TÖÖKINDLATE ARVUTISÜSTEEMIDE UURIMISE KESKUS

Juht prof Jaan Penjam
TTÜ Küberneetika Instituut, Akadeemia tee 21, 12618 Tallinn
Tel + 372 620 4150
Faks + 372 620 4151
jaan@cs.ioc.ee
http://cdc.ioc.ee/

UURIMISRÜHMAD

ARVUTITEADUSE MATEMAATILISED ALUSED JA PROGRAMMEERIMISKEELTE TEHNIKA
Juht dr Tarmo Uustalu
TTÜ Küberneetika Instituut
Akadeemia tee 21, 12618 Tallinn
Tel +372 620 4250
Faks +372 620 4151
tarmo@cs.ioc.ee

FORMAALMEETODID SÜSTEEMIARENDUSES
Juht prof Jaan Penjam
TTÜ Küberneetika Instituut
Akadeemia tee 21, 12618 Tallinn
Tel +372 620 4150
Faks +372 620 4151
jaan@cs.ioc.ee

INFOTURVE JA KRÜPTOGRAAFIA
Juht prof Ahto Buldas
Cybernetica AS
Akadeemia tee 21, 12618 Tallinn
Tel +372 665 4241
Faks +372 639 7992
ahtbu@cyber.ee

DIGITAALSÜSTEEMIDE DISAIN JA TESTIMINE
Juht prof Raimund-Johannes Ubar
TTÜ arvutitehnika instituut
Raja 15, 12618 Tallinn
Tel +372 620 2252
Faks +372 620 2253
raiub@pld.ttu.ee

Töökindlate Arvutisüsteemide Uurimise Keskus on erinevate teadusasutuste uurimisrühmade võrk, mis ühendab sarnaste uurimiseesmärkidega teadlasi. Keskusesse ühendatud uurimisrühmad kujutavad endast juba aastaid *de facto* koos töötanud uurijate võrku, mis sõltuvalt finantsoludest ja teaduspoliitilisest taustast on teinud koostööd üleriigiliste seminaride vormis, arvutiteadusliku hariduse arendamise sildi all (TEMPUS-projektid) või rahvusvaheliste talvekoolide korraldamisel. Tippkeskuse moodustamine uurimisrühmade võrgustiku kujul võimaldas ühistegevust süsteemsemalt korraldada ning selle kaudu ka efektiivsemaks muuta. Keskusel on fikseeritud ning töörühmade baasasutustega kooskõlastatud uurimisplaan.

Keskuse koosseisu kuuluvad teadlased järgmistest teadusasutustest:

- TTÜ Küberneetika Instituut (IoC),
- TTÜ arvutiteaduse instituut (CS/TTU),
- TTÜ automaatika instituut (CC/TTU),
- TTÜ arvutitehnika instituut (CE/TTU),
- TÜ arvutiteaduse instituut (CS/UT),
- TÜ Tehnoloogiainstituut (TUIT),
- Cybernetica AS (CybAS).

Keskuse tööd koordineerib juhatus, kuhu kuuluvad töörühmade juhid ja Keskuse juht.

Tegevuse süstemaatiliseks rahvusvaheliseks hindamiseks ning temaatikaalaseks nõustamiseks on keskusel juhtkomitee, mille moodustavad neli tunnustatud Euroopa teadlast: prof Reino Kurki-Suonio, Tampere Tehnoloogiaülikool, Soome; prof Kim G. Larsen, Ålborgi Ülikool, Taani; prof Reinhard Wilhelm, Saarimaa Ülikool, Saksamaa; prof José Oliveira, Minho Ülikool, Braga, Portugal.

UURIMISTÖÖ PLAANID LÄHIAASTATEKS

Keskuse uurimistööde teemad käesoleval hetkel valdkondade kaupa on järgmised:

ARVUTITEADUSE MATEMAATILISED ALUSED JA PROGRAMMEERIMISKEELTE TEHNIKA

- (Ko)induktiivsete tüüpide ja (ko)rekursiooniskeemide uurimine tüübi- ja kategooriateoreetiliste vahenditega.
- Intermediaar- ja modaalloogikate algebraline ja kategoorne semantika ning nende rakendused programmikeeltes.
- Tõestusteoreetilised uurimused konstruktiivsest hulgateooriast, Martin-Löfi tüübiteooriast ja eksplitsiitsest matemaatikast.
- Abstraktse interpretatsiooni põhiste staatilise analüüsi ja abstraktse testimise meetodite arendamine.
- Programmiteisendused tugevate funktsionaalkeelte jaoks, eriti deforesteerimine.

- Meetodite arendamine magasinikoodi valideerimiseks ja tüübikontrolliks magasinipõhistes keeltes.

FORMAALMEETODID SÜSTEEMIARENDUSES

- Programmide struktuurse sünteesi meetodi arendamine hajusarhitektuuriga arvutisüsteemidele.
- Programmide sünteesi erinevate meetodite (deduktiivne, induktiivne ja transformatsiooniline süntees) integreerimine.
- Automaatne teoreemitõestamine, rakendused riistvara verifitseerimises.
- Deduktiivseid ja algoritmilisi tehnikaid kombineerivate formaalse spetsifitseerimise ja verifitseerimise meetodite väljatöötamine.
- Formaalse verifitseerimise meetodite ühendamine süsteemide kasvu toetavate meetoditega.
- Ajatundlikud interaktsioonikesksed arvutusmudelid süsteemide temporaalsete omaduste ja käitumise uurimiseks.

