CENTRE FOR DEPENDABLE COMPUTING

Head Prof Jaan Penjam
Institute of Cybernetics at Tallinn University of Technology,
Akadeemia tee 21, 12618 Tallinn, Estonia
Tel. +372 620 4150
Fax +372 620 4151
jaan@cs.ioc.ee
http://cdc.ioc.ee/

RESEARCH TEAMS

MATHEMATICAL FOUNDATIONS & PROGRAMMING LANGUAGE TECHNOLOGY
Supervisor Tarmo Uustalu
Institute of Cybernetics
Akadeemia tee 21, 12618 Tallinn, Estonia
Tel. +372 620 4250
Fax +372 620 4151
tarmo@cs.ioc.ee

FORMAL METHODS IN SOFTWARE ENGINEERING
Supervisor Prof Jaan Penjam
Institute of Cybernetics
Akadeemia tee 21, 12618 Tallinn, Estonia
Tel. +372 620 4150
Fax +372 620 4151
jaan@cs.ioc.ee

TRUST AND CONFIDENCE
Supervisor Prof Ahto Buldas
Cybernetica AS
Akadeemia tee 21, 12618 Tallinn, Estonia
Tel. +372 665 4241
Fax +372 639 7992
ahtbu@cyber.ee

DESIGN AND TEST OF DIGITAL SYSTEMS
Supervisor Prof Raimund-Johannes Ubar
Department of Computer Engineering
Tallinn University of Technology
Raja 15, 12618 Tallinn, Estonia
Tel. +372 620 2252
Fax +372 620 2253
raiub@pld.ttu.ee

Centre for Dependable Computing (CDC) unites scientists from different institutions sharing common research interests and working on common themes following a jointly agreed research plan. In fact, the associated research groups have for years constituted an informal research network that, depending on the prevailing political and financial situation, has worked together organising all-Estonian seminars, conducting projects for supporting computer science higher education (TEMPUS projects) or running international winter schools for graduate students. Establishing a centre of excellence enabled a more systematic consolidation of these efforts. The research plan of the Centre is in agreement with the plans of the participating institutions.

The Centre involves scientists from seven institutions:

- Institute of Cybernetics at TUT (IoC),
- Dept. of Computer Science, TUT (CS/ TUT),
- Dept. of Computer Control, TUT (CC/ TUT)
- Dept. of Computer Engineering, TUT (CE/ TUT),
- Institute of Computer Science, University of Tartu (CS/UT),
- Tartu University Inst. of Technology (TUIT),
- Cybernetica AS (CybAS).

The Centre is coordinated by a Research Council, consisting of the leaders of its research groups and the head of the Centre. Strategic supervision is in the hands of an international Advisory Board of four renowned European scientists: Prof Reino Kurki-Suonio, Tampere University of Technology, Finland; Prof Kim G. Larsen, Aalborg University, Denmark; Prof Reinhard Wilhelm, University of Saarland, Germany; Prof José Oliveira, Universidade do Minho, Braga, Portugal.

RESEARCH PLAN

The research topics of CDC grouped by research areas for the closest years are:

MATHEMATICAL FOUNDATIONS & PROGRAMMING LANGUAGE TECHNOLOGY

- Type-theoretic and category-theoretic studies of (co)inductive types and (co)recursion schemes.
- Algebraic and categorical semantics of intermediate and modal logics, with applications to programming languages;
- Proof-theoretical studies on constructive set theory, Martin-Löf type theory, and explicit mathematics.
- Development of methods for static analysis and abstract testing methods based on abstract interpretation.

- Development of program transformation methods for strong functional programming languages; specifically deforestation, supercompilation etc.
- Development of methods for stack code validation and type checking in stack-based languages.

FORMAL METHODS IN SOFTWARE ENGINEERING

- Development of structural program synthesis methods for systems with distributed architecture.
- Integration of different program synthesis paradigms (deductive, inductive, transformational synthesis).
- Automatic theorem proving and its application for verification of hardware.
- Development of formal specification, verifycation methods and tools combining deductive and algorithmic techniques.
- Integrating formal verification with techniques allowing extending the size of systems that can be verified.
- Time-aware, interaction-based computational models for timing and behavioural analysis.

TRUST AND CONFIDENCE

- Development of efficient techniques for public key distribution and certificate validation (both on-line and off-line). Efficient protocols for long-term preservation of validity confirmations.
- Secure and auditable queries from public databases and registries.
- Time-stamping schemes, their security and efficient implementation.

