Theoretische Informatik

Die Arbeitsgruppe forscht auf den Gebieten Logik in der Informatik, Automatentheorie und Verifikationstheorie, auf letzterem hauptsächlich mit dem Ziel der Entwicklung effizienter Verifikationsverfahren und der Abgrenzung automatisch lösbarer Verikationsprobleme von solchen, die nur durch menschliche Hilfe lösbar sind. Ein aktueller Forschungsschwerpunkt ist die Verifikation kryptographischer Protokolle.

Ergebnisse

Die Forschungsergebnisse der Arbeitsgruppe, die im Jahr 2003 veröffentlicht wurden, betreffen inkrementelle Model-Checking-Probleme, Minimierung von Büchi-Automaten zu Formeln linearer temporaler Logik, die Klassifizierung von Spezifikationen in linearer temporaler Logik und die automatische Verifikation kryptographischer Protokolle.

Die algorithmische Komplexität des Model-Checking-Problems für lineare temporale Logik ist hinreichend untersucht und verstanden. Weniger untersucht wurde jedoch bislang die Erweiterung um eine dynamische Komponente, bei der man (der Realität folgend) in Betracht zieht, dass sich sowohl die Spezifikation wie auch das betrachtete System im Laufe des Entwicklungsprozesses ändern können. Der Arbeitsgruppe ist es gelungen, ein erstes greifbares Ergebnis über diese Variante des Model-Checking-Problems zu erzielen: das Problem kann für eine feste Formel und ein variables System durch Schaltkreise kleiner Größe gelöst werden.

Alle automatischen Verifikationswerkzeuge, die Spezifikationen in linearer temporaler Logik zulassen, wandeln Formeln dieser Logik in geeignete Automaten um. Dabei ist darauf zu achten, dass die Automaten nicht zu groß werden und die Übersetzung effizient bleibt. Die Arbeitsgruppe hat hier eine konkurrenzfähige Alternative zu den bekannten Verfahren entwickelt, und zwar durch den Aufbau einer geeigneten Minimierungstheorie für alternierende Automaten.

Spezifikationen in linearer temporaler Logik werden in erster Linie durch Verschachtelung der zweistelligen modalen Operatoren „seit“ und „bis“ schwer lesbar. Deshalb stellt sich die Frage, ob bzw. wie man eine solche Schachtelung ggf. beseitigen kann. Diese Frage wurde durch die Arbeitsgruppe in Zusammenarbeit mit Forschern aus Montreal unter Benutzung der Theorie der endlichen Halbgruppen abschließend beantwortet.

Bisherige Verfahren zur vollständig automatischen Verifikation kryptographischer Protokolle sind auf Klassen von Protokollen und Angreifern auf diese Protokolle beschränkt, bei denen die verwendeten kryptographischen Primitive, wie zum Beispiel Verschlüsselungsverfahren, keinerlei algebraische Eigenschaften aufweisen. In Zusammenarbeit mit Forschern aus Nancy ist es der Arbeitsgruppe gelungen, in der Praxis häufig vorkommende algebraische Eigenschaften in die Analyse der Protokolle miteinzubeziehen und so die Klasse der automatisch analysierbaren Protokolle deutlich zu erweitern sowie die Genauigkeit der Analysen selbst wesentlich zu erhöhen.

Personal

Leiter: Prof. Dr. Th. Wilke; Sekretariat: M. Krause (50%)
Technisches Personal: Dipl.-Inf. F. Steiner

Wissenschaftliche Mitarbeiter:

Dipl.-Inf. C. Fritz Automatenminimierung	01.01.-31.07.2003	DFG
Dipl.-Inf. C. Fritz Sicherung der Lehre	01.08.-31.12.2003	CAU
Dr. R. Küsters Kryptographische Protokolle	01.01.-31.12.2003	CAU

