Helsinki University of Technology Laboratory for Theoretical Computer Science
Annual Report 2004
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosiraportti 2004
Espoo 2005 HUT-TCS-Y2004

ANNUAL REPORT FOR THE YEAR 2004

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 2004
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion vuosiraportti 2004
Espoo 2005 HUT-TCS-Y2004

ANNUAL REPORT FOR THE YEAR 2004

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
Tel. +358-0-451 1
Fax. +358-0-451 3369
E-mail: lab@tcs.hut.fi

Multiprint Oy
Helsinki 2005

ABSTRACT: This report describes the educational and research activities of the Laboratory for Theoretical Computer Science at Helsinki University of Technology during the year 2004. In the PDF version of this report, URL addresses are links to those addresses. For example, you get to the home page of the laboratory by clicking http://www.tcs.hut.fi/.

CONTENTS

1 **Introduction** 1

2 **Personnel** 1
- 2.1 Professors 1
- 2.2 Docents 2
- 2.3 Staff 2
- 2.4 Researchers not mentioned in 2.3 2
- 2.5 Research Assistants not mentioned above 3
- 2.6 Teachers and Teaching Assistants not mentioned above 4

3 **Educational activities** 4
- 3.1 Active courses in 2004 4

4 **Research activities** 8
- 4.1 Computational logic 8
- 4.2 The STRATUM system: automated home assignments 14
- 4.3 Computational complexity and combinatorics 15
- 4.4 Mobility management 17
- 4.5 Verification and state space analysis 18
- 4.6 Generative string rewriting 20
- 4.7 Cryptology 20

5 **Conferences, visits and guests** 22
- 5.1 Conferences 22
- 5.2 Visits 30
- 5.3 Guests 31

6 **Publications** 32
- 6.1 Journal articles 32
- 6.2 Articles in collections 33
- 6.3 Conference papers 33
- 6.4 Books 39
- 6.5 Reports (see also 6.6) 40
- 6.6 Doctoral dissertations 41
- 6.7 Licentiate's theses 42
- 6.8 Master's theses 42
- 6.9 Patents 43
- 6.10 Software 43

7 **Pedagogical education** 44

1 INTRODUCTION

Laboratory for Theoretical Computer Science is a part of the Department of Computer Science and Engineering at Helsinki University of Technology. It is responsible for teaching of basic theoretical computer science in the degree programme of computer science and engineering. The Master's level and postgraduate education and research in the laboratory focus on five main areas: computational logic, computational complexity, verification, mobility management, and cryptology.

The budget of the laboratory is heavily based on external funding and in 2004 less than 40% of the total incoming funding was provided by the university. The biggest external sources of funding have been the National Technology Agency of Finland (TEKES) and industry, Academy of Finland and Helsinki Graduate School in Computer Science and Engineering (HeCSE). The external funding grew for more than 10% and, for example, three new research projects funded by the Academy of Finland started in 2004. Over 50 persons were employed in research or teaching positions and the list of publications includes 90 items for the year 2004. More detailed information on personnel, education, research, visits, and publications in the laboratory in 2004 can be found in the following sections.

2 PERSONNEL

The personnel of the Laboratory for Theoretical Computer Science in 2004 is listed in this section. Repetition of names is avoided to a certain extent in the way expressed by the subsection titles. In Sections 2.4 and 2.5, omission of a job title indicates that the title of the subsection already specifies the job title for the whole year.

2.1 Professors

Niemelä, Ilkka; D.Sc.(Tech.); Professor; Head of the Laboratory

Kari, Hannu H.; D.Sc.(Tech.); Professor

Orponen, Pekka; D.Phil.; Professor (on leave until July 31); Senior Scientist funded by the Academy of Finland until July 31

Lipmaa, Helger; PhD; Professor (pro tem)

Ojala, Leo; Lic.Sc.(Tech.); Professor Emeritus

2.2 Docents

Husberg, Nisse; D.Sc.(Tech.); Docent in Verification

Lilius, Johan; D.Sc.(Tech.); Docent in Reactive Systems; Professor (Åbo Akademi University, Department of Computer Science)

Janhunen, Tomi; D.Sc.(Tech.); Docent in Theoretical Computer Science, especially Computational Logic

Nyberg, Kaisa; D.Phil.; Docent in Cryptology

Ukkonen, Esko; D.Phil; Docent in Theoretical Computer Science; Academy Professor (University of Helsinki, Department of Computer Science)

Varpaaniemi, Kimmo; D.Sc.(Tech.); Docent in Formal Verification Methods for Parallel and Distributed Systems

2.3 Staff

Haanpää, Harri; D.Sc.(Tech.); Teaching Researcher until July 31; Researcher since August 1

Heljanko, Keijo; D.Sc.(Tech.); Teaching Researcher (on leave until March 31 (cf. 5.2) and since September 1); Academy Research Fellow since September 1

Janhunen, Tomi; D.Sc.(Tech.); Teaching Researcher

Kangasniemi, Ulla; Secretary

Klaus, Katja; Secretary

Kotimäki, Jaakko; Stud.Tech.; System Administrator

Lassila, Eero; Lic.Sc.(Tech.); Laboratory Manager

Saastamoinen, Taneli; M.Sc.; System Administrator
(Non-Military Serviceman) until September 15

Varpaaniemi, Kimmo; D.Sc.(Tech.); Teaching Researcher

2.4 Researchers not mentioned in 2.3

Autere, Antti; M.Sc.(Tech.); external funding

Candolin, Catharina; Lic.Sc.(Tech.)

Elkind, Edith; M.Sc., Researcher during August 1–31 (cf. 5.3)

Hietalahti, Maarit; M.Sc.(Tech.)

Junttila, Tommi; D.Sc.(Tech.); Researcher until January 14 (cf. 5.2) and since September 1

Jussila, Toni; Lic.Sc.(Tech.)

Järvisalo, Matti; M.Sc.(Tech.); Research Assistant until March 31; Researcher since April 1

Kaski, Petteri; Lic.Sc.(Tech.)

Keinänen, Misa; M.A.

Kortesniemi, Yki; Lic.Sc.(Tech.), Researcher since August 1

Latvala, Timo; Lic.Sc.(Tech.)

Laur, Sven; M.Sc.; Researcher since February 1

Lundberg, Janne; M.Sc.(Tech.)

Mäkelä, Marko; D.Sc.(Tech.); Researcher until February 29

Oikarinen, Emilia; M.Sc.(Tech.)

Petander, Henrik; M.Sc.(Tech.)

Saarinen, Markku-Juhani O.; M.Sc.; Researcher until October 31

Schaeffer (née Virtanen), Satu Elisa; Lic.Sc.(Tech.)

Syrjänen, Tommi; Lic.Sc.(Tech.)

Särelä, Mikko; M.Sc.(Tech.); Research Assistant until April 30; Researcher since May 1

Tauriainen, Heikki; Lic.Sc.(Tech.)

Wallén, Johan; M.Sc.(Tech.)

2.5 Research Assistants not mentioned above

Falck, Emil; Stud.Tech.; Research Assistant until November 11

Gallagher, Michael; Stud.Tech.; Trainee during June 1 – August 31 (cf. 5.3)

Hyvärinen, Antti; Stud.Tech.; Research Assistant since June 1

Kalsi, Petri; Stud.Tech.; Research Assistant during June 1 – August 31

Kullberg, Tuulia; Stud.Tech.; Research Assistant since May 13

Käsper, Emilia; B.Sc.; external funding

Laine, Jaakko; Stud.Tech.

Nuorvala, Ville; Stud.Tech.

Nykopp, Janne; Stud.Tech.; Research Assistant since June 1

Rantanen, Heikki; M.Sc.(Tech.); Research Assistant during June 1 – July 31

Seitz, Sakari; Stud.Tech.; Research Assistant until May 31

Silander,Tapio; Stud.Tech.; Research Assistant until August 31

Tuominen, Antti; Stud.Tech.; on leave (in military service) since July 12

2.6 Teachers and Teaching Assistants not mentioned above

Aho, Pauli; Stud.Tech.; Teaching Assistant in T-79.148

Herttua, Ilkka; Stud.Tech.; Teacher in T-79.232

Honkola, Jukka; Stud.Tech.; Teaching Assistant in T-79.179

Huima, Antti; M.Sc.(Tech.); Teacher in T-79.190

Riihimäki, Vesa; M.Sc.(Tech.); Teaching Assistant in T-79.165

Ritvanen, Kaarle; M.Sc.(Tech.); Teaching Assistant in T-79.503

Tynjälä, Teemu; Lic.Sc.(Tech.); Teacher in T-79.232

Östergård, Patric R.J.; D.Sc.(Tech.); Professor (HUT, Department of Electrical and Communications Engineering); Teacher in T-79.165

3 EDUCATIONAL ACTIVITIES

The aim of the education at the undergraduate level is to give students basic insight into theoretical computer science and parallel and distributed digital systems, as well as learning in applying the theoretical results to practice. At the post-graduate level knowledge in the aforementioned areas will be completed further, especially in some particular theoretical questions.

3.1 Active courses in 2004

In 2004, the following courses were active, that is, arranged as lectures, seminars or projects.

T-79.144 Logic in Computer Science: Foundations
(Autumn, 2 credits ; Teacher: Tomi Janhunen;
Teaching Assistants: Toni Jussila, Janne Nykopp, and
Emilia Oikarinen)

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;
Teaching Assistant: Misa Keinänen)

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

T-79.148 Introduction to Theoretical Computer Science
(Spring, Autumn, 2 credits ;
Teachers: Harri Haanpää (Spring) and Pekka Orponen (Autumn);
Teaching Assistants: Pauli Aho (Spring),
Antti Hyvärinen (Autumn), Matti Järvisalo (Spring, Autumn),
Emilia Oikarinen (Autumn), Tommi Syrjänen (Spring, Autumn),
and Mikko Särelä (Spring, Autumn))

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-79.149 Discrete Structures
(Autumn, 2 credits ; Teacher: Pekka Orponen)

Contents: Annually varying topics concerned with the basic structures and methods of computer science theory. The course in Autumn 2004 was concerned with enumerative combinatorics, i.e. the counting of combinatorial objects by means of their complex-valued generating functions.

T-79.154 Logic in Computer Science: Special Topics II
(Autumn, 2 credits ; Teacher: Tomi Janhunen;
Teaching Assistant: Tommi Syrjänen)

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

T-79.159 Cryptography and Data Security
(Spring, 3 credits ; Teacher: Helger Lipmaa;
Teaching Assistants: Markku-Juhani O. Saarinen and
Johan Wallén)

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;
Teaching Assistant: Emilia Oikarinen)

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-79.165 Graph Theory
(Spring, 3 credits ;
Teachers: Patric R.J. Östergård and Petteri Kaski
Teaching Assistant: Vesa Riihimäki)

Contents: Introduction to graph theory. Trees, planar graphs and digraphs. Graph coloring. Random graphs. Algorithms for central graph problems. Applications. Additional information: The course T-79.165, also occurring with the code S-72.343, is organized jointly by the Communications Laboratory and the Laboratory for Theoretical Computer Science.

T-79.179 Parallel and Distributed Digital Systems
(Spring, 3 credits ; Teacher: Marko Mäkelä;
Teaching Assistant: Jukka Honkola)

Contents: Modelling digital systems. Concurrency. Basics of Petri nets, stochastic systems and process algebra. Using computer-aided methods.

T-79.185 Verification
(Autumn, 3 credits ; Teachers: Tommi Junttila and
Kimmo Varpaaniemi)

Contents: Verification and analysis of parallel and distributed systems using tools. The course in Autumn 2004 considered two famous techniques for symbolic model checking: binary decision diagram manipulation and bounded model checking.

T-79.186 Reactive Systems
(Spring, 2 credits ; Teacher: Timo Latvala)

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: Professors and Teaching Researchers
of HUT-TCS)

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

T-79.190 Testing of Concurrent Systems
(Spring, 2 credits ; Teacher: Antti Huima)

Contents: Introduction to conformance testing. Formal conformance testing and its automatization. On testing timed and infinite-state systems. Estimation of testing coverage.

T-79.192 Special Course in Theoretical Computer Science
(Autumn, 2 credits ; Teacher: Hannu H. Kari)

Contents: Current topics in theoretical computer science. The course in Autumn 2004 was concerned with mobility management problematics in wireless ad hoc networks.

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 2004 was concerned with constraint programming.