DESIGN AND TEST OF DIGITAL SYSTEMS

- Development of new methods of modelling physical defects and logic faults to increase the quality of testing of today's complex digital systems.
- Development of new hierarchical diagnostic models of digital systems and highly efficient algorithms for test generation, fault grading and design error and fault diagnosis.
- Development of new efficient design methods based on new paradigms like SOC, co-design, and oriented to testability and built-in self-test criteria.

The research activities of the research groups of CDC are primarily funded from the governmental budget for basic scientific research (target financing) or grants from the Estonian Science Foundation, in total 7,08 million Estonian crowns in the year 2003. The research groups of CDC are also participating in a number European projects funded by the 5th Framework Programme of the EU. At the current moment (Nov. 2003), five EU projects are running:

Thematic network IST-2001-38957 APPSEM II

Thematic network IST-2001-33123 CoLogNet

Accompanying measures project IST-2001-37592 eVikings II

Accompanying measures project IST-2000-30193 REASON

Accompanying measures project IST-2001-35174 OpenEvidence.

Improving the effectiveness of doctoral PhD studies in computer science is a strategic objective of the CDC. The Centre is annually organizing winter and summer schools for PhD students in computer science with lecturers from abroad. The Centre is also in charge of several series of all-Estonian seminars (computer science theory days, formal methods seminar days etc.) as well as master classes of invited foreign lectures.

In 1998-2002 the following young scientists defended their doctoral degrees under supervision of members of CDC: S. Tupailo (Stanford U., 1998), T. Uustalu (KTH, 1998), A. Buldas (TTU, 1999), H. Lipmaa (UT, 1999), V. Vene (UT 2000), P. Ellervee (KTH, 2000), O. Sokratova (UT, 2001), J. Raik (TTU, 2001), A. Kuusik (TTU, 2001), J. Willemson (UT, 2002), P. Laud (U. des Saarlandes, 2002), M. Brik (TTU, 2002). Currently, 24 PhD students are being supervised by members of CDC.

An overview of the scientific results grouped by the research groups is presented in the following sections.

The main research directions of the group are logic and algebra as the foundational disciplines of theoretical computer science, and programming language theory (semantics, design, implementation). More specifically, the group is focusing on structural proof theory and type theory, categorical logic, ordinal analysis, algebraic combinatorics, semiring theory and algebraic automata theory, programming language semantics and programming language implementation, program analysis, incl. type-based methods, semantics-based program manipulation, language-based security.

MAIN RESULTS

A number of new results has been obtained in the theory of inductive and coinductive types, monads and comonads, with applications to modularity in representing and reasoning about syntax and computations with effects and to type-based termination: A novel structured recursion scheme based on a comonad and a distributive law has been formulated which makes it possible to treat a variety of standard structured recursion schemes as instances of one generic scheme. A general account has been given of the so-called Mendler style of formulating structured recursion schemes where the totality of the function being defined (termination of the program) is ensured by the polymorphic type imposed on the scheme. A strong generalization has been given for the theorem by Adámek and colleagues on non-well-founded term algebras as free completely iterative monads. CPS and monadic translations have been defined for languages with inductive and coinductive types. Frameworks for representing and reasoning about syntax with variable binding have been studied for non-well-founded syntax and explicit substitution. A fixed-point-theoretic construction has been given for calculating the coproduct of two ideal monads. This construction enables one, e.g., to calculate the combination of the monads capturing non-determinism and probabilistic choice.

A novel definition of secure information flow has been given which is based on computational rather than information-theoretic independence of the public outputs of a program from its secret inputs. It has been shown how to analyse a program for security in a language

From the 8th Estonian Winter School in Computer Science (EWSCS'03) at Palmse.

with an encryption operator and how to analyse a program for relative security (security on the assumption that some of the outputs of a program are non-secret).

A method for exact static analysis of multi-threaded programs has been developed which avoids state space explosion by use of global invariants. The method has been implemented in a prototype for validation of avionics software.

Several constructive foundational mathematical theories (constructive set theory, Martin-Löf's type theory) have been shown to be realizable into Feferman's explicit mathematics.

A number of results has been obtained on rewriting on semirings and the algebraic theory of automata.

The group initiated the Estonian computer science theory days that have been held twice a year since autumn 2002. In 2004, two international events will take place in Estonia organised by members of the group: the IST TN APPSEM II 2nd Annual Meeting, APPSEM 2004 (Tallinn, 14-16 April 2004) and the 5th International Summer School and Workshop on Advanced Functional Programming, AFP 2004 (Tartu, 16-21 August 2004).

