Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2002
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosiraportti 2002
Espoo 2003 HUT-TCS-Y2002

ANNUAL REPORT FOR THE YEAR 2002

Kimmo Varpaaniemi (Ed.)

TEKNILLINEN KORKEAKOULU
TEKNISKA HÖGSKOLAN
HELSINKI UNIVERSITY OF TECHNOLOGY
TECHNISCHE UNIVERSITÄT HELSINKI
UNIVERSITE DE TECHNOLOGIE D'HELSINKI

Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2002
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosiraportti 2002
Espoo 2003 HUT-TCS-Y2002

ANNUAL REPORT FOR THE YEAR 2002

Kimmo Varpaaniemi (Ed.)

Helsinki University of Technology
Department of Computer Science and Engineering
Laboratory for Theoretical Computer Science

Teknillinen korkeakoulu
Tietotekniikan osasto
Tietojenkäsittelyteorian laboratorio

Distribution:
Helsinki University of Technology
Laboratory for Theoretical Computer Science
P.O.Box 5400
FIN-02015 HUT, Finland
Tel. +358-9-451 1
Fax. +358-9-451 3369
E-mail: lab@tcs.hut.fi

Printing: Multiprint Oy,
Helsinki 2003

Abstract: This report describes the educational and research activities of the Laboratory for Theoretical Computer Science at Helsinki University of Technology during the year 2002. In the PDF version of this report, URL addresses are links to the corresponding addresses. For example, you get to the home page of the laboratory by clicking http://www.tcs.hut.fi/.

CONTENTS

1 PERSONNEL

1.1 University staff

Niemelä, Ilkka, D.Sc. (Tech.) (cf. 1.3)	Professor. Head of the Laboratory.
Kari, Hannu H., D.Sc (Tech.) (cf. 1.3)	Professor in Computer Science (Mobility Management in Computer Networks) since September 1. Professor (pro tem) until August 31.
Orponen, Pekka, D.Phil. (cf. 1.3)	Professor.
Husberg, Nisse, D.Sc. (Tech.) (cf. 1.2, 1.3, 1.5)	Professor (pro tem) until May 31 and since October 1.
Lipmaa, Helger, PhD (cf. 1.3)	Professor (pro tem).
Ojala, Leo, Lic.Sc. (Tech.) (cf. 1.3)	Professor Emeritus.
Kangasniemi, Ulla	Secretary.
Klaus, Katja	Secretary since April 1.
Lassila, Eero, Lic.Sc. (Tech.) (cf. 1.5)	Laboratory Manager (on leave).
Lintulaakso, Tuomo	Laboratory Manager (acting).
Heljanko, Keijo, D.Sc. (Tech.) (cf. 1.3, 1.5, 5.5)	Senior Assistant (on leave).
Janhunen, Tomi, D.Sc. (Tech.) (cf. 1.3)	Teaching Researcher.
Varpaaniemi, Kimmo, D.Sc. (Tech.)	Senior Assistant.

1.2 Docents

Husberg, Nisse, D.Sc. (Tech.) (cf. 1.1, 1.3, 1.5)	Docent in Verification.
Lilius, Johan, D.Sc. (Tech.)	Docent in Reactive Systems. Professor in Computer Science and Engineering (Åbo Akademi University).
Ukkonen, Esko, D.Phil.	Docent in Theoretical Computer Science. Professor in Computer Science (University of Helsinki and the Academy of Finland).

1.3 Teachers of the active courses of the year 2002

Haanpää, Harri, Lic.Sc. (Tech.) (cf. 1.5)	T-79.161	Combinatorial Algorithms (spring)
Heljanko, Keijo, D.Sc. (Tech.) (cf. 1.1, 1.5, 5.5)	T-79.186	Reactive Systems (spring)
Herttua, Ilkka, Stud.Tech.	T-79.232	Safety-Critical Systems (spring)
Huima, Antti, M.Sc. (Tech.)	T-79.190	Testing of Concurrent Systems (autumn)
Husberg, Nisse, Professor (pro tem) (cf. 1.1, 1.2, 1.5)	T-79.185 T-79.193	Verification (autumn) Formal Description Techniques for Concurrent Systems (spring)
Janhunen, Tomi, D.Sc. (Tech.) (cf. 1.1)	T-79.144 T-79.154 T-79.230	Logic in Computer Science: Foundations (autumn) Logic in Computer Science: Special Topics II (autumn) Foundations of Agent-Based Computing (spring)
Kari, Hannu H., Professor (cf. 1.1)	T-79.300	Postgraduate Course in Theoretical Computer Science (autumn)
Lipmaa, Helger, Professor (pro tem) (cf. 1.1)	T-79.159 T-79.512 T-79.514	Cryptography and Data Security (spring) Cryptology: Special Topics (spring) Special Course on Cryptology (autumn)
Mäkelä, Marko, Lic.Sc. (Tech.) (cf. 1.5)	T-79.179	Parallel and Distributed Digital Systems (spring)
Niemelä, Ilkka, Professor (cf. 1.1)	T-79.146 T-79.194 T-79.240	Logic in Computer Science: Special Topics I (spring) Seminar on Theoretical Computer Science (spring) Special Course in Computational Complexity (autumn)
Ojala, Leo, Professor Emeritus (cf. 1.1)	T-79.157	Formal Description and Verification of Computing Systems (spring)
Orponen, Pekka, Professor (cf. 1.1)	T-79.148 T-79.192 T-79.300	Introduction to Theoretical Computer Science (spring, autumn) Special Course in Theoretical Computer Science (autumn) Postgraduate Course in Theoretical Computer Science (spring)
Tynjälä, Teemu, M.Sc. (Tech.) (cf. 1.5)	T-79.231	Parallel and Distributed Digital Systems (autumn)

1.4 Teaching assistants in the active courses of the year 2002

Hietalahti, Maarit M.Sc. (Tech.) (cf. 1.5)	T-79.300	Postgraduate Course in Theoretical Computer Science (autumn)
Honkola, Jukka, Stud.Tech. (cf. 1.5)	T-79.179	Parallel and Distributed Digital Systems (spring)
	T-79.231	Parallel and Distributed Digital Systems (autumn)
Huuskonen, Jorma, M.Sc. (Tech.)	T-79.157	Formal Description and Verification of Computing Systems (spring)
Junttila, Tommi, Lic.Sc. (Tech.) (cf. 1.5)	T-79.240	Special Course in Computational Complexity (autumn)
Jussila, Toni, Lic.Sc. (Tech.) (cf. 1.5)	T-79.144	Logic in Computer Science: Foundations (autumn)
	T-79.148	Introduction to Theoretical Computer Science (spring, autumn)
Järvisalo, Matti, Stud.Tech. (cf. 1.5)	T-79.148	Introduction to Theoretical Computer Science (spring, autumn)
Kaski, Petteri, Lic.Sc. (Tech.) (cf. 1.5, 5.6)	T-79.161	Combinatorial Algorithms (spring)
Keinänen, Misa, M.A. (cf. 1.5)	T-79.144	Logic in Computer Science: Foundations (autumn)
	T-79.186	Reactive Systems (spring)
Latvala, Timo, Lic.Sc. (Tech.) (cf. 1.5, 5.6)	T-79.148	Introduction to Theoretical Computer Science (spring, autumn)
Oikarinen, Emilia, Stud.Tech. (cf. 1.5)	T-79.144	Logic in Computer Science: Foundations (autumn)
	T-79.148	Introduction to Theoretical Computer Science (spring)
Parviainen, Elina, Stud.Tech. (cf. 1.5, 5.7)	T-79.148	Introduction to Theoretical Computer Science (spring)
Pyhälä, Tuomo, Stud.Tech. (cf. 1.5)	T-79.148	Introduction to Theoretical Computer Science (spring)
	T-79.190	Testing of Concurrent Systems (autumn)
Saarinen, Markku-Juhani O. (cf. 1.5)	T-79.159	Cryptography and Data Security (spring)
Syrjänen, Tommi, M.Sc. (Tech.) (cf. 1.5)	T-79.148	Introduction to Theoretical Computer Science (spring, autumn)
	T-79.154	Logic in Computer Science: Special Topics II (autumn)
	T-79.230	Foundations of Agent-Based Computing (spring)

Särelä, Mikko, Stud.Tech. (cf. 1.5)	T-79.148	Introduction to Theoretical Computer Science (spring, autumn)
Tauriainen, Heikki, M.Sc. (Tech.) (cf. 1.5)	T-79.146	Logic in Computer Science: Special Topics I (spring)
Virtanen, Satu M.Sc. (Tech.) (cf. 1.5)	T-79.192	Special Course in Theoretical Computer Science (autumn)
Wallén, Johan, Stud.Tech. (cf. 1.5)	T-79.159	Cryptography and Data Security (spring)

1.5 Researchers and research assistants

Autere, Antti	M.Sc. (Tech.)	Researcher (since February 11)
Auvinen, Janne	Stud.Tech.	Research Assistant (June 1 – October 15)
Candolin, Catharina	M.Sc. (Tech.) (cf. 5.7)	Research Assistant (January) Researcher (since February 1)
Falck, Emil	Stud.Tech.	Research Assistant
Gangl, Thomas	(cf. 4.3)	Trainee (July 1 – August 31)
Haanpää, Harri	Lic.Sc. (Tech.) (cf. 1.3)	Researcher
Haddad, Wassim	M.Sc. (cf. 4.3)	Researcher (March 1 – June 30, external funding)
Heljanko, Keijo	D.Sc. (Tech.) (cf. 1.1, 1.3, 5.5)	Researcher
Hietalahti, Maarit	M.Sc. (Tech.) (cf. 1.4)	Researcher
Honkola, Jukka	Stud.Tech. (cf. 1.4)	Research Assistant
Husberg, Nisse	D.Sc. (Tech.) (cf. 1.1, 1.2, 1.3)	Researcher (June 1 – September 30)
Junttila, Tommi	Lic.Sc. (Tech.) (cf. 1.4)	Researcher
Jussila, Toni	Lic.Sc. (Tech.) (cf. 1.4)	Researcher
Järvenpää, Jukka	M.Sc. (Tech.)	Researcher (until August 31, external funding)
Järvisalo, Matti	Stud.Tech. (cf. 1.4)	Research Assistant (since June 1)
Kaski, Petteri	Lic.Sc. (Tech.) (cf. 1.4, 5.6)	Researcher
Keinänen, Misa	M.A. (cf. 1.4)	Researcher
Kodym, Petr Ladislav	M.Sc.	Researcher (since March 20)
Lassila, Eero	Lic.Sc. (Tech.) (cf. 1.1)	Researcher
Latvala, Timo	Lic.Sc. (Tech.) (cf. 1.4, 5.6)	Researcher