T-79.230 Foundations of Agent-Based Computing
(Spring, 3 credits ; Teacher: Tomi Janhunen;
Teaching Assistant: Mikko Särelä)

Contents: Decision-making on the basis of uncertain information. Theory, architectures and applications for agent-based computing. As a project assignment in Spring 2004, one was supposed to implement a soccer playing software agent.

T-79.232 Safety-Critical Systems
(Spring, 2 credits ; Teachers: Ilkka Herttua and Teemu Tynjälä)

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;
Teaching Assistant: Matti Järvisalo)

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

T-79.295 Individual Studies
(1–10 credits ; Teachers: Professors of 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, Autumn, 2–10 credits ;
Teachers: Hannu H. Kari (Spring) and Helger Lipmaa (Autumn))

Contents: Current research problems in theoretical computer science. The course in Spring 2004 was concerned with security in ad hoc networks, whereas the course in Autumn 2004 was concerned with derandomization.

T-79.503 Foundations of Cryptology
(Spring, 2–6 credits ; Teacher: Kaisa Nyberg;
Teaching Assistant: Kaarle Ritvanen)

Contents: The course concerns the mathematical foundations of modern cryptographic methods. It can be taken as special course within computer science, mathematics or applied mathematics.

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 2004 was concerned with cryptanalysis of secret-key primitives.

T-79.515 Cryptology: Special Topics
(Spring, 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 Spring 2004 was concerned with data mining in the context of cryptology.

4 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 4.1, 4.2, 4.3, 4.5, and 4.6. For more applied research funding has been awarded by non-academic partners. This research is described in Sections 4.4 and 4.7.

4.1 Computational logic

Research in the area of computational logic has been carried our in a project funded by the Academy of Finland titled “Applications of rule-based constraint programming” led by Prof. Ilkka Niemelä. More detailed description of the research is given below.

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) 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.

We have continued our prior work on researching the theoretical background of ASP. We have developed an extended language of cardinality constraint programs [49], defined a declarative formal semantics for it and examined the computational complexity of the language.

We have studied some practical aspects of ASP programming. The current ASP systems are research tools and they lack most of the standard programming tools that are present in more established languages. The declarative nature of ASP makes it difficult to apply the standard methodology directly so we have studied how the existing concepts can be translated into ASP. We have developed a prototype ASP debugger that is based on meta-programming: the core of the debugger is an ASP program that gets as an input the program that is debugged.

We have investigated [44] the proof theory of programs with monotone cardinality atoms (mca-programs) and demonstrated that the operational concept of the one-step provability operator used in normal logic programs can be extended to mca-programs but this extension involves nondeterminism. The resulting proof theory is shown to generalize the corresponding concepts in normal logic programs and in disjunctive logic programs with the possible-model semantics of Sakama and Inoue.

In many applications preferences need to be expressed. In order to capture preferences as ranked options we have studied a new connective ($\times$) that allows to represent alternative, ranked options for problem solutions in the heads of rules. Expression $A \times B$ 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 [1]. 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 [1].

We have studied a flexible framework to specify problem solutions (outcomes) and preferences among them. The proposal combines ideas from answer-set programming (ASP), answer-set optimization (ASO) and CP-nets. The problem domain is structured into components. ASP techniques are used to specify values of components, as well as global (inter-component) constraints among these values. ASO methods are used to describe preferences among the values of a component and CP-net techniques to represent inter-component dependencies and corresponding preferences.

Translation-based techniques for knowledge representation
Tomi Janhunen

In 2004, we continued our research on translating normal logic programs into sets of classical clauses. The goal of this research is to utilize efficient Boolean satisfiability (SAT) solvers when computing answer sets for normal logic programs. The translation described in [22] is based on a novel characterization of stable models in terms of *level numberings*. In contrast to earlier approaches, the following unique combination of properties results: (i) a bijective relationship between stable models and classical models, (ii) each normal logic program has a fixed translation that need not to be augmented later on when classical models are computed, (iii) the time needed to translate a normal logic program given as input remains sub-quadratic. Our preliminary experiments with an implementation of the transformation, namely translators called `lp2atomic` and `lp2sat`, and SAT solvers such as `chaff` and `relsat` suggest that our approach becomes competitive when the task is to compute not just one but all stable models for the program given as input.

Our second research topic concerns the stable semantics of disjunctive logic programming under which every atom appearing in a disjunctive program is false by default. This is sometimes undesirable from the knowledge representation point of view and a more refined control of minimization is called for. Such features are already present in Lifschitz's parallel circumscription where certain atoms are allowed to vary or to have fixed values while all other atoms are minimized. In [26], we prove formally that the expressive power of minimal models is properly increased in the presence of varying atoms. In spite of this, we show how parallel circumscription can be embedded into disjunctive logic programming in a relatively systematic fashion using a linear and faithful, but *non-modular* translation. This enables the conscious use of varying atoms in disjunctive logic programs — leading to more elegant and concise problem representations in a number of domains.

Disjunctive logic programming
Tomi Janhunen and Ilkka Niemelä

In [24], we describe an implementation of disjunctive logic programming under the (partial) stable model semantics. The key idea in our approach is to unfold partiality and disjunctions from a logic program using suitable program transformations. This enables us to use an existing implementation of stable models for normal (disjunction-free) programs as the core inference engine. To assess the feasibility of such an architecture we have implemented a system called GnT [81] for computing stable models of disjunctive programs. The performance of the system is surprisingly close to that of `dlv` which is a state-of-the-art system for disjunctive programs.

Verifying the equivalence of logic programs

Tomi Janhunen and Emilia Oikarinen

It is typical in *answer set programming* (ASP) that a programmer ends up with a series of improving answer set programs for the problem being solved when optimizing memory consumption and/or the running time elapsed on a particular ASP implementation. This gives rise to a meta-level problem of ensuring that the various version of the program are equivalent. To address this problem, we have developed translation-based methods for the automated verification of equivalence. The idea is to translate any two logic programs of interest into a single logic program whose answer sets (if such exist) yield counter-examples to the equivalence of the two. Then existing ASP implementations can be used to check the existence of counter-examples and special-purpose search engines need not be developed. In 2003–2004, an existing translation-based method designed for weight constraint programs supported by the `smodels` system was generalized to the disjunctive case [45]. The implementation, a translator called `dlpeq`, enables the verification of equivalence using the GnT system [81]. To summarize [25], our translators `lpeq` and `dlpeq` cover now the following cases: (i) the weak equivalence of weight constraint programs; (ii) the classical equivalence of normal logic programs; (iii) the strong equivalence of normal logic programs under the stable model semantics; and (iv) the weak equivalence of disjunctive logic programs [45].

SAT-based planning

Keijo Heljanko and Ilkka Niemelä

Together with Jussi Rintanen (Albert-Ludwigs-Universität Freiburg, Germany) we have studied a number of semantics for plans with parallel operator application [47, 68]. The standard semantics used most often in earlier work requires that parallel operators are independent and can therefore be executed in any order. We consider a more relaxed definition of parallel plans, first proposed by Dimopoulos et al., as well as normal forms for parallel plans that require every operator to be executed as early as possible. We formalize the semantics of parallel plans emerging in this setting, and propose effective translations of these semantics into the propositional logic. And finally we show that one of the semantics yields an approach to classical planning that is sometimes much more efficient than the existing SAT-based planners.

Boolean satisfiability checking

Tommi Junttila, Matti Järvisalo, and Ilkka Niemelä

A variety of interesting propositional satisfiability problem (SAT) instances stem from, e.g., such areas as planning, model checking of finite state systems, testing, and hardware verification. Therefore there is a high demand for more efficient SAT checkers [4]. Recognizing the factors that affect the difficulty of SAT checking is crucial if one is to find more efficient methods for the task.

Most current state-of-the-art SAT checkers assume that the input formulae are in conjunctive normal form (CNF). However, using CNF makes efficient modeling of an application cumbersome, and additionally often hides information about the structure of the original problem. Boolean circuits provide a compact and structure-preserving presentation for problems in many domains. A non-clausal generalization of the Davis-Putnam-Logemann-Loveland (DPLL) procedure to Boolean circuits has been developed and implemented by Junttila and Niemelä during recent years. We have studied [31, 32, 63] the relative efficiency of variations of this method. The variations are obtained by restricting the use of the cut (splitting) rule in several natural, locality based ways. It is shown that the more restricted variations cannot polynomially simulate the less restricted ones. The results also apply to DPLL for formulas in conjunctive normal form obtained from Boolean circuits by using Tseitin's translation. Thus DPLL with the considered cut restrictions, such as allowing splitting only on the variables corresponding to the input gates, cannot polynomially simulate DPLL with unrestricted splitting.

We have studied the relationship between SAT and constraint satisfaction problems (CSP) and developed a binary CSP encoding for SAT [33] which is linear in the number of variables, domain size and constraint size w.r.t. the size of the SAT instance.

In cooperation with the ITC-IRST research institute (Trento, Italy), we have also done research on extending satisfiability checking beyond the propositional case. During 2004 new results concerning the satisfiability problem of propositional logic with linear arithmetic constraints have been achieved and implemented in the MathSAT system (http://mathsat.itc.it/). The results were submitted during 2004 and accepted for publication in 2005.

Solution techniques for boolean equation systems
Misa Keinänen and Ilkka Niemelä

Boolean equation systems provide a useful framework to study verification problems of finite state concurrent systems. For instance, many model checking problems and behavioral equivalences can be encoded as such systems. We have studied efficient solution techniques for classes of Boolean equation systems. We have devised algorithms for solving conjunctive/disjunctive form Boolean equation systems which may contain alternating fixed points [21, 56]. We have applied answer set programming techniques to solve generic systems of Boolean equations. This is based on a mapping from Boolean equation systems to normal logic programs which allows for determining the solutions by using an answer set programming approach [38]. We have study the space complexity of solving general Boolean equation systems and prove a NL-hardness result which appears to be new [37]. This helps to understand the theoretical minimum of space storage needed for solving Boolean equation systems.

Bounded model checking

Keijo Heljanko, Tommi Junttila, Toni Jussila, Timo Latvala, and Ilkka Niemelä

Bounded model checking (BMC) is a memory efficient method for locating design errors in reactive systems. The basic idea is to look for counterexample executions of bounded length by mapping the problem to, e.g., a propositional satisfiability problem and then using propositional satisfiability solvers to solve the problem at hand. We have continued to do research on bounded model checking techniques and very significant progress has been made on this topic during the reporting period. The focus has been on ways to more efficiently encode temporal logic properties and on how to exploit the concurrency in bounded model checking of distributed systems.

Firstly, in [39, 64] we have published the first encoding of the bounded LTL model checking problem into propositional logic which is linear in both the formula size and the bound used. This is a significant improvement for systems containing large formulas as specifications. The experimental work has been carried out on top of the NuSMV2 model checker. The approach has been extended to PLTL which expands LTL with past operators. An implementation of this approach [83] on top of NuSMV2 came out already in the reporting period, with the related publication to appear in 2005.

The concurrency of a distributed system is exploited in [29] to obtain an efficient bounded model checking approach for a system composed of labelled transition systems (LTSs). This continues earlier work on using non-standard execution models for bounded model checking. The main contribution is a new execution model which allows a sequence of transitions to be merged to an atomic block and the related efficient BMC implementation. This approach is made more efficient by the use of iterative strengthening of the employed bounded model checking encoding in [30].

Testing and synthesis of distributed systems

Keijo Heljanko

In formal conformance testing of distributed systems a black-box implementation is tested against a specification. The main focus of the research is 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. A technical report version of the Master's Thesis of Tuomo Pyhälä [67] on the topic came out in the reporting period.

In the area of synthesis of distributed systems the idea is to create a distributed implementation of a system specified in a non-distributed manner. Several different setups and notions of synthesis exists and the theoretical complexities of the subproblems of synthesis were not well known. The main result on this topic in the reporting period is [60] which settles several open problems of computational complexity relating to open subproblems of synthesis. It also contains prototype implementations of some synthesis procedures implemented on top of the `smodels` system.

Automata-theoretic methods for the verification of linear time temporal logic
Heikki Tauriainen

This research presents new heuristics for automata-based explicit state model checking to improve the worst-case memory efficiency of on-the-fly language emptiness checking algorithms for generalized Büchi automata, which are commonly used, for example, for model checking propositional linear time temporal logic (LTL). The results have been published in the conference paper [51].