INFOTURVE JA KRÜPTOGRAAFIA

- Efektiivsete meetodite väljatöötamine avaliku võtme levituseks ja sertifikaatide kehtivuse kontrolliks sidus- (*on-line*) ja vallasrežiimis (*off-line*).
- Meetodite väljatöötamine avalikest andmebaasidest ja registritest turvaliste ja auditeeritavate päringute realiseerimiseks.
- Ajatembeldamisskeemi turvalisuse formaalne definitsioon ja seosed traditsiooniliste krüptograafiliste primitiividega.

DIGITAALSÜSTEEMIDE DISAIN JA TESTIMINE

- Füüsikaliste defektide ja loogikarikete modelleerimise uute meetodite väljatöötamine, suurendamaks keerukate digitaalsüsteemide testimise kvaliteeti.
- Digitaalsüsteemide uute hierarhiliste diagnostikamudelite ja testide genereerimise, rikete analüüsi ning disainivigade ja rikete diagnoosi efektiivsemate meetodite ja algoritmide väljatöötamine.
- Efektiivsemate disaini meetodite väljatöötamine, võttes aluseks uued paradigmad "kiipsüsteemide disain, riist- ja tarkvara koosdisain" ning orienteerudes uutele disainikriteeriumitele, nagu "hästitestitavad süsteemid" ja "isetestivad süsteemid".

Teadustöö efektiivsust on oluliselt suurendanud osalemine reas rahvusvahelistes projektides ja programmides. Keskuse töörühmad osalevad viies EÜ 5. raamkava projektis:
EÜ 5RP temaatiline võrgustik IST-2001-38957 APPSEM II;

EÜ 5RP temaatiline võrgustik IST-2001-33123 CoLogNet;

EÜ 5RP kaasnevate meedete projekt IST-2001-37592 eVikings II;

EÜ 5RP kaasnevate meedete projekt IST-2000-30193 REASON;

EÜ 5RP kaasnevate meedete projekt IST-2001-35174 OpenEvidence.

Keskuse üheks olulisemaks eesmärgiks on arvutiteaduse alase kraadiõppe efektiivsuse parandamine. Regulaarselt viiakse läbi rahvusvahelisi talve- ja suvekoole kursustega maailma tippteadlastelt. Samuti organiseeritakse süstemaatiliselt üleriigilisi seminare (arvutiteaduse teooriapäevad, formaalmeetodite seminarpäevad jms) ning meistriklasse kutsutud välisõppejõududega.

Aastatel 1998–2002 kaitsti järgmised doktoritööd: S. Tupailo (Stanford U., 1998), T. Uustalu (KTH, 1998), A. Buldas (TTÜ, 1999), H. Lipmaa (TÜ, 1999), V. Vene (TÜ 2000), P. Ellervee (KTH, 2000), O. Sokratova (TÜ, 2001), J. Raik (TTÜ, 2001), A. Kuusik (TTÜ, 2001), J. Willemson (TÜ, 2002), P. Laud (U. des Saarlandes, 2002), M. Brik (TTÜ, 2002). Praegu on keskuse liikmete juhendamisel 24 doktoranti.

ARVUTITEADUSE MATEMAATILISED ALUSED JA PROGRAMMEERIMISKEELTE TEHNIKA

Uurimisgrupi põhilisteks teadussuundadeks on loogika ja algebra kui teoreetilise arvutiteaduse alusdistsipliinid ning programmeerimiskeelte teooria (semantika, disain, realiseerimine). Konkreetsemalt on uurimisvaldkondadeks struktuurne tõestusteooria ja tüübiteooria, kategoorne loogika, ordinaalanalüüs, algebraline kombinatoorika, poolringide teooria ja algebraline automaaditeooria, programmikeelte semantika ja realisatsioon, programmianalüüs, sh tüübipõhised analüüsid, programmide semantikapõhine teisendamine, turvalisus programmikeeltes.

OLULISEMAID TULEMUSI

On saavutatud rida uusi tulemusi induktiivsete ja koinduktiivsete tüüpide ning monaadide ja komonaadide teoorias rakendustega süntaksi ning kõrvalefektidega arvutuste esitamise ja nende üle arutlemise modulariseerimiseks ning tüübipõhise termineeruvuse alal. On formuleeritud komonaadi ja jaotuvusseadust kasutav uudne struktuurne rekursiooniskeem, mis võimaldab rida hästituntud standardskeeme käsitleda ühe geneerilise skeemi erijuhtudena. On uuritud nn Mendleri-laadi struktuurseid rekursiooniskeeme, kus defineeritava funktsiooni totaalsuse (programmi termineeruvuse) tagab rekursiooni-operaatori polümorfne tüüp. On antud oluline üldistus Adámeki ja kolleegide teoreemile mittefundeeritud termialgebratest kui vabadest täielikult iteratiivsetest monaadidest. On uuritud induktiivseid ja koinduktiivseid tüüpe toetavate keelte jätkustiili ja monaadilist tõlgitavust. On uuritud sidujatega süntaksi esitamise ja manipuleerimise probleeme ning antud eksplitsiitse substitutsiooni uudne käsitlus. On leitud püsipunktiteoreetiline konstruktsioon kahe ideaalse monaadi koprodukti arvutamiseks, mis võimaldab arvutada nt mittedeterminismile ja tõenäosuslikule valikule vastavate monaadide kombinatsiooni.