Litkey, David	Stud.Tech.	Research Assistant (April 1 – July 31)
Lundberg, Janne	M.Sc. (Tech.) (since January 21)	Researcher
Mürk, Oleg	B.Sc.	Research Assistant (February 1 – June 30)
Mustonen, Kimmo	Stud.Tech.	Research Assistant (June 24 – October 31)
Mäkelä, Marko	Lic.Sc. (Tech.) (cf. 1.3)	Researcher
Oikarinen, Emilia	Stud.Tech. (cf. 1.4)	Research Assistant
Parviainen, Elina	Stud.Tech. (cf. 1.4, 5.7)	Research Assistant (until May 31)
Pyhälä, Tuomo	Stud.Tech. (cf. 1.4)	Research Assistant
Pääkkönen, Rauni	M.Sc. (Tech.)	Researcher (until June 12)
Saarinen, Markku-Juhani O.	(cf. 1.4)	Research Assistant (since February 1)
Seitz, Sakari	Stud.Tech.	Research Assistant (February 4 – May 3, and since September 1)
Sten, Antti	Stud.Tech.	Research Assistant (June 1 – October 15)
Syrjänen, Tommi	M.Sc. (Tech.) (cf. 1.4)	Researcher
Särelä, Mikko	Stud.Tech. (cf. 1.4)	Research Assistant (since March 1)
Tauriainen, Heikki	M.Sc. (Tech.) (cf. 1.4)	Researcher
Tynjälä, Teemu	M.Sc. (Tech.) (cf. 1.3)	Researcher
Virtanen, Satu	M.Sc. (Tech.) (cf. 1.4)	Researcher (Teaching Researcher, on leave, Laboratory of Information Processing Science)
Wallén, Johan	Stud.Tech. (cf. 1.4)	Research Assistant (since February 1)

2 EDUCATIONAL ACTIVITIES

The aim of the education at the undergraduate level is to give students basic insight into theoretical computer science as well as learning in applying theoretical results to practice. At the post-graduate level knowledge in the aforementioned areas will be completed further, especially in some particular theoretical questions. During the year 2002, the following courses were active, i.e. arranged as lectures, seminars or projects. In addition, a number of intensive short courses were given by visiting researchers. These can be found in Section 4.3.

T-79.144 Logic in Computer Science: Foundations
(autumn, 2 credits ; teacher: Tomi Janhunen)

Contents: Propositional and predicate logic, their syntax, semantics and proof theory. Applications of logic in computer science.

T-79.146 Logic in Computer Science: Special Topics I
(spring, 2 credits ; teacher: Ilkka Niemelä)

Contents: Basics of modal logic. Current applications in computer science.

T-79.148 Introduction to Theoretical Computer Science
(spring, autumn, 2 credits ; teacher: Pekka Orponen)

Contents: Finite automata and regular languages. Context-free grammars and pushdown automata. Context-sensitive and unrestricted grammars. Turing machines and computability. Additional information: The course is given in two sections: the Spring section is primarily oriented towards students in the Computer Science program, and the Autumn section towards students in other programs.

T-79.154 Logic in Computer Science: Special Topics II
(autumn, 2 credits ; teacher: Tomi Janhunen)

Contents: Efficient implementation methods for propositional logic. Logical foundations and implementation techniques of rule-based systems. Current applications.

T-79.157 Formal Description and Verification of Computing Systems (spring, 2 credits ; teacher: Leo Ojala)

Contents: The use of net theoretic models in the exact modelling of distributed algorithms and the efficient verification of the models. Applications primarily to communication protocols.

T-79.159 Cryptography and Data Security
(spring, 3 credits ; teacher: Helger Lipmaa)

Contents: Unconditional and computational security. Symmetric and asymmetric cryptography. Block ciphers, stream ciphers, public key cryptosystems, digital signatures, key distribution, secret sharing and other algorithms and protocols. Security proofs and definitions. Modern cryptography (zero-knowledge, proofs of knowledge). New directions in cryptography. Practical applications.

T-79.161 Combinatorial Algorithms
(spring, 2 credits ; teacher: Harri Haanpää)

Contents: Basic algorithms and computational methods for combinatorial problems. Combinatorial structure generation (e.g. permutations). Search methods. Graph algorithms and combinatorial optimization. Symmetries of combinatorial structures.

T-79.179 Parallel and Distributed Digital Systems
(spring, 3 credits ; teacher: Marko Mäkelä)

Contents: Modelling and analysis of parallel and distributed digital systems. Concurrency. Basics of Petri nets and process algebra (CCS). Using computer-aided methods for the analysis and verification of telecommunication systems, especially communication protocols.

T-79.185 Verification
(autumn, 3 credits ; teacher: Nisse Husberg)

Contents: Verification and analysis of parallel and distributed systems using tools. Applications to telecommunication protocols. Practical verification methods, e.g. partial reachability analysis. Introduction to current research problems.

T-79.186 Reactive Systems
(spring, 2 credits ; teacher: Keijo Heljanko)

Contents: Specification and verification of reactive systems with temporal logic. Basics of computer-aided verification methods and their algorithms.

T-79.189 Student Project in Theoretical Computer Science
(3 credits ; teachers: all professors at HUT-TCS)

Contents: Independent student project on a subject from the field of theoretical computer science.

T-79.192 Special Course in Theoretical Computer Science
(autumn, 2 credits ; teacher: Pekka Orponen)

Contents: Current topics in theoretical computer science. The course in Autumn 2002 was concerned with algorithmic issues in distributed systems.

T-79.193 Formal Description Techniques for Concurrent Systems (spring, 2 credits ; teacher: Nisse Husberg)

Contents: Validation, testing and analysis methods for large concurrent systems, embedded systems and real-time software.

T-79.194 Seminar on Theoretical Computer Science
(spring, 2 credits ; teacher: Ilkka Niemelä)

Contents: Current research topics in theoretical computer science. The course in Spring 2002 was concerned with foundations of electronic marketplaces.

T-79.230 Foundations of Agent-Based Computing
(spring, 3 credits ; teacher: Tomi Janhunen)

Contents: Structure of software agents. Rational and intelligent agents. Architectures, implementation technologies and applications for agent-based computing.

T-79.231 Parallel and Distributed Digital Systems
(autumn, 3 credits ; teacher: Teemu Tynjälä)

Contents: Modelling and analysis of parallel and distributed digital systems. Concurrency. Basics of Petri nets and process algebra (CCS). Using computer-aided methods for the analysis and verification of telecommunication systems, especially communication protocols.

T-79.232 Safety-Critical Systems
(spring, 2 credits ; teacher: Ilkka Herttua)

Contents: Safety-critical systems. The use of formal methods in the specification, modelling and verification of systems.

T-79.240 Special Course in Computational Complexity
(autumn, 3 credits ; teacher: Ilkka Niemelä)

Contents: NP-completeness. Randomized algorithms. Cryptography. Approximation algorithms. Parallel algorithms. Polynomial hierarchy. PSPACE-completeness.

T-79.295 Individual Studies
(1–10 credits ; teachers: all professors at HUT-TCS)

Contents: Individual studies on a subject from the field of theoretical computer science.

T-79.300 Postgraduate Course in Theoretical Computer Science (spring, 2–10 credits ; teacher: Pekka Orponen)

Contents: Current research problems in theoretical computer science. The course in Spring 2002 was concerned with fitness landscapes, i.e. the geometrical, statistical and computational characteristics of the hypersurfaces determined by natural or artificial fitness (cost, potential, energy) functions.

T-79.300 Postgraduate Course in Theoretical Computer Science (autumn, 2–10 credits ; teacher: Hannu H. Kari)

Contents: Current research problems in theoretical computer science. The course in Autumn 2002 was concerned with special issues on mobility, e.g. mobility management, security, quality of service, access control and adaptive applications.

T-79.512 Cryptology: Special Topics
(spring, 2 credits ; teacher: Helger Lipmaa)

Contents: This is a graduate level course that every semester concentrates on one concrete area of cryptology. The course in Spring 2002 was concerned with provable security,

T-79.514 Special Course on Cryptology
(autumn, 2–6 credits ; teacher: Helger Lipmaa)

Contents: This is a graduate level course that every semester concentrates on one concrete area of cryptology. The course in Autumn 2002 was concerned with multi-party computation.

3 RESEARCH ACTIVITIES

A major part of the research has been funded by the Academy of Finland with substantial support from Helsinki Graduate School in Computer Science and Engineering (HeCSE). More details on this research is given in Sections 3.1, 3.2, 3.4, 3.5, and 3.6. For more applied research funding has been awarded by non-academic partners. This research is described in Sections 3.3 and 3.7.

3.1 Computational logic

Research in the area of computational logic has been carried out in two projects funded by the Academy of Finland titled "Applications of rule-based constraint programming" and "Formal methods in distributed systems". More detailed description of the research is given below.

3.1.1 Applications of rule-based constraint programming

Extensions of rule-based constraint programming
Ilkka Niemelä and Tommi Syrjänen

The development of declarative semantics, such as the stable model semantics, for logic programming type rules has led to an interesting new paradigm for solving computationally challenging problems. In the novel answer set programming (ASP) paradigm a problem is solved by devising a logic program whose answer sets correspond to the solutions of the problem and then using an efficient answer set solver to find answer sets of the program. The project has developed an efficient ASP system called `Smodels` which is used in dozens of research groups world wide.

In many applications normal logic program rules lack expressivity to handle cardinalities, weights and optimization. We have developed an extended rule language which allows for cardinality and weight constraints and optimization capabilities and devised a generalization of the stable model semantics for it [3]. The rule language has been further extended

to allow the use of logical variables, function symbols and built-in arithmetic. In order to keep the language decidable the rules are required to be domain-restricted such that the domain of each variable is defined using a domain predicate. We have devised a method for allowing recursive definitions of domain predicates and studied the expressivity and computational complexity of the resulting rule language.

In many applications preferences need to be expressed. In order to capture preferences as ranked options we have studied a new connective that allows to represent alternative, ranked options for problem solutions in the heads of rules: $A \times B$ intuitively means: if possible A, but if A is not possible, then at least B. The semantics of logic programs with ordered disjunction is based on a preference relation on answer sets [9]. We show that this can be implemented using answer set solvers for normal programs. The implementation is based on a generator which produces candidate answer sets and a tester which checks whether a given candidate is maximally preferred and produces a better candidate if it is not. The complexity of reasoning tasks based on the new connective has also been studied [9].