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 2004, two papers [27, 28], based on Junttila's doctoral dissertation, reporting results 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, were published.

4.2 The STRATUM system: automated home assignments

Tomi Janhunen, Toni Jussila, Matti Järvisalo, Petri Kalsi, Janne Nykopp, Emilia Oikarinen, and Pekka Orponen

In 2000–2004, our laboratory has developed a web-based learning environment which can be used to automate home assignments on basic courses in (theoretical) computer science. In the environment, (i) personal home assignments are automatically generated for students, (ii) home assignments are put available for download on the WWW, (iii) students are provided automated tools, such as graphical editors and theorem provers, for doing/solving their home assignments, (iv) the tools deliver the answers of students for approval using electronic mail, and (v) the answers of the students are checked automatically several times every day using assignment-specific verifiers such as proof checkers or theorem provers. At the moment, a variety of home assignments related with logical proofs, finite automata and grammars can be taken within this environment [23]. A system called STRATUM provides a common infrastructure for the environment. A central design criteria of the STRATUM system has been scalability for hundreds of students.

4.3 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
Satu Elisa Schaeffer, Sakari Seitz, and Pekka Orponen

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.

S.Sch. continued her doctoral work on algorithmic issues in the modelling, analysis and management of large nonuniform networks. Novel, efficient methods for online clustering and sampling of large graphs were designed in collaboration with P.O. Two conference papers on these topics, first presented as a technical report [66], have already been accepted for publication in 2005. The methods developed are also applicable to ad hoc clustering of hierarchical networks of mobile devices, and S.Sch.'s joint paper on this topic with Doc. Pekka Nikander (Ericsson NomadicLab) was presented in [53]. In June 2004, S.Sch. participated in the annual Santa Fe Institute Summer School on Complex Systems, in connection to which she completed a collaborative research project on fault-tolerance in sensor networks [48]. S.Sch.'s work has been supported by research grant *Algorithms for Nonuniform Networks (ANNE)* from the Academy of Finland.

S.Stz and P.O. continued their investigations into the theory and applications of stochastic search methods. Experimental data collected in Autumn 2004 revealed the surprising effectiveness of the WalkSAT algorithm and a modified version of the Metropolis dynamics in the solution of large randomly generated 3-SAT instances. Reports on this work have been accepted for publication in 2005.

In the academic year 2004-2005, P.O. was on sabbatical from his professor position, supported by a senior researcher grant from the Academy of Finland. As part of this research period, P.O. was visiting the Santa Fe Institute of Complex Systems in March – April 2004.

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 R.J. Östergård and his group at the Electrical Engineering Department.

In 2004 the group continued their work on classification algorithms. With algorithms of this type, computational classification results have been obtained for various structures, including Steiner triple systems, near resolvable 2-designs, conference matrices, one-factorizations of regular graphs, sum and difference coverings of Abelian groups, etc. One special topic of interest has been the classification of structures with a prescribed group of automorphisms, in particular Steiner triple systems of order 21. Structures for which other (algebraic, combinatorial, and computational) methods have been applied include point codes of Steiner triple systems of order 19 and whist tournaments. 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.

H.H. defended his doctoral thesis [70] in February 2004; the last two articles of the thesis were published as research reports [57, 59]. In 2004, the group contributed to the journal articles [2, 3, 5, 6, 7, 8, 9] and to the extended abstract [20].

Distributed algorithmics
Antti Autere, Emil Falck, Harri Haanpää, Maarit Hietalahti, Petteri Kaski, Mikko Särelä, and Pekka Orponen

The group applies combinatorial and complexity-theoretic methods to the solution of algorithmic problems in distributed systems. Much of the work is done in close collaboration with researchers from the University of Helsinki Department of Computer Science and the HUT Networking Laboratory, as part of 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. This collaboration was further strengthened in Autumn 2004 by the postdoctoral grant *Algorithms and Combinatorics for Sensor Networks (ACSENT)* received from the Academy of Finland. A related industrial project *Security and Mobility in Hierarchical Ad Hoc Networks (SAMOYED)* has been funded by TEKES.

The NAPS collaboration focused in 2004 on the problem of energy-efficient and fault-tolerant data gathering techniques in wireless sensor networks. A conference report on this work was presented in [19], and a journal version has been accepted for publication.

Within the SAMOYED project, M.S. completed his M.Sc. thesis on mobility models [77] in April 2004, and M.H. continued to work on her Lic.Sc. thesis on security and trust relations in mobile networks. In addition, M.S. published a conference paper together with Doc. Pekka Nikander on host identification in tactical ad hoc networks [50].

Supported by a personal grant from TKK, A.A. continued his doctoral work on the theory and applications of the A^* search algorithm. A conference paper on applying the A^* methodology to energy-efficient routing in ad hoc networks was presented in [16]. A.A. will defend his dissertation in 2005.

4.4 Mobility management

Work in the area of mobility management led by Prof. Hannu H. Kari is structured in three research projects CAN, Brocom, and GO-CORE which are described below.

CAN: core ad hoc networks
Catharina Candolin and Hannu H. Kari

An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to establish and maintain communications. Naturally, if such an infrastructure exists, the nodes will take advantage of it for better performance, security, and quality of service. In most cases the ad hoc network will have access to at least some kind of fixed infrastructure, which also may have been established dynamically and for temporary usage only. Such an infrastructure can be called a core ad hoc network, as it functions as a core network for more mobile ad hoc networks, but it is also established in an ad hoc fashion, i.e. on demand.

Ad hoc networks have been seen as a solution for military and disaster recovery networking in the future. Wireless networks have already now been successfully deployed on the battlefields around the world, and research is going on to improve the capabilities of the systems to allow more flexibility and better survivability. In this project, survivability is enhanced by allowing nodes to reconfigure their tasks in the network as the environment changes. Nodes are reconfigured by relying on an architecture for context aware management. The main criteria considered in this project are security, reliability, and performance.

The development of better networking solutions support the network-centric approach that many armed forces around the world are deploying. The purpose of network-centric warfare (NCW) is to connect sensors, shooters, and decision makers in order to achieve information superiority. NCW recognizes three domains: the physical domain, which is the traditional domain of warfare and where the networks reside, the information domain, which is ground zero in this new concept of warfare, and the cognitive domain. The main asset is information. The networks are merely a tool for distributing information in a timely fashion to all needing entities regardless of their location. However, for the NCW concept to function, the underlying networks must be robust and secure. The same applies for the networks of armed forces that do not directly deploy NCW, but still rely on technical solutions to distribute information between entities.

The Mobility/Multicast subproject of Brocom
Hannu H. Kari and Janne Lundberg

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) 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.

GO-CORE — a mobility architecture for heterogeneous wireless networks
Hannu H. Kari, Jaakko Laine, Ville Nuorvala, Henrik Petander, Tapio Silander, and Antti Tuominen

Ubiquitous access to services, potentially tailored for mobile users, is the main driver of wireless data networking. Short range wireless communications technologies allow users to access these services locally at high speeds and potentially at low prices. However, due to the short range, these networks often have limited coverage. Use of IP based mobility management protocols makes it possible to bind these short range networks together and join them to wide area networks providing broader coverage.

The GO-CORE project administered by IDC (Institute of Digital Communications in Helsinki University of Technology) develops a mobility architecture with the aim of providing users with seamless communications in a heterogeneous networking environment. The architecture brings together mobile networks and use of multiple wireless interfaces in mobile nodes.

GO-CORE has developed a prototype of the Mobile IPv6 mobility management protocol for use in the mobility architecture [86, 87]. The prototype is used for managing mobility in heterogeneous wireless IPv6 networks and is also used as a basis for further work in the field of node and network mobility.

4.5 Verification and state space analysis

Software verification
Marko Mäkelä and Timo Latvala

The group applies state space exploration methods to the verification of distributed software systems. Our efforts focused on techniques for model checking modular Petri nets. We have worked on extending our previous research on model checking safety properties to model checking liveness properties of modular Petri nets. During the year 2004, this research contributed to the conference paper [40].

Model checking algorithms

Timo Latvala and Heikki Tauriainen

We study fundamental algorithmic problems in model checking. Our research investigates different models of concurrency and different ways to specify properties. Recently, we have focused on studying verification with *testers*. This year our research contributed to the journal paper [10]. We also continued studying different techniques for efficiently generating automata specifications of safety properties. The research resulted in an updated version of the `scheck` software [82].

Modeling and analysis of Margolus quantum cellular automata using net-theoretical methods

Leo Ojala, Olli-Matti Penttinen, and Elina Parviainen

Petri net methods have been very successful in modeling the operation of classical parallel systems. In our work [46], these methods are applied to designing parallel quantum computers. The demonstration object of our study is a quantum Billiard Ball Model Cellular Automaton (BBMCA) suggested by Margolus. Firstly, a high-level Petri net model of a classical reversible version of this automaton is constructed. Subsequently, this Petri net model is used as a so-called kernel net of the quantum BBMCA. The time-independent Hamiltonian needed to generate the time-evolution of a quantum computer can be automatically generated from the reachability graph of a kernel net. Also, a new numerical method for solving the resulting Schrödinger differential equation system needed for time simulation of the quantum automaton is given. Quantum Maria, a software package for modeling and numerical simulation of quantum computers, is introduced.

Stubborn sets for priority nets

Kimmo Varpaaniemi

Partial order methods, such as the stubborn set method and the priority method, reduce verification effort by exploiting irrelevant orders of events. In the work done during the year 2004 [52], it was shown how the stubborn set method can be applied to priority nets. In this context, applicability means that for a given priority net, the stubborn set method constructs a reduced reachability graph that sufficiently represents the full reachability graph of the priority net. Since the end of June 2004, the reachability analysis tool PROD [80] has had a version of the stubborn set method that works in the case of priority nets in all those verification tasks that were in the scope of the stubborn set method for unprioritised nets in the earlier versions of PROD. Applications of the stubborn set method to priority nets can also be considered as combinations of the stubborn set method and the priority method, to be used in “complete or moderated incomplete” verification when the original models are unprioritised nets.

4.6 Generative string rewriting

Eero Lassila

What does one want from a generative string rewriting process? If we were mainly concerned of easy analyzability of the rewriting result, we would be wise to stick to formal language theory and to context-free Chomsky grammars in particular. But here we are not at all interested in such analyzability (which would benefit us only after the generation and only if we for some reason had to parse the output). In contrast, we want to boost the generative process itself: for optimization, we want unbounded context-sensitivity, and for speed, we want optional parallelism. On the other hand, we must take care that our process always remains semantics-preserving. (So while context-free Chomsky grammars closely relate to the front end of a programming language compiler, our work relates to the back end.)

Both synchronously and asynchronously parallel rewriting, in addition to sequential rewriting, should be dealt with. Each of these three rewriting types moreover has several subtypes: for instance, sequential rewriting embraces both Chomsky grammars and macro processors, while Lindenmayer systems constitute a prominent example of synchronous parallelism. We have devised a simple unifying formal framework that tries to capture the three types and their subtypes.

Our goal is to formulate a fairly wide variety of such constraints that if the rewriting rule base as a whole meets one of the constraints, the degree of parallelism in the rewriting process may be selected freely as long as the limits implied by the particular constraint are not exceeded. Adjusting this selection often changes the structure but never the semantics of the output.

4.7 Cryptology

Helger Lipmaa, Sven Laur, 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 real life. During 2004, our group produced one invited conference paper [42], six international conference papers ([15, 18, 41, 43] and the two papers published in 2005 that are mentioned in the August and December subsections of Section 5.1: "Encrypted Watermarks and Linux Laptop Security" and "On Secure Scalar Product Computation for Privacy-Preserving Data Mining"), and one research report [65].

We continued our research on the properties of the mix of arithmetic operations and bitwise operations with respect to differential and linear cryptanalysis. In [43], we introduce a new technique for analysing these kinds of operations, and present the first analysis of the differential properties of bitwise exclusive-or when differences are expressed using integer addition. This analysis is crucial when evaluating the security of ciphers that mix arithmetic operations with bitwise exclusive-or against differential cryptanalysis.

A major research area of the group is cryptographic protocols and their real-life applications. A very important example application is electronic auctions. Up to now, the game-theoretic functionality of auctions and cryptographic auctions have been studied separately. In [18], we propose a new cryptographically protected auction mechanism for on-line auctions that provide security, cognitive convenience and round-efficiency. We are aware of no previous work that interleaves cryptography explicitly with the mechanism design, and think that this paper opens a very interesting and important research direction.