Cooperation partners: Ludwig-Maximilians-Universität München, INRIA Sophia Antipolis, Universidade do Minho, University of Leicester, University of Nottingham, Universität des Saarlandes, Universität Trier, University of Calgary, University of Leeds.

Research team: Tarmo Uustalu, Peeter Laud, Jaanus Pöial, Olga Sokratova, Mati Tombak (prof), Sergei Tupailo, Varmo Vene; Reimo Palm; Härmel Nestra, Ahti Peder, Tiina Zingel (PhD students).

PUBLICATIONS

Abel, A., Matthes, R., Uustalu, T. Generalized iteration and coiteration for higher-order nested datatypes. In: Gordon, A. D. (Ed.) Proc. of 6th Int. Conf. on Foundations of Software Science and Computation Structures, FoSSaCS 2003, Lect. Notes in Comp. Sci. 2620, 54-69 (2003).

Barthe, G., Giménez, E., Frade, M. J., Pinto, L., Uustalu, T. Type-based termination of recursive definitions. Math. Struct. Comp. Sci. 14, 1, 97-141 (2004).

Kelarev, A., Sokratova, O. On congruences of automata defined by directed graphs. Theor. Comput. Sci. 301, 1-3, 31-43 (2003).

Laud, P. Handling encryption in an analysis for secure information flow. In: Degano, P. (Ed.) Proc. of 12th Europ. Symp. on Programming, ESOP 2003, Lect. Notes in Comp. Sci. 2618, 159-173 (2003).

Sokratova, O. The Mal'cev lemma and rewriting on semirings. Theor. Comput. Sci. 255, 1-2, 611-614 (2001).

Tupailo, S. Realization of analysis into explicit mathematics. J. Symb. Logic 66, 4, 1818-1864 (2001).

Tupailo, S. Realization of constructive set theory into explicit mathematics. Ann. Pure and Appl. Logic 120, 1-3, 165-196 (2003).

Uustalu, T. Monad translating inductive and coinductive types. In: Geuvers, H., Wiedijk, F. (Eds.), Selected Papers from 2nd Int. Wksh. on Types for Proofs and Programs, TYPES'02, Lect. Notes in Comp. Sci. 2646, 299-315 (2003).

Uustalu, T., Vene, V. Least and greatest fixed-points in intuitionistic natural deduction. Theor. Comput. Sci. 272, 1-2, 315-339 (2002).

Uustalu, T., Vene, V., Pardo, A. Recursion schemes from comonads. Nordic J. of Computing 8, 3, 366-390 (2001).

FORMAL METHODS IN SOFTWARE ENGINEERING

To meet the high requirements on the reliability of complex systems and to speed up productivity of software development teams, methods for getting provably correct programs are needed. Formal proof theory provides a basis for two different approaches to correct software development: program construction (program is derived from its specification) and program verification (program is proven to meet requirements of the specification). In practice, a variety of combinations of these two diametrically opposed approaches is used.

The main aim of this research is studying logic, algebra and systems theory based methods for proving properties and synthesising programs and systems, and also studying properties of the proof methods themselves. Current rese-

arch is addressing developing techniques and tools applicable for obtaining both transformational and reactive (embedded) systems.

The rapidly increasing number of embedded and distributed computer applications has revealed the need for development of new models of computing based on concept of non-linear time. The software-intensive systems are often operating in incompletely known environments, in an interface between natural and artificial world that is not always predictable in the phase of system development. Introducing time to computer science in a sufficiently sophisticated form has become essential for verification of timing properties of such systems. Research of this team is also focused on formal description and analysis methods of time-sensitive multi-agent systems, and on methods for assessment of structural and behavioural properties of time-sensitive software.

The research team has competence in the areas of proof theory and automated theorem proving, program synthesis, timed and hybrid automata, compositional program verification, correctness by construction techniques, and application domains such as mechanical engineering and control.

SYNTHESIS OF PROGRAMS

A common formal basis for representing semantics of computations both at the level close to hardware primitives, and at the level of software components is presented. This logic is expressive enough for describing, first, the structure of hierarchical configurations and, second, dataflow both at signal and object level. It is sufficiently efficient for synthesis of large configurations and algorithms from their high-level specifications.

Automatic knowledge based program construction based on declarative description of ontology of a problem domain has been investigated. An algorithm for coding sequential programs by real numbers was developed together with a method of transforming a task for program synthesis (on a first-order computational model) into an optimisation problem. This is an inductive approach based on the idea to search for the optimal program from among all possible sequences of relations of the computational model using genetic programming techniques. Actually, the same computational models by Tõugu are used for specification of problem ontology that are utilised for knowledge representation in structural program synthesis (deductive approach). We believe that combining these two types of techniques might provide more general and effective procedures to automate software development. This would simulate human reasoning where deductive inference steps are interleaved with drawing conclusions from samples of experimental data.

