# Theoretical Computer Science

The theory group specializes in logic in computer science, automata theory (and formal languages), verification, computational complexity, and cryptographic protocols.

## Results

*Automata on infinite objects.* The theory of automata on infinite words is intimately connected with parts of mathematical logic. Since around 1960 this theory has received ever growing attention, in particular, as it forms the basis for current technology for automated verification of reactive and non-terminating systems.

In 2008, the work aiming at a general theory for complementation and determinization of automata on infinite words (Büchi automata) has been continued. A breakthrough was reached by improving the theory developed the previous year in several respects: There is now a convincing unified theory for complementation and determinization of Büchi automata which covers disambiguation as well.

*Analysis and design of cryptographic protocols.* The group has worked on several problems. First, the question of how message exchange in web services can be authenticated in a formal sense was addressed. To this end, the group formalized a straightforward protocol—which works under realistic assumptions and is inspired by current web service standards and web service security standards—and showed that it is provably secure.

Second, the theory group has continued its work on the security of contract-signing protocols in various directions. One line of research is devoted to specifying properties of these protocols in a logical formalism. Such a formalism, based on alternating-time temporal logic, was developed and successfully applied. Another line of research deals with the question of when and how computational soundness can be achieved, given that a protocol is secure in a symbolic setting. First results in this respect were obtained.

*Complexity of satisfiability-related problems.* The theory group obtained (1) a complexity classification of „balanced" satisfiability in the context of constraint satisfaction problems; (2) a classification of the complexity of the modal satisfiability problems when the class of admissible models can be described by certain formulas (universally quantified first-order Horn formulas); and (3) a classification of the model checking and satisfiability problem for linear temporal logic, parametrized by the expressibility of the considered fragment of propositional operators. Further, complexity results were obtained in the context of various problems related to manipulation of elections where „manipulation" refers to voters casting a vote not representing their true preference (in order to obtain a more desirable result).

## Personnel

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

Scientific Staff:

| | | |
|---|---|---|
| Dipl.-Inf. N. Gruschka | 01.-31.01.2008 | CAU |
| M.Sc. I. Khan | 01.01.-31.12.2008 | DAAD |
| Trust Management in Public Key Infrastructure | | |
| Dipl.-Inf. K. O. Kürtz | 01.01.-31.03.2008 | DFG |
| Verifikation kryptographischer Protokolle | | |
| Dipl.-Inf. K. O. Kürtz | 01.04.-30.09.2008 | CAU |

| | | |
|---|---|---|
| Dipl.-Inf. K. O. Kürtz | 01.10.-31.12.2008 | DFG |
| Verifikation kryptographischer Protokolle | | |
| Dipl.-Inf. D. Kähler | 01.01.-31.08.2008 | CAU |
| Dr. H. Schnoor | 01.04.-31.12.2008 | CAU |
| Dr. R. Thöle | 01.10.-31.12.2008 | |
| Dr. E. Valkema | 01.01.-31.03.2008 | CAU |

## Lectures, Seminars, and Laboratory Course Offers

*Winter 2007/2008*

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

Kryptographie, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ D. Kähler)

Theoretische Informatik, 1 hrs Advanced Seminar/Week,
Th. Wilke

*Summer 2008*

Informatik II - Algorithmen und Datenstrukten, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ K. O. Kürtz)

Secure Communications, 2 hrs Lecture/Week,
Th. Wilke (+ H. Schnoor)

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

Theoretische Informatik, 1 hrs Advanced Seminar/Week,
Th. Wilke

*Winter 2008/2009*

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

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

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

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

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

## Third-Party Funds

Deutsche Forschungsgemeinschaft (DFG), *Automatische Analyse kryptographischer Protokolle mit komplexen Nachrichtenformaten*, 01.03.2006-27.02.2008 (125000 EUR)
Deutsche Forschungsgemeinschaft (DFG), *Automatische Analyse kryptographischer Protokolle mit komplexen Nachrichtenformaten*, 01.09.2008-30.08.2010 (119500 EUR)

## Further Cooperation, Consulting, and Technology Transfer

The theory group cooperates with groups in Trier (Prof. Dr. Ralf Küsters), 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).

## Diploma, Bachelor and Master Theses

M. Aizatulin, *A Timely and Balanced Optimistic Contract-Signing Protocol*, 31.03.2008
D. Meyer, *Digitale Signaturen in der Prüfungsorganisation*, 01.02.2008

## Dissertations / Postdoctoral Lecture Qualifications

D. Kähler, *Strategy Properties for Cryptographic Protocols*, 17.08.2008

## Publications

Published in 2008

M. Bauland, T. Schneider, H. Schnoor, I. Schnoor, H. Vollmer, *The Complexity of Generalized Satisfiability for Linear Temporal Logic*, Logical Methods of Computer Science, **5**, 1 - 21 (2009)
M. Bauland, M. Mundhenk, T. Schneider, H. Schnoor, I. Schnoor, H. Vollmer, *The Tractability of Model-Checking for LTL: The Good, the Bad, and the Ugly Fragments*, ECCC, **08-028**, (2008)
E. Brelsford, P. Faliszewski, E. Hemaspaandra, H. Schnoor, I. Schnoor, *Approximability of Manipulating Elections*, Proceedings of AAAI, 44 - 49 (2008)
N. Creignou, H. Schnoor, I. Schnoor, *Non-uniform Boolean Constraint Satisfaction Problems with Cardinality Constraint*, Proceedings of CSL, 109 - 123 (2008)
P. Faliszewski, E. Hemaspaandra, H. Schnoor, *Copeland Voting: Ties Matter*, Proceedings of AAMAS, 983 - 990 (2008)
E. Hemaspaandra, H. Schnoor, *On the Complexity of Elementary Modal Logics*, Proceedings of STACS, **2008**, 349 - 360 (2008)
E. Hemaspaandra, H. Schnoor, I. Schnoor, *Generalized Modal Satisfiability*, CORR, **arXiv:0804.2729v1**, (2008)
D. Kaehler, T. Wilke, *Complementation, Disambiguation, and Determinization of Buechi Automata*, ICALP, 724 - 735 (2008)
K. O. Kuertz, H. Schnoor, T. Wilke, *Computationally Secure Two-Round Authenticated Message Exchange*, Technischer Bericht, CAU, **0810**, (2008)
H. Schnoor, *Symbolic Verification of Computational Security for Branching-Time Properties*, Technischer Bericht, CAU, **0809**, (2008)
H. Schnoor, I. Schnoor, *Partial Polymorphisms and Constraint Satisfaction Problems*, Complexity of Constraints, **LNCS 5250**, 229 - 254 (2008)

## 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 CSL and FoSSaCS, a summer school on semigroup theory in Portugal, a workshop of Informatik 2008 and he was part of the workshop selection board for Informatik 2008.

Th. Wilke was member of the executive committee of the GI working group *Logik in der Informatik* and the GI technical committee *Theoretische Informatik*.

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