Theoretical Computer Science

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

Results

Complex Security Properties of Cryptographic Protocols. Part of the work of the theory group focuses on properties of cryptographic protocols that have *strategic* and *epistemic* (i.e. knowledge-related) aspects. One example for such a property is abuse-freeness of contract signing protocols, where it is required that no involved party can „prove" to an outside party (the „verifier") that she has certain strategic abilities, for instance, being able to choose between getting a valid copy of a contract and preventing a potential contracting partner obtaining one. In joint work with the security group at Trier University, a new attack on such a protocol was identified in 2010. The interesting aspect about the attack is that the „verifier" plays a more active part than in prior considerations. As a consequence of the discovery of the attack, a notion of online abuse-freeness was introduced. Part of the joint work with the group in Trier was an analysis of well-known contract signing protocols with respect to the new security property. Additionally, the group worked on a notion of security for two-round authenticated message exchange in a concrete/computational model. This security notion is relevant for the study of web services; it was proved that a new protocol is secure with respect to the new definition.

Computational Complexity of Logic-Related Problems. In joint work with researchers from Hannover, Jena, Lübeck, Marseille, and Rochester, the theory group worked on several algorithmic problems related to applications of logic in computer science. One example is the use of linear temporal logic (LTL) in verification. More precisely, in the joint work the complexity of variations of the corresponding model-checking problem (to determine whether a given system satisfies a given specification) was analyzed with respect to its computational complexity. Similar results were obtained in the context of modal logics (for the related satisfiability problem) and for quantified and non-uniform constraint satisfaction problems.

Computational Social Choice. The group continued to work on computational aspects of manipulating elections, i.e., the question how human or electronic voters can use dishonesty in elections to achieve a strategic advantage. This research was carried out in cooperation with groups in Rochester and Krakow.

Algorithms in Automata Theory. One of the most prominent applications of regular expressions is in text searching: text searching tools are widespread and valuable tools for programmers (and, sometimes, even users). In joint work with the programming languages research group of the department, a purely functional program for regular expression matching was developed. This program is comparable in terms of efficiency with the Google tools released in the same year.

Computer Science Education. The research group increasingly focuses on topics in computer science education. In 2010, two projects began. One of the projects is a study where a class of high school students (6th grade) is taught according to a curriculum designed for the CS curriculum framework of Schleswig-Holstein as established in 2010. The aim of the study is to evaluate this curriculum. The objective of the other project is to find out to which extent it is possible to convey basic programming and algorithmic skills by (simply) using a specifically designed tool for designing computer animations and computer games in art courses. The tool used is Scratch, which was developed at MIT. First findings show that, in contrast to our assumptions, it is easier for children to use message passing (for structuring a distributed program) than to use loops (as a means of abstraction).

Personnel

Head of the group: Prof. Dr. Th. Wilke; Secretary: H. Capell (15 percent, 3 months), F. Lorenz (50 percent)
Technical Staff: Th. Hess (50%)

Scientific Staff:

Dipl.-Math. S. Eggert	01.01.-31.12.2010		CAU
M.Sc. I. Khan	01.01.-31.12.2010		DAAD
Dipl.-Inf. K. O. Kürtz	01.01.-30.09.2010		DFG Trier
Dipl.-Inf. K. O. Kürtz	01.10.-31.12.2010		CAU
Dipl.-Math. T. Radtke	01.02.-30.09.2010	(50%)	CAU
Dipl.-Math. T. Radtke	01.10.-31.12.2010		ISH
Dr. H. Schnoor	01.01.-31.12.2010		CAU
StR S. Schulmeister	01.01.-31.12.2010	(50%)	CAU
Dipl.-Inf. J. Schönborn	01.01.-30.11.2010	(50%)	CAU
Dr. L. Willert	01.08.-31.12.2010		CAU

Lectures, Seminars, and Laboratory Course Offers

Summer 2010

Secure Communications, 2 (+ 1) hrs Lecture (+ Exercises)/Week,
H. Schnoor

Informatik IV - Theoretische Grundlagen der Informatik, 4 hrs Lecture/Week,
Th. Wilke

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

Winter 2010/2011

Boolesche Schaltkreise, 2 (+ 1) hrs Lecture (+ Exercises)/Week,
H. Schnoor

IT-Sicherheit, 1 (+ 1) hrs Lecture (+ Exercises)/Week,
Th. Wilke

Theoretische Grundlagen der Informatik, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ S. Eggert)

Grundlagen fachbezogenen Lehrens und Lernens im Fach Informatik, 2 hrs Seminar/Week,
L. Willert

Planung, Durchführung und Analyse von Informatikunterricht (im Praxismodul 2), 2 hrs Seminar/Week,
S. Schulmeister

