Theoretical Computer Science

The theory group of the Department of Computer Science is specialized in automata theory, verification, logic in computer science, foundations of IT-security, computational complexity theory, and didactics of computer science.

Results

UML. The Unified Modelling Language (UML) is by now a widespread modelling language in software engineering: the theory group studies its formal foundation. From a formal methods point of view, a major problem with UML is that it is ambiguous and admits many different semantics. In 2009, one of the achievements in this respect was a rigorous semantics for UML state machines with interlevel transitions. This result was complemented by an appropriate notion of refinement, which supports hierarchical system design, and transformations that preserve the semantics of UML. Further research went into the study of sub-state machine behaviour, in particular, readiness.

Manipulating Elections. In social choice theory, a collective decision is viewed as the aggregate of individual interests. One direction of research in this area is to develop appropriate election systems. The theory group is interested in the complexity of such systems. In 2009, the theory group focused on the Copeland election system, where a group of voters each ranks the possible alternatives (candidates) as a total order. The winner(s) of the election are computed by granting each candidate 1 point for every candidate that he „beats" in the majority of voters, and a variable (alpha) amount of points for each candidate that he ties with. We resolved the complexity of the manipulation problem for the practically relevant cases.

Logics for Probabilistic Strategic Games. Strategic games play an important role in the modelling and analysis of various kinds of systems. The theory group is interested in alternating-time temporal logic (ATL), which is used to reason about strategic abilities of agents. Aiming at strategies that can realistically be implemented in software, many variants of ATL study a setting where strategies may only take available information into account. Another generalization of ATL is Probabilistic ATL, where strategies achieve their goal with a certain probability. We introduced a semantics of ATL that takes into account both of these aspects. We prove that our semantics allows simulation relations similar in spirit to usual bisimulations, and has a decidable model checking problem in the case of memoryless strategies: A key property of our logic is that it allows the modelling of prior agreement as relevant for jointly developed software agents.

Security of Contract-Signing Protocols. As in recent year, the theory group has worked on modelling, analyzing, and designing contract-signing protocols. In 2009, we developed a probabilistic contract signing protocol that achieves the crucial security notion of balance even in the presence of an adversary that may delay messages sent over secure channels. To show that this property holds in a computational setting, we first proposed a probabilistic framework for protocol analysis, then proved that in a symbolic setting the protocol satisfies a probabilistic alternating-time temporal formula expressing balance, and finally established a general result stating that the validity of formulas such as our balance formula is preserved when passing from the symbolic to a computational setting. The key idea of the protocol is to take a „gradual commitment" approach.

Authenticated Message Exchange. The last topic the theory group has worked on in 2009 is simulation-based security of cryptographic protocols. The main objective is to give rigorous proofs of the security of practically relevant protocols. Simulation-based security notions for cryptographic protocols are regarded as highly desirable, primarily because they admit strong composability and, consequently, a modular design. We developed a simulation-based security definition for two-round authenticated message exchange and showed that a concrete, natural protocol, 2AMEX-1, satisfies our security property, that is, we provided an ideal functionality for two-round authenticated message exchange and show that 2AMEX-1 realizes it securely.

Personnel

Head of the group: Prof. Dr. Th. Wilke; Secretary: F. Lorenz (50%)
Technical Staff: Th. Hess (50%)

Scientific Staff:

Dipl.-Math. S. Eggert	01.07.-31.12.2009		CAU
M.Sc. I. Khan	01.01.-31.12.2009		DAAD
Trust Management in Public Key Infrastructure			
Dr. H. Schnoor	01.01.-31.12.2009		CAU
StR S. Schulmeister	01.08.-31.12.2009	(50%)	CAU
Dipl.-Inf. J. Schönborn	01.04.-31.12.2009	(50%)	CAU
Dipl.-Inf. M. Tropmann	01.06.-31.07.2009		CAU

Lectures, Seminars, and Laboratory Course Offers

Winter 2008/2009

Automaten, Logiken, Spiele, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke

Kryptographie: Verfahren und Angriffe, 2 (+ 1) hrs Lecture (+ Exercises)/Week,
H. Schnoor

Mathematik für Informatiker III - Logik für Informatiker, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ R. Thöle)

Theoretische Informatik, 2 hrs Seminar/Week,
Th. Wilke

Anleitung zum wissenschaftlichen Arbeiten, 1 hrs Lecture/Week,
Th. Wilke

Summer 2009

G2.3: - Programmierpraktikum II (ProgPrak) (080064), 3 hrs Exercise/Week,
T. Slawig (+ J. Schönborn, A. Jordt)

