Theoretische Informatik

Die Arbeitsgruppe forscht auf den Gebieten Logik in der Informatik, Automaten und formale Sprachen, automatische Verifikation und kryptographische Protokolle.

Ergebnisse

Die Forschungsergebnisse der Arbeitsgruppe, die im Jahr 2004 veröffentlicht wurden, betreffen Anfragesprachen für räumliche Datenbanken, automatische Analyse kryptographischer Protokolle und Sicherheitsdefinitionen für kryptographische Protokolle.

Anfragesprachen für räumliche Datenbanken: In der Theorie der relationalen Datenbanken fällt der Prädikatenlogik erster Stufe eine zentrale Rolle zu, da sie in ihrer Ausdrucksstärke mit SQL übereinstimmt. Will man nun die Ausdrucksstärke von Anfragesprachen für räumliche Datenbanken studieren, so liegt es nahe, auch hier die Prädikatenlogik erster Stufe zu Grunde zu legen, jedoch mit dem reellen Zahlkörper als Grundbereich und versehen mit einem eigenen Prädikat, das auf die in der Datenbank abgelegten Punkte zutrifft. Um die Ausdrucksstärke dieser natürlichen Anfragesprache zu charakterisieren, hat die Arbeitsgruppe in einem internationalen Team mit Kollegen aus Aachen, Belgien und den USA gezeigt, dass sie sich nicht unterscheidet von der Ausdrucksstärke einer Sprache, die lediglich Aussagen darüber treffen kann, wie häufig Punkte mit bestimmten Umgebungsformen vorkommen.

Analyse kryptographischer Protokolle: Der automatischen Analyse kryptographischer Protokolle sind wegen der Komplexität der Fragestellung enge Grenzen gesteckt. Ein Ziel der Arbeitsgruppe ist es, diese Grenzen auszuloten und dadurch eine möglichst große Klasse von kryptographischen Protokollen einer automatischen Analyse zugänglich zu machen. Im Berichtszeitraum ist es der Arbeitsgruppe gelungen, entsprechende Ergebnisse zu erzielen. Zum einen hat die Arbeitsgruppe ein erstes Modell für Protokolle mit listenartigen Datenstrukturen vorgestellt und gezeigt, dass sich Sicherheit in diesem Modell entscheiden lässt. Zum anderen hat die Arbeitsgruppe zusammen mit Wissenschaftlern aus Nancy zeigen können, dass sich Sicherheitseigenschaften kryptographischer Protokolle auch dann noch entscheiden lassen, wenn man die Annahme der perfekten Verschlüsselung abschwächt. Insbesondere lässt sich Sicherheit dann entscheiden, wenn man bei asymmetrischen Verfahren Kommutativität annimmt, wie dies zum Beispiel bei RSA der Fall ist.

Sicherheitsdefinitionen für kryptographische Protokolle: Auf der Suche nach geeigneten Sicherheitsbegriffen für kryptographische Protokolle wurden in den letzten Jahren weltweit diverse miteinander konkurrierende, sehr komplexe Definitionen vorgeschlagen. Um Aufschluss zu gewinnen über Gemeinsamkeiten und Unterschiede dieser Definitionen, hat die Arbeitsgruppe zusammen mit Kollegen aus den USA unter Benutzung von Prozesskalkülen einen geeigneten Rahmen entwickelt und auf dessen Grundlage erste Vergleichsergebnisse erzielt.

Personal

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

Wissenschaftliche Mitarbeiter:

Dipl.-Inf. C. Fritz Sicherung der Lehre	01.01.-29.02.2004	CAU
Dipl.-Inf. C. Fritz Verifikation	01.03.-31.12.2004	DFG
Dr. R. Küsters Kryptographische Protokolle	01.01.-31.12.2004	CAU

Dipl.-Inf. D. Kähler	01.01.-31.12.2004	CAU
Verifikation kryptographischer Protokolle		
Dr. E. Valkema	01.01.-31.12.2004	CAU

Vorlesungen, Seminare und Praktika

Winter 2003/2004

Informatik IV, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke (+ H. Fecher, D. Kähler)

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

Bioinformatik, 2 Std. Vorlesung/Woche,
J. Grötzinger, M. Krawczak, Th. Wilke

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

Hardware-Praktikum, 4 Std. Praktikum/Woche,
E. Valkema

Sommer 2004

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

Informatik II für Ingenieure, 2 Std. Praktikum/Woche,
D. Kähler

Secure Communications, 2 (+ 1) Std. Vorlesung (+ Übungen)/Woche,
R. Küsters (+ D. Kähler)

Secure Communications, 1 Std. Diskussionsrunde/Woche,
D. Kähler

Verifikation kryptographischer Protokolle, 1 (+ 1) Std. Vorlesung (+ Übungen)/Woche,
R. Küsters

Winter 2004/2005

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

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

Automaten und formale Sprachen, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
R. Küsters, Th. Wilke (+ C. Fritz)

(t,i)-Café, 1 Std. Seminar/Woche,
C. Fritz, D. Kähler, R. Küsters, Th. Wilke

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

Drittmittel

German-Israeli Foundation for Scientific Research and Development (GIF), *Incremental Model Checking*, 01.01.2001-31.12.2004 (59400 EUR)
Deutsche Forschungsgemeinschaft (DFG), *Minimierung von Automaten mit Anwendungen in der Verifikation nichtterminierender Systeme*, 01.03.2004-28.02.2006 (125000 EUR)
Deutscher Akademischer Austauschdienst (DAAD), *PROCOPE - Personenaustausch mit Frankreich*, 01.01.2003-31.12.2004 (10056 EUR)
EU-Programm IST: Network of Excellence (NoE), *Semantic Interoperability and Datamining in Biomedicine*, 01.01.2004-31.12.2006 (28520 EUR)