A new architecture of the system for synthesising distributed programs for GRIDs was developed (Fig. 1). This research is motivated by utilisation and developing further existing paradigms (program synthesis using intuitionistic propositional calculus, Java language etc.) by increasing their performance via parallel computing.

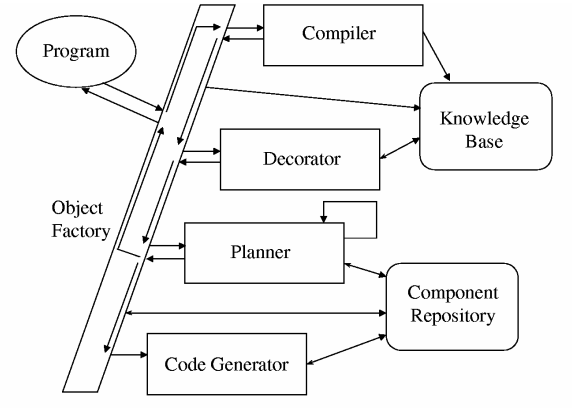

Fig. 1.
Modular structure of the distributed program synthesizer.

Co-operation partners: Royal Institute of Technology in Stockholm, Norwegian University of Science and Technology, Stanford University.

MULTIAGENT SYSTEMS

Theoretical studies aim at developing time-sensitive interaction-centred model of computation, the experimental studies focus on the development and assessment of pilot applications as multi-agent systems. Time models and time-sensitive ontologies of agents have been of prime interest. Interactive computations, roles of (intermediate) interaction were analysed in temporal aspects. Software architecture of time-aware agents was designed and implemented in C# for .Net. A generic collection of map agents has been implemented as a pilot application. Another prototype system – compiler agents for proactive translation – is under development.

Towards the fault-tolerant parallel computing models a fault-tolerant communication model for parallel computation package DOUG (Domain Decomposition on Unstructured Grids) has been developed. This prototype implantation has been successfully used in stability assessment of flow simulation with the Navier-Stokes equations.

Co-operation partners: University of Lübeck, University of Bath, Pennsylvania State University, University of Toulouse.

VERIFICATION OF HYBRID DYNAMIC SYSTEMS

New methods have been proposed for construction of finite models for first-order predicate formulas describing real-time systems. New techniques for proving non-derivability have been found and implemented in the automatic theorem proving system Gandalf. The continuously developing module of the abovementioned theorem prover won the yearly international contest of proving systems held as a part of the CADE-19 conference in Miami.

A representation of taxonomies has been developed that allows using an inference engine for classical logic for systems verification and solving queries in semantic web.

The first prototype system has been implemented that is able to extract facts and rules from the specifications of correctness of the systems and in several semantic web languages, translating them into first-order logic. The representation of taxonomies used allows to increase efficiency of inference engines if certain classes of subproblems are recognised in a particular context and the system can reuse the corresponding solution strategies.

Co-operation partners: Chalmers Technical University, Danish Technical University, Ålborg University.

Research team: Jaan Penjam (prof), Mait Harf, Merik Meriste, Leo Mõtus (prof), Tanel Tammet (prof), Enn Tõugu, Jüri Vain (prof), Eero Vainikko; Marko Kääramees; Juhan Ernits, Heiki Hiisjärv, Vadim Kimlaychuk, Vahur Kotkas, Andres Kull, Aleksander Petrov, Jelena Sanko, Raul Savimaa, Risto Serg, Konstantin Skaburskas (PhD students).

PUBLICATIONS

Fermüller, C. G., Leitsch, A., Hustadt, U., Tammet T. Resolution decision procedures. In: Robinson, A., Voronkov, A. (Eds.) Handbook of Automated Reasoning, 2. Elsevier and MIT Press, 1791-1847 (2001).

Graham, I. G., Spence A., Vainikko, E. Parallel iterative methods for Navier-Stokes equations and application to eigenvalue computation. Concurrence and Computation: Practice and Experience 15, 11-12, 1151-1168 (2003).

Küttner, R., Ernits, J., Vain, J. An open tool integration environment for manufacturing control software development. Machine Engineering 3, 1-2, 23-32 (2003).

Matskin, M., Tyugu, E. Strategies of stuctural synthesis and its extensions. Computing and Informatics 20, 1, 1-25 (2001).