Testing the Equivalence of Logic Programs
Tomi Janhunen and Emilia Oikarinen

In the answer set programming (ASP) paradigm, a programmer solves a problem at hand by constructing a logic program whose answer sets correspond to the solutions of the problem. However, it is typical that a particular problem can be programmed in many different ways and the programmer ends up with a series of alternative formulations when minimizing the amount of memory reserved by the program, and/or the running time elapsed on a particular ASP implementation. Consequently, the programmer is confronted by another problem: the subsequent logic program formulations ought to be equivalent. In this research, we have developed methodology for testing the equivalence of logic programs [16]. The idea is to translate any two programs of interest into a single logic program whose answer sets (if such exist) yield counter-examples to the equivalence of the two. We have implemented a translator `lpeq` [60] that enables the equivalence testing of logic programs within the `Smodels` system [3]. Our experiments suggest that our method is competitive compared to explicit cross-checking of answer sets.

Product configuration
Ilkka Niemelä

Together with the product data management group at Helsinki University of Technology (Timo Soininen, Juha Tiihonen, Reijo Sulonen) we have been developing general methodology for product configuration. It has turned out that the new types of rules supported by `Smodels` play an important role in representing configuration knowledge in a compact and maintainable form. Empirical testing of a configurator built on top of `Smodels` indicates that this is a promising approach to building in-

telligent automatic configurators [32].

Software configuration management
Tommi Syrjänen

Modern software products are large and complex and they may contain hundreds or thousands of interacting components. Also, software products are generally volatile in the sense that new versions of individual components are introduced regularly. The aim of software configuration management research is to find new methods for representing configuration knowledge and constructing valid configurations that satisfy user requirements. The current software configuration research in the laboratory concentrates on developing high-level rule-based methods for expressing configuration knowledge using the stable model semantics of normal logic programs as a formal framework.

Boolean circuit satisfiability checking
Tommi Junttila and Ilkka Niemelä

Propositional satisfiability (SAT) checking can be seen as a special case of stable model computation for logic program type rules. As this case appears frequently in applications, special purpose methods for it have been developed using ideas from the implementation techniques for stable model computation developed in the project. Most state of the art SAT checkers require that the input must be transformed into conjunctive normal form (CNF) and the algorithms are based on working with CNF formulae. We decided to study an alternative approach where Boolean circuits are used as the input format for the SAT checker. Boolean circuits provide a natural and compact way of encoding problems allowing structure sharing. A tableau algorithm for solving satisfiability problems has been devised. It works directly on Boolean circuits without any CNF transformation. A C++ implementation of the algorithm, the `BCSat` system, has been developed and applied, e.g., to bounded model checking.

We have published a translator `bc2cnf` [61] that converts Boolean circuits to CNF formulae in the DIMACS format. It enables one to describe problems with Boolean circuits and then to use state-of-the-art SAT solvers to solve the problem. The system has also been applied especially to bounded model checking problems [17, 39].

Bounded model checking
Keijo Heljanko, Toni Jussila, and Ilkka Niemelä

Bounded model checking has been recently introduced as a memory efficient way of locating errors in reactive systems. We have continued to work on bounded model checking using both the `BCSat` and the `Smodels` system developed in the laboratory as the underlying NP-solvers.

The work with `BCSat` has concentrated on efficiently using the parallelism present in the model to speed up model checking. We have devel-

oped an efficient encoding for 1-safe Petri Nets. The work on the SPINB language [39, 17] has been continued by considering compact ways of encoding models from a more abstract domain, labeled transition systems (LTS). The idea is to try to process the model as far as possible in a single step by exploiting both the local structure of a single LTS and the parallelism of the synchronization product, while still maintaining a linear (in the size of the bound) size of the resulting circuit. It is expected that the challenges and trade-offs met with LTSs can be utilized in the analysis of SPINB.

The work based on Smodels has resulted in an improved LTL model checking translation for 1-safe Petri Nets implemented in a tool called boundsmodels. The use of logic programs with the stable model semantics leads to a compact (linear size) encoding of bounded LTL model checking.

Modal mu-calculus model checking
Misa Keinänen and Ilkka Niemelä

Modal mu-calculus is an expressive logic for system verification. Variety of model checking logics can be encoded in mu-calculus, and many important features of system models can be expressed with the logic. For these reasons, mu-calculus is a logic widely studied in the recent systems verification literature. Various effective model checking techniques have been developed for the mu-calculus. Yet, an important open question about the logic is the complexity of the model checking problem. We have continued this line of research with the aim of taking a stand on the issue. In brief, the model checking problem for the modal mu-calculus can be formulated by means of solving so-called Boolean equation systems (BESs). We have analyzed the complexity of BES resolution and studied techniques to build a mu-calculus model checker based on the resolution of BESs. The developed methods will be applied to implement a tool to verify mu-calculus specifications.

Conformance testing
Keijo Heljanko and Tuomo Pyhälä

In formal conformance testing, a black-box implementation is tested against a specification. The main focus of our research has been on on-the-fly conformance testing algorithms where an implementation is tested against a specification by doing test generation from the specification during test execution. The main new feature of the project is to employ specification coverage information to guide test selection, and to come up with efficient on-the-fly algorithms for specification coverage based test selection.

3.1.1 Formal methods in distributed systems

Prefix-based model checking
Keijo Heljanko

The research is focused on using symbolic methods to alleviate the state explosion problem in model checking. The main approach used is a method called *complete finite prefixes* originally devised by McMillan. The approach is summarized and compared to other model checking approaches in [44]. We have also worked on efficient implementation methods for prefix generation. The main result is the parallelization of a prefix generation procedure [15].

Testing implementations of algorithms for translating linear time temporal logic formulae into Büchi automata
Keijo Heljanko and Heikki Tauriainen

Automata-theoretic model checking tools for linear time temporal logic (LTL) use algorithms that translate LTL properties into Büchi automata. These algorithms have to be implemented very carefully to ensure the correctness of model checking results in practice. In this research we have devised methods for detecting errors in LTL-to-Büchi translation algorithm implementations by (i) checking for known relationships between a pair of automata obtained from two complementary LTL formulae and (ii) comparing the model checking results obtained using independent LTL-to-Büchi translation algorithm implementations. Incorrect implementations are identified with a restricted LTL model checking algorithm for single computation paths. The results of this research were published in [4]. A software package called `lbtt` integrating most of the test methods is also available.

Symmetries in verification
Tommi Junttila

The symmetry reduction method is a way to alleviate the combinatorial explosion problem occurring in the state space analysis of concurrent systems. It exploits the symmetries (i.e., automorphisms) of the state space by considering only one representative state from each orbit of states induced by the symmetries. Thus a potentially much smaller set of states has to be considered during the state space analysis. The work is concentrated on the application of the symmetry reduction method to Petri nets and related formalisms. During the year 2002, new results were published concerning the core algorithms needed in the symmetry reduction method, namely the algorithms for the *orbit problem* either comparing whether two states are equivalent under the symmetries or producing a canonical representative for a state. In [38], new algorithms are presented for data symmetries, i.e., symmetries that are produced by the symmetric use of data values. New algorithms for the orbit problem under the structural symmetries of Place/Transition nets are presented in [37]. The proposed algorithms use and combine techniques from computational group theory and from the algorithms for the graph isomorphism problem. The experimental results show that the new algorithms are competitive against the ones proposed in the literature.

A framework for agent-based computing

Tomi Janhunen and Rauni Pääkkönen

The aim of this research is to create a framework for agent-based computing where agents have communication and coordination capabilities, and perform non-trivial reasoning tasks. We have previously brought forth *agent programs* as declarative specifications of multi-agents systems. Such programs were obtained by synthesizing two existing formalisms: (i) Petri nets which have been introduced as models of parallel and distributed systems and (ii) logic programs that capture rule-based knowledge representation and reasoning. This year we made some extensions to our prototypical implementation under the Linux operating system. The implementation consists of an interpreter which operates according to the agent description that it receives as its input, and which enables distributed coordination of Linux processes.

3.2 Computational complexity and combinatorics

Work in the area of computational complexity and combinatorics at the laboratory is structured in three research groups, *Computational Models and Mechanics*, *Coding Theory and Optimisation*, and *Distributed Algorithmics*.

Computational models and mechanics

Pekka Orponen, Sakari Seitz, and Satu Virtanen

The group studies methods for the solution of computational problems in structurally complex state spaces, focusing on techniques that are algorithmically relatively simple, but which adapt effectively to the characteristics of the problem instance at hand. In 2002, S.S. investigated the applicability of stochastic search methods, especially the so called *Record-to-Record Travel (RRT)* algorithm to finding solutions for random instances of the Satisfiability problem close to its phase transition threshold. The results were extremely encouraging, and will be reported in the literature in 2003. S.V., on her part, completed the extensive survey she had prepared as part of her Lic.Sc. (Tech.) thesis on the characteristics of several nonuniform graph models proposed in the literature, and continued to work with P.O. on finding efficient algorithms for various combinatorial and statistical problems that arise in such graphs. Her Lic.Sc. (Tech.) thesis will be reviewed in early 2003.

The group is the coordinating partner in the multidisciplinary consortium *Stochastic Adaptive Dynamics of Complex Systems (STADYCS)* (http://www.math.utu.fi/MaDaMe/projects/orponen.html), funded by the Academy of Finland as part of its *Mathematical Methods and Modelling in the Sciences (MaDaMe)* research programme. The other partners in this consortium are the Laboratories of Physics, Mathematics, and Computational Engineering at HUT, the Departments of Mathematics, Economics, and Ecology and Systematics at the University of Helsinki, and the Department of Mathematics at the University of Turku.

Coding theory and optimisation

Harri Haanpää and Petteri Kaski

The area of research of this group is the study of existence and enumeration problems in coding theory and discrete mathematics using computational methods, and enhancing these by algebraic and combinatorial results. The methods are developed in a general framework, and have been applied to numerous discrete structures such as codes, designs and graphs. The group works in close collaboration with Prof. Patric Östergård and his group at the Electrical Engineering Department.

