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. Die Theorie der Automaten auf unendlichen Objekten und der Spiele von unendlicher Dauer ist eng verknüpft mit Teilen der mathematischen Logik. Sie hat seit Anfang der sechziger Jahre zunehmend an Bedeutung gewonnen, insbesondere vor dem Hintergrund ihrer Nähe zur automatischen Verifikation. Gerade in letzter Zeit wurden durch die stärkere Berücksichtigung der Spieltheorie neue Perspektiven für die Forschung eröffnet.

Ein großer Teil der Arbeit der Forschungsgruppe bestand deshalb im Jahr 2007 darin, diese Perspektiven zu identifizieren und darauf basierend gemeinsam mit den Professoren Flum aus Freiburg und Grädel aus Aachen einen mehr als 700 Seiten starken Überblick über den Stand der Forschung und aktuelle Herausforderungen herauszugeben. Zu dem im Schriftenverzeichnis nachgewiesenen Band *Logic and Automata: History and Perspectives* haben mehr als 40 Autoren beigetragen.

Der technische Beitrag der Arbeitsgruppe zu diesem Gebiet bestand im Jahr 2007 aus einem Ansatz für die Vereinheitlichung der zentralen automatentheoretischen Konstruktionen: Komplementierung und Determinisierung von Büchi-Automaten. Seit mehr als 30 Jahren werden Verfahren für diese beiden Konstruktionsprobleme entwickelt und verbessert; unsere Arbeiten zeigen, wie eine einheitliche Theorie aussehen kann, auf deren Grundlage effiziente Algorithmen für beide Probleme entstehen können.

Analyse kryptographischer Protokolle. Die Arbeitsgruppe arbeitete in diesem Zusammenhang auf drei Feldern.

Versucht man, Sicherheitseigenschaften kryptographischer Protokolle informell zu spezifizieren, so führt dies häufig zu Beschreibungen, die Bedingungen an das Wissen der beteiligten Agenten stellen. Das führte zum Beispiel zu einer speziellen Form der Modallogik, der so genannten BAN-Logik, als Spezifikationssprache für kryptographische Protokolle. Die Arbeitsgruppe hat hier im letzten Jahr einen anderen Weg eingeschlagen. Sie hat die klassische Wissenslogik wieder belebt und durch ein so genanntes Übertragungsergebnis gezeigt, dass sich in Wissenslogik spezifizierte Sicherheitseigenschaften von idealen auf real implementierte Protokolle übertragen, wenn bei der Implementierung informationstheoretisch sichere kryptographische Grundbausteine genutzt werden.

Das zweite Feld betrifft die automatische Analyse von Gruppenprotokollen. Nachdem die Arbeitsgruppe in den vorangegangenen Jahren einen automatentheoretischen Ansatz zu deren Analyse favorisiert und untersucht hatte, befasste sie sich im Jahr 2007 intensiver mit einem andernorts entwickelten Ansatz, bei dem Protokolle durch Horn-Klauseln beschrieben werden. Offen war gewesen, ob in diesen Ansatz frische Werte (nonces) einbezogen werden können und ob gewisse technische Beschränkungen notwendig sind. Beide Fragen konnte die Arbeitsgruppe beantworten.

Schliesslich beschäftigte sich die Arbeitsgruppe mit komplexen Sicherheitseigenschaften, die einen spieltheoretischen Charakter haben und bislang nur wenig studiert wurden. In der Arbeitsgruppe wurde ein Modell entwickelt, in dem mit Hilfe der Logik AMC solche Sicherheitseigenschaften spezifiert und untersucht werden können. Durch die Kombinition von Techniken aus verschiedenen Gebieten wurden grundlegende (Un-)Entscheidbarkeitsresultate und komplexitätstheoretische Ergebnisse für die Frage erzielt, ob die Spezifikation eines Protokolls eine durch eine AMC-Formel beschriebene Sicherheitseigenschaft erfüllt.