On esitatud turvalise infovoo uudne definitsioon, kus aluseks on avalike väljundite arvu-

8. Eesti Arvutiteaduse Talvekoolist (EWSCS'03 Palmses).

tuslik (mitte informatsiooniteoreetiline) sõltumatus salajastest sisenditest, ning arendatud sellel põhinevaid programmianalüüse. On näidatud, kuidas turvalise infovoo analüüsi teha krüptimistehtega keele puhul ning kuidas analüüsida suhtelist salajasust, mille puhul programmi osade väljundite suhtes lähtutakse eeldusest, et need on mittesalajased.

On välja töötatud meetod mitmelõimeliste programmide täpseks staatiliseks analüüsiks, mis väldib olekuruumi plahvatust, kasutades globaalinvariante, ning realiseeritud vastav prototüüp avioonikas kasutatava tarkvara valideerimiseks.

On näidatud mitme konstruktiivse matemaatilise alusteooria (konstruktiivse hulgateooria, Martin-Löfi tüübiteooria) realiseeritavus Fefermani eksplitsiitsesse matemaatikasse.

On uuritud termiümberkirjutamist poolringidel ning algebralist automaaditeooriat.

Grupp on alates sügisest 2002 kaks korda aastas toimuvate Eesti arvutiteaduse teooripäevade mootoriks. 2004. a toimuvad Eestis uurimisgrupi korraldamisel IST TN APPSEM II 2nd Annual Meeting, APPSEM 2004 (Tallinn, 14.–16.4.2004) ja 5th International Summer School and Workshop on Advanced Functional Programming, AFP 2004 (Tartu, 16.–21.8.2004).

Koostööpartnerid: Müncheni Ülikool, INRIA Sophia Antipolis, Minho Ülikool, Leicesteri Ülikool, Nottinghami Ülikool, Saarimaa Ülikool, Trieri Ülikool, Calgary Ülikool, Leedsi Ülikool.

Koosseis: Tarmo Uustalu (vanemteadur,), Peeter Laud (vanemteadur), Jaanus Pöial (dotsent), Olga Sokratova (vanemteadur), Mati Tombak (prof), Sergei Tupailo (vanemteadur), Varmo Vene (vanemteadur); Reimo Palm (teadur); Härmel Nestra, Ahti Peder, Tiina Zingel (doktorandid).

PUBLIKATSIOONE

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).

FORMAALMEETODID SÜSTEEMIARENDUSES

Keerukatele süsteemidele esitatavate töökindlusenõuete rahuldamiseks ja produktiivsuse saavutamiseks süsteemide realiseerimisel vajatakse nii meetodeid korrektsete programmide saamiseks kui ka efektiivseid tarkvaratehnikaid. Formaalne tõestusteooria on aluseks kahele erinevale korrektse tarkvara loomise mudelile: programmide automaatne genereerimine tema spetsifikatsioonist ja verifitseerimine (tõestatakse programmi vas-

tavus spetsifikatsioonile). Praktikas kasutatakse nende kahe vastandliku lähenemise mitmesuguseid kombinatsioone.

Töörühma eesmärgiks on uurida loogikal, algebral ja süsteemiteoorial põhinevaid programmide omaduste tõestamise ja programmide sünteesi meetodeid, samuti arendada automaattõestuse tehnikaid. Aktuaalne on meetodite ja vahendite loomine nii transformatsiooniliste kui reaktiivsete (reaalaja-) süsteemide arendamiseks.

Sard- ja hajutatud süsteemide kiire areng tingib arvutiteaduses uute, mittelineaarsel ajal baseeruvate meetodite arendamise. Reaalsed arvutisüsteemid töötavad tihti muutuvas keskkonnas (interaktsioonis keskkonnaga), mille kogu dünaamikat ei ole võimalik süsteemi projekteerimisel ette näha. Keerukamate aja mudelite kasutuselevõtt on vältimatu eeltingimus selliste süsteemide omaduste verifitseerimisel. Töörühm on muuhulgas keskendunud nii interaktiivsete arvutuste mudelitele üldiselt kui ka nn ajatundlike agentsüsteemide formaalsele kirjeldamisele ja analüüsile.

