Eesti teaduse tippkeskus / Estonian Centre of Excellence in Research
Töökindlate Arvutisüsteemide Uurimise Keskus / Centre for Dependable Systems
Publikatsioonid / Publications 2003–2007

Matemaatilised alused ja programmikeelte tehnoloogia / Mathematical foundations and programming language technology

2003

- A. Abel, R. Matthes, T. Uustalu. Generalized iteration and coiteration for higher-order nested datatypes. In A. D. Gordon, ed., *Proc. of 6th Int. Conf. on Foundations of Software Science and Computation Structures, FoSSaCS'03 (Warsaw, Apr. 2003)*, v. 2620 of *Lect. Notes in Comput. Sci.*, pp. 54-69. Springer, Berlin, 2003. article at SpringerLink
- N. Ghani, T. Uustalu. Coproducts of ideal monads (extended abstract). In Z. Ésik, I. Walukiewicz, eds., *Proc. of 5th Int. Wksh. on Fixed Points in Computer Science, FICS'03 (Warsaw, Apr. 2003)*, pp. 32-36. Warsaw Univ., 2003.
- N. Ghani, T. Uustalu. Explicit substitutions and higher-order syntax. In F. Honsell, M. Miculan, A. Momigliano, eds., *Proc. of 2nd ACM SIGPLAN Wksh. on Mechanized Reasoning about Languages with Variable Binding, MERλIN'03 (Uppsala, Aug. 2003)*, 7 pp. ACM Press, 2003. doi: 10.1145/976571.976580
- A. Kelarev, O. Sokratova. On congruences of automata defined by directed graphs. *Theor. Comput. Sci.*, v. 301, n. 1-3, pp. 31-43, 2003. doi: 10.1016/S0304-3975(02)00544-3
- P. Laud. Handling encryption in an analysis for secure information flow. In P. Degano, ed., *Proc. of 12th Europ. Symp. on Programming, ESOP 2003 (Warsaw, Apr. 2003)*, v. 2618 of *Lect. Notes in Comput. Sci.*, pp. 159-173. Springer, Berlin, 2003. article at SpringerLink
- P. Laud, R. Corin. Sound computational interpretation of formal encryption with composed keys. In *Pre-Proc. of 6th Int. Conf. on Information Security and Cryptology, ICISC 2003 (Seoul, Nov. 2003)*. 2003.
- R. Matthes, T. Uustalu. Substitution in non-wellfounded syntax with variable binding. In H. P. Gumm, ed., *Proc. of 6th Int. Wksh. on Coalgebraic Methods in Computer Science, CMCS'03 (Warsaw, Apr. 2003)*, v. 82, n. 1 of *Electron. Notes. in Theor. Comput. Sci.*, 15 pp., Elsevier, 2003. doi: 10.1016/S1571-0661(04)80639-X
- J. Pöial. Program analysis for stack based languages. In *Proc. of 19th EuroForth Conference (Ross-on-Wye, Oct. 2003)*, pp. 9-13. 2003.
- J. Pöial. Implementation of directed multigraphs in Java. In *Proc. of 2nd Int. Conf. on Principles and Practice of Programming in Java, PPPJ 2003 (Kilkenny City, June 2003)*, v. 42 of *ACM Int. Conf. Proc. Series*, p. 163. Comput. Sci. Press, 2003. article at ACM DL
- H. Seidl, V. Vene, M. Müller-Olm. Global invariants for analysing multi-threaded applications. *Proc. of Estonian Acad. of Sci., Phys., Math.*, v. 52, n. 4, pp. 413-436, 2003.
- M. Tombak. Logical method in combinatorial counting. In *Proc. of Int. Conf. on Advances on Internet, Processing, Systems and Interdisciplinary Research, IPSI 2003 (Sveti Stefan, Oct. 2003)*, 4 pp. 2003.
- S. Tupailo. Realization of constructive set theory into explicit mathematics: a lower bound for impredicative Mahlo universe. *Ann. of Pure and Appl. Logic*, v. 120, n. 1-3, pp. 165-196, 2003. doi: 10.1016/S0168-0072(02)00065-9
- S. Tupailo. Epsilon-substitution method for Δ^1_1-CR: a constructive termination proof. *Logic J. of the IGPL*, v. 11, n. 3, pp. 367-377, 2003. doi: 10.1093/jigpal/11.3.367
- S. Tupailo. On non-wellfounded constructive set theory: construction of non-wellfounded sets in explicit mathematics. In G. Mints, R. Muskens, eds., *Games, Logic, and Constructive Sets*, v. 161 of *CSLI Lect. Notes*, pp. 109-125. CSLI Publications, 2003.
- T. Uustalu. Generalizing substitution. *Theor. Inform. and Appl.*, v. 37, n. 4, pp. 315-336, 2003. doi: 10.1051/ita:2003022

- T. Uustalu. Monad translating inductive and coinductive types. In H. Geuvers, F. Wiedijk, eds., *Selected Papers from 2nd Int. Wksh. on Types for Proofs and Programs, TYPES'02 (Berg en Dal, Apr. 2002)*, v. 2646 of *Lect. Notes in Comput. Sci.*, pp. 299-315. Springer, Berlin, 2003. article at SpringerLink

- T. Uustalu, V. Vene. An alternative characterization of complete iterativeness (extended abstract). In Z. Ésik, I. Walukiewicz, eds., *Proc. of 5th Int. Wksh. on Fixed Points in Computer Science, FICS'03 (Warsaw, Apr. 2003)*, pp. 81-83. Warsaw Univ., 2003.

2004

- T. Altenkirch, T. Uustalu. Normalization by evaluation for $\lambda^{\rightarrow,2}$. In Y. Kameyama, P. J. Stuckey, eds., *Proc. of 7th Int. Symp. on Functional and Logic Programming, FLOPS 2004 (Nara, Apr. 2004)*, v. 2998 of *Lect. Notes in Comput. Sci.*, pp. 260-275. Springer, 2004. article at SpringerLink

- G. Barthe, E. Giménez, M. J. Frade, L. Pinto, T. Uustalu. Type-based termination of recursive definitions. *Math. Struct. in Comput. Sci.*, v. 14, n. 1, pp. 97-141, 2004. doi: 10.1017/S0960129503004122

- V. Capretta, T. Uustalu, V. Vene. Recursive coalgebras from comonads. In J. Adámek, S. Milius, eds., *Proc. of 7th Int. Wksh. on Coalgebraic Methods in Computer Science, CMCS '04 (Barcelona, March 2004)*, v. 106 of *Electron. Notes in Theor. Comput. Sci.*, pp. 43-61. Elsevier, 2004. doi: 10.1016/j.entcs.2004.02.034

- N. Ghani, T. Uustalu. Coproducts of ideal monads. *Theor. Inform. and Appl.*, v. 38, n. 4, pp. 321-342, 2004. doi: 10.1051/ita:2004016

- N. Ghani, T. Uustalu, V. Vene. Build, augment and destroy, universally. In W.-N. Chin, ed., *Proc. of 2nd Asian Symp. on Programming Languages and Systems, APLAS 2004 (Taipei, Nov. 2004)*, v. 3302 of *Lect. Notes in Comput. Sci.*, pp. 327-347. Springer, 2004. article at SpringerLink

- N. Ghani, T. Uustalu, V. Vene. Generalizing the augment combinator. In H.-W. Loidl, ed., *Proc. of 5th Symp. on Trends in Functional Programming, TFP '04 (München, Nov. 2004)*, pp. 65-76. Ludwig-Maximilians-Univ. München, 2004.

- P. Laud, R. Corin. Sound computational interpretation of formal encryption with composed keys. In J. I. Lim, D. H. Lee, eds., *Revised Papers from 6th Int. Conf. on Information Security and Cryptology, ICISC 2003 (Seoul, Nov. 2003)*, v. 2971 of *Lect. Notes in Comput. Sci.*, pp. 55-66. Springer, 2004. article at SpringerLink

- P. Laud. Encryption in automatic analyses for confidentiality against active adversaries. In *Proc. of 2004 IEEE Symp. on Security and Privacy, S&P 2004 (Berkeley, CA, May 2004)*, pp. 71-85. IEEE CS Press, 2004. doi: 10.1109/secpri.2004.1301316

- R. Matthes, T. Uustalu. Substitution in non-wellfounded syntax with variable binding. *Theor. Comput. Sci.*, v. 327, n. 1-2, pp. 155-174, 2004. doi: 10.1016/j.tcs.2004.07.025

- F. Otto, O. Sokratova. Reduction relations for monoid semirings. *J. of Symb. Comput.*, v. 37, n. 3, pp. 343-376, 2004. doi: 10.1016/j.jsc.2003.07.002

- S. Tupailo. On the intuitionistic strength of monotone inductive definitions. *J. of Symb. Logic*, v. 69, n. 3, pp. 790-798, 2004.

2005

- A. Abel, R. Matthes, T. Uustalu. Iteration schemes for higher-order and nested datatypes. *Theor. Comput. Sci.*, v. 333, n. 1-2, pp. 3-66, 2005. doi: 10.1016/j.tcs.2004.10.017

- G. Barthe, T. Rezk, A. Saabas. Proof obligations preserving compilation. In T. Dimitrakos, F. Martinelli, P. Ryan, S. Schneider, eds., *Proc. of 3rd Int. Wksh. on Formal Aspects in Security and Trust, FAST '05 (Newcastle upon Tyne, July 2005)*, Techn. report IIT TR-13/2005, pp. 109-124. Ist. di Informatica e Telematica, Consiglio Nazionale delle Ricerche, 2005.

- N. Ghani, P. Johann, T. Uustalu, V. Vene. Monadic augment and generalised short cut fusion. In *Proc. of 10th ACM SIGPLAN Int. Conf. on Functional Programming, ICFP'05 (Tallinn, Sept. 2005)*, pp. 294-305. ACM Press, 2005. doi: 10.1145/1086365.1086403

- N. Ghani, P. Johann, T. Uustalu, V. Vene. Monadic augment and generalised short cut fusion. *ACM SIGPLAN Notices*, v. 40, n. 9, pp. 294-305, 2005. doi: 10.1145/1090189.1086403

- A. Kelarev, M. Miller, O. Sokratova. Languages recognized by two-sided automata of graphs. *Proc. of Estonian Acad. of Sci.: Phys., Math.*, v. 54, n. 1, pp. 46-54, 2005.
- P. Laud. Secrecy types for a simulatable cryptographic library. In *Proc. of 12th ACM Conf. on Computer and Communications Security, CCS 2005 (Alexandria, VA, Nov. 2005)*, pp. 26-35. ACM Press, 2005. doi: 10.1145/1102120.1102126
- P. Laud, T. Uustalu, V. Vene. Type systems equivalent to dataflow analyses for imperative languages. In M. Hofmann, H.-W. Loidl, eds., *Proc. of 3rd APPSEM II Wksh., APPSEM '05 (Frauenchiemsee, Sept. 2005)*, 12 pp. Ludwig-Maximilians-Univ. München, 2005.
- P. Laud, V. Vene. A type system for computationally secure information flow. In M. Liskiewicz, R. Reischuk, eds., *Proc. of 15th Int. Symp. on Fundamentals of Computation Theory, FCT 2005 (Lübeck, Aug. 2005)*, v. 3623 of *Lect. Notes in Comput. Sci.*, pp. 365-377. Springer, 2005. doi: 10.1007/11537311_32
- H. Nestra. Transfinite corecursion. *Nordic J. of Computing*, v. 12, n. 2, pp. 133-156, 2005.
- H. Nestra. Transfinite semantics in program slicing. In V. Vene, M. Meriste, eds., *Proc. of 9th Symp. on Programming Languages and Software Tools, SPLST 2005 (Tartu, Aug. 2005)*, pp. 126-140. Univ. of Tartu, 2005.
- H. Nestra. Transfinite semantics in program slicing. *Proc. of Estonian Acad. of Sci., Engineering*, v. 11, n. 4, pp. 313-328, 2005.
- O. Shkaravska. Amortized heap-space analysis for first-order functional programs. In M. van Eekelen, ed., *Proc. of 6th Symp. on Trends in Functional Programming, TFP '05 (Tallinn, Sept. 2005)*, pp. 281-296. Inst. of Cybern., 2005.
- O. Shkaravska. Types with semantics: soundness proof assistant. In A. Momigliano, R. Pollack, eds., *Proc. of 3rd ACM SIGPLAN Wksh. on Mechanized Reasoning about Languages with Variable Binding, MERλIN '05 (Tallinn, Sept. 2005)*, pp. 50-57. ACM Press, 2005. doi: 10.1145/1088454.1088461
- T. Uustalu, V. Vene. Comonadic functional attribute evaluation. In M. van Eekelen, ed., *Proc. of 6th Symp. on Trends in Functional Programming, TFP '05 (Tallinn, Sept. 2005)*, pp. 33-43. Inst. of Cybern., 2005.
- T. Uustalu, V. Vene. Signals and comonads. In M. A. Musicante, R. M. F. Lima, eds., *Proc. of 9th Brazilian Symp. on Programming Languages, SBLP'05 (Recife, PE, May 2005)*, pp. 215-228. Univ. de Pernambuco, Recife, 2005.
- T. Uustalu, V. Vene. Signals and comonads. *J. of Univ. Comput. Sci.*, v. 11, n. 7, pp. 1310-1326, 2005. article at publisher's website
- T. Uustalu, V. Vene. The essence of dataflow programming (short version). In K. Yi, ed., *Proc. of 3rd Asian Symp. on Programming Languages and Systems, APLAS 2005 (Tsukuba, Nov. 2005)*, v. 3780 of *Lect. Notes in Comput. Sci.*, pp. 2-18. Springer, 2005. doi: 10.1007/11575467_2
- V. Vene, T. Uustalu, eds. *Revised Lectures from 5th Int. School on Advanced Functional Programming, AFP 2004 (Tartu, Aug. 2004)*, v. 3622 of *Lect. Notes in Comput. Sci.*, x+357 pp. Springer, 2005. doi: 10.1007/11546382

2006

- M. Backes, P. Laud. A mechanized, cryptographically sound type inference checker. In V. Cortier, S. Kremer, eds., *Abstracts of 2nd Wksh. on Formal and Computational Cryptography, FCC 2006 (Venice, July 2006)*, 6 pp. INRIA, 2006.
- M. Backes, P. Laud. Computationally sound secrecy proofs by mechanized flow analysis. In *Proc. of 13th ACM Conf. on Computer and Communications Security, CCS 2006 (Alexandria, VA, Oct./Nov. 2006)*, pp. 370-379. ACM Press, 2006. doi: 10.1145/1180405.1180450
- G. Barthe, T. Rezk, A. Saabas. Proof obligations preserving compilation. In T. Dimitrakos, F. Martinelli, P. Y. A. Ryan, S. Schneider, eds., *Revised Selected Papers from 3rd Int. Wksh. on Formal Aspects in Security and Trust, FAST 2005 (Newcastle upon Tyne, July 2005)*, v. 3866 of *Lect. Notes in Comput. Sci.*, pp. 112-126. Springer, 2006. doi: 10.1007/11679219_9