Although both exhaustive and stochastic search methods are applicable to existence problems, in 2002 the emphasis was on exhaustive search methods. The main focus has been on orderly generation of discrete structures — backtracking search with isomorph pruning. With algorithms of this type, classification results have been obtained for various structures, including balanced incomplete block designs (BIBDs), resolvable and almost resolvable BIBDs, whist tournaments, sum and difference packings and coverings of Abelian groups, etc. Structures for which other (algebraic, combinatorial, and computational) methods have been applied include point codes and weak 3-colorings of Steiner triple systems of order 19, among others.

Many of the computational results have been obtained with very CPU-intensive computations, some of which have been distributed using the distributed batch system `autoson` over the computer network of the laboratory. During the year 2002, this research contributed to the journal paper [6] and to P.K.'s Lic.Sc. (Tech.) thesis [46].

Distributed algorithmics

Antti Autere, Petteri Kaski, and Pekka Orponen

The group applies combinatorial and complexity-theoretic methods to the solution of algorithmic problems in distributed systems. The group commenced operation in 2002, and the first year's research was focused on energy management issues in ad hoc communication networks. A.A. and P.O. studied the design and analysis of novel energy-efficient routing algorithms on 2-D grids, and P.K. and P.O. investigated, in collaboration with colleagues from the University of Helsinki, the lifetime maximisation problem in sensor networks with adjustable transmission power levels. Two manuscripts describing this work are presently under review.

In 2002 the work of the group was funded by the HeCSE graduate school and the HUT Department of Computer Science, but from the beginning of 2003 the group joins the consortium *Networking and Architecture for Proactive Systems (NAPS)* (http://www.cs.helsinki.fi/u/floreen/naps.html), funded by the Academy of Finland as part of its *Proactive Computing (PROACT)* research programme. The other partners in this consortium are the Networking Laboratory at HUT and the Department of Computer Science of the University of Helsinki.

3.3 Mobility management

Work in the area of mobility management at the laboratory is structured in two research groups, 007 and Brocom. The 007 research group developed security solutions for military ad hoc networks, whereas the Brocom group focused on multicast caching and on the efficient use of the air interface in wireless networks.

3.3.1 The 007 research project

Catharina Candolin, Maarit Hietalahti, Hannu H. Kari, and Mikko Särelä

An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to establish and maintain network connectivity [2, 49]. The network nodes are typically able to enter and leave the network on frequent basis, and to move both within the ad hoc network or from one ad hoc network to another. To support such frequent mobility, most of the ad hoc network nodes are typically wireless. However, a network node is able to support several networking technologies simultaneously, including both wired and wireless technologies.

The military environment is especially difficult for ad hoc networking. Most of the security requirements are the same as in conventional networks, but the same assumptions no longer hold. For example, ad hoc networks lack most of the centralized entities that may be found in conventional systems, there are not necessarily any well-defined network boundaries, the wireless network medium is extremely vulnerable to attacks, and trust management is more difficult as nodes may become compromised.

The 007 research project developed a security architecture for military ad hoc networks [8, 11, 26], focusing especially on dynamic group key agreement, mobility management [7, 12, 35], *incomplete trust* management, and QoS [10].

3.3.2 The Mobility/Multicast subproject of Brocom

Wassim Haddad, Hannu H. Kari, Janne Lundberg, Oleg Mürk, and Kimmo Mustonen

Multicast enables sending data efficiently from one or more senders to a group of receivers. The size of the group of receivers has virtually no upper limit, and in the Internet, it can potentially be as large as millions.

The Mobility/Multicast subproject of the Brocom (Broadcast communication, http://www.hut.fi/Units/IDC/projects/brocom/) project administered by IDC (Institute of Digital Communications in Helsinki University of Technology) develops new ways of distributing data to mobile clients using multicast delivery. The clients can be connected to the Internet through some wireless or wireline technology.

The subproject is designing and implementing a prototype of a multicast system that can utilize any current or future wireless technology that can transmit IP-packets. The focus of the subproject is on developing multicast caching and on the efficient use of the air interface. The subproject is building the necessary multicast and mobility related software that will allow other Brocom subprojects to build applications that support multicast as well as to test new radio access technologies. A description of our architecture was presented in [23].

3.4 Verification

Software verification
Jukka Järvenpää and Marko Mäkelä

The group applies state space exploration methods to the verification of safety properties in distributed software systems. During the year 2002, this research contributed to the conference paper [25] and two workshop papers [24] and [18].

Automatic formal model generation and analysis of SDL
Thomas Gangl, Nisse Husberg, Marko Mäkelä, and Kimmo Varpaaniemi

`SDL2PN`, a prototype of an SDL Z.100 front-end to the `MARIA` tool [25], was demonstrated in the final meeting of the `ANNA-MARIA` project in January. During the year, the tool was exhaustively tested w.r.t. correctness of translation. Translation of analysis results back to the SDL level in the form of message sequence charts was designed.

Analysis of the RLC protocol
Teemu Tynjälä

The analysis of the RLC (Radio Link Control) protocol (a UMTS radio network layer protocol and an OSI data link layer protocol) had started in the `ANNA-MARIA` project and was continued. Several `MARIA` models of the SDL specification of the protocol were manually constructed. Due to carefully selected abstractions, certain fundamental positive analysis results were eventually obtained [33].

Model Checking Safety Properties
Keijo Heljanko, Jukka Honkola, and Timo Latvala

We studied different techniques for efficient model checking of safety properties. The research focused on three directions: efficient translation of LTL safety properties to finite state automata [62], theory of abstraction for Coloured Petri Nets, and efficient implementation of the hash compaction technique for the Maria analyser. Results have been documented in the Licentiate's Thesis of Latvala [47].

Computational complexity in stubborn set optimization
Kimmo Varpaaniemi

The stubborn set method can be used e.g. for constructing an LTS (a labelled transition system) that is CFFD-equivalent to a parallel compo-

sition of a given collection of LTSs. The method tries to alleviate combinatorial explosion. Earlier results concerning stubborn set optimization were refined w.r.t. computational complexity [34]. New connections to extensions of the widely known propositional satisfiability problem (SAT) were found.

3.5 Modelling and simulating quantum computers using Petri nets

Leo Ojala, Elina Parviainen, and Teemu Tynjälä

The aim of our study has been to model and simulate Margolus quantum cellular automaton [54] and Feynman's serial quantum computer [28] using Petri nets. The first step in both cases has been to find out the free quantum evolution of the computer in the form of a recurrence formula derived from Schrödinger differential equation. High-level Petri nets are then proper to implement the generation of time evolution. However, to model the necessary measurements of quantum states stochastic Petri net formalism is also needed. The challenge for further studies is to find out a direct net-theoretical method to generate the free quantum evolution from Schrödinger differential equation without any mathematical preprocessing.

3.6 Generative string rewriting

Eero Lassila

The aim of this research is to enable the parallelization of context-sensitive rewriting operations without disrupting the semantics of the string under rewriting. Specifically, it should be possible to freely adjust the degree of parallelism in the rewriting process without any need to modify the rewriting rules. Such an adjustment is allowed to change the structure but not the semantics of the output. Even if the introduction of parallelism in one hand dampens optimization, it on the other hand enhances maintainability of the rewriting rules.

The concrete short-term goal of this research is to devise a general formal model, and the long-term one is to apply the model to practical tasks like optimizing code generation.

3.7 Cryptology

Helger Lipmaa, Markku-Juhani O. Saarinen, and Johan Wallén

This group studies the security of different cryptographic primitives and protocols, their efficiency but also applications of cryptology in the real life. H.L. created this relatively new group in 2001, and it was joined by M-J.S. and J.W. in the beginning of 2002. During 2002, our group produced one journal publication [1], three conference papers [19, 21, 20], one workshop paper [31] and two publicly available software libraries [63, 64]. One MSc thesis [58] was defended under H.L.'s supervision.

In particular, we studied the security of symmetric primitives. We solved a long-standing open problem by showing how to efficiently analyze the strength of modular addition w.r.t. differential cryptanalysis [22, 20]. We also proposed an efficient algorithm to break the stream cipher LILI-128 [30].

Our work on the computational number theory and on the security of the public-key cryptosystems resulted in two software packages, [63, 64] that implement the MPQS (multiple-polynomial quadratic sieve) and ECM (elliptic curve method) factorization algorithms. Together these algorithms provide the best known method for factoring integers of 140 digits or less.

We looked also at the efficiency of different cryptosystems. This resulted in publications [19, 31] where we more concretely came up with the world fastest implementations of the block cipher SC2000.

From the applications side, we studied the possibility of replacing certificate revocation lists by more efficient but as secure primitives called attesters. This work resulted in an invited publication [1]. We also proposed an efficient algorithm for interval time-stamping [21] (preprint published as [41]), and showed how to analyze its average-case communication and storage complexity.

4 CONFERENCES, VISITS AND GUESTS

4.1 Conferences

January

HeCSE (Helsinki Graduate School in Computer Science and Engineering) Winter School, Vyborg, Russia, January 7–8. Invited talks given by Ilkka Niemelä (*Formal Methods in Basic Research*) and Pekka Orponen (*Basic Research in Computer Science: What could it be?*). An ordinary talk given by Heikki Tauriainen (*The Automatic Testing of Compilers Transforming Linear Temporal Logic Formulas to Büchi automata*). Other participants: Harri Haanpää, Petteri Kaski, Janne Lundberg, and Satu Virtanen.