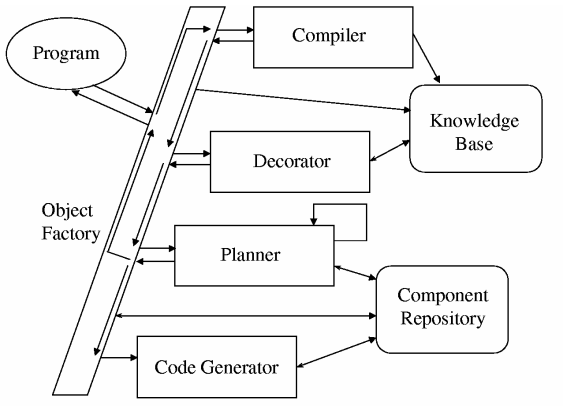
Töörühma kompetents langeb valdkondadesse, nagu tõestusteooria ja teoreemide automaatne tõestamine, mudelite teooria ajaga ja hübriid-automaadid, kompositsiooniline programmide verifitseerimine, konstruktsiooniga tagatud korrektsus, tarkvara ajastamisprobleemide formaalne analüüs ning rakendusvaldkonnad, nagu näiteks masinaehitus ja automaatjuhtimine.

PROGRAMMIDE SÜNTEES

Esitatud on üldine formaalloogiline meetod arvutuste semantika spetsifitseerimiseks, mis kasutab osistena kas tarkvara või riistvara komponente. Kasutatav loogikaarvutus on küllalt väljendusrikas, et esitada samaaegselt süsteemide hierarhilist struktuuri ja andmevoogu nii signaali kui objekti tasandil. Meetod on küllalt võimas genereerimaks keerukaid konfiguratsioone ja algoritme kõrgtaseme spetsifikatsioonide põhjal.

Edasi on arendatud meetodeid programmide automaatseks konstrueerimiseks algoritmide probleemvaldkonna ontoloogia formaalse kirjelduse põhjal. Töötati välja algoritm esimest järku arvutusmudeli relatsioonidest moodustatud järjestikprogrammide kodeerimiseks reaalarvudega ning meetod programmide sünteesi ülesande taandamiseks (stohhastilise) optimeerimise ülesandele. Lähenemise aluseks on idee valida kõigi arvutusmudelil genereeritavate programmide hulgast optimaalseim, kasutades diferentsiaalevolutsiooni meetodit (induktiivset programmide sünteesi). Ontoloogia spetsifitseerimiseks kasutatavad arvutusmudelid on samad, mida kasutatakse ülesannete kirjeldamiseks Enn Tõugu struktuurse programmide sünteesi korral ning see asjaolu loob aluse induktiivse ja deduktiivse meetodi kooskasutamiseks programmide konstrueerimisel.

Välja on töötatud hajusprogrammide süntesaatori arhitektuur, mis võimaldaks sünteesitud programmide käivitamist arvutikobaratel (vt programmisünteesi süsteemi moodularhitektuuri joonis 1). Töö motivatsiooniks on olemasolevate paradigmade (intuitsionistliku lauseloogika abil programmide genereerimine, Java programmeerimiskeel) edasiarendamine, et kasvatada nende jõudlust paralleelarvutust kasutades.



Joonis 1.
Hajusprogrammide süntesaatori moodulstruktuur.

Koostööpartnerid: Rootsi Kuninglik Tehnoloogiaülikool, Norra Teaduse ja Tehnoloogiaülikool, Stanfordi Ülikool.

MULTIAGENTSÜSTEEMID

Töö eesmärgiks on ajatundliku interaktsioonikeskse arvutusmudeli väljatöötamine ning eksperimendid pilootrakenduste omaduste uurimiseks. Analüüsitud on ajatundlike multiagentide ajamudeleid ning koostatud ajatundliku interaktiivse arvutuse formaalne mudel – voopõhine atribuutautomaat. Projekteeritud on ajateadlike agentide tarkvaraarhitektuur ning realiseeritud vastav instrumentaaltarkvara (keeles C# .Net keskkonnas). Pilootrakendusena on realiseeritud kaardiagentide geneeriline pere ning teostamisel on proaktiivsete transleerimisagentide uurimisprojekt.

Tõrkekindlate paralleelarvutuse mudelite uurimiseks on arendatud edasi paralleelarvutuste paketti DOUG (*Domain Decomposition on Unstructured Grids*). Paketti on edukalt katsetatud Navier-Stokesi vooluvõrrandite stabiilsusarvutuste realiseerimisel.

Koostööpartnerid: Lübecki Ülikool, Bathi Ülikool, Pennsylvania Osariigi Ülikool, Toulouse'i Ülikool.

HÜBRIIDSETE DÜNAAMILISTE SÜSTEEMIDE VERIFITSEERIJMINE

Leiti meetodid lõplike mudelite ehitamiseks reaalaja süsteeme kirjeldatavatele esimest järku predikaatarvutuse valemitele, töötati välja uued mittetõestatavuse näitamise meetodid. Loodud meetodid realiseeriti teoreemitõestamissüsteemis Gandalf. Antud töö käigus valminud ja pidevalt täiustatav moodul nimetatud teoreemitõestamissüsteemis võitis vastava ülesanneteklassi iga-aastasel rahvusvahelisel teoreemitõestajate võistlusel konverentsi CADE-19 raames Miamis USAs.

Töötati välja mehhanism taksonoomiate esitamiseks ja kasutamiseks klassikalise teoreemitõestamise kontekstis, mis on vajalik järeldusmootorite efektiivseks kasutamiseks verifitseerimisülesannete ja semantilise veebiga seotud ülesannete lahendamisel.