- V. Capretta, T. Uustalu, V. Vene. Recursive coalgebras from comonads. *Inform. and Comput.*, v. 204, n. 4, pp. 437-468, 2006. doi: 10.1016/j.ic.2005.08.005
- N. Ghani, M. Hamana, T. Uustalu, V. Vene. Representing cyclic structures as nested datatypes. In H. Nilsson, ed., *Proc. of 7th Symp. on Trends in Functional Programming, TFP 2006 (Nottingham, Apr. 2006)*, pp. 173-188. Univ. of Nottingham, 2006.
- N. Ghani, T. Uustalu, M. Hamana. Explicit substitutions and higher-order syntax. *Higher-Order and Symbolic Comput.*, v. 19, n. 2-3, pp. 263-282, 2006. doi: 10.1007/s10990-006-8748-4
- N. Ghani, T. Uustalu, V. Vene. Generalizing the augment combinator. In H.-W. Loidl, ed., *Trends in Functional Programming 5*, pp. 65-78. Intellect, 2006.
- S. Gilmore, O. Shkaravska. Estimating the cost of native method calls for resource-bounded functional programming languages. In N. Thomas, ed., *Proc. of 2nd Int. Wksh. on Practical Applications of Stochastic Modelling, PASM '05 (Newcastle upon Tyne, July 2005)*, v. 151, n. 3 of *Electron. Notes in Theor. Comput. Sci.*. Elsevier, 2006. doi: 10.1016/j.entcs.2006.03.010
- M. Hamana, N. Ghani, T. Uustalu, V. Vene. Representing cyclic structures as nested datatypes. In A. Takana, ed., *Proc. of 23th Conf. of Japan Society for Software Science and Technology, JSSST 06 (Tokyo, Sept. 2006)*, 8 pp. Univ. of Tokyo, 2006.
- M. Johnson, V. Vene, eds., *Proc. of 11th Int. Conf. on Algebraic Methodology and Software Technology, AMAST 2006 (Kuressaare, July 2006)*, v. 4019 of *Lect. Notes in Comput. Sci.*, xi+389 pp. Springer, 2006. doi: 10.1007/11784180
- J. Kabanov, V. Vene. Recursion schemes for dynamic programming. In T. Uustalu, ed., *Proc. of 8th Int. Conf. on Mathematics of Program Construction, MPC 2006 (Kuressaare, July 2006)*, v. 4014 of *Lect. Notes in Comput. Sci.*, pp. 235-252. Springer, 2006. doi: 10.1007/11783596_15
- P. Laud, T. Uustalu, V. Vene. Type systems equivalent to data-flow analyses for imperative languages. *Theor. Comput. Sci.*, v. 364, n. 3, pp. 292-310, 2006. doi: 10.1016/j.tcs.2006.08.013
- C. McBride, T. Uustalu, eds. *Proc. of Wksh. on Mathematically Structured Functional Programming, MSFP 2006 (Kuressaare, July 2006)*, *Electron. Wkshs. in Computing*. British Comput. Soc., 2006. volume at publisher's website
- O. Mürk, J. Kabanov. Aranea: web framework construction and integration kit. In *Proc. of 4th Int. Conf. on Principles and Practice of Programming in Java, PPPJ 2006 (Mannheim, Aug./Sept. 2006)*, v. 178 of *ACM Int. Conf. Proc. Series*, pp. 163-172. ACM Press, 2006. doi: 10.1145/1168054.1168077
- H. Nestra. Fractional semantics. In M. Johnson, V. Vene, eds., *Proc. of 11th Int. Conf. on Algebraic Methodology and Software Technology, AMAST 2006 (Kuressaare, July 2006)*, v. 4019 of *Lect. Notes in Comput. Sci.*, pp. 278-292. Springer, 2006. doi: 10.1007/11784180_22
- H. Nestra. Iteratively defined transfinite trace semantics and program slicing with respect to them. V. 49 of *Diss. Math. Univ. Tartuensis*. Univ. of Tartu, 2006. handle: 10062/1109
- J. Peetre, J. Penjam, eds. *Semigroups and Automata: Selecta Uno Kaljulaid (1941-1999)*, xxiv+472 pp. IOS Press, 2006. book at IOS Press BooksOnline
- J. Pöial. Typing tools for typeless stack languages. In *Proc. of 22nd EuroForth Conf. (Cambridge, Sept. 2006)*, pp. 40-46. 2006.
- M. Rathjen, S. Tupailo. Characterizing the interpretation of set theory in Martin-Löf type theory. *Ann. of Pure and Appl. Logic*, v. 141, n. 3, pp. 442-471, 2006. doi: 10.1016/j.apal.2005.12.008
- A. Saabas, T. Uustalu. A compositional natural semantics and Hoare logic for low-level languages. In P. D. Mosses, I. Ulidowski, eds., *Proc. of 2nd Wksh. on Structured Operational Semantics, SOS 2005 (Lisbon, July 2005)*, v. 156, n. 1 of *Electron. Notes in Theor. Comput. Sci.*, pp. 151-168. Elsevier, 2006. doi: 10.1016/j.entcs.2005.09.031
- A. Saabas, T. Uustalu. Compositional type systems for stack-based low-level languages. In B. Jay, J. Gudmundsson, eds., *Proc. of 12th Computing, Australasian Theory Symp., CATS 2006 (Hobart, Jan. 2006)*, v. 51 of *Confs. in Research and Practice in Inform. Techn.*, pp. 27-39. Australian Comput. Soc., 2006. article at ACM DL

- H. Tamm, M. Nykänen, E. Ukkonen. Size reduction of multitape automata. In J. Farré, I. Litovsky, S. Schmitz, eds., *Revised Selected Papers from 10th Int. Conf. on Implementation and Application of Automata, CIAA 2005 (Sophia Antipolis, June 2005)*, v. 3845 of *Lect. Notes in Comput. Sci.*, pp. 307-318. Springer, 2006. doi: 10.1007/11605157_26

- H. Tamm, M. Nykänen, E. Ukkonen. On size reduction techniques for multitape automata. *Theor. Comput. Sci.*, v. 363, n. 2, pp. 234-246, 2006. doi: 10.1016/j.tcs.2006.07.027

- T. Uustalu, ed. *Proc. of 8th Int. Conf. on Mathematics of Program Construction, MPC 2006 (Kuressaare, July 2006)*, v. 4014 of *Lect. Notes in Comput. Sci.*, x+455 pp. Springer, 2006. doi: 10.1007/11783596

- T. Uustalu, V. Vene. The essence of dataflow programming (full version). In Z. Horváth, ed., *Revised Selected Lectures from 1st Central-European Functional Programming School, CEFP 2005 (Budapest, July 2005)*, v. 4164 of *Lect. Notes in Comput. Sci.*, pp. 135-167. Springer, 2006. doi: 10.1007/11894100_5

2007

- M. J. Frade, A. Saabas, T. Uustalu. Foundational certification of data-flow analyses. In *Proc. of 1st Joint IEEE/IFIP Symp. on Theor. Aspects of Software Engineering, TASE 2007 (Shanghai, June 2007)*, pp. 107-116. IEEE CS Press, 2007. doi: 10.1109/tase.2007.27

- I. Hasuo, B. Jacobs, T. Uustalu. Categorical views on computations on trees. In L. Arge, C. Cachin, T. Jurdzinski, A. Tarlecki, eds., *Proc. of 34th Int. Coll. on Automata, Languages and Programming, ICALP 2007 (Wroclaw, July 2007)*, v. 4596 of *Lect. Notes in Comput. Sci.*, pp. 619-630. Springer, 2007. doi: 10.1007/978-3-540-73420-8_54

- B. Jacobs, T. Uustalu. Semantics of grammars and attributes via initiality. In E. Barendsen, V. Capretta, H. Geuvers, M. Niqui, eds., *Reflections on Type Theory, Lambda-Calculus, and the Mind: Essays Dedicated to Henk Barendregt on the Occasion of His 60th Birthday*, pp. 181-196. Radboud Univ. Nijmegen, 2007.

- P. Laud. On the computational soundness of cryptographically masked flows. In *Proc. of 35th Ann. ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages, POPL 2008 (San Francisco, CA, Jan. 2008)*, pp. 337-348. ACM Press, 2008. doi: 10.1145/1328438.1328479

- P. Laud. On the computational soundness of cryptographically masked flows. *ACM SIGPLAN Notices*, v. 43, n. 1, pp. 337-348, 2008. doi: 10.1145/1328897.1328479

- C. McBride, T. Uustalu, guest eds. *J. of Funct. Program.* (Selected Papers from Wksh. on Mathematically Structured Functional Programming, MSFP 2006, Kuressaare, July 2006), to appear.

- A. Saabas, T. Uustalu. A compositional natural semantics and Hoare logic for low-level languages. *Theor. Comput. Sci.*, v. 373, n. 3, pp. 273-302, 2007. doi: 10.1016/j.tcs.2006.12.020

- A. Saabas, T. Uustalu. Type systems for optimizing stack-based code. In M. Huisman, F. Spoto, eds., *Proc. of 2nd Wksh. on Bytecode Semantics, Verification, Analysis and Transformation, Bytecode 2007 (Braga, March 2007)*, v. 190, n. 1 of *Electron. Notes in Theor. Comput. Sci.*, pp. 103-119. Elsevier, 2007. doi: 10.1016/j.entcs.2007.02.063

- A. Saabas, T. Uustalu. Program and proof optimizations with type systems. *J. of Logic and Algebraic Program.*, to appear.

- A. Saabas, T. Uustalu. Proof optimization for partial redundancy elimination. In *Proc. of 2008 ACM SIGPLAN Wksh. on Partial Evaluation and Semantics-Based Program Manipulation, PEPM 2008 (San Francisco, CA, Jan. 2008)*, pp. 91-101. ACM Press, 2008. doi: 10.1145/1328408.1328422

- H. Tamm. On transition minimality of bideterministic automata. In T. Harju, J. Karhumäki, A. Lepistö, eds., *Proc. of 11th Int. Conf. on Developments in Language Theory, DLT 2007 (Turku, July 2007)*, v. 4588 of *Lect. Notes of Comput. Sci.*, pp. 411-421. Springer, 2007. doi: 10.1007/978-3-540-73208-2_38

- H. Tamm. On transition minimality of bideterministic automata. *Int. J. of Found. of Comput. Sci.*, to appear.

- M. Tombak. Keerukusteooria. 114 lk. TÜ, 2007.

- A. Toom, T. Näks, M. Pantel, M. Gandriau, I. Wati. GeneAuto: an automatic code generator for a safe subset of SimuLink/StateFlow and Scicos. In *Proc. of 4th Europ. Conf. on Embedded Real-Time Software, ERTS 2008 (Toulouse, Jan./Feb 2008)*, to appear.
- S. Tupailo. Monotone inductive definitions and consistency of New Foundations. In C. Dimitracopoulos, L. Newelski, D. Normann, eds., *Proc. of Logic Coll. 2005 (Athens, July/Aug. 2005)*, v. 28 of *Lect. Notes in Logic*, pp. ?-?. Cambridge Univ. Press, 2007.
- S. Tupailo. Fixpoints of models construction. *Logique et Analyse (Nouvelle Série)*, v. 50, n. 197, pp. 63-78, 2007.
- T. Uustalu, guest ed. *Sci. of Comput. Program.* (Selected Papers from 8th Int. Conf. on Mathematics of Program Construction, MPC 2006, Kuressaare, July 2006), to appear.
- T. Uustalu, V. Vene. Comonadic functional attribute evaluation. In M. van Eekelen, ed., *Trends in Functional Programming 6*, pp. 145-162. Intellect, 2007.
- V. Vojdani, V. Vene. Goblint: path-sensitive data race analysis. In Z. Horváth, L. Kozma, V. Zsók, eds., *Proc. of 10th Symp. on Programming Languages and Software Tools, SPLST 2007 (Dobogókö, June 2007)*, pp. 130-141. Eötvös Loránd Univ., 2007.

Formaalsed meetodid tarkvaratehnikas / Formal methods in software engineering

2003

- I. G. Graham, A. Spence, E. Vainikko. Parallel iterative methods for Navier-Stokes equations and application to eigenvalue computation. *Concurrency and Computation: Practice and Experience*, v. 15, n. 11-12, pp. 1151-1168, 2003. doi: 10.1002/cpe.785
- G. Grossschmidt, M. Harf. Multi-pole modelling and simulation of an electro-hydraulic servo-system with a non-linear regulator in NUT environment. In *Fünftes Deutsch-Polnisches Seminar Innovation und Fortschritt in der Fluidtechnik (Warsaw, Sept. 2003)*, pp. 146-161. 2003.
- M. Haveraaen, J. Vain, guest eds., *Nordic J. of Computing*, v. 10, n. 4 (Selected Papers from 14th Nordic Wksh. on Programming Theory, NWPT'02, Tallinn, Nov. 2002), 2003.
- V. Kotkas. Synthesis of distributed programs. In P. Kilpeläinen, N. Päivinen, eds., *Proc. of 8th Symp. on Programming Languages and Software Tools, SPLST '03 (Kuopio, June 2003)*, Report A/2003/01, pp. 21-33. Univ. of Kuopio, 2003.
- A. Kuusik, T. Otto, J. Vain. Handling industrial hazards by pre-emptive model checking. In *Proc. of 4th Int. Conf. on Industrial Automation (Montréal, 9-11 June 2003)*. 2003.
- R. Küttner, J. Ernits, J. Vain, An open tool integration environment for manufacturing control software development. *Machine Engineering*, v. 3, n. 1-2, pp. 23-32, 2003.
- M. Meriste, T. Kelder, J. Helekivi, L. Mõtus. Domain-specific language agents. In P. Kilpeläinen, N. Päivinen, eds., *Proc. of 8th Symp. on Programming Languages and Software Tools, SPLST '03 (Kuopio, June 2003)*, Report A/2003/01, pp. 82-90. Univ. of Kuopio, 2003.
- L. Motus. Modeling metric time. In L. Lavagno, G. Martin, B. Selic, eds., *UML for Real: Design of Embedded Real-Time Systems*, pp. 205-220. Kluwer Acad. Publ., 2003.
- L. Motus, M. Meriste. Time modelling for requirements and specification analysis. In M. Colnaric, M. Adamski, Wegrzyn, eds., *Proc. of 27th IFAC/IFIP/IEEE Wksh. on Real-Time Programming, WRTP 2003 (Lagow, May 2003)*, pp. 13-18. 2003.
- L. Motus, M. Meriste, T. Kelder, J. Helekivi, V. Kimlaychuk. A test-bed for time-sensitive agents - some involved problems. In *Proc. of 9th IEEE Int. Conf. on Emerging Technologies and Factory Automation, ETFA 2003 (Lisbon, Sept. 2003)*, v. 2, pp. 645-651. IEEE, 2003. doi: 10.1109/etfa.2003.1248759
- J. Penjam, J. Sanko. Deductive and inductive methods for program synthesis. In W. Dosch, R. Y. Lee, eds., *Proc. of ACIS 4th Int. Conf. on Software Engineering, Artif. Intell., Networking, and Parallel/Distributed Computing, SNPD '03 (Lübeck, Oct. 2003)*, pp. 188-195. ACIS, 2003.

- J. Sanko, J. Penjam. Program construction in the context of evolutionary computation. In *Prel. Proc. of Andrei Ershov 5th Int. Conf. Perspectives of System Informatics, PSI 2003 (Novosibirsk, July 2003)*, pp. 20-24. A. P. Ershov Inst. of Informatics Systems, Novosibirsk, 2003.

- R. Savimaa. On modelling emerging behavior of multifunctional non-profit organisations. In M. Kirikova et al., eds., *Information Systems Development: Advances in Methodologies, Components, and Management*, pp. 203-214. Kluwer Acad. Publ. / Plenum Press, 2003.

- B. Selic, L. Motus. Using models in real-time software design: model driven development based on the unified modelling language. *IEEE Control Systems Magazine*, v. 23, n. 3, pp. 31-42, 2003. doi: 10.1109/mcs.2003.1200244

- T. Tammet. Finite model building: improvements and comparisons. In *Proc. of CADE-19 Wksh. W4 on Model Computation: Principles, Algorithms, Applications (Miami, FL, July 2003)*, 10 pp. 2003.