Sanko, J., Penjam, J. Program construction in the context of evolutionary computation. In: Broy, M., Zamulin, A. V. (Eds.) Revised Papers from 5th Andrei Ershov Int. Conf. Perspectives of System Informatics, PSI 2003, Lect. Notes in Comp. Sci. 2980, 50-58 (2004).

Selic, B., Motus, L. Modeling of real-time software with UML. IEEE Control Systems Magazine 23, 3, 31-42, (2003).

Tammet, T., Kadarpik, V. Combining an interface engine with databases: a rule server. In: Schroeder, M., Wagner, G. (Eds.) Proc. of 2nd Int. Wksh. on Rules and Rule Markup Languages for the Semantic Web, RuleML 2003, Lect. Notes in Comp. Sci. 2876, 23-32 (2003).

The main goal of the research is to develop and analyze security solutions for electronic documents and databases, as well as to study theoretical limits of cryptographic security measures.

TIME STAMPS

Methods have been studied for producing reliable proofs that an electronic document was created at certain time, without assuming the presence of unconditionally secure third parties.

Main results: (i) It has been shown that construction of systems for proving the creation time of electronic documents (so called time-stamping schemes) in which the proofs are verifiable off-line is possible. (ii) Upper bounds for efficiency have been proved in several practical cases. (iii) A prototype-service for such a time-stamping scheme has been developed that accounts for all practical aspects related to such services. Hence, the applicability of such services has been proved in practice as well.

A large fraction of electronic data, in addition to cultural or esthetical value, also has an evidentialry value. Electronic data are sometimes used as proofs of events or facts. In order to guarantee the reliability of such proofs, data must be obtained from reliable sources and the origin of data should be verifiable (and sometimes provable).

Time stamps guarantee one aspect of reliability – the verifiability of creation time. A time stamp is a confirmation (or proof) that an electronic data item existed at certain time. The results obtained by the research group in the last five years show that such proofs are possible without involvement of trusted third parties. At the same time, the system still remains efficient enough for practical implementations.

Interesting theoretical results have been obtained about the limits of mathematically provable security properties of time-stamping schemes. It turns out that, without adding additional checking procedures to time-stamping systems, there exists no formal proofs that a time-stamping system is secure, based on collision-resistance of the cryptographic hash function used in the system.

SECURE DATABASES

It has been studied to what extent and how it is possible to protect data in databases, assumed that the holder of the database is not completely trustworthy.

Results: (i) It has been proved that one can construct secure databases that enable so called undeniable proofs. The holder of such a database cannot give contradictory replies to queries, so that the replies at the same time have correctly verifiable cryptographic codes.

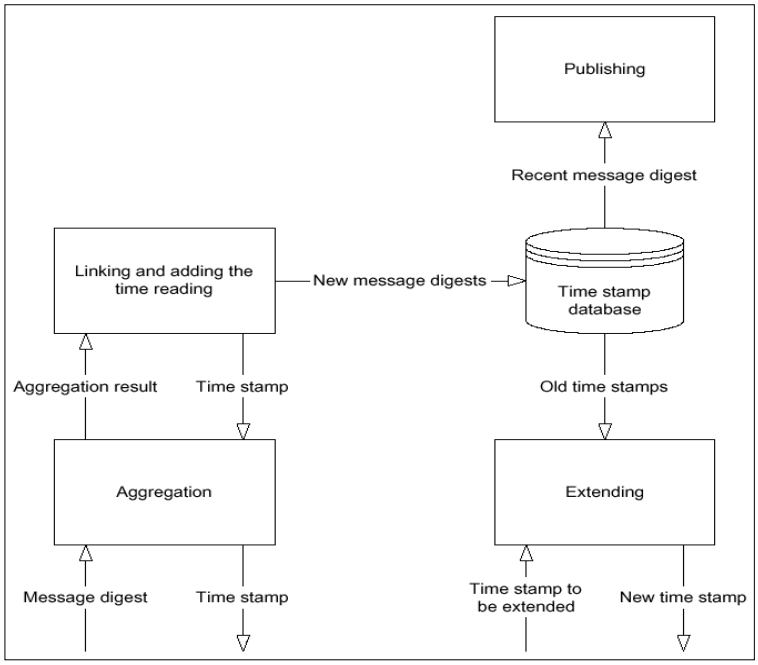

Figure 2.
General scheme of a time-stamping service that enables off-line verification.

(ii) A practical security solution has been developed, based on both the secure database and the time-stamping technologies.

The security of databases and registries does not mean just the aspect of confidentiality – data must be readable only for authorized persons – but also the aspect of integrity – a reply of the database to a query must be provably authentic and reflect the actual content of the database at the moment of receiving the query.