Another important application are polls on sensitive issues. In sensitive polls, it is clear that people do not want to answer honestly if their privacy is not guaranteed. In [15], we develop cryptographically secure techniques that guarantee unconditional privacy of the respondents of polls. The constructions are efficient and practical, and are shown not to allow the cheating respondents to affect the tally by more than their own vote. We present solutions to this problem based both on traditional cryptographic techniques and quantum cryptography. The protocols can also be used in other scenarios like electronic voting: by allowing a slight error in vote counting, one can achieve information-theoretically private voting.

The results of [15] also have applications in privacy-preserving data mining. The main objective of data mining is to find new and interesting relations in existing data. Since individuals and organisations are not willing to share their data due to privacy concerns, privacy-preserving protocols for data mining is an important area. In a couple of papers, we show that some previously proposed privacy-preserving data mining protocols are insecure.

In private similarity search protocols, a client receives from a data base the entry that is closest to the query, without letting the client or the data base owner to learn more information than necessary. In [41], we show that the previously proposed private similarity search protocols by Du and Atallah have serious weaknesses. In several cases, we show that even maximally securified versions of these protocols are not private in the sense needed in practise. We present a few new protocols that are better from the privacy viewpoint, but none of the proposed protocols is really efficient.

In many contexts, the security of the full privacy-preserving data mining protocol depends on the security of an underlying private scalar product protocol. In the paper "On Secure Scalar Product Computation for Privacy-Preserving Data Mining", we show that two of the private scalar product protocols, one of which was proposed in a leading data mining conference, are insecure. We then describe a provably secure private scalar product protocol and improve its efficiency so that it can be used on massive data sets.

Most of the work on cryptographic protocols use zero-knowledge protocols. In 2003, we proposed a new methodology for developing efficient statistical zero-knowledge arguments for a relatively large class of problems. In the invited survey [42], we give an overview of the definitions of statistical zero-knowledge, our previous work on the topic, and related work, both preceding and subsequent to our own work.

Finally, in [65], we present a one-round 1-out-of-n private information retrieval protocol with log-squared communication that can be based on general public-key cryptosystems. The proposed protocols can be transformed into 1-out-of-n oblivious transfer protocols with computational privacy for the chooser and information-theoretical privacy for the sender.

5 CONFERENCES, VISITS AND GUESTS

5.1 Conferences

January

The 8th International Symposium on Artificial Intelligence and Mathematics, Fort Lauderdale, FL, USA, January 4–6. Participants: Tomi Janhunen, Matti Järvisalo, Ilkka Niemelä, and Emilia Oikarinen. Work done by Matti Järvisalo, Tommi Junttila and Ilkka Niemelä was presented [32].
http://rutcor.rutgers.edu/~amai/aimath04/

The 7th International Conference on Logic Programming and Nonmonotonic Reasoning, Fort Lauderdale, FL, USA, January 6–8. Ilkka Niemelä is a co-chair and Tomi Janhunen a member of the programme committee. Sessions chaired by Tomi Janhunen and Ilkka Niemelä. Other participants: Matti Järvisalo and Emilia Oikarinen. Presentations on work done by Tomi Janhunen and Ilkka Niemelä [24], Tomi Janhunen and Emilia Oikarinen [25, 45], and on work partially done by Ilkka Niemelä [44].
http://www.tcs.hut.fi/Conf/lpnmr-7/

Estonian Theory Days, Koke, Estonia, January 30 – February 1. Helger Lipmaa is a member of the organising committee. He also chaired a session and gave a talk (*Interleaving Cryptography and Mechanism Design: The Case of Online Auctions*). Other participants: Emilia Käsper and Sven Laur.
http://www.cs.ut.ee/~varmo/tday-koke/

February

The 11th International Workshop on Fast Software Encryption, Delhi, India, February 5–7. Participant: Johan Wallén. Work partially done by Helger Lipmaa and Johan Wallén was presented [43]. http://www.isical.ac.in/~fse2004/

The 8th International Conference on Financial Cryptography, Key West, FL, USA, February 9–12. Work done by Edith Elkind and Helger Lipmaa was presented [18]. A session chaired by Helger Lipmaa who is also a member of the programme committee. http://www.ifca.ai/fc04/

The Annual Connectathon Interoperability Testing Event, San Jose, CA, USA, February 19–26. Talks given by Henrik Petander (*Route Optimization & IPSec Interactions for Userspace MIPv6*) and Antti Tuominen (*Implementing Mobile IPv6 in the User Space*). http://www.connectathon.org/talks04/

The 9th Estonian Winter School in Computer Science, Palmse, Estonia, February 29 – March 5. Talks given by Matti Järvisalo (*Cut in a Tableau Method for Boolean Circuits*), Emilia Oikarinen (*Verifying the Equivalence of Disjunctive Logic Programs*), and Johan Wallén (*Rational Series in Cryptanalysis*). Other participant: Sven Laur. Helger Lipmaa is a member of the programme committee. http://www.cs.ioc.ee/yik/schools/win2004/

March

The 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1–4. Work partially done by Helger Lipmaa was presented [15]. A session chaired by Helger Lipmaa.
http://pkc2004.lit.org.sg/ConferenceProgramme.html

Executive IT Summit, Helsinki, Finland, March 2–3. An invited talk given by Hannu H. Kari (*Tieto kilpailuetuna: Osaavatko yritykset turvata valttinsa?*).

The 15th International Conference on Applications of Declarative Programming and Knowledge Management, Potsdam, Germany, March 4–6. A talk given by Misa Keinänen [38]. http://inap.dialogengines.com/Past/INAP2004/

The 18th Workshop W(C)LP on Constraint Logic Programming, Potsdam, Germany, March 4–6. Participant: Misa Keinänen.
http://inap.dialogengines.com/Past/INAP2004/

DIMACS/PORTIA Workshop on Privacy-Preserving Data Mining, Rutgers, The State University of New Jersey, Piscataway, NJ, USA, March 15–16. Work partially done by Helger Lipmaa was presented by Markus Jakobsson (*Cryptographic Randomized Response Techniques*).
http://dimacs.rutgers.edu/Workshops/Privacy/program.html

Data Security Seminar of the Signals Officers' Association (Viestiupseeriyhdistys ry), m/s Silja Opera, Gulf of Finland, March 18–19. Participant: Catharina Candolin.
http://www.viestiupseeriyhdistys.fi/toiminta/laivaseminaari2004_kertomus.shtml

Cisco iVision Conference, Tallinn, Estonia, March 24–25. An invited talk given by Hannu H. Kari [34]. http://cisco.evolvis.net/ivision/

The 2nd Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Cambridge, UK, March 24–26. Participant: Satu Elisa Schaeffer. Work partially done by Satu Elisa Schaeffer was presented [53].
http://www.cl.cam.ac.uk/Research/SRG/wiopt04/

The 10th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Barcelona, Spain, March 29 – April 2. Participant: Misa Keinänen. Work partially done by Misa Keinänen was presented [21]. http://www.daimi.au.dk/~cpn/tacas04/

CSC (Centre for Scientific Computing) Grid Workshop, Espoo, Finland, March 31. Participants: Matti Järvisalo, Petteri Kaski, and Ilkka Niemelä.
http://www.csc.fi/suomi/koulutus/grid_workshop.phtml

April

The 3rd National Conference on Military Science, Helsinki, Finland, April 15–16. Janne Lundberg gave a talk in the Seminar of the Technology Section (*A System for Combining Forward Error Correction and Source Authentication in Wireless Multicast Networks*).

http://www.mpkk.fi/fi/ajankohtaista/sotatieteidenpaivat/tekniikanjaosto.html

Security Forum Workshop, Espoo, Finland, April 20–23. Two invited talks given by Hannu H. Kari. (Talk 1: *Battlefield Internet — Is Internet Collapsing Now or Later?* Talk 2: *PLA Packet Level Authentication.*) An ordinary talk given by Markku-Juhani O. Saarinen (*Encrypted Watermarks: Security Vulnerabilities in Laptop Encryption*), Hannu H. Kari is the chairman of the organising committee. http://www.tcs.hut.fi/Workshop/sfw2004/

May

The 23rd Annual International Eurocrypt Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2–6. Participants: Helger Lipmaa and Johan Wallén.

http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3027

The 3rd International Workshop on Commercial Information Technology for Military Operations, Sofia, Bulgaria, May 10–14. Participant: Catharina Candolin. http://www.citmo.net/citmo2004/

Laajakaistoja ja uusia palveluita (Seminar), Seinäjoki, Finland, May 11. An invited talk given by Hannu H. Kari (*Tietoverkkoriippuvuus — Olemmeko jo liian riippuvaisia tietoverkoista?*).

http://www.etelapohjanmaa.fi/seminaari/seminaari115.htm

E-Voting and Estonia (Seminar), Tartu, Estonia, May 17. The panel discussion chaired by Helger Lipmaa.

http://www.cyber.ee/english/company/news/2004/evoting.html

Tietojenkäsittelytieteen päivät, Joensuu, Finland, May 24–25. A talk given by Matti Järvisalo [31]. http://www.cs.joensuu.fi/tktpaivat2004/

DIMACS Workshop on Electronic Voting, Rutgers, The State University of New Jersey, Piscataway, NJ, USA, May 26–27. An invited talk given by Helger Lipmaa (*How Hard is it to Manipulate Voting?*).

http://dimacs.rutgers.edu/Workshops/Voting/

Teleware Corporate Security Conference, Helsinki, Finland, May 27–28. A plenary talk given by Hannu H. Kari [35]. http://www.teleware.fi/corpsec2004/

Seutuverkkoseminaari, Kauhajoki, Finland, May 31. An invited talk given by Hannu H. Kari (*Laajakaistaverkkojen tulevaisuus*).

International Workshop on Wireless Networks, Oulu, Finland, May 31 – June 3. Participants: Maarit Hietalahti and Mikko Särelä.

http://www.cwc.oulu.fi/iwwan2004/

June

The 9th International Conference on the Principles of Knowledge Representation and Reasoning, Whistler, British Columbia, Canada, June 2–5. A session chaired by Tomi Janhunen. Other participant: Ilkka Niemelä who is also a member of the programme committee. http://www.kr.org/KR2004/

The 10th International Workshop on Non-Monotonic Reasoning, Whistler, British Columbia, Canada, June 6–8. Tomi Janhunen is a member of the programme committee of the whole workshop, a co-chair of the organising committee of the Subworkshop on Computational Aspects of Non-Monotonic Reasoning, and a member of the programme committee of that subworkshop. He also chaired a session. http://www.pims.math.ca/science/2004/NMR/

The Annual Santa Fe Institute Complex Systems Summer School, Santa Fe, NM, USA, June 7 – July 2. Participant: Satu Elisa Schaeffer. Work partially done by Satu Elisa Schaeffer was presented [48].
http://www.santafe.edu/education/csss/summerSchool04.php

The 2nd International Conference on Applied Cryptography and Network Security, Yellow Mountain (Huangshan), Anhui, China, June 8–11. Helger Lipmaa is a member of the programme committee.
http://icisa.freewebtools.com/acns2004/

Nordic Research Training Course on Cryptology and Its Applications, Bergen, Norway, June 10–18. A lecture course given by Helger Lipmaa (*Zero Knowledge and Some Applications*). http://www.selmer.uib.no/researchcourse2004/

Workshop on Statistical Physics and Computational Problems, Paris, France, June 14–16. Participant: Pekka Orponen.
http://www.lpt.ens.fr/~monasson/Sphinx/intro.html

The 4th International Conference on Application of Concurrency to System Design, Hamilton, Ontario, Canada, June 16–18. Talks given by Tommi Junttila [27], Toni Jussila [29], and Heikki Tauriainen [51]. http://acsd.mcmaster.ca/

Conference on Optimization Algorithms and Quantum Disordered Systems, Paris, France, June 17–18. An invited talk given by Pekka Orponen (*Local Search Algorithms for Random Decision Problems*).
http://www.lpt.ens.fr/~monasson/Aci-JC/aci-conf.html

IEEE International Conference on Communications, Paris, France, June 20–24. Participant: Mikko Särelä. http://www.see.asso.fr/htdocs/main.php/passees.php/124/

The 25th International Conference on Application and Theory of Petri Nets, Bologna, Italy, June 21–25. Talks given by Tommi Junttila [28] and Timo Latvala [40]. http://www.cs.unibo.it/atpn2004/

Workshop on the Definition, Implementation and Application of a Standard Interchange Format for Petri Nets, Bologna, Italy, June 26. Nisse Husberg is a member of the programme committee. http://wwwcs.upb.de/cs/kindler/events/XML4PN/

The 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, June 28–29. A session chaired by Catharina Candolin who is also a member of the programme committee. Work partially done by Catharina Candolin was presented [14].

