wilke

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,
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. Oberseminar/Woche,
Th. Wilke

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,* 01.01.2004-31.12.2007 (84000 EUR)

Deutsche Forschungsgemeinschaft (DFG), *Automatische Analyse kryptographischer Protokolle mit komplexen Nachrichtenformaten,* 06.04.2005-05.04.2007 (125000 EUR)

Weitere Zusammenarbeiten, Technologie Transfers und Konsultationen

Die Arbeitsgruppe unterhält 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,* 06.05.2005

Veröffentlichungen

erschienen im Jahre 2005

R. van der Meyden, Th. Wilke, *Synthesis of Distributed Systems from Knowledge-Based Specifications,* CONCUR 2005, 562 - 576 (2005)

D. Kähler, R. Küsters, Th. Wilke, *Deciding Properties of Contract-Signing Protocols,* STACS 2005, 158 - 169 (2005)

K. Etessami, R. A. Schuller, Th. Wilke, *Fair Simulation Relations, Parity Games, and State Space Reduction for Büchi Automata,* SIAM Journal on Computing, **34(5)**, 1159 - 1175 (2005)

C. Fritz, Th. Wilke, *Simulation relations for alternating Büchi automata,* Theoretical Computer Science, **338(1-3)**, 275 - 314 (2005)

C. Fritz, *Concepts of Automata Construction from LTL*, LPAR 2005, 728 - 742 (2005)
D. Kähler, R. Küsters, *Constraint Solving for Contract-Signing Protocols*, CONCUR, 233 - 247 (2005)
A. Datta, R. Küsters, J. Mitchell, A. Ramanathan, *On the Relationships Between Notions of Simulation-Based Security*, TCC, 476 - 494 (2005)
Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, *Deciding the Security of Protocols with Commuting Public Key Encryption*, ENTCS, 55 - 66 (2005)
R. Küsters, *On the decidability of cryptographic protocols with open-ended data structures*, Int. J. Inf. Sec., 49 - 70 (2005)
R. Küsters, R. Molitor, *Structural Subsumption and Least Common Subsumers in a Description Logic with Existential and Number Restrictions*, Studia Logica, 227 - 259 (2005)
Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, *An NP decision procedure for protocol insecurity with XOR*, Theoretical Computer Science, 247 - 274 (2005)
R. Küsters, J. Mitchell, *Hrsg., Proceedings of the 2005 ACM Workshop on Formal Methods in Security Engineering (co-located with CCS 2005)*, (2005)
D. Kähler, R. Küsters, *A Constraint-Based Algorithm for Contract-Signing Protocols*, Workshop on Foundationcs of Computer Security (FCS 2005), (2005)
Th. Wilke, *D. Perrin and J.-E. Pin, Infinite words: automata, semigroups, logic and games (book review)*, The Bulletin of Symbolic Logic, **11(2)**, 246 - 247 (2005)

Präsentationen

C. Fritz, *Simulationsrelationen als Minimierungsheuristiken für omega-Automaten*, 52. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen, Lübeck, Deutschland, 16.08.2005
C. Fritz, *Concepts of Automata Construction from LTL*, LPAR 2005, Montego Bay, Jamaika, 02.12.2005
D. Kähler, *A Constraint-Based Algorithm for Contract-Signing Protocols*, Foundations of Computer Security - FCS'05, Chicago, USA, 01.07.2005
R. Küsters, *On the Relationships Between Notions of Simulation-Based Security*, TCC 2005, Cambridge (MIT), USA, 12.02.2005
R. Küsters, *Sequential Probabilistic Process Calculus —A New Computational Model for Simulation-Based Security*, Seminar in the Cryptography Research Group at IBM T.J. Watson Research Center, Hawthorne, NY, USA, 14.02.2005
R. Küsters, *Deciding Properties of Contract-Signing Protocols*, STACS 2005, Stuttgart, Deutschland, 24.02.2005
R. Küsters, *On the Relationships Between Notions of Simulation-Based Security*, Seminaire Informatique Fondamentale, Nancy (INRIA), Frankreich, 01.03.2005
R. Küsters, *On the Relationships Between Notions of Simulation-Based Security*, Workshop on the link between formal and computational models, Paris (ENS), Frankreich, 23.06.2005
R. Küsters, *Constraint Solving for Contract Signing Protocols*, CONCUR 2005, San Francisco, USA, 24.08.2005
Th. Wilke, *Synthesis from Knowledge-based Specifications*, Kolloquium Fachbereich Informatik, Universität Stuttgart, Stuttgart, Deutschland, 22.02.2005
Th. Wilke, *Synthesis from Knowledge-based Specifications*, Spring School on Infinite Games and Their Applications, Bonn, Deutschland, 15.03.2005
R. Küsters, Th. Wilke, *Automated Analysis of Cryptographic Protocols by Automata-Theoretic Means*, AFL 2005, Dobgoko, Ungarn, 17.05.2005
Th. Wilke, *Synthesis from Knowledge-based Specifications*, Dagstuhl Workshop on Synthesis and Planning, Wadern, Deutschland, 12.06.2005
Th. Wilke, *Synthesis from Knowledge-based Specifications*, Kolloquium Turku Center for Computer Science (anlässlich der Promotion von Saeed Salehi), Turku, Finnland, 11.08.2005
Th. Wilke, *Synthesis from Knowledge-based Specifications*, 52. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen, Lübeck, Deutschland, 16.-17.08.2005

Andere Aktivitäten und Ereignisse

An der Fakultät habilitierte sich Dr. R. Küsters am 29.06.2005.

Die Arbeitsgruppe richtete das Jahrestreffen der Fachgruppe Formale Methoden und Software Engineering für sichere Systeme der GI aus.

R. Küsters war Mitglied des Programmkomitees des folgenden internationalen Workshops: FCS.

R. Küsters war Co-Vorsitzender des Programkommitees des folgenden internationalen Workshops: FMSE.

Th. Wilke war Associate Editor der Zeitschrift Formal Methods in System Design.

Th. Wilke war Mitglied des Programmkomitees der folgenden internationalen Konferenzen: CAV, FCT, CIAA.

Th. Wilke war Mitglied des Programmkomitees des folgenden internationalen Workshops: WITS.

Th. Wilke war stellvertretender Sprecher der Fachgruppe Logik in der Informatik der GI und stellvertretender Sprecher des Fachbereiches Grundlagen der Informatik der GI.

Th. Wilke war Dozent der Spring School on Infinite Games and Applications des EU network GAMES.

Th. Wilke war als Redner eingeladen zu der internationalen Konferenz AFL.

Im Rahmen der Öffentlichkeitsarbeit beteiligt sich die Arbeitsgruppe am Girls' Day 2005, einem Schnupperstudium Informatik für Schülerinnen und der b + m-Software-Challenge (2004/5 und 2005/6).