Dipl.-Inf. D. Kähler	01.01.-30.04.2003	GIF
Incremental Model Checking		
Dipl.-Inf. D. Kähler	01.11.-31.12.2003	CAU
Verifikation kryptographischer Protokolle		
Dr. E. Valkema	01.01.-31.12.2003	CAU

Vorlesungen, Seminare und Praktika

Winter 2002/2003

Software-Praktikum, 1 (+ 1) Std. Praktikum (+ Übungen)/Woche,
Th. Wilke

Oberseminar Theoretische Informatik, 2 Std. Seminar/Woche,
Th. Wilke

Informatik für Nebenfächler, 4 Std. Vorlesung/Woche,
E. Valkema

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

Sommer 2003

Secure Communications, 2 (+ 1) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke

Moderne Kryptographie, 2 Std. Seminar/Woche,
Th. Wilke

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

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

Informatik II, 4 (+ 2) Std. Vorlesung (+ Übungen)/Woche,
Th. Wilke (+ C. Fritz)

Programmierpraktikum zu Informatik II, 3 Std. Praktikum/Woche,
Th. Wilke

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 (+ x x, x x)

Informatik für Nebenfächler, 4 Std. Vorlesung/Woche,
E. Valkema

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

Drittmittel

German-Israeli Foundation for Scientific Research and Development (GIF), *Incremental Model Checking,* 01.01.2001-31.12.2003 (60.000 EUR)

Deutsche Forschungsgemeinschaft (DFG), *Minimierung von Automaten mit Anwendungen in der Verifikation nichtterminierender Systeme,* 01.08.2001-31.07.2003 (126.740 EUR)

Deutscher Akademischer Austausch Dienst (DAAD), *PROCOPE - Personenaustausch mit Frankreich,* 01.01.2003-31.12.2004 (10.056 EUR)

Weitere Zusammenarbeiten, Technologie Transfers und Konsultationen

Die Arbeitsgruppe pflegt intensive nationale und internationale Kontakte. So waren denn auch in 2003 Arbeitsgruppen z. B. aus Dresden, Nancy und Montreal an den Veröffentlichungen der Arbeitsgruppe beteiligt.

Veröffentlichungen

erschienen im Jahre 2003

Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, *An NP Decision Procedure for Protocol Insecurity with XOR,* Proceedings of the Eighteenth Annual IEEE Symposium on Logic in Computer Science (LICS), 261 - 270 (2003)

C. Fritz, *Constructing Büchi Automata from Linear Temporal Logic Using Simulation Relations for Alternating Büchi Automata,* Proceedings of the 8th International Conference on Implementation and Application of Automata (CIAA), 35 - 48 (2003)

Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, *Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents,* 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 124 - 135 (2003)

Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, *Extending the Dolev-Yao Intruder for Analyzing an Unbounded Number of Sessions,* Annual Conference of the European Association for Computer Science Logic (CSL), 128 - 141 (2003)

S. Brandt, A. Turhan, R. Küsters, *Extensions of Non-standard Inferences to Description Logics with Transitive Roles,* Proceedings of the 10th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR), 122 - 136 (2003)

F. Baader, R. Küsters, F. Wolter, *Extensions to Description Logics,* The Description Logics Handbook: Theory, Implementations, and Applications, 219 - 261 (2003)

D. Therien, Th. Wilke, *Nesting until and since in linear temporal logic,* Theory of Computing Systems, **37**, 111 - 131 (2003)

D. Kähler, Th. Wilke, *Program Complexity of Dynamic LTL Model Checking,* Annual Conference of the European Association for Computer Science Logic (CSL), 271 - 284 (2003)

Präsentationen

C. Fritz, *Constructing Büchi Automata from Linear Temporal Logic Using Simulation Relations for Alternating Büchi Automata,* 8th International Conference on Implementation and Application of Automata (CIAA 2003), Santa Barbara, CA, USA, 16.-18.07.2003

D. Kähler, *Program Complexity of Dynamic LTL Model Checking,* Annual Conference of the European Association for Computer Science Logic, Wien, Österreich, 28.-30.08.2003