QIP (The 5$^{\text{th}}$ Workshop on Quantum Information Processing), Yorktown Heigts, New York State, USA, January 14–17. Participant: Leo Ojala.
http://www.research.ibm.com/quantuminfo/qip2002/home.html

POPL (The 29$^{\text{th}}$ Annual ACM SIGPLAN – SIGACT Symposium on Principles of Programming Languages), Portland, Oregon, USA, January 16–18. Participant: Toni Jussila. http://www.cse.ogi.edu/PacSoft/conf/popl/

Inauguration Celebration of the International Quality Network on Rational Mobile Agents, Dresden, Germany, January 29. An invited talk given by Ilkka Niemelä (*Logic Programs with Weight Constraints*).
http://www.ki.inf.tu-dresden.de/Research/IQN/

February

FSE (The 9th International Workshop on Fast Software Encryption), Leuven, Belgium, February 4–6. A talk given by Markku-Juhani O. Saarinen [30]. http://www.cryptomathic.com/fse2002/fseprogram.html

NordU (The 4th EurOpen/USENIX Conference), Scandic Marina Congress Center, Helsinki, Finland, February 18–22. A talk given by Catharina Candolin [35]. http://www.nordu.org/NordU2002/

March

EWSCS (The 7th Estonian Winter School in Computer Science), Palmse, Estonia, March 3–8. A talk given by Oleg Mürk (*Distributed Time-Stamping*). Other participants: Petteri Kaski, Helger Lipmaa, and Johan Wallén. Lipmaa is a member of the organising committee.
http://www.cs.ioc.ee/yik/schools/win2002/

AdHoc (The 2nd Swedish Workshop on Wireless Ad Hoc Networks), Stockholm (venue outside Stockholm: Johannesberg Estate, Gottröra), Sweden, March 5–6. Talks given by Catharina Candolin [10] and Hannu H. Kari [12]. Other participant: Maarit Hietalahti. http://wireless.kth.se/adhoc02/

FC (The 6th International Conference on Financial Cryptography), Southampton, Bermuda, March 11–14. A talk given by Helger Lipmaa (*Secure Vickrey Auctions without Threshold Trust*). http://ifca.ai/fc02/

TestCom (The IFIP 14th International Conference on Testing Communicating Systems), Berlin, Germany, March 19–22. Participant: Tuomo Pyhälä. http://www.fokus.gmd.de/events/testcom2002/

April

ETAPS (European Joint Conferences on Theory and Practice of Software), Grenoble, France, April 6–14. Participant: Keijo Heljanko.
http://www-etaps.imag.fr/

Workshop / Concentrated Course on Complexity and Probability, Chalmers University of Technology, Gothenburg, Sweden, April 15–19. Participants: Petteri Kaski, Timo Latvala, Satu Virtanen, and Johan Wallén. http://www.math.chalmers.se/%7efredrikl/events/RandomWorkshop/

Mobile Communications Conference and Expo, Helsinki Fair Centre, Helsinki, Finland, April 16–17. A talk given by Hannu H. Kari (*Security in IP-Based Mobile Services*). http://www.mobile.commerce.net/mobile2002/speakers.html

NMR (The 9th International Workshop on Non-Monotonic Reasoning), Toulouse, France, April 19–21. A session chaired by Ilkka Niemelä. Niemelä is a co-chair of the programme committee of the Special Session on Answer Set Programming and Abductive Reasoning.
http://www.irit.fr/NMR2002/NMR2002.html

KR (The 8th International Conference on Principles of Knowledge Representation and Reasoning), Toulouse, France, April 22–25. A session chaired by Ilkka Niemelä. Niemelä is a member of the programme committee. http://www.kr.org/kr/kr02/

Eurocrypt (The 21st Annual International Conference on the Theory and Applications of Cryptographic Techniques), Amsterdam, The Netherlands, April 28 – May 2. Participants: Helger Lipmaa and Markku-Juhani O. Saarinen. http://www.ec2002.tue.nl/

May

IJCNN (IEEE / INNS International Joint Conference on Neural Networks), Honolulu, Hawaii, USA, May 12–17. Pekka Orponen is a member of the programme committee. http://www.wcci2002.org/program/wcciprogram.pdf

Seminar on Evolution, Computation and Landscapes Turku, Finland, May 30. Participants: Tomi Janhunen, Petteri Kaski, Pekka Orponen, and Satu Virtanen. http://users.utu.fi/evakis/evocomp.htm

June

The 2nd HIIT (Helsinki Institute for Information Technology) – UCB (University of California at Berkeley) Summer School, Berkeley, California, USA, June 4–7. Talks given by Catharina Candolin (*Security in Military Ad Hoc Networks*) and Toni Jussila (*Bounded Model Checking Verification Technique*). Other participant: Janne Lundberg.
http://www.cs.helsinki.fi/u/kraatika/Courses/berkeley02s.html

MOVEP (Summer School on Modelling and Verification of Parallel Processes), Nantes, France, June 17–21. Participant: Toni Jussila.
http://www.cs.bham.ac.uk/%7emdr/movep/

Workshop on Software Engineering and Formal Methods, Adelaide, Australia, June 24. A talk given by Marko Mäkelä [24].
http://www.unisa.edu.au/eie/csec/pn2002/SEFM.html

ICATPN (The 23rd International Conference on Application and Theory of Petri Nets), Adelaide, Australia, June 24–30. A talk given by Marko Mäkelä [25]. Other participant: Leo Ojala. Nisse Husberg is a member of the programme committee. http://www.unisa.edu.au/eie/csec/pn2002/

PDPTA (International Conference on Parallel and Distributed Processing Techniques and Applications), Las Vegas, Nevada, USA, June 24–27. A talk given by Teemu Tynjälä [28].
http://www.ashland.edu/%7eiajwa/conferences/2002/PDPTA/schedule.html

July

The 54th IETF (Internet Engineering Task Force) Meeting, Yokohama, Japan, July 14–19. Participants: Catharina Candolin and Janne Lundberg. http://www.ietf.org/proceedings/02jul/

ECAI (The 15th European Conference on Artificial Intelligence), Lyon, France, July 21–26. Participant: Toni Jussila. http://ecai2002.univ-lyon1.fr/show_en.pl

MoChArt (ECAI Workshop on Model Checking and Artificial Intelligence), Lyon, France, July 22–23. A talk given by Toni Jussila [17]. Ilkka Niemelä is a member of the programme committee.
http://www.csc.liv.ac.uk/%7emjw/mochart/

CADE (The 18th Conference on Automated Deduction), Copenhagen, Denmark, July 27–30. Ilkka Niemelä is a member of the programme committee. http://www.uni-koblenz.de/%7ecade-18/

CAV (The 14th International Conference on Computer-Aided Verification), Copenhagen, Denmark, July 27–31. Participant: Heikki Tauriainen. http://floc02.diku.dk/CAV/

August

The 12th Jyväskylä Summer School, Jyväskylä, Finland, August 12–30. Participant: Satu Virtanen. http://www.jyu.fi/summerschool/JSS12report.pdf

SAC (The 9th Annual Workshop on Selected Areas in Cryptography), St. John's, Newfoundland, Canada, August 15–16. Helger Lipmaa is a member of the programme committee.
http://www.engr.mun.ca/%7esac2002/sac_web_main.htm

CRYPTO (The 22nd Annual International Cryptology Conference), Santa Barbara, California, USA, August 18–22. Participants: Maarit Hietalahti, Helger Lipmaa, and Johan Wallén. http://www.iacr.org/conferences/crypto2002/

CONCUR (The 13th International Conference on Concurrency Theory) and affiliated workshops, Brno, Czech Republic, August 19–24. Participant: Kimmo Varpaaniemi. http://www.fi.muni.cz/concur2002/

MOCA (The 2nd Workshop on Modelling of Objects, Components and Agents), Aarhus, Denmark, August 26–27. A talk given by Jukka Järvenpää [18]. Other participant: Marko Mäkelä. Nisse Husberg is a member of the programme committee.
http://www.informatik.uni-hamburg.de/TGI/events/moca02/MOCA02-programme.html

CPN (The 4th Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools), Aarhus, Denmark, August 28–30. Nisse Husberg is a member of the programme committee.
http://www.daimi.au.dk/CPnets/workshop02/cpn/programme.html

September

HeCSE (Helsinki Graduate School in Computer Science and Engineering) Summer School, Nokia, Finland, September 2–3. A talk given by Toni Jussila (*Parallel Program Verification Using Bounded Model Checking*). Other participants: Harri Haanpää, Petteri Kaski, Timo Latvala, and Satu Virtanen.

Workshop on Nonmonotonic Reasoning, Answer Set Programming and Constraints, Schloss Dagstuhl, Wadern, Germany, September 15–20. Talks given by Tomi Janhunen (*An Approach to Capture Stable Models with Classical Ones*) and Ilkka Niemelä (*Logic Programs with Weight Constraints*). Sessions chaired by Janhunen and Niemelä. Niemelä is one of the co-chairs of the workshop. http://www.dagstuhl.de/02381/Report/

SECI (Workshop on Security of Communication on the Internet), Tunis, Tunisia, September 19–21. A talk given by Catharina Candolin [14]. Other participant: Janne Lundberg. http://lwn.net/2002/0425/a/seci.php3

JELIA (The 8th European Conference on Logics in Artificial Intelligence), Cosenza, Italy, September 23–26. Talks given by Tomi Janhunen [16] and Tommi Syrjänen [9]. Other participant: Emilia Oikarinen. Ilkka Niemelä is a member of the programme committee. http://si.deis.unical.it/jelia/hr/indexNS_bg.htm

Fall School on Algorithms for Hard Problems, Schwarzenberg, Switzerland, September 23–27. Participant: Satu Virtanen.
http://www.tik.ee.ethz.ch/%7ethe/school/

ISC (The 5th International Conference on Information Security), São Paulo, Brazil, September 30 – October 2. Two talks given by Helger Lipmaa [19, 21]. A session chaired by Lipmaa. http://www.ime.usp.br/%7eisc2002/

October

CS&P (Workshop on Concurrency, Specification and Programming), Berlin, Germany, October 7–9. A talk given by Kimmo Varpaaniemi [34].

MILCOM (IEEE Military Communications Conference), Anaheim, California, USA, October 7–10. A talk given by Catharina Candolin [11].
http://www.comsoc.org/confs/milcom/new/2002/

ICCON (WSEAS International Conference on Computer Networks), Rio de Janeiro, Brazil, October 14–17. A talk given by Janne Lundberg [23]. Other participant: Catharina Candolin.