The necessary cryptographic protocols were developed two years ago by the researchers of this group. The security of the protocols was also proved using methods of computational complexity theory.

Theoretical results have been applied in the development of a practical database security solution X-road, which is widely used today in the Estonian public sector to facilitate co-operation of state-level databases and registers. The X-road system has received high grades and awards at international level.

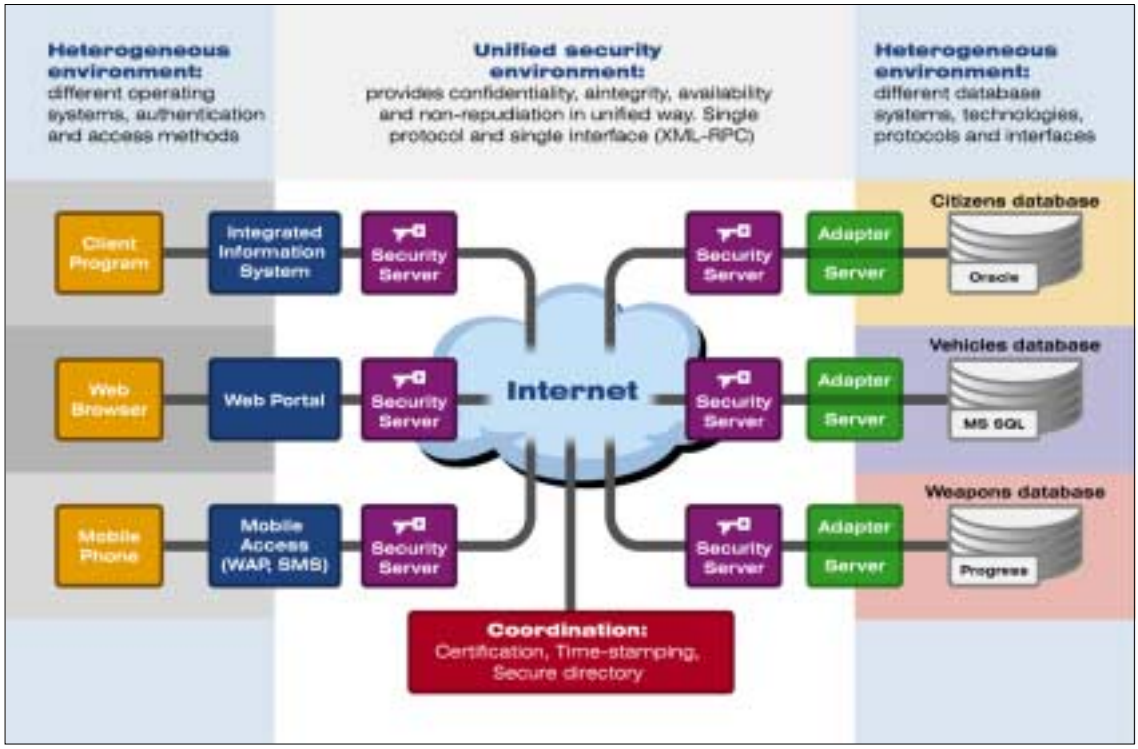

Fig. 3.
General scheme of the X-road secure database system.

Often, it is necessary that the authenticity of the reply stays verifiable for a certain period of time after its creation. For example, such a requirement is important, if the replies are used as legal documents. In addition to external threats (such as hackers) one must account for a possible misbehaviour of the database holder. Also the holder is capable of modifying records in the database, as well as reply to queries incorrectly.

The newest cryptographic methods enable us to set certain limits to the misbehaviour of database holders. Namely, they cannot give contradictory replies (with respect to certain semantics that the records of the database define).

Co-operation partners: Helsinki University of Technology.

Research team: Ahto Buldas, Peeter Laud Jan Willemson; Sven Laur, Meelis Roos, Jelena Zaitseva (PhD students).

PULICATIONS

Ansper, A., Buldas, A., Freudenthal, M., Willemson, J. Scalable and efficient PKI for inter-organizational communication. In: Proc. of Ann. Computer Security Appl. Conf., ACSAC 2003 IEEE CS Press (2003).

Ansper, A., Buldas, A., Saarepera, M., Willemson, J. Improving the availability of time-stamping services. In: Varadharajan, V., Mu, Y.

(Eds.) Proc. of 6th Australasian Conf. on Inform. Security and Privacy, ACISP 2001, Lect. Notes in Comp. Sci. 2119, 360-375 (2001).