July

Workshop on Foundations of Computer Security, Turku, Finland, July 12–13. Participant: Maarit Hietalahti. http://www.cs.chalmers.se/~andrei/FCS04/

The 31st International Colloquium on Automata, Languages and Programming, Turku, Finland, July 12–16. Participants: Harri Haanpää, Matti Järvisalo, Petteri Kaski, and Pekka Orponen. http://www.math.utu.fi/ICALP04/

The 13th Annual IEEE Symposium on Logic in Computer Science, Turku, Finland, July 13–17. Participants: Harri Haanpää, Matti Järvisalo, and Petteri Kaski. http://homepages.inf.ed.ac.uk/als/lics/lics04/

The 1st International Workshop on Algorithmic Aspects of Wireless Sensor Networks, Turku, Finland, July 16. A talk given by Emil Falck [19]. Other participants: Harri Haanpää, Petteri Kaski, and Pekka Orponen.
http://ru1.cti.gr/algosensors04/

The 4th European Congress on Computational Methods in Applied Sciences and Engineering, Jyväskylä, Finland, July 24–28. A talk given by Helger Lipmaa [42]. http://www.mit.jyu.fi/eccomas2004/proceedings/session/session20.html

The 19th National Conference on Artificial Intelligence, San Jose, CA, USA, July 25–29. Tomi Janhunen and Ilkka Niemelä are members of the programme committee. http://www.aaai.org/Conferences/National/2004/aaai04.html

August

Laajakaistaseminaari, Helsinki, Finland, August 19. An invited talk given by Hannu H. Kari (*Laajakaistaverkkojen palvelut ja tulevaisuus*).

Scandinavic ICT Business Seminar, Helsinki, Finland, August 23. A plenary talk given by Hannu H. Kari (*Adaptive Applications and Services in Future Heterogeneous Wired and Wireless Networks, Impact on Scandinavian ICT Sector*).

Tietoverkkoseminaari, Helsinki, Finland, August 23. An invited talk given by Hannu H. Kari (*Tietoverkkojen kehitysnäkymät ja haasteet*).

The 5th International Workshop on Information Security Applications, Jeju Island, Korea, August 23–25. A talk given by Markku-Juhani O. Saarinen (*Encrypted Watermarks and Linux Laptop Security*). A paper corresponding to the talk was published in 2005. No proceedings during the year 2004.
http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3325

Laajakaistoja ja uusia palveluita (Seminar), Pello, Finland, August 26. An invited talk given by Hannu H. Kari (*Laajakaistaverkot — avain tulevaisuuden palveluihin*). http://www.lapinliitto.fi/ajankohtaista/kari.pdf

September

HeCSE Poster Day, Helsinki, Finland, September 2. Posters presented by Antti Autere (*New Online Power-Aware Routing Algorithms in Wireless Networks*), Catharina Candolin (*Military Networking in Network-Centric Warfare*), Maarit Hietalahti (*Security in Hierarchical/Clustered Ad Hoc Networks*), Toni Jussila (*Bounded Model Checking with Non-Standard Execution Models*), Petteri Kaski (*Algorithms for Classification of Combinatorial Structures*), Misa Keinänen (*Solutions Techniques for Boolean Equation Systems*), Janne Lundberg (*Multicasting Securely to Wireless Mobile Devices*), Emilia Oikarinen (*Declarative Rule-Base Constraint Programming*), Satu Elisa Schaeffer (*Algorithms for Nonuniform Networks*), and by Heikki Tauriainen (*Questionable Tricks for Automata-Theoretical LTL Model Checking*). http://www.cs.helsinki.fi/hecse/Students/Abstracts-2004/

The 20th International Conference on Logic Programming, Saint-Malo, France, September 6–10. Ilkka Niemelä is a member of the programme committee. He also chaired a session and gave an invited tutorial (*The Implementation of Answer Set Solvers*). http://www.irisa.fr/manifestations/2004/ICLP04/

The 4th International School on Foundations of Security Analysis and Design, Bertinoro, Italy, September 6–11. Participant: Maarit Hietalahti. http://www.sti.uniurb.it/events/fosad04/

Uudenmaan laajakaistastrategia (Seminar), Helsinki, Finland, September 7. An invited comment presented by Hannu H. Kari. http://www.uudenmaanliitto.fi/chapter_files/laajakaistaselvitys.doc

The 1st International Workshop on Views on Designing Complex Architectures, Bertinoro, Italy, September 11–12. Participant: Catharina Candolin. http://www-gris.det.uvigo.es/~rebeca/vodca/vodca_pages/home_page.htm

Workshop on Physical Aspects of Multiscale Modeling, Bled, Slovenia, September 13–15. Participant: Catharina Candolin. http://multiscale.boku.ac.at/

Teleware Tietoliikenne Conference, Helsinki, Finland, September 16–17. A plenary talk given by Hannu H. Kari [36]. http://www.teleware.fi/TL2004/

The 9th International Workshop on Formal Methods for Industrial Critical Systems, Linz, Austria, September 20–21. A talk given by Misa Keinänen [37]. http://www.fmics04.cclrc.ac.uk/

Workshop on Concurrency, Specification and Programming, Caputh near Potsdam, Germany, September 24–26. A talk given by Toni Jussila [30]. http://www.ki.informatik.hu-berlin.de/CSP2004/

The 3rd International Workshop on Modelling and Reformulating Constraint Satisfaction Problems, Toronto, Ontario, Canada, September 27. A talk given by Matti Järvisalo [33]. http://www-users.cs.york.ac.uk/~frisch/Reformulation/04/

The 9th European Conference on Logics in Artificial Intelligence, Lisbon, Portugal, September 27–30. A talk given by Tommi Syrjänen [49]. Other participants: Tomi Janhunen and Emilia Oikarinen. Work done by Tomi Janhunen and Emilia Oikarinen was presented [26]. Jussi Rintanen presented work partially done by Keijo Heljanko and Ilkka Niemelä [47]. Ilkka Niemelä is a member of the programme committee. http://centria.di.fct.unl.pt/~jelia2004/

The 10th International Conference on Principles and Practice of Constraint Programming, Toronto, Ontario, Canada, September 27 – October 1. Participant: Matti Järvisalo. http://ai.uwaterloo.ca/~cp2004/

October

Tallinn–Tartu Computer Science Theory Days, Veskisilla, Estonia, October 1–3. Talks given by Sven Laur (*Privaatne otsing: indeksid ning alternatiivid*) and Helger Lipmaa (*An Oblivious Transfer Protocol with Log-Squared Communication*). Other participant: Emilia Käsper. Helger Lipmaa is a member of the organising committee. http://www.cs.ioc.ee/~tarmo/tday-veskisilla/

The 4th Finnish / Baltic Sea Conference on Computer Science Education, Koli, Finland, October 1–3. A talk given by Tomi Janhunen [23].
http://www.cs.joensuu.fi/kolistelut/program2004.htm

Tietoturvallisuus — lainsäädäntö, uhat ja käytännön toteutukset (Seminar), Espoo, Finland, October 5. An invited talk given by Hannu H. Kari (*Digitaalinen sisältö Internetissä: ongelmat, ratkaisut ja tulevaisuus*).
http://www.mimesweeper.fi/ajankohtaista.html

Pohjois-Karjalan laajakaistapäivät, Joensuu, Finland, October 8. An invited talk given by Hannu H. Kari (*Laajakaistaverkot — avain tulevaisuuden palveluihin*).

The 5th Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools, Aarhus, Denmark, October 8–11. Nisse Husberg is a member of the programme committee. http://www.daimi.au.dk/CPnets/workshop04/cpn/cfp.html

The 12th International Conference on Software, Telecommunications and Computer Networks; Split, Croatia; Dubrovnik, Croatia; Venice, Italy; October 10–13. A talk given by Antti Autere [16].
http://www.fesb.hr/SoftCOM/2004/Program.htm

The 3rd Workshop on Modelling of Objects, Components and Agents, Aarhus, Denmark, October 11–13. Nisse Husberg is a member of the programme committee. http://www.informatik.uni-hamburg.de/TGI/events/moca04/moca04.html

The 5th ETSI IPv6 Plugtests Event, Mandelieu, France, October 11–15. Participants: Jaakko Laine and Ville Nuorvala.
http://www.etsi.org/plugtests/history/2004ipv6.htm

Tieturi Data Security Conference, Helsinki, Finland, October 13–14. A keynote speech given by Hannu H. Kari (*Internetin romahtaminen uhkaa — miten siihen voi varautua?*). http://www.tieturi.fi/resources/ds2004_web.pdf

Workshop on the State of the Art of Stream Ciphers, Brugge, Belgium, October 14–15. Participants: Emilia Käsper and Helger Lipmaa.
http://www.isg.rhul.ac.uk/research/projects/ecrypt/stvl/sasc.html

The 45th Annual IEEE Symposium on Foundations of Computer Science, Rome, Italy, October 17–19. Participant: Helger Lipmaa.
http://www.dis.uniroma1.it/~focs04/

The 8th Nordic Combinatorial Conference, Aalborg, Denmark, October 20–22. Talks given by Harri Haanpää [20] and Petteri Kaski (*Classification of Designs with Small Prescribed Groups of Automorphisms*).
http://www.math.aau.dk/norcom/

The 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, October 25–29. Helger Lipmaa is a member of the programme committee. http://portal.acm.org/toc.cfm?id=1030083

The 19th International Symposium on Computer and Information Sciences, Kemer-Antalya, Turkey, October 27–29. A talk given by Kimmo Varpaaniemi [52]. http://www.cs.bilkent.edu.tr/iscis04/

IEEE Military Communications Conference, Monterey, CA, USA, October 31 – November 3. Participants: Catharina Candolin and Mikko Särelä. Work partially done by Mikko Särelä was presented [50].
http://expo.jspargo.com/milcom04/csn.asp

November

Workshop on Privacy and Security Aspects of Data Mining, Brighton, UK, November 1. Helger Lipmaa is a member of the programme committee.
http://chacs.nrl.navy.mil/projects/psdm04/

Pirkanmaan laajakaistapäivät, Tampere, Finland, November 3. An invited talk given by Hannu H. Kari (*Laajakaistaverkot — avain tulevaisuuden palveluihin*).

The Autumn Seminar of the Finnish Regional Networks Association, Tampere, Finland, November 3. An invited talk given by Hannu H. Kari (*Miten taata laadullisia sisältöpalveluita seutuverkkoihin?*).
http://www.seutuverkot.net/30uut/zzMuu/Arkisto/syysSemi.pdf

The 9th Nordic Workshop on Secure IT Systems, Espoo, Finland, November 4–5. A talk given by Sven Laur [41]. A session chaired by Helger Lipmaa. Hannu H. Kari and Helger Lipmaa are members of the programme committee. http://www.tml.hut.fi/Nordsec2004/

The 61st IETF (Internet Engineering Task Force) Meeting, Washington, DC, USA, November 7–12. Participant: Catharina Candolin.
http://www.ietf.org/meetings/IETF-61.html

Seminar for the Peda-Forum's 10th Anniversary, Kuusamo, Finland, November 10–12. A talk given by Harri Haanpää (*Kyselytutkimus opiskelijoiden ajankäytöstä tietojenkäsittelyteorian peruskurssilla*). Other participant: Emilia Oikarinen. http://www.oulu.fi/Pf2004/

The 5th International Conference on Formal Methods in Computer-Aided Design, Austin, TX, USA, November 15–17. A talk given by Timo Latvala [39]. http://www.cs.utexas.edu/users/hunt/FMCAD/2004/

IIR (Institute for International Research) Security Seminar, Helsinki, Finland, November 23. A plenary talk given by Hannu H. Kari (*Internet is Deteriorating and Close to Collapse: What We Can Do to Survive?*).