Estonian Theory Day, Roosta, Estonia, October 16–17. A talk given by Helger Lipmaa (*Turvalised Vickrey oksjonid ilma läveusalduseta (Secure Vickrey Auctions without Threshold Trust)*). Lipmaa is a member of the organising committee. http://www.cs.ioc.ee/%7etarmo/tday-roosta/

November

Microsoft Research Seminar Series: Security Workshop, Cambridge, UK, November 4–6. Participant: Catharina Candolin.
http://research.microsoft.com/collaboration/university/europe/events/Workshop/sec2002/default.asp

The 3rd NESSIE (New European Schemes for Signature, Integrity, and Encryption) Workshop, Munich, Germany, November 6–7. Participant: Markku-Juhani O. Saarinen. http://www.di.ens.fr/%7ewwwgrecc/NESSIE3/

NordSec (The 7th Nordic Workshop on Secure IT Systems), Karlstad, Sweden, November 7–8. Participants: Catharina Candolin, Maarit Hietalahti, and Mikko Särelä. Helger Lipmaa is a member of the steering committee. http://www.cs.kau.se/nordsec2002/

FORTE (The 22nd IFIP WG 6.1 International Conference on Formal Techniques for Networked and Distributed Systems), Houston, Texas, USA, November 11–14. A talk given bu Teemu Tynjälä [33].
http://www.cs.rice.edu/FORTE02/

KOLKOM (Kolloquium über Kombinatorik, The 22nd Annual Colloquium on Combinatorics), Magdeburg, Germany, November 15–16. A talk given by Harri Haanpää (*The near resolvable 2-(13,4,3) designs and 13-player whist tournaments*).
http://www.informatik.uni-trier.de/GI/FG-014/Announce/2002/Combinatorics.CP.html

InfoWarCon (The 3rd Australian Information Warfare and Security Conference), Perth, Australia, November 28–29. A talk given by Catharina Candolin [13]. http://www.mindsystems.com.au/autt.nsf/pages/conf_aiwsc02/

December

INDOCRYPT (The 3rd International Conference on Cryptology in India), Hyderabad, India, December 16–18. A talk given by Helger Lipmaa [20].
http://www.idrbt.ac.in/acin/indo/index.html

A Newton Institute Workshop on Topics in Computer Communication and Networks, Cambridge, UK, December 16–20. Participants: Pekka Orponen and Satu Virtanen. http://www.newton.cam.ac.uk/programs/CMP/cmpw03.html

4.2 Visits

Acting as an official opponent of a doctoral dissertation

Hannu H. Kari was the official opponent in the public examination of Alberto Escudero-Pascual's doctoral dissertation (*Privacy in the Next Generation Internet: Data Protection in the Context of the European Union Policy*) in Royal Institure of Technology, Kista, Stockholm, Sweden, on December 4. http://www.it.kth.se/visa.html?artikelid=373

Helger Lipmaa and Pekka Orponen were the official opponents in the public examination of Jan Villemson's doctoral dissertation (*Size-Efficient Interval Time Stamps*) in University of Tartu, Estonia, on June 17. http://www.cyber.ee/uudised/20020625.html

Other visits

Petr Ladislav Kodym worked as a Research Associate in Edinburgh Parallel Computing Centre in School of Informatics at University of Edinburgh, UK, from October 1 on. http://www.informatics.ed.ac.uk/people/Visiting.html

Marko Mäkelä visited University of Adelaide, Australia, on June 14 – July 7.

Ilkka Niemelä visited three universities in Germany in the end of January: University of Dresden on January 29 (cf. 4.1), University of Leipzig on January 30, and University of Potsdam on January 31.
http://www.cs.uni-potsdam.de/wv/gaeste/

Niemelä visited University of Kentucky, Lexington, KY, USA, On December 9–15 (guest lecture: *Bounded Model Checking with Stable Models*).

Pekka Orponen gave a guest lecture at University of Turku, Finland, on May 23.

Tommi Syrjänen visited University of Kentucky, Lexington, KY, USA, on May 17–26.

Satu Virtanen visited Chalmers University of Technology, Gothenburg, Sweden, on November 18–19.

4.3 Guests

Official opponents of doctoral dissertations

Professor Eike Best from University of Oldenburg, Germany, was the official opponent in the public examination of Keijo Heljanko's doctoral dissertation [44] on March 22.

Professor Kaisa Sere from Åbo Akademi University, Turku, Finland, and D.Sc. (Tech.) Timo Honkela from Gurusoft Oy, Helsinki, Finland, were the official opponents in the public examination of Sam Sandqvist's doctoral dissertation [45] on November 1.

Other guests

The abstracts of the talks mentioned below (except those of the short courses) can be found from http://www.tcs.hut.fi/Current/FMF/. (URL addresses for the short courses are mentioned separately.)

Dr. Andris Ambainis from University of Latvia, Riga, Latvia, stayed for five days, lectured a minicourse (*Short Course on Quantum Computing*, http://www.tcs.hut.fi/Research/Crypto/minicourses/) on November 20–22, and was hosted by Helger Lipmaa.

Dr. Dirk Arnold from University of Dortmund, Germany, stayed for one day, gave a talk (*Theoretical Aspects of Evolutionary Optimization in Continuous Search Spaces*) on May 31, and was hosted by Pekka Orponen.

Professor Gerhard Brewka from University of Leipzig, Germany, stayed for six days, gave a talk (*Logic Programs with Ordered Disjunction*) on March 13, and was hosted by Ilkka Niemelä.

M.Sc. Edith Elkind from University of Princeton, NJ, USA, stayed for one day, gave a talk (*Advanced Notions of Security for Encryption*) on September 6, and was hosted by Helger Lipmaa.

Professor Javier Esparza from University of Edinburgh, UK, stayed for four days, gave a talk (*Model Checking Pushdown Processes*) on April 19, and was hosted by Ilkka Niemelä.

B.Sc. Alan Franzi from University of Milan, Italy, stayed for six months, writing his Master's thesis for University of Milan under the instruction of Ilkka Niemelä. Franzi gave a talk (*An Efficient Way to Calculate Stable Models for Kernel Programs*) on April 12. (The talk was a joint talk with Fabrizio Magni, another student from University of Milan temporarily studying at Helsinki University of Technology.)

Student Thomas Gangl from University of Salzburg, Austria, stayed for two months, developing software for laying out message sequence charts. Gangl worked under the instruction of Marko Mäkelä, in the research group led by Nisse Husberg.

M.Sc. Wassim Haddad from Hewlett-Packard Research Laboratories, Bristol, UK, stayed for four months and was hosted by Hannu H. Kari.

Dr. Manfred Jaeger from Max-Planck-Institut für Informatik, Saarbrücken, Germany, stayed for one day, gave a talk (*Probabilistic Relational Models: Meaning, Reperesentation & Inference*) on May 17, and was hosted by Ilkka Niemelä.

Dr. Leila Kallel from École Polytechnique Université Paris Dauphine, Paris, France, stayed for one day, gave a talk (*Genetic Algorithms: Convergence Bounds from Simple Functions to Long Paths*) on May 31, and was hosted by Pekka Orponen.

Senior Lecturer, Dr. Charles Lakos from University of Adelaide, Australia, stayed for one month, gave a talk (*Towards the Analysis of Object-Oriented Petri Nets*) on April 14, and was hosted by Nisse Husberg.

Professor Victor W. Marek from University of Kentucky, Lexington, KY, USA, stayed for eleven days, gave a talk (*On Logic Programs with Cardinality Constraints and Some Generalization*) on October 1, and was hosted by Ilkka Niemelä.

Professor Valery Alexandrovitch Nepomniaschy from A.P. Ershov Institute of Informatics Systems at the Siberian Division of the Russian Academy of Sciences, Novosibirsk, Russia, stayed for four days, gave a talk (*Basic-REAL: Integrated Approach for Design, Specification and Verification of Distributed Systems*) on May 21, and was hosted by Nisse Husberg.

Professor Alessandro Provetti from University of Messina, Italy, stayed for six days, gave a talk (*Consistency Monitors in Condition-Event-Action Systems: Preliminary Thoughts*) on May 15, and was hosted by Ilkka Niemelä.

Professor Phillip Rogaway from University of California at Davis, CA, USA, and from Chiang Mai University, Chiang Mai, Thailand, lectured a minicourse (*Provable Security as a Tool for Practical Protocol Design: The Case of Authenticated Encryption*, http://www.tcs.hut.fi/Research/Crypto/guests.shtml) on April 22–24, gave a talk (*A Block-Cipher Mode on Operation for Parallelizable Message Authentication*) on April 23, and was hosted by Helger Lipmaa.

Professor Paul M.B. Vitányi from CWI (Centrum voor Wiskunde en Informatica) and from University of Amsterdam, The Netherlands, stayed for twelve days, lectured an intensive course (*An Introduction to Kolmogorov Complexity and Its Applications*, http://www.tcs.hut.fi/%7epkaski/kca/) on April 8–12, gave a talk (*Time and Space Bounds on Reversible Computing*) on April 9, and was hosted by Pekka Orponen.

5 PUBLICATIONS

5.1 Journal articles

[1] Ahto Buldas, Peeter Laud, and Helger Lipmaa. Eliminating Counterevidence with Applications to Accountable Certificate Management. *Journal of Computer Security*, 10(3):273–296. IOS Press, Amsterdam, The Netherlands. http://search.epnet.com/direct.asp?an=6969839&db=afh

[2] Catharina Candolin. Ad hoc -johtamisverkot. *Suomen Sotilas — Maanpuolustuksen aikakauslehti*, 1:14–15. In Finnish. Kustannus Oy Suomen Mies, Helsinki, Finland. http://www.suomensotilas.fi/edelliset/102.pdf

[3] Patrik Simons, Ilkka Niemelä, and Timo Soininen. Extending and Implementing the Stable Model Semantics. *Artificial Intelligence*, 138(1–2):181–234. Elsevier Science, Amsterdam, The Netherlands. http://www.compsciweb.com/compsciweb/show/Index.htt?Issn=00043702

[4] Heikki Tauriainen and Keijo Heljanko. Testing LTL Formula Translation into Büchi Automata. *International Journal on Software Tools for Technology Transfer (STTT)*, 4(1):57–70. Springer-Verlag, Berlin, Germany. http://link.springer.de/link/service/journals/10009/bibs/2004001/20040057.htm

[5] Kimmo Varpaaniemi. Minimizing the Number of Successor States in the Stubborn Set Method. *Fundamenta Informaticae (Annales Societatis Mathematicae Polonae, Series IV)*, 51(1–2):215–234. IOS Press, Amsterdam, The Netherlands. http://fi.mimuw.edu.pl/abs51.html

[6] Patric R.J. Östergård and Petteri Kaski. Enumeration of 2-(9,3,λ) Designs and Their Resolutions. *Designs, Codes and Cryptography*, 27(1–2):131–137. Kluwer Academic Publishers, Dordrecht, The Netherlands. http://www.kluweronline.com/issn/0925-1022/contents/

5.2 Articles in collections

[7] Pekka Nikander, Catharina Candolin, and Janne Lundberg. From Address Orientation to Host Orientation. Thomas Noel (Ed.), *Wireless Mobile Phone Access to the Internet*. Innovative Technology Series, Kogan Page / Hermès Penton, London, UK.
http://www.hermespenton.com/asp/bookdetails.asp?key=3667