Diplom- und Master-Arbeiten

A. Obermann, *Verifikation kryptographischer Protokolle mit Baumtransduktionen*, 28.10.2004
J. Solomon, *A Java Library for Linear Cryptanalysis*, 17.11.2004
M. Sridharan, *A Java Library for Differential Cryptanalysis*, 11.11.2004
M. Wendel, *Implementierung und Bewertung eines Constraint-basierten Ansatzes zur Verifikation kryptographischer Protokolle*, 15.01.2004

Veröffentlichungen

erschienen im Jahre 2004

D. Thérien, Th. Wilke, *Nesting Until and Since in Linear Temporal Logic*, Theory Comput. Syst., **37(1)**, 111 - 131 (2004)
R. Küsters, Th. Wilke, *Automata-Based Analysis of Recursive Cryptographic Protocols*, STACS 2004, 21st Annual Symposium on Theoretical Aspects of Computer Science, Montpellier, Frankreich, 382 - 393 (2004)
M. Benedikt, C. Löding, J. van den Bussche, Th. Wilke, M. Benedikt, M. Benedikt, M. Benedikt, *A Characterization of First-Order Topological Properties of Planar Spatial Data*, Proceedings of the Twenty-third ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, Paris, Frankreich, 107 - 114 (2004)
R. Küsters, *On the Decidability of Cryptographic Protocols with Open-ended Data Structures*, International Journal of Information Security, **DOI: 10.1007/s10207-004-0050-z**, 1 - 22 (2004)
Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, *Deciding the Security of Protocols with Commuting Public Key Encryption*, IJCAR 2004, Workshop W6, Automated Reasoning for Security Protocol Analysis (ARSPA 2004), 1 - 11 (2004)
A. Datta, R. Küsters, J. Mitchell, A. Ramanathan, V. Shmatikov, *Unifying Equivalence-Based Definitions of Protocol Security*, IFIP 2004, WG 1.7, ACM SIGPLAN and GI FoMSESS Workshop on Issues in the Theory of Security (WITS 2004), 1 - 16 (2004)

Präsentationen

Th. Wilke, *Automata-based Analysis of Recursive Cryptographic Protocols*, Kolloquium Departement Informatik, ETH Zürich, Zürich, Schweiz, 02.07.2004
Th. Wilke, *Automata-based Analysis of Recursive Cryptographic Protocols*, DIMACS Workshop on Protocol Analysis, Piscataway, NJ, USA, 07.06.2004
Th. Wilke, *Verifikation kryptographischer Protokolle*, Jährliches Treffen Algorithmische Modelltheorie, Berlin, Deutschland, 25.02.2004
Th. Wilke, *Automaten – Theorie und Anwendung*, Kolloquium Fachbereich Informatik, TU Darmstadt, Darmstadt, Deutschland, 08.07.2004

R. Küsters, *Sequential Probabilistic Process Calculus and Machine Models for Simulation-based Security*, DIMACS Workshop: Security Analysis of Protocols, Piscataway, USA, 08.06.2004

R. Küsters, *Automatische Analyse kryptographischer Protokolle*, GI-Fachgruppentreffen FoMSESS, Darmstadt, Deutschland, 24.06.2004

R. Küsters, *Sequential Probabilistic Process Calculus and Machine Models for Simulation-based Security*, Stanford Security Seminar, Stanford, USA, 03.08.2004

R. Küsters, *Automatic Analysis of Recursive Cryptographic Protocols*, Security Seminar at University of Pennsylvania, Philadelphia, USA, 09.08.2004

R. Küsters, *Deciding Cryptographic Protocols with Game-theoretic Security Requirements*, Meeting of the EU Training Network GAMES 2004, Bordeaux, Frankreich, 18.09.2004

R. Küsters, *Tree Transducer-based Analysis of Cryptographic Protocols*, 14. Theorietag der GI-Fachgruppe Automaten und Formale Sprachen, Caputh, Deutschland, 30.09.2004

R. Küsters, *Automatic Analysis of Cryptographic Protocols with Exclusive Or and Diffie-Hellman Exponentiation*, Gemeinsames Jahrestreffen der GI-Fachgruppen Deduktionssysteme und Logik in der Informatik, Saarbrücken, Deutschland, 10.10.2004

C. Fritz, *From LTL to Small Büchi Automata Via Alternating Büchi Automata*, Minerva Formal Verification School, Kibbutz Shfayim, Israel, 19.05.2004

D. Kähler, *Program Complexity of Dynamic LTL Model Checking*, Minerva Formal Verification School, Kibbutz Shfayim, Israel, 16.05.2004

Andere Aktivitäten und Ereignisse

Th. Wilke war im Berichtszeitraum stellv. Sprecher der Fachgruppe Logik in der Informatik der Gesellschaft für Informatik.

Th. Wilke war Mitglied des Programmkomitees von FOSSACS 2004 (Foundations of Software Sciences and Computations Structures).

R. Küsters war Mitglied des Programmkomitees von DL 2004 (International Workshop on Description Logics).