Theoretical Computer Science

The group studies topics in cryptography, complexity theory, logic in computer science, automata theory, and computer science education.

Results

Security Analysis for Cryptographic Protocols

Many cryptographic protocols achieve (or aim to) complex security goals that have both strategic and epistemic (knowledge-related) components. For such properties, a violation of the security property cannot be defined as a property of a single run of the protocol but one has to consider dependencies and relations between different runs to decide whether a protocol is secure.

In the working group, a suitable ATL-based logic (QAPI) was developed that allows the formal specification of such security goals and a decidability result was proven: it is decidable whether a given a protocol satisfies a given security property specified in QAPI.

Computational Social Choice

An problem often studied in the context of (electronic) elections is that of *manipulation*: the question is how a group of voters, who have complete knowledge about the votes of all other voters, have to cast their votes in an election to achieve a desired result. Classical results show that every non-trivial voting system yields situations in which it is "better" for a voter not to vote honestly, but "strategically"; in the literature on computational social choice, this is known as manipulation.

In joint work with co-authors in Kraków and Rochester, the group achieved a complexity result for the manipulation problem concerning the case of 4 candidates: the *Llull* voting system can be efficiently manipulated. (Note that in this context, this is a negative result, as one hopes the manipulation problem to be computationally hard, meaning that voters cannot solve it in practice.) The result also applies to the "weighted" case in which different voters have varying degrees of influence over the election outcome.

The reason why this result is interesting is that it is one of the very few cases in which a non-trivial algorithm is exhibited for the manipulation problem: most efficient manipulation algorithms simply let all "manipulating" voters vote identically, which in the case of a fixed number of candidates leads to a trivial algorithm (with usually a non-trivial correctness proof). Our algorithm is significantly more complex and uses techniques from approximation algorithms to obtain an exact solution of the manipulation problem.

Automata on Infinite Words and Temporal Logic

The model of a Büchi automaton is widely considered *the* model of an automaton on infinite words. In 2012, two fundamental results on this automaton model were obtained and published by the theory group. First, it was shown that different complementation procedures known from earlier work can be unified elegantly. Second, a new framework for classifying discrete temporal properties over the natural numbers was developed: the use of so-called prophetic automata, special reverse deterministic Büchi automata, turned out to be especially suited for classification purposes.

Dynamic Information Flow Security

Information-flow security is a well-established technique to model security issues arising in MILS-based architectures (Multiple Independent Levels of Security). The main idea is that data that should only be visible to agents with a high security clearance should never change the view for agents that have a lower security clearance. In the working group, this notion was studied in a dynamic setting. In addition to creating precise security definitions (correcting mistakes made by earlier definitions in the literature), unwinding relations, notions of uniform and consistent policies, and complexity results were established.

Computing Education

See separate section on *computer science education*.

Personnel

Head of the group: Prof. Dr. Th. Wilke; Secretary: K. Flöth (halbe Stelle, 19.05.-31.12.), F. Lorenz (halbe Stelle, 01.01.-31.03.), D. Patz
Technical Staff: H. Schmidt (halbe Stelle, Krankheitsvertretung)

Scientific Staff:

Dipl.-Math. S. Eggert	01.01.-31.12.2012	CAU
Dipl.-Päd. J. Lembke	01.02.-31.08.2012	ISH, 25 %
Dipl.-Math. S. Preugschat	01.04.-30.09.2012	CAU, 50 %
Dipl.-Math. S. Preugschat	01.01.-31.12.2012	CAU, 50 %
Dipl.-Math. T. Radtke	01.02.-31.07.2012	ISH, 50 %
Dipl.-Math. T. Radtke	01.-31.01.2012	ISH, 75 %
Dr. H. Schnoor	01.01.-31.12.2012	CAU
StR S. Schulmeister	01.01.-31.12.2012	CAU, 50 %

Lectures, Seminars, and Laboratory Course Offers

Summer 2012

Inf-LogInf: Logik in der Informatik, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ S. Preugschat)

Inf-MS-Sem-Theorie: Masterseminar Theoretische Informatik, 2 hrs Lecture/Week,
Th. Wilke

Inf-Sem-Theorie: Bahnbrechende Beiträge zur Informatik, 2 hrs Lecture/Week,
S. Eggert (+ Th. Wilke)