The 5th Australian Information Warfare and Security Conference, Fremantle near Perth, Western Australia, November 25–26. Catharina Candolin chaired a session and gave a talk [17]. http://www.we-bcentre.com/conferences/IWar04/

December

The 15th Annual Australasian Conference on Information Systems, Hobart, Tasmania, Australia, December 1–3. Participant: Catharina Candolin. http://acis2004.infosys.utas.edu.au/

The 7th International Conference on Information Security and Cryptology, Seoul, Korea, December 2–3. Participants: Emilia Käsper, Sven Laur, and Helger Lipmaa. Work partially done by Sven Laur and Helger Lipmaa was presented (*On Secure Scalar Product Computation for Privacy-Preserving Data Mining*). A paper corresponding to the presentation was published in 2005. No proceedings during the year 2004. http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3506

The 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5–9. Participants: Emilia Käsper, Sven Laur, and Helger Lipmaa. http://www.iris.re.kr/ac04/

Nordic Workshop on Networks, Copenhagen, Denmark, December 16–18. Participant: Satu Elisa Schaeffer. http://www.nordita.dk/~trusina/workshop/home0.html

5.2 Visits

Keijo Heljanko and Toni Jussila visited the Institute of Formal Methods in Computer Science in the University of Stuttgart, Germany, on January 1 – March 31. (Heljanko's visit had started on April 1 of the previous year.) http://www.fmi.uni-stuttgart.de/szs/people/gaeste.en.shtml

Tommi Junttila visited the Centre for Scientific and Technological Research (Istituto per la Ricerca Scientifica e Tecnologica) in the Trentino Cultural Institute (Istituto Trentino di Cultura) in Trento, Italy, on January 15 – August 31 and on December 12–18. Within these two periods, he also visited the University of Trento. http://sra.itc.it/projects/calculemus/task1.2.html

Pekka Orponen visited the Santa Fe Institute in Santa Fe, NM, USA, on March 2 – April 28.

Hannu H. Kari visited ONRIFO (the US Office of Naval Research, International Field Office) in Washington, DC, USA, on April 14–17 and gave a talk (*Military Grade Wireless Ad Hoc Networks*) on April 16.

Also on April 14–17, Catharina Candolin and Hannu H. Kari visited the University of Maryland in College Park, MD, USA, and the US Naval Research Laboratory in Washington, DC, USA.

Ilkka Niemelä visited the University of Leipzig, Germany, on May 10–15.

Pekka Orponen visited the Institute for Mathematical Optimization in the Technical University Carolo-Wilhelmina at Brunswick (Braunschweig), Germany, on May 23–28 and gave a talk (*Balanced Data Gathering in Energy-Constrained Sensor Networks*) on May 24.

On October 28, Ilkka Niemelä visited the Department of Computer and Information Science in the Linköping University, Sweden, and gave a talk (*Answer Set Programming: an Approach to Declarative Problem Solving*).
http://www.ida.liu.se/zope/divisions/sas/SaSSeminars/

Catharina Candolin visited the NICTA (National Information and Communications Technology Australia) research centre in Sydney, New South Wales, Australia, on December 6.

Henrik Petander visited the University of New South Wales and the NICTA (National Information and Communications Technology Australia) research centre in Sydney, New South Wales, Australia, for three months.
http://www.cse.unsw.edu.au/~ocean/emotion/people.html

5.3 Guests

Official opponents of doctoral dissertations

Professor Clement Lam from the Department of Computer Science in the Concordia University, Montréal, Québec, Canada, stayed for February 22–28, gave a talk (*After n Years of Computing, Is the Answer Correct?*) (abstract available via http://www.tcs.hut.fi/Current/TCSF/tcs-s2004.shtml)) on February 24, was the official opponent in the public examination of Harri Haanpää's doctoral dissertation [70] on February 27, and was hosted by Pekka Orponen.

Other guests

The abstracts of the talks mentioned in this section are available via
http://www.tcs.hut.fi/Current/TCSF/tcs-a2004.shtml.

Prof.Dr. Jürgen Dix from the Institute of Computer Sciences in the Technical University of Clausthal, Germany, stayed for August 28 – September 1, gave a talk (*Planning in Answer Set Programming using Ordered Task Decomposition*) on September 1, and was hosted by Ilkka Niemelä.

M.Sc. Edith Elkind (cf. 2.4) from the Department of Computer Science in the Princeton University, NJ, USA, stayed for August 1–31, gave a talk (*How Hard Is It to Manipulate Voting?*) on August 26, and was hosted by Helger Lipmaa.

Stud.Tech. Michael Gallagher (cf. 2.5) from the Dublin Institute of Technology, Ireland, stayed for June 1 – August 31 and was hosted by Hannu H. Kari.

RNDr. (Rerum Naturalium Doctoris) Jiři Šima from the Institute of Computer Science at Prague in the Academy of Sciences of the Czech Republic, stayed for November 1–21 and was hosted by Pekka Orponen.

Dr. Jan Villemson (a.k.a. Willemson) from the Institute of Computer Science in the University of Tartu, Estonia, stayed for September 27, gave a talk (*Game Theoretic Methods in Data Security*), and was hosted by Helger Lipmaa.

6 PUBLICATIONS

6.1 Journal articles

[1] Gerhard Brewka, Ilkka Niemelä, and Tommi Syrjänen: *Logic Programs with Ordered Disjunction.* Computational Intelligence, Vol. 20, No. 2, May, pp. 335–357. Blackwell Publishing Ltd., Oxford, UK.
http://dx.doi.org/10.1111/j.0824-7935.2004.00241.x

[2] Harri Haanpää: *Minimum Sum and Difference Covers of Abelian Groups.* Journal of Integer Sequences, Vol. 7, No. 2, Article 04.2.6. School of Computer Science, University of Waterloo, Ontario, Canada.
http://www.cs.uwaterloo.ca/journals/JIS/VOL7/Haanpaa/haanpaa.html

[3] Harri Haanpää, Antti Huima, and Patric R.J. Östergård: *Sets in $\mathbb{Z}_n$ with distinct sums of pairs.* Discrete Applied Mathematics, Vol. 138, No. 1–2, March, pp. 99–106. Elsevier B.V., Amsterdam, The Netherlands.
http://dx.doi.org/10.1016/S0166-218X(03)00273-7

[4] Matti Järvisalo: *Lauselogiikan toteutuvuustarkastus: käytännönläheistä teoriaa.* Tietojenkäsittelytiede, No. 22, December, pp. 47–63. Society for Computer Science, Helsinki, Finland. In Finnish.
http://www.funet.fi/org/tkts/lehti/22-index.html

[5] Petteri Kaski: *Packing Steiner Trees with Identical Terminal Sets.* Information Processing Letters, Vol. 91, No. 1, July, pp. 1–5. Elsevier B.V., Amsterdam, The Netherlands. http://dx.doi.org/10.1016/j.ipl.2004.03.006

[6] Petteri Kaski and Patric R.J. Östergård: *Enumeration of Balanced Ternary Designs.* Discrete Applied Mathematics, Vol. 138, No. 1–2, March, pp. 133–141. Elsevier B.V., Amsterdam, The Netherlands.
http://dx.doi.org/10.1016/S0166-218X(03)00276-2

[7] Petteri Kaski and Patric R.J. Östergård: *Miscellaneous Classification Results for 2-Designs.* Discrete Mathematics, Vol. 280, No. 1–3, April, pp. 65–75. Elsevier B.V., Amsterdam, The Netherlands.
http://dx.doi.org/10.1016/j.disc.2003.07.002

[8] Petteri Kaski and Patric R.J. Östergård: *The Steiner Triple Systems of Order 19.* Mathematics of Computation, Vol. 73, No. 248, pp. 2075–2092. American Mathematical Society, Providence, RI, USA.
http://www.ams.org/mcom/2004-73-248/S0025-5718-04-01626-6/home.html

[9] Petteri Kaski and Patric R.J. Östergård: *There Exist Nonisomorphic STS(19) with Equivalent Point Codes.* Journal of Combinatorial Designs, Vol. 12, No. 6, pp. 443–448. John Wiley & Sons, Inc., Hoboken, NJ, USA. http://dx.doi.org/10.1002/jcd.20007

[10] Timo Latvala and Heikki Tauriainen: *Improved On-the-Fly Verification with Testers.* Nordic Journal of Computing, Vol. 11, No. 2, Summer, pp. 148–164. Publishing Association Nordic Journal of Computing, Helsinki, Finland. http://www.cs.helsinki.fi/njc/bibliography.html

6.2 Articles in collections

[11] Catharina Candolin: *A Study of Infrastructure Warfare in Relation to Information Warfare, Net Warfare and Network-Centric Warfare.* In [61], pp. 9–18.

[12] Janne Lundberg: *A System for Combining Forward Error Correction and Source Authentication in Wireless Multicast Networks.* In [61], pp. 218–227.

[13] Janne Lundberg: *Packet Level Authentication Implementation for Linux.* In [62].

6.3 Conference papers

[14] Pauli Aho and Catharina Candolin: *Enabling Network-Centric Warfare by Securing the Core Infrastructure.* In: Andy Jones (Ed.): *Proceedings of the ECIW 2004: the 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, 28–29 June 2004.* Academic Conferences Ltd., Curtis Farm, Kidmore End near Reading, UK, pp. 9–14.
http://www.academic-conferences.org/eciw2005/2-proceedings-eciw2004.htm

[15] Andris Ambainis, Markus Jakobsson, and Helger Lipmaa: *Cryptographic Randomized Response Techniques*. In: Feng Bao, Robert H. Deng, and Jianying Zhou (Eds.): *Public Key Cryptography — PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1–4, 2004, Proceedings*. Lecture Notes in Computer Science, Vol. 2947, Springer-Verlag, Berlin, Germany, pp. 425–438.

http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=2947&spage=425

[16] Antti Autere: *New Online Power-Aware Routing Algorithms in Wireless Networks*. In: Nikola Rožic and Dinko Begušic (Eds.): *Proceedings of the 12th International Conference on Software, Telecommunications and Computer Networks; Split, Croatia; Dubrovnik, Croatia; Venice, Italy; October 10–13, 2004*. Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split, Croatia, pp. 439–443.

[17] Catharina Candolin: *Self-Healing Ad Hoc Networks*. In: Bill Hutchinson (Ed.): *5th Australian Information Warfare & Security Conference, Perth, Western Australia, 25 & 26 November 2004, Conference Proceedings*. We-B Centre, School of Management Information Systems, Edith Cowan University, Joondalup, Western Australia.

http://www.we-bcentre.com/conferences/IWar04/content/IWAR Program 2004.pdf

[18] Edith Elkind and Helger Lipmaa: *Interleaving Cryptography and Mechanism Design: The Case of Online Auctions*. In: Ari Juels (Ed.): *Financial Cryptography, 8th International Conference, FC 2004, Key West, FL, USA, February 9–12, 2004, Revised Papers*. Lecture Notes in Computer Science, Vol. 3110, Springer-Verlag, Berlin, Germany, pp. 117–131.

http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3110&spage=117

[19] Emil Falck, Patrik Floréen, Petteri Kaski, Jukka Kohonen, and Pekka Orponen: *Balanced data gathering in energy-constrained sensor networks*. In: Sotiris Nikoletseas and José D.P. Rolim (Eds.): *Algorithmic Aspects of Wireless Sensor Networks, First International Workshop, ALGOSENSORS 2004, Turku, Finland, July 16, 2004, Proceedings*. Lecture Notes in Computer Science, Vol. 3121, Springer-Verlag, Berlin, Germany, pp. 59–70.

http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3121&spage=59

[20] Malcolm Greig, Harri Haanpää, and Petteri Kaski: *On the Existence of Conference Matrices and Near Resolvable 2-(2k+1,k,k-1) Designs*. In: Olav Geil and Lars Døvling Andersen (Eds.): *Proceedings of the 8th Nordic Combinatorial Conference, Aalborg, Denmark, October 20–22, 2004*. Department of Mathematical Sciences, Aalborg University, Denmark, pp. 65–69.

http://vbn.dk/VBN/AAU/tek-nat/Matematik/vbn:PublikationContainer/
Proceedings_of_the_8th_Nordic_Combinatorial_Conference/

[21] Jan Friso Groote and Misa Keinänen: *Solving Disjunctive/Conjunctive Boolean Equation Systems with Alternating Fixed Points*. In: Kurt Jensen and Andreas Podelski (Eds.): *Tools and Algorithms for the Construction and Analysis of Systems, 10^th^ International Conference, TACAS 2004, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2004, Barcelona, Spain, March 29 – April 2, 2004, Proceedings*. Lecture Notes in Computer Science, Vol. 2988, Springer-Verlag, Berlin, Germany, pp. 436–450.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=2988&spage=436