Realiseeriti esimene prototüüpsüsteem, mis suudab mõista fakte ja reegleid süsteemide korrektsust kirjeldavates spetsifikatsioonides ja mitmes erinevas semantilise veebi keeles, teisendades neid esimest järku loogikasse. Kasutatav taksonoomiate esitamise meetod võimaldab tõsta järeldusmootorite efektiivsust juhul, kui konkreetses kontekstis on äratuntavad kindlad alamülesannete klassid, ja valida neile vastavad lahendusstrateegiad.

Koostööpartnerid: Chalmersi Tehnikaülikool, Taani Tehnikaülikool, Ålborgi Ülikool.

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

PUBLIKATSIOONE

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).

INFOTURVE JA KRÜPTOGRAAFIA

Uurimistöö põhieesmärk on elektrooniliste dokumentide ja andmebaaside turvalahenduste loomine ja analüüs, samuti teoreetilised piirid turvalisuse saavutamisel krüptograafia meetoditega.

AJATEMPLID

On uuritud meetodeid, kuidas tagada usaldusväärne tõestus mingi elektroonilise dokumendi loomise aja kohta, eeldamata seejuures tingimusteta turvaliste osapoolte olemasolu.

Põhitulemused: (i) On näidatud, et saab konstrueerida elektrooniliste dokumentide loomisaja tõestamise süsteeme (nn ajatempliskeeme), milles ajatõestust saab kontrollida vallasrežiimis (*off-line*) ja (ii) tõestatud ajatempliskeemide efektiivsuse ülempiirid mitmel praktilisel juhul. (iii) On loodud aja-templiteenuse prototüüp, milles on arvestatud kõiki teenusega seotud praktilisi aspekte, mis kinnitab ajatemplialase teooria praktilist rakendatavust.

Suur osa elektroonilisi andmeid omab lisaks muudele väärtustele (kultuuriline, esteetiline jne) ka tõestusväärtust, st andmeid võidakse kasutada mingi aset leidnud sündmuse tõendamiseks. Selleks, et tagada tõendi usaldusväärsust, peab tõend pärinema autoriteetsest allikast ja selle pärinevust nimetatud allikast peab saama kontrollida ja vahel ka tõestada.

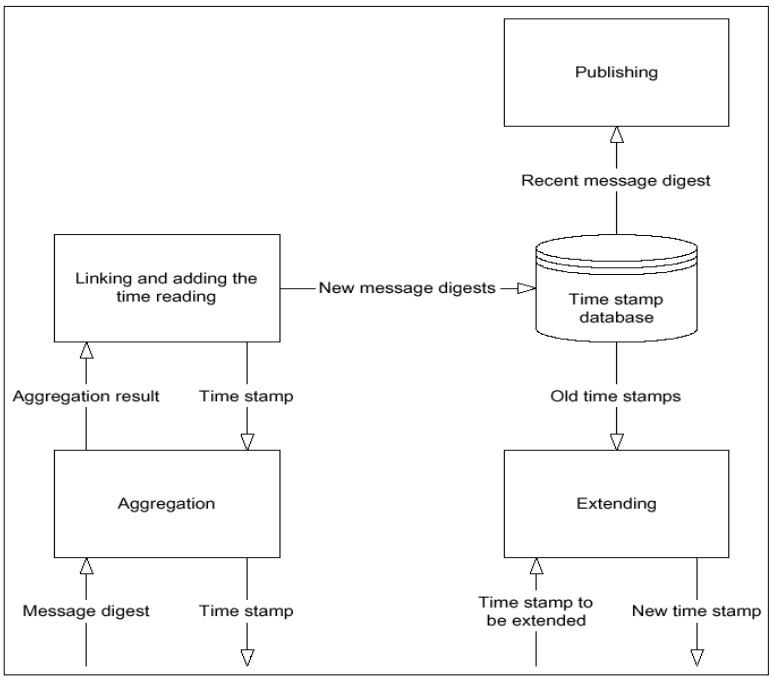
Ajatemplid tagavad dokumendi usaldusväärsuse üht aspekti – nad on mõeldud dokumendi loomise aja tõestamiseks. *Ajatempel* on elektroonilisel viisil salvestatud kinnitus (tõestus), et mingid andmed olid olemas mingil ajal. Uurimisgrupi poolt viimase viie aasta jooksul ajatemplite alal tehtud töö näitab, et aja tõestamine on võimalik praktiliselt ilma usaldatud osapooli (st nende tunnistusi) kasutamata, kaotamata seejuures tehnilist efektiivsust.

On saadud ka huvitavaid teoreetilisi tulemusi, mis selgitavad ajatempliskeemide turvalisuse matemaatilise tõestatavuse piire. Selgub, et vastupidiselt erinevate teoreetikute seas laialt levinud arvamusele, ei saa ajatemplisüsteemide turvalisust formaalselt tõestada, lähtudes kasutatava krüptograafilise räsifunktsiooni kollisioonivabaduse (*collision-resistance*) omadusest.

TURVALISED ANDMEBAASID

On uuritud, mil määral ja kuidas on võimalik andmebaasides olevaid andmeid kaitsta, eeldusel, et andmebaasi pidaja ei ole täielikult usaldatav.