Buldas, A., Laud, P., Lipmaa, H. Eliminating counterevidence with applications to accountable certificate management. J. of Computer Security 10, 3, 273-296 (2002).

Buldas, A., Laud, P., Lipmaa, H., Willemson, J. Time-stamping with binary linking schemes. In: Krawczyk, H. (Ed.) Proc. of 18th Ann. Int. Cryptology Conf., CRYPTO'98, Lect. Notes in Comp. Sci. 1462, 486-501 (1998).

Buldas, A., Lipmaa, H., Schoenmakers, B. Optimally efficient accountable time-stamping. In: Kim, K. (Ed.) Proc. of 4th Int. Wksh. on Practice and Theory of Public Key Cryptography, PKC 2000, Lect. Notes in Comp. Sci. 1751, 293-305 (2000).

DESIGN AND TEST OF DIGITAL SYSTEMS

The scientific goals of the research group are closely related to the most highly recognized guidelines for design and test solutions of "The MEDEA Design Automation Roadmap". MEDEA (Micro-Electronics Development for European Applications) is a part of the pan-European EUREKA network for cooperative R&D in computeraided design (CAD) and design automation. The team is involved in design and test of digital systems, self-testing and fault tolerance. The main objective of the research is to develop new efficient methods for modelling, design and test of digital systems to guarantee the efficiency, high quality and fault tolerance of systems in the conditions of ever increasing complexities. To achieve this target the team has competence in and is actively working on the following more specific problems: diagnostic models for digital systems, automation of test program generation, fault simulation and fault diagnosis in digital systems, physical defect oriented fault analysis, decompositional design and design error diagnosis in digital systems, analysis and partitioning methods for hardware / software codesign, and development of unified representation of systems for control and memory intensive applications.

MAIN RESULTS

A novel diagnostic model for digital systems based on decision diagrams (DDs) has been introduced into the theory of testing. The new model affords generalization of testing problems allowing uniform formal handling of systems on logic, procedural, functional as well as behavioural levels. Introduction of the new class of structurally synthesized binary DDs (SSBDDs), as well as discovering several interesting properties of SSBDDs afforded to increase the efficiency of algorithms for test generation, fault simulation, and fault diagnosis.

A new hierarchical approach to test generation for digital systems based on using the DD-model was proposed. Combining the high-level efficiency of solving complex deterministic search problems and medium-level accuracy of fault "transportation" analysis with low-level exact fault activation allowed to reach high efficiency and high quality in test generation.

A uniform approach to solving logic tasks of digital test was developed. The basis of this approach is the diagnostic model in form of structurally synthesized binary DDs (SSBDDs) that differently from the common BDDs preserve the structural features of gate-level circuits in the model. This feature made it possible to solve numerous logical tasks of a digital test like test generation, multi-valued simulation, timing simulation, and fault diagnosis at the macro level (instead of the gate level), which allowed to reduce the complexity of the model and to speed up the algorithms. Based on the SSBDD model the conception for a diagnostic software Turbo-Tester was developed and implemented as a set of different diagnostic tools: test generation, fault simulation, and testability analysis.

A new approach to increase the speed of high-level simulation of synchronous digital systems was developed based on using High-Level DDs