Third-Party Funds

DFG, *Automatische Analyse kryptographischer Protokolle mit komplexen Nachrichtenformaten*, 01.01.-30.08.2010 (119500 EUR)

Innovationsstiftung Schleswig-Holstein, *Wenn Bilder laufen lernen, ist Informatik nicht weit!*, 16.06.2010-30.04.2012 (133080 EUR)

Further Cooperation, Consulting, and Technology Transfer

The theory group cooperates with groups in Trier (Prof. Dr. Ralf Küsters), Hannover (Prof. Dr. Heribert Vollmer), Rochester (Prof. Dr. Edith Hemaspaandra), Marseille (Prof. Dr. Nadia Creignou), Paris (Prof. Dr. Arnaud Durand), Krakow (Prof. Dr. Piotr Faliszewski), and Sydney (Prof. Dr. Ron van der Meyden).

Diploma, Bachelor and Master Theses

J. Dahlke, *Papierbasierte digitale Signaturen,* 15.02.2010
S. Schäfer, *Ein Interpreter für Termersetzungssysteme,* 08.11.2010

Dissertations / Postdoctoral Lecture Qualifications

K. O. Kürtz, *Secure Two-Round Message Exchange,* 10.12.2010

Publications

Published in 2010

R. Küsters, H. Schnoor, T. Truderung, *A formal definition of online abuse-freeness,* Security and Privacy in Communication Networks, **2010**, 484 - 497 (2010)
E. Hemaspaandra, H. Schnoor, I. Schnoor, *Generalized modal satisfiability,* Journal of Computer and System Sciences, **76 (7)**, 561 - 578 (2010)
M. Bauland, E. Böhler, N. Creignou, S. Reith, H. Schnoor, H. Vollmer, *The Complexity of Problems for Quantified Constraints,* Theory of Computing Systems, **47 (2)**, 454 - 490 (2010)
N. Creignou, H. Schnoor, I. Schnoor, *Nonuniform Boolean constraint satisfaction problems with cardinality constraint,* ACM Transactions on Computational Logic, **11 (4)**, (2010)
K. O. Kürtz, H. Schnoor, Th. Wilke, *Computationally secure two-round authenticated message exchange,* ACM Symposium on Information, Computer and Communications Security, **2010**, 214 - 225 (2010)
S. Fischer, Frank Huch, Th. Wilke, *A play on regular expressions: functional pearl,* International Conference on Functional Programming, 357 - 368 (2010)
D. Kähler, R. Küsters, Th. Wilke, *Deciding strategy properties of contract-signing protocols,* ACM Transactions on Computational Logic, **10**, 171 - 1742 (2010)

Presentations

K. O. Kürtz, H. Schnoor, Th. Wilke, *Computationally secure two-round authenticated message exchange,* ASIACCS, Beijing, China, 13.-16.04.2010
H. Schnoor, *Strategic planning for probabilistic games with incomplete information.,* AAMAS 2010, Toronto, Canada, 10.-14.05.2010
P. Faliszewski, E. Hemaspaandra, H. Schnoor, *Manipulation of copeland elections,* AAMAS 2010, Toronto, Canada, 10.-14.05.2010
R. Küsters, H. Schnoor, T. Truderung, *A Formal Definition of Online Abuse-Freeness,* Workshop on Foundations of Security and Privacy, Edinburgh, UK, 14.-15.07.2010
R. Küsters, H. Schnoor, T. Truderung, *A Formal Definition of Online Abuse-Freeness,* SecureComm 2010, Singapore, Singapore, 07.-09.09.2010
H. Schnoor, *Deciding epistemic and strategic properties of cryptographic protocols,* GIPSy 2010, Rennes, France, 15.-16.11.2010

Th. Wilke, *Functional Programs for Regular Expression Matching*, Seminar über Automaten, Wadern, Germany, 13.-17.12.2010
Th. Wilke, *Logic in Cryptography and Cryptographic Protocols*, Logic Colloquium, Paris, France, 25.-31.07.2010
Th. Wilke, *Functional Programs for Regular Expression Matching*, Authomatha 2010, Vienna, Austria, 22.-24.11.2010

Further Activities and Events

- Th. Wilke has been a member of the Council of the European Association for Theoretical Computer Science.
- Th. Wilke has been vice speaker of the division »Grundlagen« of the »Gesellschaft für Informatik«.
- Th. Wilke has been a member of the editorial boards of the following journals and series: Fundamenta Informaticae, Formal Methods in System Design, Lecture Notes in Logic.
- Th. Wilke was a member of the programme committee of LATA 2010.
- Consulting for the curriculum »Angewandte Informatik« (Schulmeister, Wilke),
- Organization of a workshop for computer science and art teachers,
- organization of two weeks »Schnupperstudium Informatik«,
- representation of the department at the »Schleswig-Holstein-Tag 2010«,
- organization of part of the Girls' Day 2010.