Põhitulemused: (i) On tõestatud, et saab konstrueerida nn vaidlustamatuid tõestusi võimaldavaid turvalisi andmebaase, mille halduril ei ole võimalik esitada üksteisega vastuolus olevaid ja samas krüptograafiliselt kor-



Joonis 2.
Vallasrežiimis kontrolli võimaldava ajatempliteenuse üldskeem.

rektseid päringuvastuseid. (ii) On loodud andmebaaside ühendamiseks vajalik praktiline turvalahendus, millesse on integreeritud nii ajatempli- kui ka turvalise andmebaasi tehnoloogia.

Andmebaaside ja registrite turvalisuse all ei mõelda mitte ainult konfidentsiaalsuse aspekti – andmed on kättesaadavad ainult volitatud subjektidele – vaid ka tervikluse aspekti – andmebaasist tehtava päringu vastus peab olema tõestatavalt autentne, st peegeldama andmebaasi tegelikku seisu vastuse moodustamise hetkel.

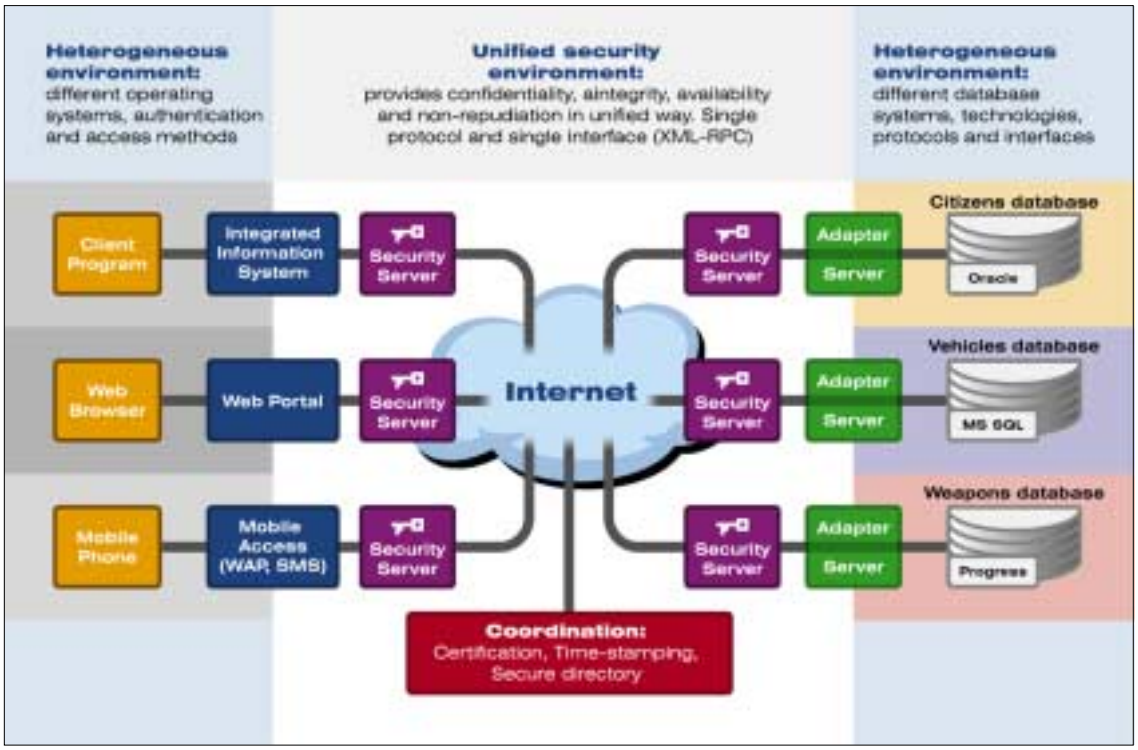
Sageli on ka vajalik, et päringuvastuse autentsus oleks tuvastatav teatud aja jooksul pärast selle moodustamist. Viimane on vajalik näiteks siis, kui päringuvastuseid kavatsetakse kasutada juriidiliste dokumentidena. Lisaks välistele ohtudele (näiteks häkkerid) tuleb arvestada ka andmebaasi halduri enda väärkäitumist. Ka haldur võib volitamatult muuta andmeid ja muuta need tegelikkusele mittevastavaks, samuti ka vastata päringutele ebakorrektselt.

Uusimad krüptograafilised meetodid võimaldavad saavutada olukorda, kus registripidaja ei saa esitada (teatud konteksti mõttes) vastuolulisi andmeid. Vajalikud krüptograafilised protokollid ja meetodid esitati esmakordselt kaks aastat tagasi uurimisgrupi teadlaste poolt ja tõestati ka nende turvalisus, kasutades algoritmide keerukusteooria meetodeid.

Teoreetilised lahendused on realiseeritud praktilises süsteemis (X-tee), mis on mõeldud erinevate riiklike andmebaaside koostöö tagamiseks. Nimetatud süsteem on töös juba üle aasta ning on pälvinud kõrgeid hinnanguid rahvusvahelistelt tehnoloogiakonkurssidelt.

Koostööpartner Helsingi Tehnikaülikool.

Koosseis: Ahto Buldas (vanemteadur), Peeter Laud (vanemteadur), Jan Willemson (vanemteadur); Sven Laur, Meelis Roos, Jelena Zaitseva (doktorandid).