- T. Tammet, V. Kadarpik. Combining an interface engine with databases: a rule server. In M. Schroeder, G. Wagner, eds., *Proc. of 2nd Int. Wksh. on Rules and Rule Markup Languages for the Semantic Web, RuleML 2003 (Sanibel Island, FL, Oct. 2003)*, v. 2876 of *Lect. Notes in Comput. Sci.*, pp. 23-32. Springer, 2003. article at SpringerLink

- T. Tammet. Extending classical theorem proving for the Semantic Web. In R. Volz, S. Decker, I. F. Cruz, eds., *Proc. of 1st Int. Wksh. on Practical and Scalable Semantic Systems, PSSS-1 (Sanibel Island, FL, Oct. 2003)*, v. 89 of *CEUR Wksh. Proc.*, 14 pp. RWTH Aachen, 2003. volume at publisher's website

- E. Tyugu. Formalization of knowledge systems. In H. R. Arabnia, R. Joshua, Y. Mun, eds., *Proc. of Int. Conf. on Artificial Intelligence, IC-AI '03 (Las Vegas, NV, June 2003)*, v. 2, pp. 654-659. CSREA Press, 2003.

- E. Tyugu, A. Saabas. Problems of visual specification languages. In *Proc. of 30th Int. Conf. Information Technologies in Science, Education, Telecommunication and Business, IT + SE'03 (Yalta-Gurzuf, May 2003)*, pp. 155-157. 2003.

- J. Vain, T. Uustalu, guest eds., *Proc. of Estonian Acad. of Sci., Phys., Math.*, v. 52, n. 4 (Selected Papers from 14th Nordic Wksh. on Programming Theory, NWPT '02, Tallinn, Nov. 2002), 2003.

2004

- G. Grossschmidt, M. Harf. Multi-pole modelling and simulation of dynamics of an electro-hydraulic servosystem. In J. Papstel, B. Katalinic, eds., *Proc. of 4th Int. DAAAM Conf. Industrial Engineering: New Challenges to SME (Tallinn, Apr. 2004)*, pp. 27-30. Tallinn Univ. of Techn., 2004.

- G. Grossschmidt, M. Harf. Simulation of statics and steady state conditions of an electro-hydraulic servosystem. In J. Papstel, B. Katalinic, eds., *Proc. of 4th Int. DAAAM Conf. Industrial Engineering: New Challenges to SME (Tallinn, Apr. 2004)*, pp. 31-34. Tallinn Univ. of Techn., 2004.

- K. Jääger, J. Vain. Pattern-based modeling and planning of machining systems. *Machine Engineering*, v. 4, n. 1-2, pp. 97-106, 2004.

- K. Jääger, J. Vain. Pattern-based analysis of fractal manufacturing systems. In A. H. Frigeri, ed., *Prep. of 11th IFAC Symp. on Information Control Problems in Manufacturing, INCOM 2004 (Salvador, Apr. 2004)*, 6 pp. 2004.

- V. Kimlaychuk. Creating intelligent agents in JADE (an example of ant colony simulation). In *Proc. of Int. Conf. on Education and Information Systems: Technologies and Applications, EISTA 2004 (Orlando, FL, July 2004)*, v. 1, pp. 55-60. IIIS, 2004.

- A. Kull. Improving embedded software testing. In *Proc. of 8th World Multi-Conf. on Systemics, Cybernetics and Informatics, SCI 2004 (Orlando, FL, July 2004)*, v. 1, pp. 270-274. IIIS, 2004.

- O. Miyashita, S. Tsukamoto, A. Kuusik, D. Miyata, T. Yoshida, J. Vain, S. Ishigami. A human-adaptive-mechatronics assisted system for training constructional ability. In *Proc. of 8th Int. Conf. on Mechatronics Technology, ICMT 2004 (Hanoi, Nov. 2004)*, pp. 551-555. Vietnam Nat. Univ., 2004.

- L. Motus, M. Meriste, T. Kelder, J. Helekivi. Agent-based templates for implementing proactive real-time systems. In H. W. Chu, M. Savoie, B. Sanches, eds., *Proc. of Int. Conf. on Computing, Communications, and Control Technologies, CCCT 2004 (Austin, TX, Aug. 2004)*, v. 1, pp. 199-204. IIIS, 2004.

- J. Penjam, J. Sanko. Deductive and inductive methods for program synthesis. *Int. J. of Comput. and Inform. Sci.*, v. 5, n. 3, pp. 171-181, 2004.
- J. Sanko, J. Penjam. Program construction in the context of evolutionary computation. In M. Broy, A. V. Zamulin, eds., *Revised Papers from 5th Andrei Ershov Int. Conf. Perspectives of System Informatics, PSI 2003 (Novosibirsk, July 2003)*, v. 2980 of *Lect. Notes in Comput. Sci.*, pp. 50-58. Springer, 2004. article at SpringerLink
- R. Savimaa. A methodology for modelling of modifications in multifunctional human organisations. In *Proc. of 8th World Multi-Conf. on Systemics, Cybernetics and Informatics, SCI 2004 (Orlando, FL, July 2004)*, v. 10, pp. 265-269. IIIS, 2004.
- R. Savimaa. Integrating UML, the Q-model and a multi-agent approach in process and behaviour models of organisations. In *Proc. of Int. Conf. on Cybernetics and Information Technologies, Systems and Applications/10th Int. Conf. on Information Systems Analysis and Synthesis, CITSA/ISAS 2004 (Orlando, FL, July 2004)*, v. 1, pp. 167-171. IIIS, 2004.
- R. Savimaa. Composition of organisational process models for supporting information systems design. In *Proc. of 11th Doctoral Consortium on Advanced Information Systems Engineering (Riga, June 2004)*, pp. 59-70. 2004.
- J. Simm. Ontology view of intelligent systems. In *Proc. of 2nd Int. IEEE Conf. on Intelligent Systems: Methodology, Models, Applications in Emerging Technologies (Varna, June 2004)*, v. 2, pp. 480-484. IEEE, 2004. doi: 10.1109/is.2004.1344797
- T. Tammet. Chain resolution for the Semantic Web. In D. A. Basin, M. Rusinowitch, eds., *Proc. of 2nd Int. Joint Conf. on Automated Reasoning, IJCAR 2004 (Cork, July 2004)*, v. 3097 of *Lect. Notes in Artif. Intell.*, pp. 307-320. Springer, 2004. article at SpringerLink
- E. Tyugu. Modularity of knowledge. In H. R. Arabnia, ed., *Proc. of Int. Conf. on Artificial Intelligence, IC-AI '04 (Las Vegas, June 2004)*, v. 1, pp. 295-301. CSREA Press, 2004.
- E. Tyugu. Knowledge systems as architectural components. In V. Stefanuk, K. Kaijiri, eds., *Proc. of 6th Joint Conf. on Knowledge-Based Software Engineering, JCKBSE 2004 (Protvino, Aug. 2004)*, v. 108 of *Frontiers in Artificial Intelligence and Applications*, pp. 199-206. IOS Press, 2004.
- J. Vain, T. Otto, A. Kuusik. Model checking for planning resource-sharing production. In M. A. Marquez R., ed., *Proc. of 20th Int. Conf. on CAD/CAM, Robotics and Factories of the Future, CARS&FOF 2004 (San Cristobal, July 2004)*, pp. 151-158. Nadie Nos Edita Editores, 2004.
- J. Vain, S. Suzuki, A. Kuusik. Formal safety validation of robot teleoperation. In *Proc. of 9th Biennial Baltic Electronic Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 161-164. Tallinn Univ. of Techn., 2004.
- E. Vainikko, I. G. Graham. A parallel solver for PDE systems and application to the incompressible Navier-Stokes equations. *Applied Numerical Mathematics*, v. 49, n. 1, pp. 97-116, 2004. doi: 10.1016/j.apnum.2003.11.015

2005

- W. Dosch, M. Meriste. High-level design of a pull protocol. In G. Hu, ed., *Proc. of 20th Int. Conf. on Computers and Their Applications (New Orleans, LA, March 2005)*, pp. 66-73. ISCA, 2005.
- E. Domiczi, J. Vain. Model driven engineering in automatic test generation. In K. Koskimies, L. Kuzniarz, J. Nummenmaa, Z. Zhang, eds., *Proc. of 3rd Nordic Wksh. on UML and Software Modeling, NWUML 2005 (Tampere, Aug. 2005)*, pp. 208-216. Univ. of Tampere, 2005.
- J. Eder, H.-M. Haav, A. Kalja, J. Penjam, eds. *Proc. of 9th East-European Conf. on Advances in Databases and Information Systems, ADBIS 2005 (Tallinn, Sept. 2005)*, v. 3631 of *Lect. Notes in Comput. Sci.*, xiii+391 pp. Springer, 2005. doi: 10.1007/11547686
- J. Eder, H.-M. Haav, A. Kalja, J. Penjam, eds. *Commun. of 9th East-European Conf. on Advances in Databases and Information Systems, ADBIS 2005 (Tallinn, Sept. 2005)*, v. 152 of *CEUR Wksh. Proc.*. RWTH Aachen, 2005. volume at publisher's website

- A. Eppendahl, R. Maigre. Mobile camera parameter recovery in an unknown environment without point features. In *Proc. of 2005 IEEE Int. Symp. on Computational Intelligence in Robotics and Automation, CIRA'05 (Espoo, June 2005)*, pp. 279-283. IEEE, 2005. doi: 10.1109/cira.2005.1554290

- J. Ernits. Memory arbiter synthesis and verification for a radar memory interface card. *Nordic J. of Computing*, v. 12, n. 2, pp. 68-88, 2005.

- P. Grigorenko, A. Saabas, E. Tyugu. COCOVILA - compiler-compiler for visual languages. In J. Boyland, G. Hedin, eds., *Proc. of 5th Wksh. on Language Descriptions, Tools and Applications, LDTA'05 (Edinburgh, Apr. 2005), Electron. Notes in Theor. Comput. Sci.*, v. 141, n. 4, pp. 137-142. Elsevier, 2005. doi: 10.1016/j.entcs.2005.05.009

- P. Grigorenko, A. Saabas, E. Tyugu. Visual tool for generative programming. In *Proc. of Joint 10th Europ. Software Engineering Conf., ESEC' 05, and 13th ACM SIGSOFT Int. Symp. on Foundations of Software Engineering, FSE-13 (Lisbon, Sept. 2005)*, pp. 249-252. ACM Press, 2005. doi: 10.1145/1081706.1081747

- P. Grigorenko, A. Saabas, E. Tyugu. Visual tool for generative programming. *ACM SIGSOFT Softw. Engin. Notes*, v. 30, n. 5, pp. 249-252. 2005. doi: 10.1145/1095430.1081747

- G. Grossschmidt, M. Harf, M. Djurovic. Modelling and simulation of steady-state conditions of a hydraulic load-sensing system. In *Proc. of Int. Scientific-Technical Conf. "Hydraulics and Pneumatics 2005"(Wroclaw, May 2005)*, pp. 439-447. 2005.

- G. Grossschmidt, M. Harf. Modelling and simulation of hydraulic load-sensing systems using object-oriented programming environment. In *Proc. of 19th Europ. Conf. on Modelling and Simulation, ECMS 2005: Simulation in Wider Europe (Riga, June 2005)*, pp. 605-609. Europ. Council for Modelling and Simulation, 2005.

- K. Koskimies, M. Meriste, guest eds., *Proc. of Estonian Acad. of Sci., Engineering*, v. 11, n. 4 (Selected Papers from 9th Symp. on Programming Languages and Software Tools, SPLST 2005, Tartu, Aug. 2005), 2005.

- V. Kotkas. Structural synthesis of programs with preconditions. In V. Vene, M. Meriste, eds., *Proc. of 9th Symp. on Programming Languages and Software Tools, SPLST 2005 (Tartu, Sept. 2005)*, pp. 70-81. Univ. of Tartu, 2005.

- T. Lints. Multiagent modelling of a bacterial cell, a DnaA titration model based agent model as an example. In V. Vene, M. Meriste, eds., *Proc. of 9th Symp. on Programming Languages and Software Tools, SPLST 2005 (Tartu, Aug. 2005)*, pp. 82-96. Univ. of Tartu, 2005.

- M. Meriste, J. Helekivi, T.Kelder, A. Marandi, L. Mõtus, J. Preden. Location awareness of information agents. In J. Eder, H.-M. Haav, A. Kalja, J. Penjam, eds., *Proc. of 9th East European Conf. on Advances in Databases and Information Systems, ADBIS 2005 (Tallinn, Sept. 2005)*, v. 3631 of *Lect. Notes in Comput. Sci.*, pp. 199-208. Springer, 2005. doi: 10.1007/11547686_15

- M. Meriste, T. Kelder, J. Helekivi, L. Motus. C# templates for time-aware agents. In C.-S. Chen, J. Filipe, I. Seruca, J. Cordeiro, eds., *Proc. of 7th Int. Conf. on Enterprise Information Systems, ICEIS 2005 (Miami, FL, May 2005)*, v. 4, pp. 247-250. INSTICC Press, 2005.

- M. Meriste, T. Kelder, J. Helekivi, A. Marandi, L. Motus. On geospatial agents. In J. Cordeiro, V. Pedrosa, B. Encarnação, J. Filipe, eds., *Proc. of 1st Int. Conf. on Web Information Systems and Technologies, WEBIST 2005 (Miami, FL, May 2005)*, pp. 210-213. INSTICC Press, 2005.

- F. Miyawaki, K. Masamune, S. Suzuki, K. Yoshimitsu, J. Vain. Scrub nurse robot system - intraoperative motion analysis of a scrub nurse and timed-automata-based model for surgery. *IEEE Trans. on Industrial Electronics*, v. 52, n. 5, pp. 1227-1235, 2005. doi: 10.1109/tie.2005.855692

- L. Motus, M. Meriste, W. Dosch. Time-awareness and proactivity in models of interactive computation. In D. Goldin, M. Viroli, eds., *Proc. of Wksh. on the Foundations of Interactive Computation, FinCo 2005 (Edinburgh, Apr. 2005), Electron. Notes in Theor. Comput. Sci.*, v. 141, n. 5, pp. 69-95, 2005. doi: 10.1016/j.entcs.2005.05.017

- L. Motus, R. Vingerhoeds, M. Meriste. Challenges for real-time systems engineering. Part 1: State of the art. *Proc. of Estonian Acad. of Sci., Engineering*, v. 11, n. 1, pp. 3-17, 2005.