Übungen zur G2.1: Informatik II - Algorithmen und Datenstrukturen, 2 hrs Exercise/Week,
H. Schnoor (+ L. Prädel, B. Kinscher, N. Prühs, H. Schade)

Winter 2009/2010

2-Fächer-AG, 2 hrs Seminar/Week,
Th. Wilke

Inf-EinfPP: Einführendes Programmierpraktikum, 3 hrs Lecture/Week,
Th. Wilke (+ S. Schulmeister)

MS010: Kryptographie, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke und H. Schnoor (+ H. Schnoor)

MS0103: Kryptographie (I - Vertraulichkeit), 2 (+1) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ H. Schnoor, S. Eggert)

MS0104: Kryptographie (II - Authentizität), 2 (+1) hrs Lecture (+ Exercises)/Week,
H. Schnoor (+ H. Schnoor, S. Eggert)

Ober-/Diplomandenseminar - Theoretische Informatik, 2 hrs Seminar/Week,
Th. Wilke

WI17: IT-Sicherheit, 4 hrs Seminar/Week,
Th. Wilke

Inf-Prog: - Programmierung, 4 (+2) hrs Lecture (+ Exercises)/Week,
M. Hanus (+ S. Eggert)

Third-Party Funds

DFG, *Automatische Analyse kryptographischer Protokolle mit komplexen Nachrichtenformaten,* 01.01.2009-30.08.2010 (119500 EUR)
DAAD, *Stipendiat Imran Khan,* 01.01.-31.12.2009 (11274 EUR)

Further Cooperation, Consulting, and Technology Transfer

The theory group cooperates with groups in Berlin (Prof. Dr. Marcel Kyas), Hannover (Prof. Dr. Heribert Vollmer), Rochester (Prof. Dr. Edith Hemaspaandra), Trier (Prof. Dr. Ralf Küsters), and Warsaw (R. Mikolaj Bojanczyk).

Publications

Published in 2009

J. Schönborn, M. Kyas, *Refinement Patterns for Hierarchical UML State Machines,* LNCS, **5961**, 371 - 386 (2009)
P. Faliszewski, E. Hemaspaandra, H. Schnoor, *Manipulation of Copeland Elections,* Proceedings of AAMAS, (2010)
H. Schnoor, *Strategic Planning for Probabilistic Games with Incomplete Information,* Proceedings of AAMAS, (2010)
M. Aizatulin, H. Schnoor, Th. Wilke, *Computationally Sound Analysis of a Probabilistic Contract Signing Protocol,* Proceedings of ESORICS, LNCS, (2009)
K. O. Kürtz, H. Schnoor, Th. Wilke, *Computationally Secure Two-Round Authenticated Message Exchange,* Proceedings of ASIACCS, (2010)
K. O. Kürtz, H. Schnoor, Th. Wilke, *A Simulation-Based Treatment of Authenticated Message Exchange,* Proceedings of ASIAN, LNCS, **5913**, 109 - 123 (2009)
H. Schnoor, *The Complexity of Model Checking for Boolean Formulas,* Journal of Foundations of Computer Science (to appear), (2010)
D. Kähler, R. Küsters, Th. Wilke, *Deciding Strategy Properties of Contract-Signing Protocols,* ACM Transactions on Computational Logic (in print), (2010)

Presentations

J. Schönborn, *Ready Semantics for UML State Machines,* 21st Nordic Workshop on Programming Theory, Kopenhagen, Dänemark, 14.-17.10.2009
M. Aizatulin, H. Schnoor, Th. Wilke, *Computationally Sound Analysis of a Probabilistic Contract Signing Protocol,* ESORICS, Saint Malo, Frankreich, 21.-23.09.2009
K.O. Kürtz, H. Schnoor, Th. Wilke, *A Simulation-Based Treatment of Authenticated Message Exchange,* ASIAN, Seoul, Korea, 14.-16.12.2009

Further Activities and Events

Th. Wilke was associate editor of Formal Methods in System Design and member of the editorial board of Fundamenta Informaticae and Lecture Notes in Logic.

Th. Wilke was PC member for the conferences AutoMatha, CSL, FSTTCS, LATA, STACS and a workshop of Informatik 2009.

Th. Wilke was member of the executive committee of the GI technical committee Theoretische Informatik and the Council of the European Association for Theoretical Computer Science.

The theory group took part in the following P.R. campaigns of the department: Girls' Day, two one-week programs for high-school students (one with more than 60 participants, and another with about 20 participants).