Joonis 3.
Turvalise andmebaasisüsteemi rakenduse X-tee üldskeem.

PUBLIKATSIOONE

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).

DIGITAALSÜSTEEMIDE DISAIN JA TESTIMINE

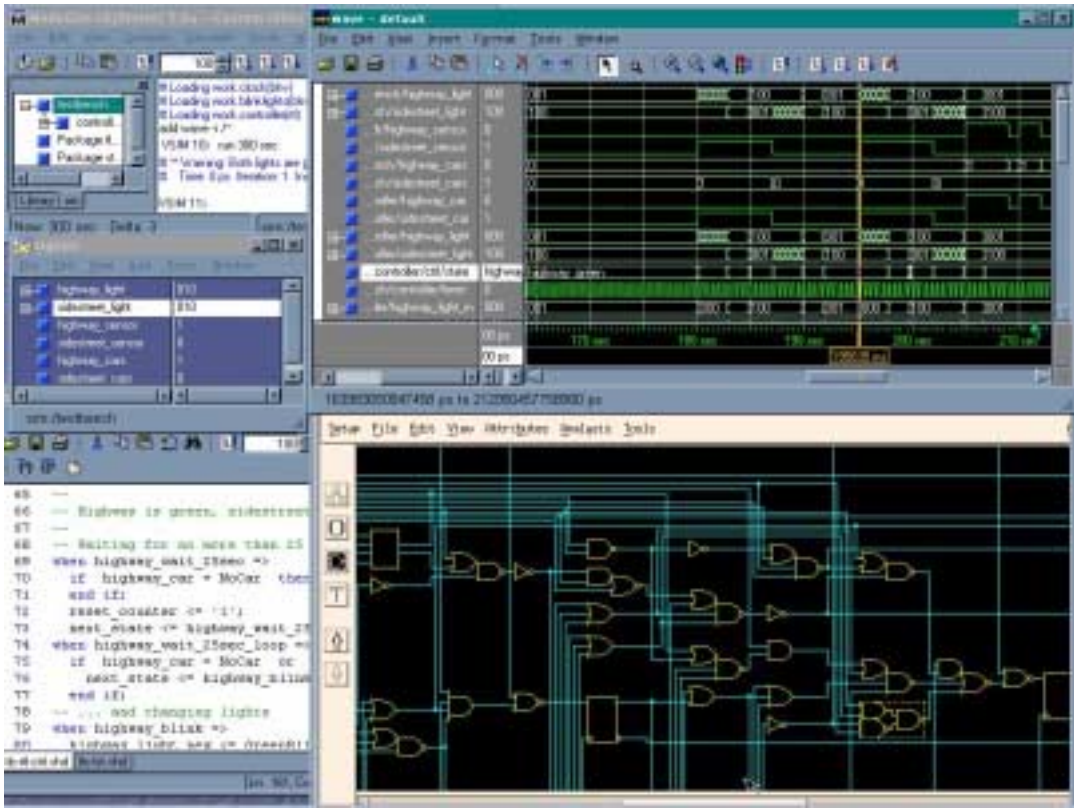
Digitaalsüsteemide disaini ja testimise uurimisgrupi (DT) teaduslikud eesmärgid on otseselt kooskõlas projekteerimise ja testi alaste juhtnööridega, mis on esitatud MEDEA visioonis *("The MEDEA Design Automation Roadmap")*. MEDEA (*Micro-Electronics Development for European Applications*) on osa üleeuroopalisest EUREKA võrgustikust, mis tegeleb digitaalsüsteemide projekteerimise alase teaduskoostööga. Grupi uurimissuundadeks on digitaalsüsteemide projekteerimine ja test, isetestivad arhitektuurid ja tõrkekindlad süsteemid. Uurimistöö on suunatud uute efektiivsete meetodite väljatöötamisele digitaalsüsteemide modelleerimiseks, projekteerimiseks ja testiks eesmärgiga tagada pidevalt kasvava keerukusega süsteemide efektiivsus, kvaliteet ja tõrkekindlus. DT grupp omab kompetentsust ning tegeleb aktiivselt järgmiste probleemidega: digitaalsüsteemide diagnostilised mudelid, testprogrammide genereerimise automatiseerimine, rikkesimuleerimine ja diagnostika, füüsikaliste defektide analüüs, dekompositsiooniline projekteerimine, projekteerimisvigade diag-noos, analüüsi- ja tükeldusmeetodid riist-/ tarkvara koosdisainis ning valdavalt mälu- ja juhtosa sisaldavate süsteemide ühtlustatud modelleerimine.

OLULISEMAID TULEMUSI

On välja töötatud uudne diagnostiline mudel, mis põhineb otsustusdiagrammide (*decision diagrams, DD*) kasutamisel testiteoorias. Mudel võimaldab üldistada diagnostikaprobleeme, lubades ühtlustatud süsteemikäsitlust loogikatasemel, protseduursel, funktsionaalsel ning käituvuslikul tasemel. Pakuti välja uudne mudel – struktuurselt sünteesitud binaarsed otsustusdiagrammid (*structurally synthesized binary DD* ehk *SSBDD*) koos omadustega, mis võimaldavad tõsta testigenereerimise, rikkesimuleerimise ja -diagnostika algoritmide jõudlust.