- L. Motus, R. Vingerhoeds, M. Meriste. Challenges for real-time systems engineering. Part 2: Towards time-aware technology. *Proc. of Estonian Acad. of Sci., Engineering*, v. 11, n. 1, pp. 18-30, 2005.
- K. Ohnuma, K. Masamune, K. Shinohara, J. Vain, Y. Fukui, F. Miyawaki. Surgical scenario for laparoscopic surgery with timed automata. *Int. Congress Series*, v. 1281, p. 1345, 2005. doi: 10.1016/j.ics.2005.03.145
- H. Rennik, J. Vain. Combined method of load planning for production lines. *Machine Engineering*, v. 5, n. 3-4, pp. 153-165, 2005.
- J. Sanko. Evolutionary program construction. In R. Matoušek, P. Ošmera, eds., *Proc. of 11th Int. Conf. on Soft Computing, MENDEL 2005 (Brno, June 2005)*, pp. 73-79. Brno Univ. of Techn., 2005.
- R. Savimaa. Using agent and UML technologies in modelling organizations: the case of a vehicle theft. *Proc. of Estonian Acad. of Sci., Engineering*, v. 11, n. 1, pp. 31-45, 2005.
- R. Savimaa. Modelling emergent behaviour of organisations: time-aware. V. 22 of *Theses of Tallinn Univ. of Technology C*. Tallinn Univ. of Technology, 2005. thesis at TUT DL
- E. Tyugu. Describing knowledge architectures. In Y. Kiyoki et al., *Proc. of 15th European-Japanese Conf. on Information Modelling and Knowledge Bases, EJC 2005 (Tallinn, May 2005)*, pp. 356-361. Tallinn Univ. of Techn., 2005.
- E. Tyugu. Metainterfaces support for structural and object-oriented software composition. In H. R. Arabnia, H. Reza, eds., *Proc. of Int. Conf. on Software Engineering Research and Practice, SERP 2005 (Las Vegas, NV, June 2005), vs. 1 and 2*, pp. 189-192. CSREA Press, 2005.
- E. Tyugu, M. Matskin. Logical instruments for dynamic service composition. In H. Arabnia, ed., *Proc. of Int. Symp. on Web Services and Applications, ISWS 2005 (Las Vegas, NV, 2005)*, pp. 87-93. CSREA Press, 2005.
- J. Vain, I. Randvee, T. Riismaa. Two-phase technique for assembly line balancing. In P. Horacek, M. Simandl, P. Zitek, eds., *Prep. of 16th IFAC World Congress (Prague, July 2005)*, 6 pp. 2006.
- E. Vainikko. Fortran95 ja MPI. 135 lk. TÜ Kirjastus, 2005.
- V. Vene, M. Meriste, eds., *Proc. of 9th Symp. on Programming Languages and Software Tools, SPLST 2005 (Tartu, Sept. 2005)*, 234 pp. Univ. of Tartu, 2005.

2006

- W. Dosch, T. Tamme. Designing a conditional merge component. In J. Jackson, ed., *Proc. of 21st Int. Conf. on Computers and Their Applications (Seattle, WA, March 2006)*, pp. 64-71. ISCA, 2006.
- A. Eppendahl, A. Ojamaa. Seeing empty space in an environment without silhouettes. In K. Murase, K. Sekiyama, N. Kubota, T. Naniwa, J. Sitte, eds., *Proc. of 3rd Int. Symp. on Autonomous Minirobots for Research and Edutainment, AMiRE 2005 (Fukui, Sept. 2005)*, pp. 27-32. Springer, 2006. doi: 10.1007/3-540-29344-2_4
- A. Eppendahl, S. Sajnani. Two steps toward a physically autonomous self-replicating system. In K. Murase, K. Sekiyama, N. Kubota, T. Naniwa, J. Sitte, eds., *Proc. of 3rd Int. Symp. on Autonomous Minirobots for Research and Edutainment, AMiRE 2005 (Fukui, Sept. 2005)*, pp. 281-286. Springer, 2006. doi: 10.1007/3-540-29344-2_42
- J. Ernits, A. Kull, K. Raiend, J. Vain. Generating tests from EFSM models using guided model checking and iterated search refinement. In K. Havelund, M. Núňez, G. Rosu, B. Wolff, eds., *Revised Selected Papers from 1st Combined Int. Wkshs. on Formal Approaches to Testing and Runtime Verification, FATES/RV 2006 (Seattle, WA, Aug. 2006)*, v. 4262 of *Lect. Notes in Comput. Sci.*, pp. 85-89. Springer, 2006. doi: 10.1007/11940197_6
- P. Grigorenko, E. Tyugu. Deep semantics of visual languages. In E. Tyugu and T. Yamaguchi, eds., *Proc. of 7th Joint Conf. on Knowledge-Based Software Engineering, JCKBSE 2006 (Tallinn, Aug. 2006)*, v. 140 of *Frontiers in Artificial Intelligence and Applications*, pp. 83-95. IOS Press, 2006. article at IOS Press BooksOnline

- G. Grossschmidt, M. Harf, T. Sallaste. Modelling and simulation of fluid power systems in object-oriented programming environment. In *Proc. of 8th Biennial ASME Conf. on Engineering Systems Design and Analysis, ESDA 2006 (Torino, July 2006)*, paper ESDA2006-95387, 10 pp. ASME, 2006.
- J. Helander, J. Preden. Adapting the auto to a new tune. In *Proc. of 1st Wksh. on Models and Analysis for Automotive Systems (Rio de Janeiro, Dec. 2006)*, pp. 21-24. 2006.
- A. Karpištšenko. Enhancement of development technologies for agent-based software engineering. In J.-M. Bruel, ed., *Revised Selected Papers from Satellite Events at MODELS 2005 Conf. (Montego Bay, Oct. 2005)*, v. 3844 of *Lect. Notes in Comput. Sci.*, pp. 343-344. Springer, 2006. doi: 10.1007/11663430_38
- V. Kotkas. Preconditions for structural synthesis of programs. In *Prel. Proc. of 6th Int. Andrei Ershov Memorial Conf. on Perspective of System Informatics, PSI 2006 (Novosibirsk, June 2006)*, pp. 166-175. A. P. Ershov Inst. of Informatics Systems, Novosibirsk, 2006.
- A. Kull, K. Raiend, J. Ernits, J. Vain. Generating TTCN-3 test cases from EFSM models of reactive software using model checking. In Ch. Hochberger, R. Liskowsky, eds., *Proc. of Informatik 2006: Informatik für Menschen (Dresden, Oct. 2006), v. 2*, v. P-94 of *Lect. Notes in Informatics*, pp. 241-248. Gesellschaft für Informatik, 2006.
- M. Matskin, E. Tyugu. Logic for higher-order workflow of composite web services. In *Proc. of Int. Conf. on Semantic Web and Web Services, SWWS '06 (Las Vegas, NV, June 2006)*, pp. 122-128. CSREA Press, 2006.
- L. Motus, M. Meriste, J.-S. Preden. Network enabled capabilities - Grassroots perspectives. In *Proc. of NATO RTO IST Panel Symp. on Dynamic Communication Management, IST-062/RSY-016*, pp. 16/1-16/13. 2006
- U. Norbisrath, I. Armac, D. Retkowitz, P. Salumaa. Modelling ehome systems. In *Proc. of 4th Int. Wksh. on Middleware for Pervasive and Ad-Hoc Computing, MPAC 2006 (Melbourne, Nov./Dec. 2006)*, v. 182 of *ACM Int. Conf. Series*, 4 pp. ACM Press, 2006. doi: 10.1145/1169075.1169079
- U. Norbisrath, C. Mosler. Functionality configuration for ehome systems. In H. Erdogmus, E. Stroulia, D. A. Stewart, eds., *Proc. of 2006 Conf. of Center for Advanced Studies on Collaborative Research, CASCON 2006 (Toronto, Oct. 2006)*, pp. 95-107. ACM Press, 2006. doi: 10.1145/1188966.1188977
- U. Norbisrath, C. Mosler, I. Armac. The ehome configurator tool suite. In R. Meersman, Z. Tari, P. Herrero, eds., *Proc. of OTM 2006 Confederated Int. Workshops and Posters (Montpellier, Oct./Nov. 2006), part 2*, v. 4278 of Lect. Notes in Comput. Sci., pp. 1315-1324. Springer, 2006. doi: 10.1007/11915072_35
- K. Ohnuma, K. Masamune, K. Yoshimitsu, T. Sadahiro, J. Vain, Y. Fukui, F. Miyawaki. Timed-automata-based model for laporoscopic surgery and intraoperative motion recognition of a surgeon as the interface connecting the surgical scenario and the real operating room. *Int. J. of Computer Assisted Radiology and Surgery*, v. 1, suppl. 7, pp. 442-445, 2006.
- T. Otto, J. Vain. Model checking in planning resource-sharing based manufacturing. In A. Dolgui, G. Morel, C. E. Pereira, eds., *Prep. of 12th IFAC Symp. on Information Control Problems in Manufacturing, INCOM 2006 (St. Etienne, May 2006), v. 2: Industrial Engineering*, pp. 535-540. École Nat. Super. des Mines, 2006.
- T. Otto, J. Vain. Model checking in planning resource-sharing based manufacturing. In A. Dolgui, G. Morel, C. E. Pereira, eds., *Proc. of 12th IFAC Symp. on Information Control Problems in Manufacturing, INCOM 2006 (St. Etienne, May 2006), v. 2: Industrial Engineering, IFAC Proc. Vols.*, pp. 523-528. Elsevier, 2006.
- J.-S. Preden. Communication area based positioning. In *Proc. of 3rd IEEE Int. Conf. on Mobile Ad-hoc and Sensor Systems, MASS 2006 (Vancouver, BC, Oct. 2006)*, pp. 336-347. IEEE, 2006. doi: 10.1109/mobhoc.2006.278573
- J.-S. Preden, J. Helander. Auto-adaptation driven by observed context histories. In *Proc. of 2nd Int. Wksh. on Exploiting Context Histories in Smart Environments - Infrastructures and Applications, ECHISE 2006 (Orange County, CA, Sept. 2006)*. 2006.
- R. Scheichl, E. Vainikko. Robust aggregation-based coarsening for additive Schwarz in the case of highly variable coefficients. In P. Wesseling, E. Oñate, J. Périaux, eds., *Proc. of Europ. Conf. on Computational Fluid Dynamics, ECCOMAS CFD 2006 (Egmond aan Zee, Sept. 2006)*, 16 pp. Techn. Univ. Delft, 2006.
- S. Schulz, G. Sutcliffe, T. Tammet, guest eds. *Int. J. of Artif. Intell. Tools*, v. 15, n. 1 (Special Issue on Empirically Successful First Order Reasoning), 130 pp., 2006. doi: 10.1142/S0218213006002539

- J. Simm. Learning methods of body schemas for robots with manipulators. In O. Vacilecas et al., *Commun. of 7th Int. Baltic Conf. on Databases and Information Systems, Baltic DB&IS 2006 (Vilnius, July 2006)*, pp. 344-348. VGTU Press Technika, 2006.

- T. Tammet, H.-M. Haav, V. Kadarpik, M. Kääramees. A rule-based approach to web-based application development. In O. Vacilecas et al., eds., *Proc. of 7th Int. Baltic Conf. on Databases and Information Systems, Baltic DB&IS 2006 (Vilnius, July 2006)*, pp. 202-211. IEEE, 2006. doi: 10.1109/dbis.2006.1678497

- T. Tammet, J. Vain, A. Kuusik. RFID-based knowledge space for service robot swarms. In O. Miyashita, ed., *Proc. of 3rd CoE Wksh. on Human Adaptive Mechatronics, HAM 2006 (Tokyo, March 2006)*, 6 pp. Tokyo Denki Univ., 2006. (CD-ROM).

- T. Tammet, J. Vain, A. Kuusik. Using RFID tags for robot swarm cooperation. *WSEAS Trans. on Systems*, v. 5, n. 5, pp. 1121-1128, 2006.

- E. Tyugu. Describing knowledge architectures. In Y. Kiyoki, J. Henno, H. Jaakkola, H. Kangassalo, eds., *Information Modelling and Knowledge Bases XVII*, v. 136 of *Frontiers of Artif. Intell. and Appl.*, pp. 329-340. IOS Press, 2006. article at IOS Press Booksonline

- E. Tyugu. Understanding knowledge architectures. *Knowledge-Based Systems*, v. 19, n. 1, pp. 50-56, 2006. doi: 10.1016/j.knosys.2005.07.006

- E. Tyugu. Extensible multipurpose simulation platform. In A. M. Madureira, ed., *Proc. of 6th WSEAS Int. Conf. on Simulation, Modelling and Optimization, SMO 2006 (Lisbon, Sept. 2006)*, pp. 738-743. WSEAS, 2006.

- E. Tyugu, T. Yamaguchi, eds. *Proc. of 7th Joint Conf. on Knowledge-Based Software Engineering, JCKBSE 2006 (Tallinn, Aug. 2006)*, v. 140 of *Frontiers in Artificial Intelligence and Applications*, xi+338 pp. IOS Press, 2006. volume at IOS Press BooksOnline

- J. Vain, I. Randvee, T. Riismaa. Two-phase technique for assembly line balancing. In P. Piztek, ed., *Proc. of 16th IFAC World Congress (Prague, July 2005)*, pp. 127-132. Elsevier, 2006.

2007

- J. Derrick, J. Vain, eds., *Proc. of 27th IFIP WG 6.1 Int. Conf. on Formal Techniques for Networked and Distributed Systems, FORTE 2007 (Tallinn, June 2007)*, v. 4574 of *Lect. Notes in Comput. Sci.*, xi+375 pp. Springer, 2007. doi: 10.1007/978-3-540-73196-2

- W. Dosch, M. Meriste, L. Motus. Enriching interactive components with again commands. In *Proc. of 2007 IEEE Int. Conf. on Electro/Information Technology (Chicago, IL, May 2007)*, v. 1, pp. 200-205. IEEE, 2007.

- J. Ernits. Two state space reduction techniques for explicit state model checking. V. 38 of *Theses of Tallinn Univ. of Technology*. Tallinn Univ. of Technology, 2007. thesis at TUT DL

- G. Grossschmidt, M. Harf. Design of a hydraulic-mechanical load-sensing system using object-oriented modelling and simulation. In I. Zelinka, Z. Oplatkova, A. Orsoni, W. W. Smari, eds., *Proc. of 21st Europ. Conf. on Modelling and Simulation, ECMS 2007: Simulations in United Europe (Prague, June 2007)*, pp. 383-390. ECMS, 2007.

- H.-M. Haav, T. Tammet, V. Kadarpik, K. Kindel, M. Kääramees. A semantic-based web service composition framework. In G. Magyar, G. Knapp, W. Wojtkowski, W. G. Wojtkowski, J. Zupancic, eds., *Advances in Information Systems Development: New Methods and Practice for the Networked Society [Proc. of 15th Int. Conf. on Information Systems Development, ISD 2006 (Budapest, Aug./Sept. 2006)], v. 1*, pp. 379-391. Springer, 2007. doi: 10.1007/978-0-387-70761-7_33

- J. Helander, R. Serg, M. Veanes, P. Roy. Adaptive futures: scalability for real-world computing. In *Proc. of 28 IEEE Int. Real-Time Systems Symp., RTSS 2007 (Tuczon, AZ, Dec. 2007)*, pp. 105-116. IEEE, 2007. doi: 10.1109/rtss.2007.8

- V. Kotkas. Preconditions for structural synthesis of programs. In A. Voronkov, I. Virbitskaite, eds., *Revised Papers from 6th Int. Andrei Ershov Memorial Conf. on Perspectives of System Informatics, PSI 2006 (Novosibirsk, June 2006)*, v. 4378 of *Lect. Notes in Comput. Sci.*, pp. 284-296. Springer, 2007. doi: 10.1007/978-3-540-70881-0_25