5.3 Conference papers

[8] Tuomas Aura and Silja Mäki. Towards a Survivable Security Architecture for Ad Hoc Networks. Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe (Eds.), *Security Protocols, 9th International Workshop, Cambridge, UK, April 25–27, 2001, Revised Papers*, pp. 63–73. Lecture Notes in Computer Science, Volume 2467, Springer-Verlag, Berlin, Germany.
http://link.springer.de/link/service/series/0558/bibs/2467/24670063.htm

[9] Gerhard Brewka, Ilkka Niemelä, and Tommi Syrjänen. Implementing Ordered Disjunction Using Answer Set Solvers for Normal Programs. Sergio Flesca, Sergio Greco, Nicola Leone, and Giovambattista Ianni (Eds.), *Logics in Artificial Intelligence, 8th European Conference, JELIA 2002, Cosenza, Italy, September 23–26, 2002, Proceedings*, pp. 444–456. Lecture Notes in Artificial Intelligence, Volume 2424, Springer-Verlag, Berlin, Germany.
http://link.springer.de/link/service/series/0558/bibs/2424/24240444.htm

[10] Catharina Candolin, Maarit Hietalahti, and Hannu H. Kari. Providing Quality of Service in Wireless Ad Hoc Networks. *Proceedings of the 2nd Swedish Workshop on Wireless Ad Hoc Networks, Stockholm, Sweden, March 5–6, 2002*. http://wireless.kth.se/adhoc02/proceedings/proceedings.html

[11] Catharina Candolin and Hannu H. Kari. A Security Architecture for Wireless Ad Hoc Networks. *Proceedings of IEEE MILCOM 2002, Anaheim, California, USA, October 7–10, 2002, Volume 2*, pp. 1095–1100. IEEE (Institute of Electrical and Electronics Engineers, Inc.). http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=26490&page=4

[12] Catharina Candolin and Hannu H. Kari. Complexity of Route Optimization and Mobility Management. *Proceedings of the 2nd Swedish Workshop on Wireless Ad Hoc Networks, Stockholm, Sweden, March 5–6, 2002.* http://wireless.kth.se/adhoc02/proceedings/proceedings.html

[13] Catharina Candolin and Hannu H. Kari. Dynamic Management of Core Ad Hoc Networks. *Proceedings of InfoWarCon 2002, Perth, Australia, November 28–29, 2002.*

[14] Catharina Candolin, Janne Lundberg, and Pekka Nikander. Experimenting with Early Opportunistic Key Agreement. Jean Goubault-Larrecq (Ed.), *Actes du ler Workshop International sur la Sécurité des Communications sur Internet (Proceedings of the Workshop on Security of Communication on the Internet, SECI'02, Tunis, Tunisia, September 19–21, 2002)*, pp. 39–45. Collection Didactique, INRIA (Institut National de Recherche en Informatique et en Automatique), Rocquencourt, France.
http://www.lsv.ens-cachan.fr/%7egoubault/SECI-02/Final/actes-seci02/

[15] Keijo Heljanko, Victor Khomenko, and Maciej Koutny. Parallelisation of the Petri Net Unfolding Algorithm. Joost-Pieter Katoen and Perdita Stevens (Eds.), *Tools and Algorithms for the Construction and Analysis of Systems, 8th International Conference, TACAS 2002, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2002, Grenoble, France, April 8–12, 2002, Proceedings*, pp. 371–385. Lecture Notes in Computer Science, Volume 2280, Springer-Verlag, Berlin, Germany.
http://link.springer.de/link/service/series/0558/bibs/2280/22800371.htm

[16] Tomi Janhunen and Emilia Oikarinen. Testing the Equivalence of Logic Programs under Stable Model Semantics. Sergio Flesca, Sergio Greco, Nicola Leone, and Giovambattista Ianni (Eds.), *Logics in Artificial Intelligence, 8th European Conference, JELIA 2002, Cosenza, Italy, September 23–26, 2002, Proceedings*, pp. 493–504. Lecture Notes in Artificial Intelligence, Volume 2424, Springer-Verlag, Berlin, Germany. http://link.springer.de/link/service/series/0558/bibs/2424/24240493.htm

[17] Toni Jussila and Ilkka Niemelä. Parallel Program Verification Using BMC. *Proceedings of the ECAI 2002 Workshop on Model Checking and Artificial Intelligence, Lyon, France, July 22–23, 2002*, pp. 59–66. http://www.tcs.hut.fi/Publications/info/ini.JN2002:mochart.shtml

[18] Jukka Järvenpää and Marko Mäkelä. Towards Automated Checking of Component-Oriented Enterprise Applications. Daniel Moldt (Ed.), *Second Workshop on Modelling of Objects, Components and Agents, Aarhus, Denmark, August 26–27, 2002*, pp. 67–85. University of Aarhus, Department of Computer Science, Report DAIMI PB-561. http://www.daimi.au.dk/CPnets/workshop02/moca/papers/

[19] Helger Lipmaa. Fast Software Implementations of SC2000. Agnes Hui Chan and Virgil Gligor (Eds.), *Information Security, 5th International Conference, ISC 2002, São Paulo, Brazil, September 30 – October 2, 2002, Proceedings*, pp. 63–74. Lecture Notes in Computer Science, Volume 2433, Springer-Verlag, Berlin, Germany.
http://link.springer.de/link/service/series/0558/bibs/2433/24330063.htm

[20] Helger Lipmaa. On Differential Properties of Pseudo-Hadamard Transform and Related Mappings. Alfred Menezes and Palash Sarkar (Eds.), *Progress in Cryptology — INDOCRYPT 2002, Third International Conference on Cryptology in India, Hyderabad, India, December 16–18, 2002, Proceedings*, pp. 48–61. Lecture Notes in Computer Science, Volume 2551, Springer-Verlag, Berlin, Germany.
http://link.springer.de/link/service/series/0558/bibs/2551/25510048.htm

[21] Helger Lipmaa. On Optimal Hash Tree Traversal for Interval Time-Stamping. Agnes Hui Chan and Virgil Gligor (Eds.), *Information Security, 5th International Conference, ISC 2002, São Paulo, Brazil, September 30 – October 2, 2002, Proceedings*, pp. 357–371. Lecture Notes in Computer Science, Volume 2433, Springer-Verlag, Berlin, Germany. http://link.springer.de/link/service/series/0558/bibs/2433/24330357.htm

[22] Helger Lipmaa and Shiho Moriai. Efficient Algorithms for Computing Differential Properties of Addition. Mitsuru Matsui (Ed.), *Fast Software Encryption, 8th International Workshop, FSE 2001, Yokohama, Japan, April 2–4, 2001, Revised Papers*, pp. 336–350. Lecture Notes in Computer Science, Volume 2355, Springer-Verlag, Berlin, Germany. http://link.springer.de/link/service/series/0558/bibs/2355/23550336.htm

[23] Janne Lundberg and Catharina Candolin. Multicast Caching: Efficient Distribution of Encrypted Content to Mobile Clients. *Proceedings of WSEAS International Conference on Computer Networks (ICCON'02), Rio de Janeiro, Brazil, October 14–17, 2002.*

[24] Marko Mäkelä. Efficiently Verifying Safety Properties with Idle Office Computers. Charles Lakos, Robert Esser, Lars M. Kristensen, and Jonathan Billington (Eds.), *Formal Methods in Software Engineering and Defence Systems 2002, Proceedings of the Workshops on Software Engineering and Formal Methods and Formal Methods Applied to Defence Systems*, pp. 11–16. Conferences in Research and Practice in Information Technology, Volume 12, Australian Computer Society Inc., Sydney, Australia. http://CRPIT.com/Vol12.html

[25] Marko Mäkelä. Maria: Modular Reachability Analyser for Algebraic System Nets. Javier Esparza and Charles Lakos (Eds.), *Application and Theory of Petri Nets 2002, 23rd International Conference, ICATPN 2002, Adelaide, Australia, June 24–30, 2002, Proceedings*, pp. 434–444. Lecture Notes in Computer Science, Volume 2360, Springer-Verlag, Berlin, Germany.
http://link.springer.de/link/service/series/0558/bibs/2360/23600434.htm

[26] Silja Mäki. Towards a Survivable Security Architecture for Ad Hoc Networks (Transcript of Discussion). Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe (Eds.), *Security Protocols, 9th International Workshop, Cambridge, UK, April 25–27, 2001, Revised Papers*, pp. 74–79. Lecture Notes in Computer Science, Volume 2467, Springer-Verlag, Berlin, Germany.
http://link.springer.de/link/service/series/0558/bibs/2467/24670074.htm

[27] Leo Ojala, Elina Parviainen, Olli-Matti Penttinen, and Juha Reunanen, "Feynman's Quantum Computer Modeled Using Petri Nets: A Case Study," in Nagib C. Callaos, Tau Leng, and Belkis Sanchez (Eds.), *SCI2002 / ISAS2002 (The 6th World Multiconference on Systemics, Cybernetics and Informatics / The 8th International Conference on Information Systems, Analysis and Synthesis), Orlando, Florida, USA, July 14–18, 2002, Proceedings, Volume V (Computer Science I)*, IIIS (International Institute of Informatics and Systemics), Orlando, Florida, USA.

[28] Leo Ojala, Elina Parviainen, Olli-Matti Penttinen, Teemu Tynjälä, and Harriet Beaver. Modeling Feynman's Serial Quantum Computer Using Stochastic Petri Nets. Hamid R. Arabnia (Ed.), *Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, PDPTA'02, Las Vegas, Nevada, USA, June 24–27, 2002, Volume III*, pp. 1223–1229. CSREA (Computer Science, Research, Education, and Applications) Press, Athens, Georgia, USA.