MS0105: Angewandte Logik, 4 (+ 2) hrs Lecture (+ Exercises)/Week,
Th. Wilke (+ H. Schnoor)

Wie wird im Internet sicher kommuniziert?, 1 hrs Lecture/Week,
Th. Wilke

Winter 2012/2013

Abschlussarbeiten AG Wilke, 2 hrs Lecture/Week,
Th. Wilke (+ S. Eggert, H. Schnoor)

Inf-AP-EdSoft: Bildungssoftware, 6 hrs Lecture/Week,
Th. Wilke

Inf-EinfPP: Einführendes Programmierpraktikum, 3 hrs Exercise/Week,
H. Schnoor (+ S. Preugschat, S. Schulmeister, S. Eggert)

Inf-MP-ITSec: Masterprojekt Kryptographie und IT-Sicherheit, 4 hrs Exercise/Week, Th. Wilke

MS0101: Kryptographie, 4 (+ 2) hrs Lecture (+ Exercises)/Week, Th. Wilke (+ H. Schnoor)

Third-Party Funds

Innovationsstiftung Schleswig-Holstein, *Wenn Bilder laufen lernen, ist Informatik nicht weit!*, 16.06.2010-31.10.2012 (133.080 EUR)
DiWiSH, *Schnupperstudium Informatik*, 15.-19.10.2012 (1.500,00 EUR)

Further Cooperation, Consulting, and Technology Transfer

The group works 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), Jerusalem (Prof. Orna Kupferman), Houston (Prof. Moshe Y. Vardi), and Sydney (Prof. Dr. Ron van der Meyden).

Diploma, Bachelor's and Master's Theses

Arnd Gongoll, *Implementierung eines eID-Servers (Bachelorarbeit)*, 19.02.2012
Hauke Reklies, *Der OpenPGP-Standard (Bachelorarbeit)*, 30.09.2012
Oliver Woizekowski, *Informationsflusssicherheit bei alternativen Systemmodellen (Diplomarbeit)*, 20.11.2012

Publications

Published in 2012

Piotr Faliszewski, Edith Hemaspaandra, H. Schnoor, *Weighted Manipulation for Four-Candidate Llull Is Easy*, Proceedings of ECAI, 318 - 323 (2012)
H. Schnoor, *Deciding Epistemic and Strategic Properties of Cryptographic Protocols*, Proceedings of ESORICS, 91 - 108 (2012)
S. Preugschat, T. Wilke, *Effective Characterizations of Simple Fragments of Temporal Logic Using Prophetic Automata*, FoSSaCS, 135 - 149 (2012)
Christoph Dürr, Thomas Wilke, *29th International Symposium on Theoretical Aspects of Computer Science, STACS 2012*, LIPIcs, **14**, (2012)
S. Eggert, H. Schnoor, Th. Wilke, *Dynamic Noninterference: Consistent Policies, Characterizations and Verification*, CoRR, **1208.5580**, 1 - 37 (2012)

Presentations

H. Schnoor, *Deciding Epistemic and Strategic Properties of Cryptographic Protocols*, ESORICS 2012, Pisa, Italien, 10.-14.09.2012
Piotr Faliszewski, Edith Hemaspaandra, H. Schnoor, *Weighted Manipulation for Four-Candidate Llull Is Easy*, ECAI 2012, Montpellier, Frankreich, 27.-31.08.2012
S. Preugschat, T. Wilke, *Effective Characterizations of Simple Fragments of Temporal Logic Using Prophetic Automata*, FOSSACS 2012, 24.01.-01.04.2012

Further Activities and Events

» Th. Wilke has been a member of the Council of the European Association for Theoretical Computer Science (EATCS).

» Th. Wilke has been vice speaker of the division Grundlagen of the Gesellschaft für Informatik (GI GB GInf).

» Th. Wilke has been a member of the editorial boards of the following journals and series: Fundamenta Informaticae, Formal Methods in System Design, and Lecture Notes in Logic.

» Th. Wilke was co-chair of the programme committee of STACS 2012 and STACS 2013.

» The group organized a workshop for computer science and art teachers.

» The group organized one week of Schnupperstudium Informatik, jointly with the business office of the department and Priv.-Doz. Dr. Frank Huch.

» The group organized a computer animation contest for schools in Schleswig-Holstein.