- M. Matskin, R. Maigre, E. Tyugu. Compositional logical semantics for business process languages. In *Proc. of 2nd Int. Conf. on Internet and Web Applications and Services, ICIW '07 (Morne, Mauritius, May 2007)*, 6 pp. IEEE CS Press, 2007. doi: 10.1109/iciw.2007.24
- U. Norbisrath. Configuring ehome systems, xiv+293 pp. Univ. of Tartu, 2007. thesis at RWTH DL
- U. Norbisrath, C. Mosler. Component-based development for ehome systems. In T. Simos, G. Psihoyios, eds., *Additional Papers from ICNAAM 2006 and ICCMSE 2006 at Int. e-Conf. of Computer Science 2006*, v. 8 of *Lect. Series on Computer and Computational Sciences*, pp. ?-?. BRILL, 2007.
- U. Norbisrath, C. Mosler. Tool support for the ehome specification, configuration, and deployment process. In O. Spaniol, ed., *Proc. of 1st Int. Wksh. on Mobile Services and Personalized Environments, MSPE 2007 (Aachen, Nov. 2006)*, v. P-102 of *Lect. Notes in Informatics*, pp. 109-122. Gesellschaft für Informatik, 2007.
- S. Nõmm, E. Petlenkov, J. Vain, K. Yoshimitsu, K. Ohnuma, T. Sadahiro, F. Miyawaki. NN-based ANARX model of the surgeon's hand for the motion recognition. In *Proc. of 4th COE Wksh. on Human Adaptive Mechatronics, HAM 2007 (Tokyo, March 2007)*, pp. 19-24. Tokyo Denki Univ., 2007.
- A. Ojamaa, E. Tyugu. Rich components of extendable simulation platform. In *Proc. of 2007 Int. Conf. on Modeling, Simulation and Visualization Methods, MSV 2007 (Las Vegas, NV, June 2007)*, pp. 121-127. CSREA Press, 2007.
- J. Preden, J. Helander. Situation aware computing in distributed computing systems. In Z. Horváth, L. Kozma, V. Zsók, eds., *Proc. of 10th Symp. on Programming Languages and Software Tools, SPLST 2007 (Dobogókö, June 2007)*, pp. 280-291. Eötvös Loránd Univ., 2007.
- J. Preden, M. Sarkans, T. Otto. Diagnostics of machining and assembly systems by networked motes. *Machine Engineering*, v. 7, n. 1-2, pp. 68-77, 2007.
- J. Preden, M. Sarkans, T. Otto, T. Reinson. Smart dust based modular laboratory kit for monitoring workshop machinery. In *Proc. of 8th Int. Wksh. on Research and Education in Mechatronics, REM 2007 (Tallinn, June 2007)*, pp. 311-316. Tallinn Univ. of Techn., 2007.
- R. Scheichl, E. Vainikko. Additive Schwarz and aggregation-based coarsening for elliptic problems with highly variable coefficients. *Computing*, v. 80, n. 4, pp. 319-343, 2007. doi: 10.1007/s00607-007-0237-z.
- T. Tammet, H.-M. Haav, V. Kadarpik, M. Kääramees. Using a rule language for capturing semantics in web-based systems. In O. Vasilecas, J. Eder, A. Caplinskas, eds., *Selected Papers from 7th Int. Baltic Conf. on Databases and Information Systems, Baltic DB&IS 2006 (Vilnius, July 2006)*, v. 155 of *Frontiers in Artificial Intelligence and Applications*, pp. 249-259. IOS Press, 2007. article at IOS Press BooksOnline
- E. Tyugu. *Algorithms and architectures of artificial intelligence*, v. 159 of *Frontiers in Artificial Intelligence and Applications*, ix+171 pp. IOS Press, 2007. book at IOS Press BooksOnline
- E. Tyugu, P. Grigorenko. Large-scale simulation platform. *WSEAS Trans. on Computers*, v. 6, n. 1, pp. 65-71, 2007.
- J. Vain, F. Miyawaki. Model learning for reactive motion planning in assisting robots. *Proc. of 27th IASTED Int. Conf. on Modelling, Identification, and Control, MIC 2008 (Innsbruck, Feb. 2008)*, Acta Press, to appear.
- J. Vain, K. Raiend, A. Kull, J. Ernits. Synthesis of test purpose directed reactive planning tester for nondeterministic systems. In *Proc. of 22nd IEEE/ACM Int. Conf. on Automated Software Engineering, ASE '07 (Atlanta, GA, Nov. 2007)*, pp. 363-372. ACM Press, 2007. doi: 10.1145/1321631.1321685
- E. Vainikko, G. Vainikko. A product quasi-interpolation method for weakly singular Volterra integral equations. In E. T. Simos, G. Psihoyios, C. Tsitouras, eds., *Proc. of Int. Conf. on Numerical Analysis and Applied Math. (Corfu, Sept. 2007)*, v. 936 of *Amer. Inst. of Phys. Conf. Proc.*, pp. 570-573. Springer, 2007. doi: 10.1063/1.2790209
- M. Veanes, J. Ernits, C. Campbell. State isomorphism in model programs with abstract data structures. In J. Derrick, J. Vain, eds., *Proc. of 27th IFIP WG 6.1 Int. Conf. on Formal Techniques for Networked and Distributed Systems, FORTE 2007 (Tallinn, June 2007)*, v. 4574 of *Lect. Notes in Comput. Sci.*, pp. 112-127. Springer, 2007. doi: 10.1007/978-3-540-73196-2_8

Krüptoloogia ja infoturve / Cryptology and information security

2003

- A. Ansper, A. Buldas, M. Freudenthal, J. Willemson. Scalable and efficient PKI for inter-organizational communication. In *Proc. of 19th Ann. Computer Security Applications Conf., ACSAC 2003 (Las Vegas, NV, Dec. 2003)*, pp. 308-318. IEEE CS Press, 2003. doi: 10.1109/csac.2003.1254335
- A. Buldas, P. Laud, J. Willemson. Graafid, 91 lk. TÜ Kirjastus, 2003.
- A. Buldas, M. Saarepera. Electronic signature system with small number of private keys. In *Pre-Proc. of 2nd Ann. PKI Research Wksh. 2003 (Gaithersburg, MD, Apr. 2003)*, pp. 96-108. 2003.
- K. Heero, M. Kruusmaa, J. Willemson. Path selection for mobile robots in dynamic environments. In *Proc. of European Conf. on Mobile Robots, ECMR 2003 (Warsaw, Sept. 2003)*. 2003
- S. Heiberg, U. Puus, P. Salumaa, A. Seeba. Pair-programming effect on developers productivity. In M. Marchesi, G. Succi, eds., *Proc. of 4th Int. Conf. on Extreme Programming and Agile Processes in Software Engineering, XP 2003 (Genova, May 2003)*, v. 2675 of *Lect. Notes in Comput. Sci.*, pp. 215-224. Springer, 2003. article at SpringerLink
- M. Kruusmaa, J. Willemson. Covering the path space: a casebase analysis for mobile robot path planning. *Knowledge Based Systems*, v. 16, n. 5-6, pp. 235-242, 2003. doi: 10.1016/s0950-7051(03)00024-8
- M. Roos, P. Laud, J. Willemson. Improving the Gnutella protocol against poisoning. In S. J. Knapskog, ed., *Proc. of 8th Nordic Wksh. on Secure IT Systems: Encouraging Cooperation, NordSec 2003 (Gjøvik, Oct. 2003)*, pp. 185-194. NTNU, Trondheim, 2003.
- J. Zaitseva, J. Willemson, J. Pöial. Tutorial environment for cryptographic protocols. In S. J. Knapskog, ed., *Proc. of 8th Nordic Wksh. on Secure IT Systems: Encouraging Cooperation, NordSec 2003 (Gjøvik, Oct. 2003)*, pp. 175-184. NTNU, Trondheim, 2003.

2004

- A. Buldas, M. Saarepera. On provably secure time-stamping schemes. In P. J. Lee, ed., *Proc. of 10th Int. Conf. on Theory and Application of Cryptology and Information Security, ASIACRYPT 2004 (Jeju Island, Dec. 2004)*, v. 3329 of *Lect. Notes in Comput. Sci.*, pp. 500-514. Springer, 2004. article at SpringerLink
- B. Goethals, S. Laur, H. Lipmaa, T. Mielikäinen. On private scalar product computation for privacy-preserving data mining. In *Pre-Proc. of 7th Int. Conf. on Information Security and Cryptology, ICISC 2004 (Seoul, Dec. 2004)*. 2004.
- K. Heero, J. Willemson, A. Aabloo, M. Kruusmaa. Robots find a better way: a learning method for mobile robot navigation in partially unknown environments. In F. Groen, N. Amato, A. Bonarini, E. Yoshida, B. Kröse, eds., *Proc. of 8th Conf. on Intelligent Autonomous Systems, IAS-8 (Amsterdam, March 2004)*, pp. 559-566. IOS Press, 2004.
- S. Laur, H. Lipmaa. On private similarity search protocols. In S. Liimatainen, T. Virtanen, eds., *Proc. of 9th Nordic Wksh. on Secure IT Systems, NordSec 2004 (Espoo, Nov. 2004)*, pp. 73-77. 2004.
- U. Puus, A. Seeba, P. Salumaa, S. Heiberg. Analyzing pair-programmer's satisfaction with the method, the result, and the partner. In J. Eckstein, H. Baumeister, eds., *Proc. of 5th Int. Conf. on Extreme Programming and Agile Processes in Software Engineering, XP 2004 (Garmisch-Partenkirchen, June 2004)*, v. 2971 of *Lect. Notes in Comput. Sci.*, pp. 246-249. Springer, 2004. article at SpringerLink
- J. Willemson, Y. Björnsson. SIX wins hex tournament. *ICGA J.*, v. 27, n. 3, p. 180, 2004.

2005

- A. Buldas, P. Laud, M. Saarepera, J. Willemson. Universally composable time-stamping schemes with audit. In J. Zhou, J. Lopez, R. H. Deng, F. Bao, eds., *Proc. of 8th Information Security Conf., ISC 2005 (Singapore, Sept. 2005)*, v. 3650 of *Lect. Notes in Comput. Sci.*, pp. 359-373. Springer, 2005. doi: 10.1007/11556992_26

- E. Elkind, H. Lipmaa. Hybrid voting protocols and hardness of manipulation. In X. Deng, D. Du, eds, *Proc. of 16th Int. Symp. on Algorithms and Computation, ISAAC 2005 (Sanya, Dec. 2005)*, v. 3827 of *Lect. Notes in Comput. Sci.*, pp. 206-215. Springer, 2005. doi: 10.1007/11602613_22

- B. Goethals, S. Laur, H. Lipmaa, T. Mielikäinen. On secure scalar product computation for privacy-preserving data mining. In C. Park, S. Chee, eds, *Revised Selected Papers from 7th Int. Conf. on Information Security and Cryptology, ICISC 2004 (Seoul, Dec. 2004)*, v. 3506 of *Lect. Notes in Comput. Sci*., pp. 104-120. Springer, 2005. doi: 10.1007/11496618_9

- K. Heero, A. Aabloo, M. Kruusmaa. Learning innovative routes for mobile robots in dynamic partially unknown environments. *Int. J. of Advanced Robotic Systems*, v. 2, n. 3, pp. 209-222, 2005. article at publisher's website

- K. Heero, A. Aabloo, M. Kruusmaa. On the utility of exploration on time-critical mobile robots missions. In *Proc. of 2nd Europ. Conf. on Mobile Robots, ECMR '05 (Ancona, Sept. 2005)*, pp. 152-157. 2005.

- S. Laur, H. Lipmaa, T. Mielikäinen. Private itemset support counting. In S. Qing, W. Mao, J. Lopez, eds., *Proc. of 5th Int. Conf. on Information and Communications Security, ICICS 2005 (Beijing, Dec. 2005)*, v. 3783 of *Lect. Notes in Comput. Sci.*, pp. 97-111. Springer, 2005. doi: 10.1007/11602897_9

- Y. Li, H. Lipmaa, D. Pei. On delegatability of four designated verifier signatures. In S. Qing, W. Mao, J. Lopez, eds, *Proc. of 5th Int. Conf. on Information and Communications Security, ICICS 2005 (Beijing, Dec. 2005)*, v. 3783 of *Lect. Notes in Comput. Sci.*, pp. 61-71. Springer, 2005. doi: 10.1007/11602897_6

- H. Lipmaa. An oblivious transfer protocol with log-squared communication. In J. Zhou, J. Lopez, R. H. Deng, F. Bao, eds., *Proc. of 8th Information Security Conf., ISC 2005 (Singapore, Sept. 2005)*, v. 3650 of *Lect. Notes in Comput. Sci.*, pp. 314-328. Springer, 2005. doi: 10.1007/11556992_23

- H. Lipmaa, D. Gollmann, eds. *Proc. of 10th Nordic Wksh. on Secure IT Systems, NordSec 2005 (Tartu, Oct. 2005)*, 167 pp. Univ. of Tartu, 2005.

- H. Lipmaa, G. Wang, F. Bao. Designated verifier signature schemes: attacks, new security notions and a new construction. In L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, M. Yung, eds., *Proc. of 32nd Int. Coll. on Automata, Languages and Programming, ICALP 2005 (Lisbon, July 2005)*, v. 3580 of *Lect. Notes in Comput. Sci.*, pp. 459-471. Springer, 2005. doi: 10.1007/11523468_38

- I. Tšahhirov, P. Laud. Digital signature in automatic analyses for confidentiality against active adversaries. In H. Lipmaa, D. Gollmann, eds., *Proc. of 10th Nordic Wksh. on Secure IT Systems, NordSec 2005 (Tartu, Oct. 2005)*, pp. 29-41. Univ. of Tartu, 2005.

- J. Willemson. Computer-clobber tournament at Tartu University. *ICGA J.*, v. 28, n. 1, pp. 51-54, 2005.

- J. Willemson, M. Winands. MILA wins clobber tournament. *ICGA J.*, v. 28, n. 3, pp. 188-190, 2005.

2006

- A. Alkassar, E. Andreeva, H. Lipmaa. SLC: efficient authenticated encryption for short packets. In J. Dittmann, ed., *Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der GI, Sicherheit 2006 (Magdeburg, Feb. 2006)*, v. P-77 of *Lect. Notes in Informatics*, pp. 270-278. Gesellschaft für Informatik (GI), 2006.

- A. Buldas, P. Laud, J. Priisalu, M. Saarepera, J. Willemson. Rational choice of security measures via multi-parameter attack trees. In J. López, ed., *Proc. of 1st Int. Wksh. on Critical Information Infrastructures Security, CRITIS '06 (Samos Island, Aug./Sept. 2006)*, pp. 232-243. Univ. of the Aegean, 2006.

- A. Buldas, P. Laud, J. Priisalu, M. Saarepera, J. Willemson. Rational choice of security measures via multi-parameter attack trees. In J. López, ed., *Revised Papers from 1st Int. Wksh. on Critical Information Infrastructures Security, CRITIS '06 (Samos Island, Aug./Sept. 2006)*, v. 4347 of *Lect. Notes in Comput. Sci.*, pp. 235-248. Springer, 2006. doi: 10.1007/11962977_19

- A. Buldas, S. Laur. Do broken hash functions affect the security of time-stamping schemes? In J. Zhou, M. Yung, F. Bao, eds., *Proc. of 4th Int. Conf. on Applied Cryptography and Network Security, ACNS 2006 (Singapore, June 2006)*, v. 3989 of *Lect. Notes in Comput. Sci.*, pp. 50-65. Springer, 2006. doi: 10.1007/11767480_4

- K. Heero. Path planning and learning strategies for mobile robots in dynamic partially unknown environment. V. 45 of *Diss. Math. Univ. Tartuensis*, 122 pp. + CD. Univ. of Tartu, 2006. handle: 10062/1354

- H. Lipmaa. Secure electronic voting protocols. In H. Bidgoli, ed., *Handbook of Information Security, v. 2: Information Warfare, Social, Legal, and International Issues and Security Foundations*, ch. 116. J. Wiley & Sons, 2006.

- S. Laur, H. Lipmaa, T. Mielikäinen. Cryptographically private support vector machines. In *Proc. of 12th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, KDD 2006 (Philadelphia, PA, Aug. 2006)*, pp. 618-624. ACM Press, 2006. doi: 10.1145/1150402.1150477

- S. Laur, K. Nyberg. Efficient mutual data authentication using manually authenticated strings. In D. Pointcheval, Y. Mu, K. Chen, eds., *Proc. of 5th Int. Conf. on Cryptology and Network Security, CANS 2006 (Suzhou, Dec. 2006)*, v. 4301 of *Lect. Notes in Comput. Sci.*, pp. 90-107. Springer, 2006. doi: 10.1007/11935070_6

- H. Lipmaa, M. Yung, D. Lin, eds. *Proc. of 2nd SKLOIS Conf. on Information Security and Cryptology, Inscrypt 2006 (Beijing, Nov./Dec. 2006)*, v. 4318 of *Lect. Notes in Comput. Sci.*, Springer, 2006. doi: 10.1007/11937807

- J. Willemson. On the Gordon and Loeb model for information security investment. In *Proc. of 5th Wksh. on the Economics of Information Security, WEIS 2006 (Cambridge, June 2006)*, pp. 87-98. Cambridge Univ., 2006.