[29] Elina Parviainen, "Reducing Size of Quantum Gate Matrices Using Pr/T-Nets," in *Proceedings of the 2002 IEEE International Conference on Systems, Man and Cybernetics, Hammamet, Tunisia, October 6–9, 2002, Volume 2*, pp. 634–639. IEEE (Institute of Electrical and Electronics Engineers, Inc.).
http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=26297&page=7

[30] Markku-Juhani O. Saarinen. A Time-Memory Tradeoff Attack Against LILI-128. Joan Daemen and Vincent Rijmen (Eds.), *Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4–6, 2002, Revised Papers*, pp. 231–236. Lecture Notes in Computer Science, Volume 2365, Springer-Verlag, Berlin, Germany. http://link.springer.de/link/service/series/0558/bibs/2365/23650231.htm

[31] Masahiko Takenaka, Helger Lipmaa, and Naoya Torii. The Implementation of the Block Cipher SC2000 (III). *Proceedings of ISEC 2002, Tohoku University, Sendai, Japan, July 18–19, 2002*. In Japanese. http://www.tcs.hut.fi/%7ehelger/papers/tlt02/

[32] Juha Tiihonen, Timo Soininen, Ilkka Niemelä, and Reijo Sulonen. Empirical Testing of A Weight Constraint Rule Based Configurator. Michel Aldanondo (Ed.), *ECAI 2002 Configuration Workshop, Lyon, France, July 22, 2002*, pp. 17–22.
http://www.enstimac.fr/recherche/gind/ecai-2002-config-ws/Config-Wrksh-ecai02.pdf

[33] Teemu Tynjälä, Sari Leppänen, and Vesa Luukkala. Verifying Reliable Data Transmission over UMTS Radio Interface with High Level Petri Nets. Doron A. Peled and Moshe Y. Vardi (Eds.), *Formal Techniques for Networked and Distributed Systems — FORTE 2002, 22nd IFIP WG 6.1 International Conference, Houston, Texas, USA, November 11–14, 2002, Proceedings*, pp. 178–193. Lecture Notes in Computer Science, Volume 2529, Springer-Verlag, Berlin, Germany.
http://link.springer.de/link/service/series/0558/bibs/2529/25290178.htm

[34] Kimmo Varpaaniemi. Towards Ambitious Approximation Algorithms in Stubborn Set Optimization. Hans-Dieter Burkhard, Ludwik Czaja, Gabriela Lindemann, Andrzej Skowron, and Peter H. Starke (Eds.), *Workshop: Concurrency, Specification and Programming, CS&P'2002, Berlin, October 7–9, Volume 2*, pp. 370–379. Humboldt University Berlin, Department of Computer Science, Technical Report 161, Berlin, Germany.
http://www.tcs.hut.fi/Publications/info/kva.Vrp02c.shtml

[35] Yuchen Zhou, Catharina Candolin, and Teemupekka Virtanen. Trust management in Mobile IPv6. *Proceedings of NordU2002, the 4th EurOpen/USENIX Conference, Helsinki, Finland, February 18–22, 2002*.

5.4 Reports (see also 5.5)

[36] Catharina Candolin and Hannu H. Kari. Context Aware Management Architecture. Internet Draft (Expired in December 2002), Internet Engineering Task Force.
http://www.ietf.cnri.reston.va.us/internet-drafts/draft-candolin-cam-00.txt

[37] Tommi Junttila. New Canonical Representative Marking Algorithms for Place/Transition-Nets. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Report HUT-TCS-A75, Espoo, Finland, 37 pp.
http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A75.shtml

[38] Tommi Junttila. Symmetry Reduction Algorithms for Data Symmetries. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Report HUT-TCS-A72, Espoo, Finland, 49 pp. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A72.shtml

[39] Toni Jussila. Bounded Model Checking for Verifying Concurrent Programs. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Report HUT-TCS-A73, Espoo, Finland, 55 pp. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A73.shtml

[40] Timo Latvala. On Model Checking Safety Properties. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Report HUT-TCS-A76, Espoo, Finland, 61 pp.
http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A76.shtml

[41] Helger Lipmaa. On Optimal Hash Tree Traversal for Interval Time-Stamping. Cryptology ePrint Archive Report 2002/124, International Association for Cryptologic Research, 15 pp.
http://eprint.iacr.org/2002/124/

[42] Janne Lundberg. Unidirectional Link Support for MLDv2. Internet Draft (Expired in December 2002), Internet Engineering Task Force.
http://www.ietf.cnri.reston.va.us/internet-drafts/draft-lundberg-umldv2-00.txt

[43] Kimmo Varpaaniemi (Ed.). Annual Report for the Year 2001. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, 29 pp.
http://www.tcs.hut.fi/Publications/kva/y01pdfm.pdf

5.5 Doctoral dissertations

[44] Keijo Heljanko. Combining Symbolic and Partial Order Methods for Model Checking 1-Safe Petri Nets. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Report HUT-TCS-A71, Espoo, Finland, 55+112 pp. Accepted by Department of Computer Science and Engineering on April 22. (The degree of D.Sc. (Tech.) was granted on the same day.) Supervised by Ilkka Niemelä. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A71.shtml

[45] Sam Sandqvist. Aspects of Modelling and Simulation of Genetic Algorithms: A Formal Approach. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Research Report HUT-TCS-A74, Espoo, Finland, 164 pp. Accepted by Department of Computer Science and Engineering on November 18. (The degree of D.Sc. (Tech.) was granted on November 27.) Supervised by Pekka Orponen. Instructed by Leo Ojala.
http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A74.shtml

5.6 Licentiate's theses

[46] Petteri Kaski. A Census of Steiner Triple Systems and Some Related Combinatorial Objects. Helsinki University of Technology, Espoo, Finland, 83 pp. Accepted by Department of Computer Science and Engineering on December 16. (The degree of Lic.Sc. (Tech.) was granted on December 19.) Supervised by Pekka Orponen.

[47] Timo Latvala. On Model Checking Safety Properties. Helsinki University of Technology, Espoo, Finland, 64 pp. Accepted by Department of Computer Science and Engineering on December 16. (The degree of Lic.Sc. (Tech.) was granted on December 19.) Supervised by Nisse Husberg.

5.7 Master's theses

[48] Terje Bergström. Context Awareness in Symbian OS Based SmartPhones. Helsinki University of Technology, Espoo, Finland, 50 pp. Accepted by Department of Computer Science and Engineering September 30. (The degree of M.Sc. (Tech.) was granted on October 21.) Supervised by Nisse Husberg.

[49] Catharina Candolin. Network Management and Routing in Mobile Military Ad Hoc Networks. Helsinki University of Technology, Espoo, Finland, 8+64 pp. Accepted by Department of Computer Science and Engineering on January 21. (The degree of M.Sc. (Tech.) was granted on the same day.) Supervised by Hannu H. Kari.

[50] Henri Grönblom. Software Quality Improvement through Software Product Process Definition and Development. Helsinki University of Technology, Espoo, Finland, 90 pp. Accepted by Department of Electrical and Communications Engineering on February 25. (The author did not graduate during the year 2002.) Supervised by Nisse Husberg.

[51] Timo Karilinna. Analysointityökalun käytettävyyden parantaminen (Improving the Usability of an Analysis Tool). Helsinki University of Technology, Espoo, Finland, 66 pp. In Finnish. Accepted by Department of Electrical and Communications Engineering on February 25. (The degree of M.Sc. (Tech.) was granted on the same day.) Supervised by Nisse Husberg.

[52] Matti Kokkola. Arkkitehtuuri aikakriittisiä lyhytviestipalveluita varten (An Architecture for Time Crical Short Message Services). Helsinki University of Technology, Espoo, Finland, 58 pp. In Finnish. Accepted by Department of Computer Science and Engineering on September 2. (The degree of M.Sc. (Tech.) was granted on September 4.) Supervised by Hannu H. Kari.

[53] Jing Liu. An Architectural Solution Driven by Business, Enabled through Technology, with and Integration Perspective. Helsinki University of Technology, Espoo, Finland, 82 pp. Accepted by Department of Computer Science and Engineering on October 28. (The degree of M.Sc. (Tech.) was granted on November 18.) Supervised by Hannu H. Kari.

[54] Elina Parviainen. Modeling the Operation of Margolus Quantum Cellular Automaton Using High-Level Petri Nets. Helsinki University of Technology, Espoo, Finland, 64 pp. Accepted by Department of Computer Science and Engineering on June 10. (The author did not graduate during the year 2002.) Supervised by Ilkka Niemelä.
http://www.tcs.hut.fi/Publications/info/bibdb.ParviainenMsc.shtml

[55] Henrik Petander. Authorization of Mobile IPv6. Helsinki University of Technology, Espoo, Finland, 69+15 pp. Accepted by Department of Electrical and Communications Engineering on September 23. (The degree of M.Sc. (Tech.) was granted on the same day.) Supervised by Hannu H. Kari.

[56] Erkki Pulliainen. Reducing Retrieval Time in High-Latency Computer Networks Using Predictive Caching. Helsinki University of Technology, Espoo, Finland, 71 pp. Accepted by Department of Computer Science and Engineering on October 28. (The degree of M.Sc. (Tech.) was granted on November 18.) Supervised by Hannu H. Kari.

[57] Matti Salonen. Solution For Content and Service Mediation. Helsinki University of Technology, Espoo, Finland, 63 pp. Accepted by Department of Electrical and Communications Engineering on September 2. (The author did not graduate during the year 2002.) Supervised by Hannu H. Kari.

[58] Lauri Tarkkala. On the Construction of Collision-Resistant Accumulators. Helsinki University of Technology, Espoo, Finland, 67 pp. Accepted by Department of Computer Science and Engineering on June 10. (The degree of M.Sc. (Tech.) was granted on the same day.) Supervised by Helger Lipmaa.

[59] Yafeng Wang. A Gateway Architecture for Content Charging. Helsinki University of Technology, Espoo, Finland, 8+53 pp. Accepted by Department of Computer Science and Engineering on September 2. (The degree of M.Sc. (Tech.) was granted on September 4.) Supervised by Hannu H. Kari.

5.8 Software

[60] Tomi Janhunen. `lpeq 1.13` — A Tool for Testing the Equivalence of Logic Programs. http://www.tcs.hut.fi/Software/lpeq/

[61] Tommi Junttila. `bc2cnf` — A Program for Translating Constrained Boolean Circuits to Equi-Satisfiable Boolean Formulae in DIMACS CNF Format. http://www.tcs.hut.fi/%7etjunttil/circuits/

[62] Timo Latvala. `scheck 1.0` — A Tool for Translating Safety LTL Formulae to Finite Automata. http://www.tcs.hut.fi/%7etimo/scheck/

[63] Markku-Juhani O. Saarinen. `ELK 1.0`. http://www.tcs.hut.fi/%7emjos/

[64] Markku-Juhani O. Saarinen. `Split 1.0`. http://www.tcs.hut.fi/%7emjos/

6 PEDAGOGICAL EDUCATION

Satu Virtanen completed in 2001–2002 a 15 credit Y00P course (yliopisto-opetuksen opintokokonaisuus; http://www.hut.fi/Yksikot/Opintotoimisto/Opetuki/yoop15ov/). This is a pedagogical course for university teachers in engineering and natural science.

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE
ANNUAL REPORT 2002