Personal

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

Wissenschaftliche Mitarbeiter/-innen:

Dipl.-Inf. N. Gruschka	01.11.-31.12.2007	CAU
M.Sc. I. Khan	01.04.-31.12.2007	DAAD
Trust Management in Public Key Infrastructure		
Dipl.-Inf. K. O. Kürtz	01.03.-31.12.2007	DFG
Verifikation kryptographischer Protokolle		
Dipl.-Inf. D. Kähler	01.01.-31.12.2007	CAU
Verifikation kryptographischer Protokolle		
Dr. T. Truderung	01.-31.01.2007	DFG
Verifikation kryptographischer Protokolle		
Dr. E. Valkema	01.01.-31.12.2007	CAU

Vorlesungen, Seminare und Praktika

Winter 2006/2007

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

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

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

Sommer 2007

Informatik II - Algorithmen und Datenstrukten, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke (+ D. Kähler)

Programmierpraktikum P2, 1 (+ 2) Std. Praktikum (+ Übungen)/Woche,
Th. Wilke (+ K. O. Kürtz)

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

Informatik II für Ingenieure, 2 Std. Praktische Übungen/Woche,
E. Valkema

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

Kryptographie, 2 Std. Seminar/Woche,
Th. Wilke

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

Winter 2007/2008

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

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

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

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

Drittmittel

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), in Edinburgh (Dr. Kousha Etessami), am LORIA, Nancy (Dr. Veronique Cortier, Dr. Michael Rusinowitch), in Sydney (Prof. Ron van der Meyden) und in Szeged (Prof. Zoltan Esik).

Diplom- und Master-Arbeiten

K. O. Kürtz, *Automatic Analysis of Recursive Cryptographic Protocols*, 06.02.2007
M. Tuengerthal, *Session Identifies in Simulation-Based Security*, 22.03.2007
D. H. Vu, *Web of Trust*, 27.09.2007

Veröffentlichungen

erschienen im Jahre 2007

J. Flum, E. Grädel, Th. Wilke, *Logic and Automata: History and Perspectives*, Texts in Logic and Games, **2**, (2007)

R. Küsters, Th. Wilke, *Transducer-Based Analysis of Cryptographic Protocols*, Information and Computation, **205(12)**, 1741 - 1776 (2007)

K. O. Kürtz, R. Küsters, Th. Wilke, *Selecting Theories and Nonce Generation for Recursive Protocols*, ACM Workshop on Formal Methods in Security Engineering (FMSE 2007), 61 - 70 (2007)

R. van der Meyden, Th. Wilke, *Preservation of Epistemic Properties in Security Protocol Implementations*, Theoretical Aspects of Rationality and Knowledge (TARK 2007), 212 - 221 (2007)

D. Kähler, R. Küsters, T. Truderung, *Infinite State AMC-Model Checking for Cryptographic Protocols*, IEEE Symposium on Logic in Computer Science (LICS 2007), 181 - 192 (2007)

M. Y. Vardi, Th. Wilke, *Automata: from logics to algorithms*, Flum, Grädel, Wilke, Logic and Automata: History and Perspectives, Texts in Logics and Games, Amsterdam University Press, **2**, 629 - 736 (2007)

Andere Aktivitäten und Ereignisse

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

Th. Wilke war Mitglied des Programmkomitees der Konferenzen AuthoMatha und FCT sowie des Workshops WEWoRC.

Th. Wilke war Mitglied des Leitungsgremiums der GI-Fachgruppe Logik in der Informatik und des Fachausschusses Theoretische Informatik.

Die Arbeitsgruppe richtete am 7. und 8. Dezember 2007 einen Workshop zum Thema *Informatik als Profil ergänzendes Fach* aus, an dem mehr als 40 Lehrerinnen und Lehrer teilnahmen.

Im Rahmen der Öffentlichkeitsarbeit beteiligte sich die Arbeitsgruppe am Girls' Day und am Enrichmentprogramm zur Begabtenförderung und richtete ein Schnupperstudium für Schülerinnen und Schüler mit mehr als 80 Teilnehmern und ein Schnupperstudium für Schülerinnen mit 22 Teilnehmerinnen aus.