- J. Willemson, M. Kruusmaa. Algorithmic generation of path fragment covers for mobile robot path planning. In *Proc. of 3rd IEEE Conf. on Intelligent Systems, IS 2006 (London, Sept. 2006)*, pp. 673-678. IEEE, 2006. doi: 10.1109/is.2006.348500

2007

- A. Buldas, A. Jürgenson. Does secure time-stamping imply collision-free hash functions? In W. Susilo, J. K. Liu, Y. Mu, eds., *Proc. of 1st Int. Conf. on Provable Security, ProvSec 2007 (Wollongong, Oct/Nov. 2007)*, v. 4784 of *Lect. Notes in Comput. Sci.*, pp. 138-150. Springer, 2007. doi: 10.1007/978-3-540-75670-5_9

- A. Buldas, S. Laur. Knowledge-binding commitments with applications in time-stamping. In T. Okamoto, X. Wang, eds., *Proc. of 10th Int. Conf. on Practice and Theory in Public-Key Cryptography, PKC 2007 (Beijing, Apr. 2007)*, v. 4450 of *Lect. Notes in Comput. Sci.*, pp. 150-165. Springer, 2007. doi: 10.1007/978-3-540-71677-8_11

- A. Buldas, T. Mägi. Practical analysis of e-voting systems. In A. Miyaji, H. Kikuchi, K. Rannenberg, eds., *Proc. of 2nd Int. Wksh. on Security, IWSEC 2007 (Nara, Oct. 2007)*, v. 4752 of *Lect. Notes in Comput. Sci.*, pp. 320-335. Springer, 2007. doi: 10.1007/978-3-540-75651-4_22

- A. Jürgenson, J. Willemson. Processing multi-parameter attacktrees with estimated parameter values. In A. Miyaji, H. Kikuchi, K. Rannenberg, eds., *Proc. of 2nd Int. Wksh. on Security, IWSEC 2007 (Nara, Oct. 2007)*, v. 4752 of *Lect. Notes in Comput. Sci.*, pp. 308-319. Springer, 2007. doi: 10.1007/978-3-540-75651-4_21

- S. Laur, H. Lipmaa. A new protocol for conditional disclosure of secrets and its applications. In J. Katz, M. Yung, eds., *Proc. of 5th Int. Conf. on Applied Cryptography and Network Security, ACNS 2007 (Zhuhai, June 2007)*, v. 4521 of *Lect. Notes in Comput. Sci.*, pp. 207-225. Springer, 2007. doi: 10.1007/978-3-540-72738-5_14

- S. Laur, S. Pasini. SAS-based group authentication and key agreement protocols. In *Proc. of 11th Int. Wksh. on Practice and Theory in Public Key Cryptography, PKC 2008 (Barcelona, March 2008), Lect. Notes in Comput. Sci.*, Springer, to appear.

- I. Tšahhirov, P. Laud. Application of dependency graphs to security protocol analysis. In *Proc. of 3rd Conf. on Global Computing, TGC 2007 (Sophia Antipolis, Nov. 2007), Lect. Notes in Comput. Sci.*, Springer, to appear.

Digitaalsüsteemide disain ja testimine / Design and test of digital systems

2003

- S. Devadze, E. Fomina, M. Kruus, and A. Sudnitson. Web-based system for sequential machines decomposition. In *Proc. of IEEE Region 8 Int. Conf. Computer as a Tool, EUROCON 2003 (Ljubljana, Sept. 2003)*, v. 1, pp. 57-61. 2003. article at IEEExplore
- S. Devadze, R. Gorjachev, A. Jutman, E. Orasson, V. Rosin, R. Ubar. E-learning tools for digital test. In *Distance Learning - Educational Environment of the XXI Century*, pp. 336-342. Minsk, 2003.
- P. Ellervee, J. Raik, V. Tihomirov. Fault emulation on FPGA: a feasibility study. In *Proc. of 21st IEEE NORCHIP Conf., 2003 (Riga, Nov. 2003)*, pp. 92-95. 2003.
- E. Fomina, A. Keevallik, M. Kruus, A. Sudnitson. A decomposition procedure for register-transfer level power management. In *Proc. of Int. Conf. on Computer Systems and Technologies, CompSysTech 2003 (Sofia, June 2003)*, v. 1, pp. 21-26. 2003.
- E. Fomina, A. Sudnitson. Synthesis of finite state machines networks guided by information relationships. In *Proc. of Int. Conf. on the Experience of Designing and Application of CAD Systems in Microelectronics, CADSM 2003 (Slavske, Feb. 2003)*. 2003.
- E. Gramatova, M. Hristov, W. Kuzmicz, V. Lantsov, M. Lobur, V. Nelayev, V. Stepanets, R. Ubar, H.-D. Wuttke. Results of international cooperation for development and exchange of Web-based educational materials. In *Distance Learning - Educational Environment of the XXI Century*, pp. 17-23. Minsk, 2003.
- V. Hahanov, R. Ubar. First East-West Design and Test Conference. *IEEE Design & Test of Computers*, v. 20, n. 6, p. 103, 2003.
- V. Hahanov, R. Ubar, S. Hyduke. Back-traced deductive-parallel fault simulation for digital systems. In *Proc. of Euromicro Symp. on Digital System Design, DSD 2003 (Belek-Antalaya, Sept. 2003)*, pp. 370-377. IEEE, 2003. doi: 10.1109/dsd.2003.1231969
- G. Jervan, P. Eles, Z. Peng, R. Ubar, M. Jenihhin. Hybrid BIST time minimization for core-based systems with STUMPS architecture. In *Proc. of 18th Int. Symp. on Defect and Fault Tolerance in VLSI Systems, DFT 2003 (Boston, MA, Nov. 2003)*, pp. 225-232. IEEE, 2003. article at IEEExplore
- G. Jervan, P. Eles, Z. Peng, R. Ubar, M. Jenihhin. Test time minimization for hybrid BIST of core-based systems. In *Proc. of 12th Asian Test Symp., ATS 2003 (Xi'an, Nov. 2003)*, pp. 318-323. IEEE, 2003. doi: 10.1109/ats.2003.1250830
- A. Jutman. On SSBDD model size and complexity. In *Proc. of 4th Electronic Circuits and Systems Conf. (Bratislava, Sept. 2003)*, pp. 17-22. 2003.
- A. Jutman, A. Sudnitson, R. Ubar, Digital design learning system based on Java applets. In *Proc. of 4th Ann. Conf. of LTSN Subject Centre for Information and Computer Sciences (Galway, Aug. 2003)*, pp. 183-187. 2003.
- A. Jutman, A. Sudnitsõn, R. Ubar. Web-based applet for teaching boundary scan standard IEEE 1149.1. In *Proc. of 10th Int. conf. on Mixed Design of Integrated Circuits and Systems, MIXDES 2003 (Lodz, June 2003)*, pp. 584-589. 2003.
- A. Jutman, A. Sudnitson, R. Ubar. Web-based training system for teaching principles of boundary scan technique. In *Proc. of 14th EAEEIE Ann. Conf. on Education in Electrical and Information Engineering, EAEEIE 2003 (Gdansk, June 2003)*, 4 pp. 2003.
- A. Jutman, A. Sudnitsõn, R. Ubar, D. Wuttke. Java applets support for an asynchronous-mode learning of digital design and test. In *Proc. of 4th Int. Conf. on Information Technology Based Higher Education and Training, ITHET 2003 (Marrakech, July 2003)*, pp. 397-401. IEEE, 2003.
- M. Kruus, A. Sudnitson. Virtual European Department of Computing project: problems and perspectives. In *Proc. of 30th Int. Conf. on Information Technologies in Science, Education, Telecommunication, Business, IT+SE 2003 (Yalta-Gurzuf, May 2003)*, pp. 280-283. 2003.

- A. Mekler, J. Raik. Multiple-objective backtrace for solving test generation constraints. In *Proc. of Int. Symp. on System-on-Chip, (Tampere, Nov. 2003)*, pp. 123-126. IEEE, 2003. doi: 10.1109/issoc.2003.1267732
- J. Raik, T. Nõmmeots, R. Ubar. New method of testability calculation to guide RT-level test generation. In *Proc. of 4th IEEE Latin-American Test Workshop, LATW 2003 (Natal, Feb. 2003)*, pp. 46-51. 2003.
- J. Raik, R. Raidma, R. Ubar. Explorations in low area overhead DfT techniques for sequential BIST. In *Proc. of 21st IEEE Conf. NORCHIP 2003 (Riga, Nov. 2003)*, pp. 220-223. 2003.
- A. Schneider, K.-H. Diener, G. Elst, R. Ubar, E. Ivask, J. Raik. Integration of digital test tools to the Internet-based environment MOSCITO. In *Proc. of 7th World Multiconf. on Systemics, Cybernetics and Informatics, SCI 2003 (Orlando, July 2003)*, pp. 136-141. IIIS, 2003.
- A. Sudnitson, A. Jamshanov. A FSM decomposition method for mixed synchronous / asynchronous implementation. In *Proc. of 17th Int. Conf. on Systems for Automation of Engineering and Research, SAER 2003 (Varna, Sept. 2003)*. 2003.
- R. Ubar. Decision diagrams and digital test. In *Proc. of 6th Int. Wksh. on Electronics, Control, Measurement and Signals (Liberec, June 2003)*, pp. 266-273. 2003.
- R. Ubar. Design error diagnosis with re-synthesis in combinational circuits. *J. of Electronic Testing: Theory and Applications*, v. 19, n. 1, pp. 73-82. 2003. doi: 10.1023/a:1021948013402
- R. Ubar. E-learning tools for the field of electronics design and test. In *Proc. of 4th Int. Conf. on Information Technology Based Higher Education and Training, ITHET 2003 (Marrakech, July 2003)*, pp. 285-290. 2003.
- R. Ubar. Mapping faults in hierarchical testing of digital systems. In *Proc. of Int. Conf. on Computer, Communication and Control Technologies, CCCT '03 (Orlando, July/Aug. 2003)*, pp. 14-19. IIIS, 2003.
- R. Ubar. Mapping physical defects to logic level for defect oriented testing. In *Proc. of Int. Symp. on Signals, Circuits and Systems, SCS 2003 (Iasi, July 2003)*, v. 2, pp. 453-456. IEEE, 2003. article at IEEExplore
- R. Ubar, M. Jenihhin, G. Jervan, Z. Peng. Test time minimization for hybrid BIST with test pattern broadcasting. In *Proc. of 21st IEEE NORCHIP Conf., 2003 (Riga, Nov. 2003)*, pp. 112-116. 2003.
- R. Ubar, E. Orasson. E-learning tool and exercises for teaching digital test. In *Proc. of 2nd IEEE Conf. on Signals, Systems, Decision and Information Technology (Sousse, March 2003)*, CIT-6, pp. 1-6. 2003.
- R. Ubar, J. Raik. Testing strategies for networks on chip. In A. Jantsch, H. Tenhunen, eds., *Networks on Chip*, pp. 131-152. Kluwer Acad. Publ., 2003. doi: 10.1007/0-306-48727-6_7
- R. Ubar, J. Raik, B. Klüver. Algorithms for hierarchical fault simulation in digital systems. In *Proc. of 10th Int. Conf. on Mixed Design of Integrated Circuits and Systems, MIXDES 2003 (Lodz, June 2003)*, pp. 530-535. 2003.

2004

- M. Brik, E. Ivask, J. Raik, R. Ubar. On using genetic algorithm for test generation. In *Proc. of 9th Biennial Baltic Electronics Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 233-236. Tallinn Univ. of Techn., 2004.
- M. Brik, J.Raik, R. Ubar, E. Ivask. GA-based test generation for sequential circuits. In *Proc. of 2nd East-West Design and Test Wksh., EWDTW 2004 (Alushta, Sept. 2004)*, pp. 30-24. 2004
- E. Dubrova, P. Ellervee, D. M. Miller, J. C. Muzio, A. J. Sullivan. TOP: an algorithm for three-level combinational logic optimisation. *IEE Proc.: Circuits, Devices and Systems*, v. 151, n. 4, pp. 307-314, 2004. doi: 10.1049/ip-cds:20040159
- P. Ellervee, J. Raik, V. Tihhomirov. Environment for fault simulation acceleration on FPGA. In *Proc. of 9th Biennial Baltic Electronics Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 217-220. Tallinn Univ. of Techn., 2004.
- P. Ellervee, J. Raik, V. Tihhomirov, K. Tammemäe. Evaluating fault emulation on FPGA. In J. Becker, M. Platzner, S. Vernalde, eds., *Proc. of 14th Int. Conf. on Field Programmable Logic and Application, FPL 2004 (Leuven, Aug./Sept. 2004)*, v. 3203 of *Lect. Notes in Comput. Sci.*, pp. 354-363. Springer, 2004. article at SpringerLink