[22] Tomi Janhunen: *Representing Normal Programs with Clauses*. In: Ramon López de Mántaras and Lorenza Saitta (Eds.): *Proceedings of the 16^th^ European Conference on Artificial Intelligence, ECAI'2004, Including Prestigious Applicants of Intelligent Systems, PAIS 2004, Valencia, Spain, August 22–27, 2004*. Frontiers in Artificial Intelligence and Engineering, Vol. 110, IOS Press, Amsterdam, The Netherlands, pp. 358–362. http://www.iospress.nl/html/faia.php

[23] Tomi Janhunen, Toni Jussila, Matti Järvisalo, and Emilia Oikarinen: *Teaching Smullyan's Analytic Tableaux in a Scalable Learning Environment*. In: Ari Korhonen and Lauri Malmi (Eds.): *Kolin Kolistelut — Koli Calling: Proceedings of the Fourth Finnish / Baltic Sea Conference on Computer Science Education, October 1–3, 2004, in Koli, Finland*. Research Report TKO-A42/04, Laboratory of Information Processing Science, Helsinki University of Technology, Espoo, Finland pp. 85–94. http://www.cs.hut.fi/u/archie/koli04/TKOA42.pdf

[24] Tomi Janhunen and Ilkka Niemelä: *GnT — A Solver for Disjunctive Logic Programs*. In [54], pp. 331–335.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=2923&spage=331

[25] Tomi Janhunen and Emilia Oikarinen: *LPEQ and DLPEQ — Translators for Automated Equivalence Testing of Logic Programs*. In [54], pp. 336–340.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=2923&spage=336

[26] Tomi Janhunen and Emilia Oikarinen: *Capturing Parallel Circumscription with Disjunctive Logic Programs*. In: José Júlio Alferes and João Leite (Eds.): *Logics in Artificial Intelligence, 9^th^ European Conference, JELIA 2004, Lisbon, Portugal, September 27–30, 2004, Proceedings*. Lecture Notes in Artificial Intelligence, Vol. 3229, Springer-Verlag, Berlin, Germany, pp. 134–146.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3229&spage=134

[27] Tommi Junttila: *New Orbit Algorithms for Data Symmetries*. In: Mike Kishinevsky and Philippe Darondeau (Eds.): *Proceedings of the 4^th^ International Conference on Application of Concurrency to System Design (ACSD 2004), Hamilton, Ontario, Canada, June 16–18, 2004*. IEEE Computer Society, Los Alamitos, CA, USA, pp. 175–184.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=29052&arnumber=1309130&count=26&index=20

[28] Tommi Junttila: *New Canonical Representative Marking Algorithms for Place/Transition-Nets.* In: Jordi Cortadella and Wolfgang Reisig (Eds.): *Applications and Theory of Petri Nets, 25th International Conference, ICATPN 2004, Bologna, Italy, June 21–25, 2004, Proceedings.* Lecture Notes in Computer Science, Vol. 3099, Springer-Verlag, Berlin, Germany, pp. 258–277.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3099&spage=258

[29] Toni Jussila: *BMC via Dynamic Atomicity Analysis.* In: Mike Kishinevsky and Philippe Darondeau (Eds.): *Proceedings of the 4th International Conference on Application of Concurrency to System Design (ACSD 2004), Hamilton, Ontario, Canada, June 16–18, 2004.* IEEE Computer Society, Los Alamitos, CA, USA, pp. 197–206.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=29052&arnumber=1309132&count=26&index=22

[30] Toni Jussila: *Efficient Bounded Reachability through Iterative Strengthening.* In: Gabriela Lindemann, Hans-Dieter Burkhard, Ludwik Czaja, Andrzej Skowron, Holger Schlingloff, and Zbigniew Suraj (Eds.): *Workshop: Concurrency, Specification and Programming, CS&P '2004, Caputh, September 24–26, Volume 2: Specification and Verification.* Informatik-Berichte, No. 170, Department of Computer Science (Institut für Informatik), Humboldt University Berlin, Germany, pp. 262–273. http://www.ki.informatik.hu-berlin.de/CSP2004/proc.html

[31] Matti Järvisalo: *Todistuskompleksisuudesta Boolen piirien toteutuvuustarkastuksessa.* In: Pasi Fränti and Esko Marjomaa (Eds.): *Tietojenkäsittelytieteen päivät 2004: 24.–26.5.2004, Joensuun Tiedepuisto.* International Proceedings Series, No. 5, Department of Computer Science, University of Joensuu, pp. 49–53. In Finnish. http://linda.linneanet.fi/

[32] Matti Järvisalo, Tommi Junttila, and Ilkka Niemelä: *Unrestricted vs. Restricted Cut in a Tableau Method for Boolean Circuits.* In: Fahiem Bacchus and Peter van Beek (Eds.): *Proceedings of the 8th International Symposium on Artificial Intelligence and Mathematics, Fort Lauderdale, FL, USA, January 4–6, 2004.* Rutgers Center for Operations Research, Piscataway, NJ, USA. http://rutcor.rutgers.edu/~amai/aimath04/

[33] Matti Järvisalo and Ilkka Niemelä: *A Compact Reformulation of Propositional Satisfiability as Binary Constraint Satisfaction.* In: Alan M. Frisch and Ian Miguel (Eds.): *Modelling and Reformulating Constraint Satisfaction Problems: Towards Systematisation and Automation, Third International Workshop, Toronto, Canada, 27 September 2004, Proceedings.* Department of Computer Science, University of York, UK, pp. 111–124. http://www-users.cs.york.ac.uk/~frisch/Reformulation/04/proceedings.pdf

[34] Hannu H. Kari: *Uudet teknologiat — Uusien palvelujen mahdollisuudet — Olemmeko jo liian riippuvaisia tietoverkoista?* In: Pasi Mäenpää (Ed.): *Proceedings of the Cisco iVision Conference, Tallinn, Estonia, March 24–25, 2004.* Cisco Systems Finland Oy, Espoo, Finland. In Finnish. http://cisco.evolvis.net/ivision/

[35] Hannu H. Kari: *Internetin lähtölaskenta on alkanut — käytä sitä vielä kun voit!* In: Kari Saarelainen (Ed.): *Proceedings of the Corporate Security 2004 Conference, Helsinki, Finland, May 27–28, 2004.* Teleware Oy, Helsinki, Finland. In Finnish. http://www.teleware.fi/corpsec2004/

[36] Hannu H. Kari: *Onko Internetillä tulevaisuutta vakavassa yrityskäytössä? — Tuhat ja yksi tapaa romahduttaa yhteiskunta.* In: Kari Saarelainen (Ed.): *Proceedings of the Tietoliikenne 2004 Conference, Helsinki, Finland, September 16–17, 2004.* Teleware Oy, Helsinki, Finland. In Finnish. http://www.teleware.fi/TL2004/

[37] Misa Keinänen: *Obtaining Memory Efficient Solutions to Boolean Equation Systems.* In: Juan Bicarregui, Andrew Butterfield, and Alvaro Arenas (Eds.).: *Proceedings of the 9th International Workshop on Formal Methods for Industrial Critical Systems, FMICS 2004, Linz, Austria, September 20–21, 2004.* Technical Report SEA-SR-03, Institute for Systems Engineering and Automation, Johannes Kepler University Linz, Austria, pp. 191–208.
http://bibliographie.onb.ac.at/biblio/content/200507/600-1.html

[38] Misa Keinänen and Ilkka Niemelä: *Solving Alternating Boolean Equation Systems in Answer Set Programming.* In: Dietmar Seipel, Michael Hanus, Ulrich Geske, and Oskar Bartenstein (Eds.): *Proceedings of INAP / WLP 2004: the 15th International Conference on Applications of Declarative Programming and Knowledge Management, and the 18th Workshop W(C)LP on Constraint Logic Programming, Potsdam, Germany, March 4–6, 2004.* Technical Report 327, Department of Computer Science, Bavarian Julius-Maximilians-University at Würzburg, Germany, pp. 255–264.
http://www.informatik.uni-wuerzburg.de/reports/tr.html

[39] Timo Latvala, Armin Biere, Keijo Heljanko, and Tommi Junttila: *Simple Bounded LTL Model Checking.* In: Alan J. Hu and Andrew K. Martin (Eds.): *Formal Methods in Computer-Aided Design, 5th International Conference FMCAD 2004, Austin, Texas, USA, November 15–17, 2004, Proceedings.* Lecture Notes in Computer Science, Vol. 3312, Springer-Verlag, Berlin, Germany, pp. 186–200.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3312&spage=186

[40] Timo Latvala and Marko Mäkelä: *LTL Model Checking for Modular Petri Nets.* In: Jordi Cortadella and Wolfgang Reisig (Eds.): *Applications and Theory of Petri Nets, 25th International Conference, ICATPN 2004, Bologna, Italy, June 21–25, 2004, Proceedings.* Lecture Notes in Computer Science, Vol. 3099, Springer-Verlag, Berlin, Germany, pp. 298–311.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3099&spage=298

[41] Sven Laur and Helger Lipmaa: *On Private Similarity Search Protocols*. In: Sanna Liimatainen and Teemupekka Virtanen (Eds.): *NordSec 2004: Proceedings of the Ninth Nordic Workshop on Secure IT Systems — Encouraging Co-Operation, Espoo, Finland, November 4–5, 2004*. Publications in Telecommunications Software and Multimedia, Series A, No. TML-A10, Helsinki University of Technology, Espoo, Finland, pp. 73–77. http://www.cs.ut.ee/~helger/papers/ll04/

[42] Helger Lipmaa: *Statistical Zero-Knowledge Arguments: Theory and Practice*. In: Pekka Neittaanmäki, Tuomo Rossi, Kirsi Majava, Olivier Pironneau, Sergey Korotov, Eugenio Oñate, Jacques Périaux, and Dietrich Knörzer (Eds.): *Proceedings of the 4th European Congress on Computational Methods in Applied Sciences and Engineering, ECCOMAS 2004, Jyväskylä, Finland, July 24–28, 2004*. Department of Mathematical Information Technology, University of Jyväskylä, Finland. http://www.mit.jyu.fi/eccomas2004/proceedings/pdf/617.pdf

[43] Helger Lipmaa, Johan Wallén, and Philippe Dumas: *On the Additive Differential Probability of Exclusive-Or*. In: Bimal Roy and Willi Meier (Eds.): *Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5–7, 2004, Revised Papers*. Lecture Notes in Computer Science, Vol. 3017, Springer-Verlag, Berlin, Germany, pp. 317–331.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3017&spage=317

[44] Victor W. Marek, Ilkka Niemelä, and Mirosław Truszczyński: *Logic Programs with Monotone Cardinality Atoms*. In [54], pp. 154–166.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=2923&spage=154

[45] Emilia Oikarinen and Tomi Janhunen: *Verifying the Equivalence of Logic Programs in the Disjunctive Case*. In [54], pp. 180–193.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=2923&spage=180

[46] Leo Ojala, Olli-Matti Penttinen, and Elina Parviainen: *Modeling and Analysis of Margolus Quantum Cellular Automata Using Net-Theoretical Methods*. In: Jordi Cortadella and Wolfgang Reisig (Eds.): *Applications and Theory of Petri Nets, 25th International Conference, ICATPN 2004, Bologna, Italy, June 21–25, 2004, Proceedings*. Lecture Notes in Computer Science, Vol. 3099, Springer-Verlag, Berlin, Germany, pp. 331–350.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3099&spage=331

[47] Jussi Rintanen, Keijo Heljanko, and Ilkka Niemelä: *Parallel Encodings of Classical Planning as Satisfiability*. In: José Júlio Alferes and João Leite (Eds.): *Logics in Artificial Intelligence, 9th European Conference, JELIA 2004, Lisbon, Portugal, September 27–30, 2004, Proceedings*. Lecture Notes in Artificial Intelligence, Vol. 3229, Springer-Verlag, Berlin, Germany, pp. 307–319.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3229&spage=307

[48] Satu Elisa Schaeffer, Jonathan C. Clemens, and Patrick Hamilton: *Decision Making in Distributed Sensor Networks.* In: Melanie Mitchell (Ed.): *Proceedings of the Santa Fe Institute Complex Systems Summer School, Santa Fe, NM, USA, June 7 – July 2, 2004.* Santa Fe Institute, Santa Fe, NM, USA.