On välja pakutud uudne hierarhiline lähenemine digitaalsüsteemide testigenereerimisele, mis põhineb DD mudeli rakendamisel. Kombineerides keerukate determineeritud otsingualgoritmide jõudluse kõrgtasemel, rikkelevitamistäpsusega kesktasemel ning madaltaseme rikete aktiveerimise täpsuse, saavutati kõrge kvaliteet ja efektiivsus testide genereerimisel.

On välja töötatud ühtlustatud lähenemine testiprobleemide lahendamiseks loogikatasemel. Lähenemine põhineb SSBDD diagnostikamudelil, mis erinevalt traditsioonilistest binaarsetest otsustusdiagrammidest lubavad säilitada skeemi struktuurset informatsiooni. Nimetatud omadus võimaldas leida mitmetele loogikataseme testiprobleemidele, nagu testigenereerimine, mitmeväärtuseline simuleerimine, viitesimuleerimine ja rikkediagnoos, tõhusa lahenduse, kus loogikalülide asemel kasutati kõrgemat makrotaset, mis omakorda tõstis algoritmide töökiirust. SSBDD mudeli kontseptsioonile toetudes töötati välja testitarkvara pakett Turbo-Tester, mis sisaldab programme testigenereerimiseks, rikkesimuleerimiseks ja testitavuse analüüsiks.



Joonis 4.
Digitaalskeemi kaasaegne projekteerimiskeskkond.

On välja töötatud uudne lähenemine kõrgtaseme simuleerimise kiirendamiseks sünkroonsetele digitaalsüsteemidele, kasutades kõrgtaseme otsustusdiagrammide (HLDD) mudelit. HLDD osutusid kompaktseks ning efektiivseks mudeliks kõrgtaseme taktipõhiseks simuleerimiseks. Selleks, et HLDD eeliseid ära kasutada, töötati välja algoritmid sündmuspõhiseks ja rekursiivseks simuleerimiseks nimetatud mudelil. Eksperimendid, mis viidi läbi realistlikel katseskeemidel, tõestasid lähenemise efektiivsust.

On välja töötatud uudne kontseptsioon defektorienteeritud rikkeanalüüsiks digitaalsüsteemidele. Lähenemine lubas esimest korda traditsioonilistel meetoditel käsitleda rikkeid, mis suurendavad olekute arvu skeemis. Funktsionaalse rikkekontseptsiooni tõttu saab kasutada ühtlustatud meetodeid defektorienteeritud mitmetasemeliseks rikkesimuleerimiseks ja testigenereerimiseks. Uus kontseptsioon võimaldab genereerida kõrge kvaliteediga testvektoreid üha kasvava skeemikeerukuse juures.

On välja töötatud uudsed analüüsi- ja tükeldusmeetodid riist- ja tarkvara koosdisainiks. Meetodid võimaldavad efektiivsemat tükeldust domineerivalt mälu- ja juhtosa sisaldavatele süsteemidele kui senikasutatud universaalsed algoritmid. Nimetatud meetodeid kasutati krüptograafilise mikroprotsessorkiibi väljatöötamisel. Realiseeriti prototüüptarkvara, mis sisaldab uudseid tükeldusmeetodeid.

On välja töötatud uudne ühtlustatud sisekuju valdavalt mälu- ja juhtosa sisaldavatele süsteemidele. Sisekuju võimaldab analüüsi- ja sünteesivahenditel vahetada informatsiooni ilma kadudeta spetsifikatsiooni detailides. Kuju on sõltumatu sisendkeelest ning toetab digitaalsüsteemide heterogeenset kirjeldamist. Esimene versioon prototüüptarkvarast, mis kasutab nimetatud sisekuju, realiseeriti Stockholmi Kuninglikus Tehnikaülikoolis. TTÜs töötatakse välja uusi meetodeid ja täiendusi prototüüpprogrammile.

E-õpe. On välja töötatud ning realiseeritud uudne kontseptsioon elektroonikaskeemide testi ja projekteerimise õpetamiseks. Valmis

töövahendite komplekt projekteerimise, testi ja diagnostika harjutuste läbiviimiseks. Töövahendid on interneti teel kättesaadavad, mis võimaldab välisülikoolidel e-õppe keskkonnale ligi pääseda sõltumata kohast ja ajast. Hetkel on DT uurimisgrupi poolt väljatöötatud vahendid kasutusel juba ligi 90 instituudis rohkem kui 30 riigis üle maailma.

Koosseis: Raimund Ubar (prof), Marina Brik (teadur), Peeter Ellervee (dotsent), Margus Kruus (inst direktor, CE/TTU), Jaan Raik (vanemteadur), Aleksandr Sunditsõn (dotsent), Kalle Tammemäe (dotsent); Margit Aarna, Eero Ivask, Artur Jutman, Helena Kruus, Aimar Liiver, Elmet Orasson (doktorandid).

PUBLIKATSIOOONE

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 resynthesis in combinational circuits. J. of Electronic Testing: Theory and Appl. 19, 1, 73-82 (2003).

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