- P. Ellervee, J. Raik, V. Tihhomirov, R. Ubar. FPGA based fault emulation of synchronous sequential circuits. In *Proc. of 22nd IEEE NORCHIP Conf., 2004 (Oslo, Nov. 2004)*, pp. 59-62. 2004. doi: 10.1109/norchp.2004.1423822
- E. Fomina, A. Sudnitson. Information relationships for decomposition of finite state machine. In *Proc. of 2nd IEEE East-West Design and Test Wksh., EWDTW 2004 (Alushta, Sept. 2004)*, pp. 41-47. 2004.
- E. Fomina, A. Sudnitson, R. Vasilyev. FSM's network encoding guided by information relationship measure. In *Proc. of 6th Int. Wksh. on Boolean Problems (Freiberg, Sept. 2004)*, pp. 55-62. 2004.
- E. Fomina, A. Sudnitsyn, R. Vasilyev. Optimization of FSMs network by new encoding strategy. In *Proc. of 9th Biennial Baltic Electronics Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 119-122. Tallinn Univ. of Techn., 2004.
- E. Fomina, P. Ellervee, M. Kruus, A. Sudnitson, K. Tammemae. Digital synthesis tools for education and research. In *Proc. of 18th Int. Conf. on Systems for Automation of Engineering and Research, SAER 2004 (Varna, Sept. 2004)*, pp. 160-164. 2004.
- V. Hahanov, R. Ubar. 2nd IEEE East-West Design and Test Workshop. *IEEE Design & Test of Computers*, v. 21, n. 6, pp. 594, 2004. doi: 10.1109/mdt.2004.82
- E. Ivask, P. Ellervee. VHDL front-end for high-level synthesis tool xTractor. In *Proc. of 9th Biennial Baltic Electronics Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 111-114. Tallinn Univ. of Techn., 2004.
- E. Ivask, J. Raik, R. Ubar, A. Schneider. Web-based environment: remote use of digital electronics test tools. In L. M. Camarinha-Matos, ed., *Virtual Enterprises and Collaborative Networks*, v. 149 of *Int. Feder. of Inform. Processing*, pp. 435-442. Kluwer Acad. Publ., 2004. doi: 10.1007/1-4020-8139-1_46
- E. Ivask, A. Jutman, E. Orasson, J. Raik, R. Ubar, H.-D. Wuttke. Research Environment for Teaching Digital Test. In *Proc. of Int. Conf. IWK (Ilmenau, Sept. 2004)*, pp. 468-473. 2004.
- G. Jervan, Z. Peng, R. Ubar, O. Korelina. An improved estimation methodology for hybrid BIST cost calculation. In *Proc. of 22nd IEEE NORCHIP Conf., 2004 (Oslo, Nov. 2004)*, pp. 297-300. 2004. doi: 10.1109/norchp.2004.1423882
- A. Jutman. At-speed on-chip diagnosis of board-level interconnect faults. In *Proc. of 9th IEEE European Test Symposium, ETS '04 (Ajaccio, May 2004)*, pp. 2-7. 2004. article at IEEExplore
- A. Jutman. Shift register based TPG for at-speed interconnect BIST. In *Proc. of 24th IEEE Int. Conf. on Microelectronics, MIEL '04 (Nis, May 2004)*, v. 2, pp. 751-754. 2004. article at IEEExplore
- A. Jutman. Selected issues of modeling, verification and testing of digital systems. V. 17 of *Theses of Tallinn Univ. of Technology C*. Tallinn Univ. of Technology, 2004.
- A. Jutman, E. Gramatova, T. Pikula, R. Ubar. E-learning tools for teaching self-test of digital electronics. In *Proc. of 15th EAEEIE Ann. Conf. on Innovation in Education for Electrical and Information Engineering (Sofia, May 2004)*, pp. 267-272. 2004.
- A. Jutman, A. Peder, J. Raik, M. Tombak, R. Ubar. Structurally synthesized binary decision diagrams. In *Proc. of 6th Int. Wksh. on Boolean Problems (Freiberg, Sept. 2004)*, pp. 271-278. 2004.
- A. Jutman, A. Sudnitson, R. Ubar, H.-D. Wuttke. Asynchronous e-learning resources for hardware design issues. In *Proc. of Int. Conf. on Computer Systems and Technologies, CompSysTech 2004 (Ruse, June 2004)*, v. IV, pp. 11.1-11.6, 2004.
- A. Jutman, A. Sudnitson, R. Ubar, H.-D. Wuttke. E-learning environment in the area of digital microelectronics. In *Proc. of 5th IEEE Int. Conf. on Information Technology Based Higher Education and Training, ITHET 2004 (Istanbul, May/June 2004)*, pp. 278-283. IEEE, 2004. doi: 10.1109/ithet.2004.1358178
- A. Jutman, R. Ubar, H.-D. Wuttke. Overview of e-learning environment for Web-based study of testing and diagnostics of digital systems. In *Pre-Proc. of 5th European Wksh. on Microelectronics Education, EWME 2004 (Lausanne, Apr. 2004)*, pp. 173-176. 2004.

- A. Jutman, R. Ubar, H.-D. Wuttke. Overview of e-learning environment for Web-based study of testing and diagnostics of digital systems. In A. M., Ionescu, M. Declercq, M. Kayal, Y. Leblebici, eds., *Proc. of 5th European Wksh. on Microelectronics Education, EWME 2004 (Lausanne, Apr. 2004)*, pp. 253-258. Kluwer Acad. Publ., 2004.
- N. Mazurova, J. Smahtina, R. Ubar. Hybrid functional BIST for digital systems. In *Proc. of 9th Biennial Baltic Electronics Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 205-208. TTU, 2004.
- J. Raik, P. Ellervee, V. Tihhomirov, R. Ubar. Fast fault emulation for synchronous sequential circuits. In *Proc. of 2nd East-West Design and Test Wksh., EWDTW 2004 (Alushta, Sept. 2004)*, pp. 35-40. 2004.
- J. Raik, A. Krivenko, R. Ubar. Comparative analysis of sequential test generation approaches. In *Proc. of 9th Biennial Baltic Electronics Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 225-228. Tallinn Univ. of Techn., 2004.
- J. Raik, E. Orasson, R. Ubar. Sequential circuits BIST with status BIT control. In *Proc. of 11th Int. Conf. on Mixed Design of Integrated Circuits and Systems, MIXDES 2004 (Szczecin, June 2004)*, pp. 507-510. 2004.
- J. Raik, R. Ubar. Enhancing hierarchical ATPG with a functional fault model for multiplexers. In *Proc. of 7th IEEE Wksh. on Design and Diagnostics of Electronic Circuits and Systems, DDECS 2004 (Stara Lesna, Apr. 2004)*, pp. 219-222. 2004.
- J. Raik, R. Ubar. Targeting conditional operations in sequential test pattern generation. In *Proc. of 9th IEEE European Test Symp., ETS 2004 (Ajaccio, May 2004)*, pp. 17-18. 2004.
- J. Raik, V. Govind, R. Ubar. RT-level test point insertion for sequential circuits. In *Proc. of 1st IEEE Int. Wksh. on Testability, IWoTA 2004 (Rennes, Nov. 2004)*, pp. 34-40. 2004. doi: 10.1109/iwota.2004.1428412
- Y. A. Skobtsov, D. E. Ivanov, V. Y. Skobtsov, R. Ubar. Evolutionary approach to the functional test generation for digital circuits. In *Proc. of 9th Biennial Baltic Electronics Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 229-232. Tallinn Univ. of Techn., 2004.
- A. Sudnitson. Register transfer low power design based on controller decomposition. In *Proc. of 24th IEEE Int. Conf. on Microelectronics, MIEL 2004 (Nis, May 2004)*, v. 2, pp. 735-738. 2004. article at IEEExplore
- R. Ubar. Diagnostic modelling of digital systems with decision diagrams. In *Proc. of Tomsk State University*, v. 1, n. 9, pp. 174-179, 2004.
- R. Ubar, M. Aarna, M. Brik, J. Raik. High-level fault modeling in digital systems. In *Proc. of Int. Conf. IWK (Ilmenau, Sept. 2004)*, pp. 486-491. 2004.
- R. Ubar, M. Aarna, H. Kruus, J. Raik. How to generate high quality tests for digital systems. In *Proc. of 2004 IEEE Int. Semiconductor Conf., CAS 2004 (Sinaia, Oct. 2004)*, v. 2, pp. 459-462. 2004. doi: 10.1109/smicnd.2004.1403048
- R. Ubar, M. Jenihhin, G. Jervan, Z. Peng. An iterative approach to test time minimization for parallel hybrid BIST architecture. In *Proc. of 5th IEEE Latin-American Test Wksh., LATW 2004, Digest of Papers (Cartagena, March 2004)*, pp. 98-103. 2004.
- R. Ubar, M. Jenihhin, G. Jervan, Z. Peng. An iterative approach to test time minimization for parallel hybrid BIST architectures. In *Proc. of System-on-Chip Conf. 2004 (Båstad, Apr. 2004)*. 2004.
- R. Ubar, M. Jenihhin, G. Jervan, Z. Peng. Hybrid BIST optimization for core-based systems with test pattern broadcasting. In *Proc. of 2nd IEEE Int. Wksh. on Electronic Design, Test and Applications, DELTA 2004 (Perth, Jan. 2004)*, pp. 3-8. IEEE, 2004. doi: 10.1109/delta.2004.10057
- R. Ubar, N. Mazurova, J. Smahtina, E. Orasson, J. Raik. HyFBIST: hybrid functional built-in self-test in microprogrammed data-paths of digital systems. In *Proc. of 11th Int. Conf. on Mixed Design of Integrated Circuits and Systems, MIXDES 2004 (Szczecin, June 2004)*, pp. 497-502. 2004.
- R. Ubar, T. Vassiljeva, J. Raik, A. Jutman, M. Tombak, A. Peder. Optimization of structurally synthesized BDDs. In *Proc. of 4th IASTED Int. Conf. on Modelling, Simulation and Optimization, MSO 2004 (Kauai, HW, Aug. 2004)*, pp. 234-240. Acta Press, 2004. article at publisher's website

- R. Ubar, H.-D. Wuttke. Research and training scenarios for design and test of SOC. *In Proc. of World Congress on Engineering and Technology Education (Guaruja/Santos, March 2004)*, pp. 320-324. 2004.
- R. Ubar, H.-D. Wuttke. Research and training environment for digital design and test. In *Proc. of 34th Ann. Frontiers in Education Conf., FIE 2004 (Savannah, GA, Oct. 2004)*, v. 3, pp. S3F/18-S3F/23. 2004. doi: 10.1109/fie.2004.1408779
- V. Vislogubov, A. Jutman, H. Kruus, E. Orasson, J. Raik, R. Ubar. Diagnostic software with WEB interface for teaching purposes. In *Proc. of 9th Biennial Baltic Electronics Conf., BEC 2004 (Tallinn, Oct. 2004)*, pp. 255-258. Tallinn Univ. of Techn., 2004.

2005

- M. Balas, M. Fisherova, E. Gramatova, A. Jutman, Z. Kotasek, O. Novak, T. Pikula, J. Raik, J. Strnadel, R. Ubar, J. Zahradka. Testing tools for training and education. In *Proc. of 12th Int. Conf. Mixed Design of Integrated Circuits and Systems, MIXDES 2005 (Kraków, June 2005)*, pp. 671-676, 2005.
- T. Bengtsson, A. Jutman, S. Kumar, R. Ubar. Delay testing of asynchronous NOC interconnects. In *Proc. of 12th Int. Conf. Mixed Design of Integrated Circuits and Systems, MIXDES 2005* (Kraków, June 2005), pp. 419-424, 2005.
- T. Bengtsson, A. Jutman, R. Ubar, S. Kumar. A method for crosstalk fault detection in on-chip buses. In *Proc. of 23rd IEEE NORCHIP Conf., 2005 (Oulu, Nov. 2005)*, pp. 285-288. 2005. doi: 10.1109/norchp.2005.1597045
- M. Brik, E. Fomina, R. Ubar. A proposal for optimisation of low-powered FSM testing. In *Proc. of 3rd East-West Design & Test Wksh., EWDTW 2005 (Odessa, Sept. 2005)*, pp. 15-20, 2005.
- S. Devadze, A. Sudnitson. FSM decomposition software for education and research. In *Proc. of IEEE Int. Conf. Computer as a Tool, EUROCON 2005 (Belgrade, Nov. 2005)*, v. 1, pp. 839-482. IEEE, 2005. article at IEEExplore
- E. Gramatová, R. Ubar, W.Pleskacz, M. Fischerová. Defects, faults, fault models. In O. Novák, E. Gramatová, R. Ubar, eds. *Handbook of Testing Electronic Systems*, ch. 2, pp. 26-96. Czech Techn. Univ. Publ. House, 2005.
- J. Fomina. Low power finite state machine synthesis. V. 28 of *Theses of Tallinn Univ. of Technology C*. Tallinn Univ. of Technology, 2005. thesis at TUT DL
- E. Fomina, M. Brik, R. Vasilyev, A. Sudnitsyn. A new approach to state encoding of low power FSM. In *Proc. of 3rd East-West Design & Test Wksh., EWDTW 2005 (Odessa, Sept. 2005)*, pp. 21-26, 2005.
- E. Fomina, A. Sudnitson. Extended finite-state machine decomposition for low power. In *Proc. of 19th Int. Conf. on Systems for Automation of Engineering and Research, SAER 2005 (Varna, Sept. 2005)*, pp. 126-131. 2005.
- Z. He, G. Jervan, P. Eles, Z. Peng. Power-constrained hybrid BIST test scheduling in an abort-on-first-fail test environment. In *Proc. of 8th Euromicro Conf. on Digital Systems Design, DSD 2005 (Porto, Aug./Sept. 2005)*, pp. 83-86. 2005. doi: 10.1109/dsd.2005.63
- G. Jervan, R. Ubar, Z. Peng, P. Eles. An approach to system level design for testability. In M. Sonza Reorda, Z. Peng, M. Violante, eds., *System-level Test and Validation of Hardware/Software Systems*, v. 17 of *Springer Series in Advanced Microelectronics*, ch. 8, pp. 121-149. Springer, 2005. doi: 10.1007/1-84628-145-8_8
- G. Jervan, R. Ubar, Z. Peng, P. Eles. Test generation: a hierarchical approach. In M. Sonza Reorda, Z. Peng, M. Violante, eds., *System-level Test and Validation of Hardware/Software Systems*, v. 17 of *Springer Series in Advanced Microelectronics*, ch. 5, pp. 67-81. Springer, 2005. doi: 10.1007/1-84628-145-8_5
- G. Jervan, Z. Peng, R. Ubar, O. Korelina. An improved estimation technique for hybrid BIST test set generation. In *Proc. of 8th IEEE Wksh. on Design and Diagnostics of Electronic Circuits and Systems, DDECS 2005 (Sopron, Apr. 2005)*, pp. 182-185. 2005.
- A. Jutman. Efficient at-speed interconnect BIST and diagnosis framework. In *Informal Digest of Papers of 10th IEEE European Test Symp., ETS 2005 (Tallinn, May 2005)*, pp. 257-258. Tallinn Univ. of Techn., 2005.

- A. Jutman. At-speed BIST for board-level interconnect. In *Proc. of IEEE European Board Test Wksh., EBTW 2005 (Tallinn, May 2005)*. 2005.
- A. Jutman, M. Kruus, A. Sudnitson, R. Ubar, H.-D. Wuttke. Web-based software package for e-learning and research training in digital system design. In *Proc. of 32nd Int. Conf. on Information Technologies in Science, Education, Telecommunication, Business, IT+SE 2005 (Gurzuf, May? 2005)*, pp. 306-308. 2005.
- A. Jutman, J. Raik, R. Ubar, V. Visloglubov. An educational environment for digital testing: hardware, tools, and Web-based runtime platform. In *Proc. of 8th Euromicro Conf. on Digital Systems Design, DSD 2005 (Porto, Aug./Sept. 2005)*, pp. 412-419. 2005. doi: 10.1109/dsd.2005.15
- A. Jutman, V. Rosin, A. Sudnitson, R. Ubar, H.-D. Wuttke. A system for teaching basic and advanced topics of IEEE 1149.1 boundary scan standard. In *Proc. of 16th EAEEIE Ann. Conf. on Innovation in Education for Electrical and Information Engineering (Lappeenranta, June 2005)*. 2005.
- A. Jutman, R. Ubar, J. Raik. Generic interconnect BIST for network-on-chip. In *Proc. of 8th IEEE Wksh. on Design and Diagnostics of Electronic Circuits and Systems, DDECS 2005 (Sopron, Apr. 2005)*, pp. 224-227. 2005.
- A. Jutman, R. Ubar, J. Raik. New built-in self-test scheme for SoC interconnect. In *Proc. of 9th World Multi-Conf. on Systemics, Cybernetics and Informatics, SCI 2005 (Orlando, FL, July 2005)*, v. 4, pp. 19-24. IIIS, 2005.
- A. Jutman, R. Ubar, V. Rosin. A software system for IEEE 1149.1 boundary scan design, simulation and demonstration. In *Proc. of IEEE European Board Test Wksh., EBTW 2005 (Tallinn, May 2005)*. 2005.
- A. Yu. Matrosova, A. G. Pleshkov, R. R. Ubar. Construction of the tests of combinational circuit failures by analyzing the orthogonal disjunctive normal forms represented by the alternative graphs. *Automation and Remote Control*, v. 66, n. 2, pp. 313-327. 2005. doi: 10.1007/s10513-005-0054-9
- A. Yu. Matrosova, A. G. Pleshkov, R. R. Ubar. Test generation for combinational circuits by orthogonal disjunctive normal forms and SSBDDs. *Avtomatika i Telemekhanika*, v. 2005, n. 2, pp. 158-174. 2005.
- O. Novák, E. Gramatová, R. Ubar, eds. *Handbook of Testing Electronic Systems*. 402 pp. Czech Techn. Univ. Publ. House, 2005.
- O. Novák, E. Gramatová, R. Ubar. IST project REASON - Handbook of testing electronic systems. In *Proc. of 5th European Dependable Computing Conf., EDCC-5 (Budapest, Apr. 2005)*, pp. 15-18. IEEE, 2005.
- J. Raik, P. Ellervee, V. Tihhomirov, R. Ubar. Improved fault emulation for synchronous sequential circuits. In *Proc. of 8th Euromicro Conf. on Digital Systems Design, DSD 2005 (Porto, Aug./Sept. 2005)*, pp. 72-78. 2005. doi: 10.1109/dsd.2005.50
- J. Raik, M. Jenihhin, R. Adelbert. Sequential circuits BIST synthesis from signal specifications. In *Proc. of 23rd IEEE NORCHIP Conf. (Oulu, Nov. 2005)*, pp. 196-199. 2005. doi: 10.1109/norchp.2005.1597023
- J. Raik, T. Nõmmeots, R. Ubar. A new testability calculation method to guide RTL test generation. *J. of Electronic Testing: Theory and Applications*, v. 21, n. 1, pp. 73-84. 2005. doi: 10.1007/s10836-005-5288-5
- J. Raik, R. Ubar, S. Devadze, A. Jutman. Efficient single-pattern fault simulation on structurally synthesized BDDs. In M. dal Chin, M. Kaåniche, A. Pataricza, eds., *Proc. of 5th European Dependable Computing Conf., EDCC-5 (Budapest, Apr. 2005)*, v. 3463 of *Lect. Notes in Comput. Sci.*, pp. 332-344. Springer, 2005. doi: 10.1007/11408901_25
- J. Raik, R. Ubar, J. Sudbrock, W. Kuzmicz, W. Pleskacz. Deterministic defect-oriented test generation for digital circuits. In *Proc. of 6th IEEE Latin-American Test Wksh., LATW 2005 (Salvador de Bahia, March/Apr. 2005)*, pp. 325-330. 2005.
- J. Raik, R. Ubar, J. Sudbrock, W. Kuzmicz, W. Pleskacz. DOT: new deterministic defect-oriented ATPG tool. In *Proc. of 10th IEEE European Test Symp., ETS 2005 (Tallinn, May 2005)*, pp. 96-101. IEEE, 2005. doi: 10.1109/ets.2005.15
- Y. A. Skobtsov, D. E. Ivanov, V. Y. Skobtsov, R. Ubar, J. Raik. Evolutionary approach to test generation for functional BIST. In *Informal Digest of Papers of 10th IEEE European Test Symp., ETS 2005 (Tallinn, May 2005)*, pp. 151-155. Tallinn Univ. of Techn., 2005.