[49] Tommi Syrjänen: *Cardinality Constraint Programs.* In: José Júlio Alferes and João Leite (Eds.): *Logics in Artificial Intelligence, 9th European Conference, JELIA 2004, Lisbon, Portugal, September 27–30, 2004, Proceedings.* Lecture Notes in Artificial Intelligence, Vol. 3229, Springer-Verlag, Berlin, Germany, pp. 187–199.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3229&spage=187

[50] Mikko Särelä and Pekka Nikander: *Applying Host Identity Protocol to Tactical Networks.* In: Manny DiMiceli, Daniel Noneaker, Stephen Squires, et al. (Eds.): *Proceedings of IEEE MILCOM 2004: Military Communications Conference, Monterey, CA, USA, October 31 – November 3, 2004.* IEEE Communications Society, New York, NY, USA. http://ieeexplore.ieee.org/xpl/conhome.jsp?punumber=1000462

[51] Heikki Tauriainen: *Nested Emptiness Search for Generalized Büchi Automata.* In: Mike Kishinevsky and Philippe Darondeau (Eds.): *Proceedings of the 4th International Conference on Application of Concurrency to System Design (ACSD 2004), Hamilton, Ontario, Canada, June 16–18, 2004.* IEEE Computer Society, Los Alamitos, CA, USA, pp. 165–174.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=29052&arnumber=1309129&count=26&index=19

[52] Kimmo Varpaaniemi: *Stubborn Sets for Priority Nets.* In: Cevdet Aykanat, Tuğrul Dayar, and İbrahim Körpeoğlu (Eds.): *Computer and Information Sciences — ISCIS 2004, 19th International Symposium, Kemer-Antalya, Turkey, October 27–29, 2004, Proceedings.* Lecture Notes in Computer Science, Vol. 3280, Springer-Verlag, Berlin, Germany, pp. 574–583.
http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3280&spage=574

[53] Satu Elisa Virtanen and Pekka Nikander: *Local Clustering for Hierarchical Ad Hoc Networks.* In: Tamer Basar and Marco Conti (Eds.): *Proceedings of WiOpt'04, the 2nd Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Cambridge, UK, March 24–26, 2004,* pp. 404–405.

6.4 Books

[54] Vladimir Lifschitz and Ilkka Niemelä (Eds.): *Logic Programming and Nonmonotonic Reasoning, 7th International Conference, LPNMR 2004, Fort Lauderdale, FL, USA, January 6–8, 2004, Proceedings.* Lecture Notes in Artificial Intelligence, Vol. 2923, Springer-Verlag, Berlin, Germany. http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2923

6.5 Reports (see also 6.6)

[55] Annikka Aalto: *Automatic Translation of SDL into High Level Petri Nets*. Technical Report HUT-TCS-B21, November, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. A revised version of [72] without major differences in content. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-B21.shtml

[56] Jan Friso Groote and Misa Keinänen: *A Sub-Quadratic Algorithm for Conjunctive and Disjunctive BESs*. Computer Science Report 0413, Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands. http://library.tue.nl/catalog/CSRPublication.csp?Action=GetByYear

[57] Harri Haanpää: *Minimum Sum and Difference Covers of Abelian Groups*. Research Report HUT-TCS-A88, February, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A88.shtml

[58] Harri Haanpää (Ed.): *Annual Report for the Year 2003*. Annual Report HUT-TCS-Y2003, June, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. http://www.tcs.hut.fi/Publications/info/bibdb.Annual03.shtml

[59] Harri Haanpää and Patric R.J. Östergård: *Sets in Abelian Groups with Distinct Sums of Pairs*. Research Report HUT-TCS-A87, February, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A87.shtml

[60] Keijo Heljanko and Alin Ştefănescu. *Complexity Results for Checking Distributed Implementability*. Technical Reports, Vol. 2004, No. 05, Faculty of Computer Science, Electrical Engineering, and Information Technology, University of Stuttgart, Germany. http://www.informatik.uni-stuttgart.de/zdi/buecherei/NCSTRL_listings/FAK/TR.html.en_mod

[61] Jorma Jormakka and Catharina Candolin (Eds.): *Technical Aspects of Network Centric Warfare*. Publications Series 1 (Research), No. 17, Department of Technology, National Defence College, Helsinki, Finland. http://www.mpkk.fi/fi/tutkimus-opetus/julkaisut/teknl/julkaisusarja1/

[62] Jorma Jormakka and Catharina Candolin (Eds.): *Military Ad Hoc Networks*. Publications Series 1 (Research), No. 19, Department of Technology, National Defence College, Helsinki, Finland. http://www.mpkk.fi/fi/tutkimus-opetus/julkaisut/teknl/julkaisusarja1/

[63] Matti Järvisalo: *Proof Complexity of Cut-Based Tableaux for Boolean Circuit Satisfiability Checking*. Research Report HUT-TCS-A90, March, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. A revised version of [74] without major differences in content. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A90.shtml

[64] Timo Latvala, Armin Biere, Keijo Heljanko, and Tommi Junttila: *Simple Bounded LTL Model Checking*. Research Report HUT-TCS-A92, July, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland.
http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A92.shtml

[65] Helger Lipmaa: *An Oblivious Transfer Protocol with Log-Squared Communication*. Technical Report 2004/063, February, Cryptology ePrint Archive, International Association for Cryptologic Research.
http://eprint.iacr.org/2004/063

[66] Pekka Orponen and Satu Elisa Schaeffer: *Efficient Algorithms for Sampling and Clustering of Large Nonuniform Networks*. Technical Report cond-mat/0406048, June, arXiv.org e-Print archive, Cornell University, Ithaca, NY, USA. http://arxiv.org/abs/cond-mat/0406048

[67] Tuomo Pyhälä: *Specification-Based Test Selection in Formal Conformance Testing*. Research Report HUT-TCS-A93, August, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A93.shtml

[68] Jussi Rintanen, Keijo Heljanko, and Ilkka Niemelä: *Parallel Encodings of Classical Planning as Satisfiability*. Technical Reports, No. 198, February, Institute of Computer Science, Albert-Ludwigs-University of Freiburg, Germany. http://www.informatik.uni-freiburg.de/tr/

[69] Mikko Särelä: *Measuring the Effects of Mobility on Reactive Ad Hoc Routing Protocols*. Research Report HUT-TCS-A91, May, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. A revised version of [77] without major differences in content. http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A91.shtml

6.6 Doctoral dissertations

[70] Harri Haanpää: *Constructing Certain Combinatorial Structures by Computational Methods*. Doctoral dissertation, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland. Published in TKK Electronic Academic Dissertations, Helsinki University of Technology Library, Espoo, Finland (http://lib.tkk.fi/Diss/2004/isbn9512269422/), and in a page-by-page line-by-line picture-by-picture symbol-by-symbol identical form as Research Report HUT-TCS-A89, February, Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland (http://www.tcs.hut.fi/Publications/info/bibdb.HUT-TCS-A89.shtml).

6.7 Licentiate's theses

[71] Catharina Candolin: *Information Warfare and Security in a Network-Centric Environment*. Licentiate's thesis, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland.

6.8 Master's theses

[72] Annikka Aalto: *Automatic Translation of SDL into High Level Petri Nets*. Master's thesis, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland. Published in a revised form as [55] without major differences in content.

[73] Harriet Beaver: *Using Rule-Based Constraint Programming to Find MAPs for Bayesian Networks*. Master's thesis, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland.

[74] Matti Järvisalo: *Proof Complexity of Cut-Based Tableaux for Boolean Circuit Satisfiability Checking*. Master's thesis, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland. Published in a revised form as [63] without major differences in content.

[75] Heikki Rantanen: *Analyzing the Random-Walk Algorithm for SAT*. Master's thesis, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland.
http://www.tcs.hut.fi/Publications/info/bibdb.RantanenMsc.shtml

[76] Erkki Ruponen: *Integrointitestauksen EXIT-kriteerit Symbian-pohjaisessa ohjelmistotuotteessa*. Master's thesis, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland. In Finnish.

[77] Mikko Särelä: *Measuring the Effects of Mobility on Reactive Ad Hoc Routing Protocols*. Master's thesis, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland. Published in a revised form as [69] without major differences in content.

6.9 Patents

[78] Janne Kalliola, Hannu H. Kari, Juha Koponen, and Hannu Mallat: *Method for Optimizing Performance in Wireless Networks*. Finnish Patent FI20011746. Patent Holder: First Hop Oy, Helsinki, Finland.

[79] Hannu H. Kari, Hannu Mallat, Janne Kalliola, and Juha Koponen: *Method for Optimizing Performance in Wireless Networks Using SNMP Agents*. European Patent EP1421749. Patent Holder: First Hop Oy, Helsinki, Finland.

6.10 Software

[80] Lasse Anderson, Johannes Helander, Keijo Heljanko, Tomi Janhunen, Robert Jürgens, Ismo Kangas, Kari J. Nurmela, Kenneth Oksanen, Olavi Pesonen, Marko Rauhamaa, James Reilly, Heikki Suonsivu, Kimmo Valkealahti, Kimmo Varpaaniemi, and Pauli Väisänen: *PROD 3.4.00 — An Advanced Tool for Efficient Reachability Analysis*. Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. http://www.tcs.hut.fi/Software/prod/

[81] Tomi Janhunen and Patrik Simons: *GnT 2.1 — Tool for Computing Stable Models for Disjunctive Logic Programs*. http://www.tcs.hut.fi/Software/gnt/

[82] Timo Latvala: `scheck1.2`. Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland.
http://www.tcs.hut.fi/~timo/scheck/

[83] Timo Latvala: *NuSMV-bPLTL*. Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland.
http://www.tcs.hut.fi/~timo/vmcai2005/

[84] Janne Lundberg: *MSEC — A Secure and Reliable Multicast Delivery Engine for Linux*. Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland.

[85] Janne Lundberg: *PLA — Implementation of Packet Level Authentication for Linux*. Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland.

[86] Ville Nuorvala, Henrik Petander, Antti Tuominen, Sami Kivisaari, Niklas Kämpe, Jaakko Laine, Marko Myllynen, Juha Mynttinen, Toni Nykänen, Jani Rönkkönen, Steven Ayer, Mika Grundström, Jamie Hicks, Venkata Jagana, Tony Jokikyyny, Timo Koskiahde, Krishna Kumar, Nanno Langstraat, Mika Lepistö, Alexandru Petrescu, and Teemu Rinta-Aho: *MIPL Mobile IPv6 Version 1.1*. GO-CORE Project, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland.
http://www.mobile-ipv6.org/software/download/mipv6-1.1-v2.4.26.tar.gz

[87] Ville Nuorvala, Henrik Petander, Antti Tuominen, Masafumi Aramoto, Gabor Fekete, Venkata Jagana, Krishna Kumar, Masahide Nakamura, Shinta Sugimoto, Noriaki Takamiya, Hideaki Yoshifuji, Sami Kivisaari, Niklas Kämpe, Jaakko Laine, Marko Myllynen, Juha Mynttinen, and Toni Nykänen: *MIPL Mobile IPv6 Version 2.0 RC1*. GO-CORE Project, Department of Computer Science and Engineering, Helsinki University of Technology, Espoo, Finland.
http://www.mobile-ipv6.org/software/download/mipv6-2.0-rc1.tar.gz

[88] Tuomo Pyhälä: *`genfacbm` — A Benchmark Generator Based on Factoring for SAT and ASP solvers*. Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland.
http://www.tcs.hut.fi/Software/genfacbm/

[89] Heikki Tauriainen: *`lbtt` — An LTL-to-Büchi Translator Testbench, Version 1.1.2*. Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. http://www.tcs.hut.fi/Software/lbtt/

[90] Antti Tuominen: *HUT AODV for IPv6, Release 0.11*. Laboratory for Theoretical Computer Science, Helsinki University of Technology, Espoo, Finland. http://www.tcs.hut.fi/~anttit/manet/aodv/hut-aodv6-0.11.tar.gz

7 PEDAGOGICAL EDUCATION

Harri Haanpää and Emilia Oikarinen completed in 2003–2004 a 15-credit YOOP (yliopisto-opetuksen opintokokonaisuus) course which is a pedagogical course for university teachers in engineering and natural science.
http://www.hut.fi/Yksikot/Opintotoimisto/Opetuki/yoop15ov/

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE
ANNUAL REPORT 2004