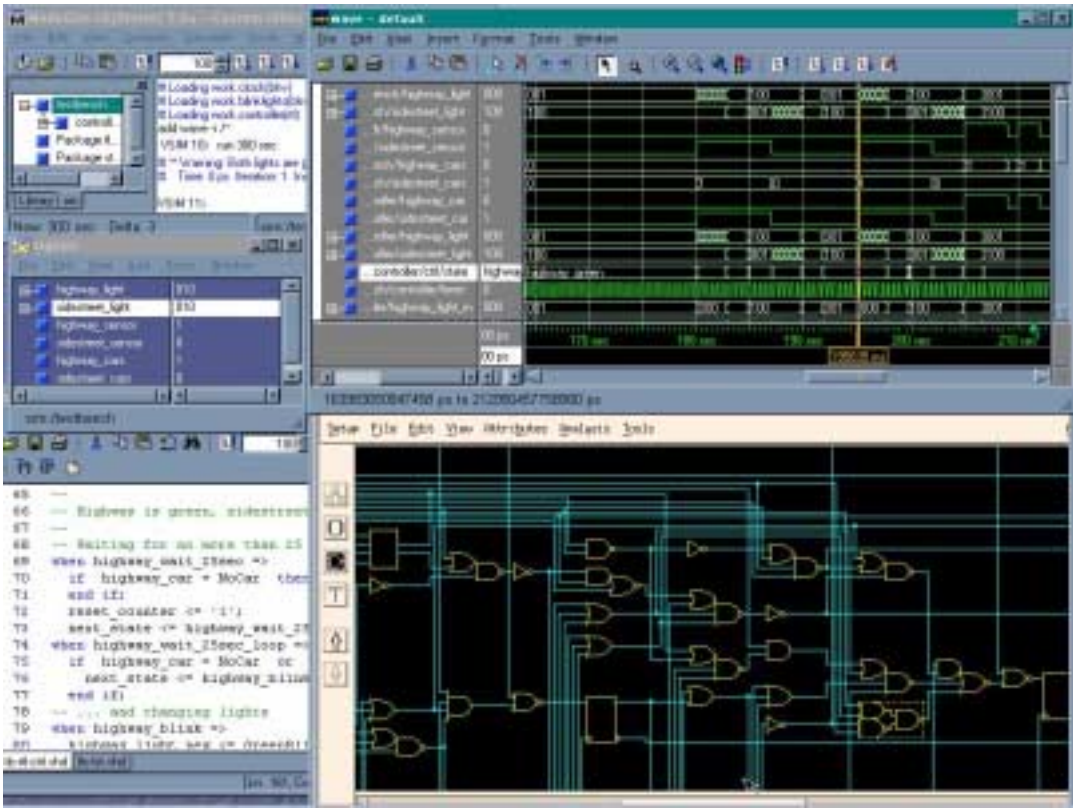

Fig. 4.
Modern environment for designing digital circuits.

(
HLDDs). HLDDs appear to be an efficient and compact representation of the system beha-viour for the high-level cycle-based simulation. In order to fully exploit the advantages of HLDDs new simulation algorithms combining forward event-driven and recursive back-tracing techniques have been proposed. Experimental results carried out on real case examples de-monstrated the gain in simulation performance of the proposed approach.

A new conception to defect oriented fault ana-lysis in digital systems has been developed. The new approach allows the first time to handle in a regular way the defects that increase the number of states in the circuit. By introducing the concept of functional faults, uniform met-hods for defect-oriented multi-level fault simu-lation and test generation were proposed. The new conception allows coping with the problem of creating high accuracy test patterns in the conditions of continuously increasing complexi-ties of digital systems.

New analysis and partitioning methods for HW/SW codesign were developed. They target control intensive applications, and allow more efficient partitioning than universal methods. The methods were used in the designing of a cryptographic processor. A prototype tool was implemented which incorporates the partitio-ning methods.

A new unified internal representation for control and memory intensive applications was develo-ped. The internal representation allows the analysis and synthesis tools to exchange infor-mation without loss of specification details. It is input language independent and allows hetero-geneous specification of digital systems. The first version of a prototype tool, which uses this internal representation, was implemented at KTH (Sweden). New methods are being added to the tool currently at TTU.

E-learning. A new conception of a training sys-tem for teaching design and test of electronic circuits was developed and implemented. A set of tools was designed for exercising design, test and diagnostics related problems in digital sys-tems. Access to the tools via Internet makes it easy for students from foreign universities to use the e-learning environment at any time in any place. At the present moment the set of test

tools developed by our group has been used in nearly 90 institutions from more than 30 countries worldwide.

Research team: Raimund Ubar (prof), Marina Brik, Peeter Ellervee, Margus Kruus, Jaan Raik, Aleksandr Sunditsõn, Kalle Tammemäe; Margit Aarna, Eero Ivask, Artur Jutman, Helena Kruus, Aimar Liiver, Elmet Orasson (PhD students).

PUBLICATIONS

Cibáková, T., Fischerová, M., Gramatová, E., Kuzmicz, W., Pleskacz, W., Raik, J., Ubar, R. Hierarchical test generation for combinational circuits with real defects coverage. J. of Microelectronics Reliability 42, 1141-1149 (2002).

Ellervee, P., Miranda, M., Catthoor, F., Hemani, A. System-level data-format exploration for dynamically allocated data structures. IEEE Trans. on CAD 20, 12, 1469-1472 (2001).

Oelmann, B., Tammemäe, K., Kruus, M., O'Nils, M. Automatic FSM synthesis for low-power mixed synchronous / asynchronous implementation. VLSI Design J. 12, 2, 167-186 (2001).

Ubar, R. Design error diagnosis with resyn-thesis in combinational circuits. J. of Electronic Testing: Theory and Appl. 19, 1, 73-82 (2003).

Ubar R., Raik, J. Testing strategies for net-works on chip. In: Jantsch, A., Tenhunen, H. Networks on Chip.. Kluwer Acad. Publ. 131-152 (2003).