- J. Sudbrock, J. Raik, R. Ubar, W. Kuzmicz, W. Pleskacz. Defect-oriented test- and layout-generation for standard-cell ASIC designs. In *Proc. of 8th Euromicro Conf. on Digital Systems Design, DSD 2005 (Porto, Aug./Sept. 2005)*, pp. 79-82. 2005. doi: 10.1109/dsd.2005.30

- R. Ubar. Decision diagrams and digital test (invited paper). In *Proc. of 41th Int. Conf. on Microelectronics, Devices and Materials, MIDEM 2005 (Ribno at Bled, Sept. 2005)*, pp. 15-26. 2005.

- R. Ubar. *Digitaalsüsteemide diagnostika I: Diagnostiline modelleerimine.* 148 lk. TTÜ Kirjastus, 2005.

- R. Ubar. Introduction. In O. Novák, E. Gramatová, R. Ubar, eds. *Handbook of Testing Electronic Systems*, ch. 1, pp. 18-23. Czech Techn. Univ. Publ. House, 2005.

- R. Ubar, E. Gramatová, M. Fischerová. Test generation techniques and algorithms. In O. Novák, E. Gramatová, R. Ubar, eds. *Handbook of Testing Electronic Systems*, ch. 3, pp. 99-173. Czech Techn. Univ. Publ. House, 2005.

- R. Ubar, E. Orasson, J. Raik, H.-D. Wuttke. Teaching advanced test issues in digital electronics. In *Proc. of 6th IEEE Int. Conf. on Information Technology Based Higher Education and Training, ITHET 2005 (Santo Domingo, July 2005)*, pp. S2B/1-S2B/6. 2005. doi: 10.1109/ithet.2005.1560318

- R. Ubar, P. Prinetto, J. Raik. 10th IEEE European Test Symposium. *IEEE Design & Test of Computers*, v. 22, n. 5, pp. 480-481, 2005. doi: 10.1109/mdt.2005.106

- R. Ubar, T. Shchenova, G. Jervan, Z. Peng. Energy minimization for hybrid BIST in a system-on-chip test environment. In *Proc. of 10th IEEE European Test Symp., ETS 2005 (Tallinn, May 2005)*, pp. 2-7. IEEE, 2005. doi: 10.1109/ets.2005.16

- R. Ubar, H.-D. Wuttke. Research and training environment for digital design and test. In *Proc. of 8th IASTED Int. Conf. on Computers and Advanced Technology in Education, CATE 2005 (Oranjestadt, Aug. 2005)*, pp. 232-237. Acta Press, 2005. article at publisher's website

- J. Öberg, J. Plosila, P. Ellervee. Automatic synthesis of asynchronous circuits from synchronous RTL descriptions. In *Proc. of 23rd IEEE NORCHIP Conf., 2005 (Oulu, Nov. 2005)*, pp. 200-205. 2005. doi: 10.1109/norchp.2005.1597024

2006

- J. Aleksejev, A. Jutman, R. Ubar. LFSR polynomial and seed selection using genetic algorithm. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 179-182. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311092

- T. Bengtsson, A. Jutman, S. Kumar, R. Ubar, Z. Peng. Off-line testing of delay faults in NoC interconnects. In *Proc. of 9th IEEE Euromicro Conf. on Digital Systems Design, DSD 2006 (Cavtat, Aug./Sept. 2006)*, pp. 677-680. IEEE, 2006. doi: 10.1109/dsd.2006.72

- T. Bengtsson, A. Jutman, S. Kumar, R. Ubar. Analysis of a test method for delay faults in NoC interconnects. In *Proc. of 4th East-West Design and Test Wksh., EWDTW '06 (Sochi, Sept. 2006)*, pp. 42-46. Kharkov Univ. of Techn., 2006.

- T. Bengtsson, S. Kumar, A. Jutman, R. Ubar. Off-line testing of crosstalk induced glitch faults in NoC interconnects. In *Proc. of 24th IEEE NORCHIP Conf., 2006 (Linköping, Nov. 2006)*, pp. 221-225. IEEE, 2006. doi: 10.1109/norchp.2006.329215

- T. Borejko, A. Jutman, W. A. Pleskacz, R. Ubar. DefSim: measurement environment for CMOS defects. In *Proc. of 25th Int. Conf. on Microelectronics, MIEL 2006 (Belgrade, May 2006)*, pp. 638-641. IEEE, 2006. article at IEEExplore

- S. Devadze, J. Raik, A. Jutman, R. Ubar. Fault simulation with parallel critical path tracing for combinational circuits using structurally synthesized BDDs. In *Proc. of IEEE Latin American Test Wksh., LATW 2006 (Buenos Aires, March 2006)*, pp. 97-102. IEEE, 2006.

- L. Ehrenpreis, P. Ellervee, K. Tammemäe. Open source on-chip logic analyzer for FPGAs. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 99-102. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311070

- P. Ellervee, A. Arhipov, K. Tammemäe. Clock manipulation for heterogenous emulation environment. In *Proc. of 24th IEEE NORCHIP Conf., 2006 (Linköping, Nov. 2006)*, pp. 213-216. IEEE, 2006. doi: 10.1109/10.1109/norchp.2006.329213

- P. Ellervee, E. Ivask, M. Kruus. Improved VHDL input for high-level synthesis tool xTractor. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 87-90. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311067

- P. Ellervee, G. Jervan. How to emulate network-on-chip? In *Proc. of 4th East-West Design and Test Wksh., EWDTW '06 (Sochi, Sept. 2006)*, pp. 282-286. Kharkov Univ. of Techn., 2006.

- P. Ellervee, J. Raik, K. Tammemäe, R. Ubar. Environment for FPGA based fault emulation. *Proc. of Estonian Acad. Sci.: Engineering*, v. 12, n. 2-3, pp. 323-335, 2006.

- P. Ellervee, U. Reinsalu, A. Arhipov. Teaching HDL for IT-students. In L.-R. Zheng, J. Nurmi, J. Liu, R.Weerasekera, H. Tenhunen, eds., *Proc. of 6th Europ. Wksh. on Microelectronics Education, EWME 2006 (Stockholm, June 2006)*, pp. 112-115. KTH, 2006.

- E. Fomina, A. Zakrevski. Graph embedding in Boolean hypercube. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 131-134. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311078

- V. Govind, J. Raik, R. Ubar. A generic synthesizable NoC switch with a scalable testbench. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 91-94. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311068

- V. Govind, J. Raik, R. Ubar. An external test approach for network-on-chip switches. In *Proc. of 15th Asian Test Symp., ATS 2006 (Fukuoka, Nov. 2006)*, pp. 437-442. IEEE, 2006. doi: 10.1109/ats.2006.260967

- V. Hahanov, M. Kaminska, E. Fomina. Testability analysis of digital design verification. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 171-174. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311090

- V. Hahanov, V. Obrizan, I. Hahanova, E. Fomina. Verification of digital system by a new asserting mechanism based on IEEE 1500 SECT standard. In *Proc. of Int. Conf. on Mixed Design of Integrated Circuits and Systems, MIXDES 2006 (Gdynia, June 2006)*, pp. 544-548. IEEE, 2006. article at IEEExplore

- K. Hermann, J. Raik, M. Jenihhin. TTBist: a DfT tool for enhancing functional test for SoC. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 191-194. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311095

- E. Ivask. Digital test in web-based environment. V. 29 of *Theses of Tallinn Univ. of Technology C*. Tallinn Univ. of Technology, 2006. thesis at TUT DL

- G. Jervan, A. Arhipov, P. Ellervee. FPGA based emulation environment. In *Proc. of 2nd Int. Wksh. on Reconfigurable Communication.Centric Systems-on-Chip, ReCoSoc '06 (Montpellier, July 2006)*, pp. 146-151. Univ. Montpellier II, 2006.

- G. Jervan, P. Eles, Z. Peng, R. Ubar, M. Jenihhin. Test time minimization for hybrid BIST of core-based systems. *J. of Comput. Sci. and Techn.*, v. 21, n. 6, pp. 907-912, 2006. doi: 10.1007/s11390-006-0907-x

- G. Jervan, Z. Peng, T. Shchenova, R. Ubar. A hybrid BIST energy minimization technique for system-on-chip testing. *IEE Proc.: Computers and Digital Techniques*, v. 153, n. 4, pp. 208-216, 2006. doi: 10.1049/ip-cdt:20050064

- G. Jervan, T. Shchenova, R. Ubar. Hybrid BIST scheduling for NoC-based SoCs. In *Proc. of 24th IEEE NORCHIP Conf., 2006 (Linköping, Nov. 2006)*, pp. 141-144. IEEE, 2006. doi: 10.1109/norchp.2006..329263

- G. Jervan, R. Ubar, Z. Peng. Hybrid BIST methodology for testing core-based systems. *Proc. of Estonian Acad. Sci.: Engineering*, v. 12, n. 2-3, pp. 300-322, 2006.

- A. Jutman, W. Pleskacz, N. Boiko, R. Ubar. DefSim-based exercises for studying defects in CMOS gates. In L.-R. Zheng, J. Nurmi, J. Liu, R. Weerasekera, H. Tenhunen, eds., *Proc. of 6th Europ. Wksh. on Microelectronics Education, EWME 2006 (Stockholm, June 2006)*, pp. ?-?. Kungl. Tekn. Högskolan, 2006.

- A. Jutman, A. Tsertov, R. Ubar. A tool for teaching pseudo-random TPG principles. In *Proc. of 17th EAEEIE Conf. on Innovation in Education for Electrical and Information Engineering (Craiova, June 2006)*, pp. 182-187. Editura Universitaria Craiova, 2006.
- A. Jutman, A. Tsertov, R. Ubar. A tool for advanced learning of LFSR-based testing principles. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 175-178. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311091
- A. Jutman, R. Ubar, V. Rosin, S. Devadze. Trainer 1149.1: a boundary-scan simulator. In *Proc. of 5th IEEE Int. Board Test Wksh., BTW 2006 (Fort Collins, CO, Sept. 2006)*, ? pp. 2006.
- M. Kruus, P. Ellervee. Four years of system-on-chip curricula: Experiences at Tallinn University of Technology. In L.-R. Zheng, J. Nurmi, J. Liu, R. Weerasekera, H. Tenhunen, eds., *Proc. of 6th Europ. Wksh. on Microelectronics Education, EWME 2006 (Stockholm, June 2006)*, pp. 88-91. Kungl. Tekn. Högskolan, 2006.
- W. Pleskacz, T. Borejko, A. Walkanis, V. Stopjakova, A. Jutman, Artur, R. Ubar. DefSim: CMOS defects on chip for research and education. In *Proc. of 7th IEEE Latin-American Test Wksh., LATW 2006 (Buenos Aires, March 2006)*, pp. 74-79. IEEE, 2006.
- W. Pleskacz, T. Borejko, A. Walkanis, V. Stopjakova, A. Jutman, Artur, R. Ubar. DefSim: CMOS defects on chip for research and education. In *Informal Digest of Papers of 11th IEEE Europ. Test Symp., ETS 2006 (Southampton, May 2006)*, pp. 241-206. 2006
- J. Raik, R. Ubar, T. Viilukas. High-level decision diagram based fault models for targeting FSMs. In *Proc. of 9th IEEE Euromicro Conf. on Digital Systems Design, DSD 2006 (Cavtat, Aug./Sept. 2006)*, pp. 353-358. IEEE, 2006. doi: 10.1109/dsd.2006.60
- T. Robal, M. Aarna, M. Brik. e-learning of digital logic: Using e-environments in teaching digital logic. In L.-R. Zheng, J. Nurmi, J. Liu, R. Weerasekera, H. Tenhunen, eds., *Proc. of 6th Europ. Wksh. on Microelectronics Education, EWME 2006 (Stockholm, June 2006)*, pp. 120-123. Kungl. Tekn. Högskolan, 2006.
- A. Smrikarov, S. Smrikarova, M. Kruus, A. Sudnitson. European thematic network for doctoral education in computing. In *Proc. of 33rd Int. Conf. on Information Technologies in Science, Education, Telecommunication, Business, IT+SE 2006 (Gurzuf, May 2006)*, pp. 339-340. 2006.
- A. Sudnitson, S. Devadze. Computer aided design support of FSM multiplicative decomposition. In *Proc. of 4th East-West Design and Test Wksh., EWDTW '06 (Sochi, Sept. 2006)*, pp. 241-246. Kharkov Univ. of Techn., 2006.
- A. Sudnitson, M. Kruus. E-learning tools for teaching the decomposition based digital synthesis. In L.-R. Zheng, J. Nurmi, J. Liu, R. Weerasekera, H. Tenhunen, eds., *Proc. of 6th Europ. Wksh. on Microelectronics Education, EWME 2006 (Stockholm, June 2006)*, pp. 63-66. Kungl. Tekn. Högskolan, 2006.
- R. Ubar, M. Brik, A. Jutman, J. Raik, T. Bengtsson, S. Kumar. Functional test generation for finite state machines. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 205-208. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311099
- R. Ubar, G. Jervan, H. Kruus, E. Orasson, I. Aleksejev. Optimization of the store-and-generate based built-in-self-test. In *Proc. of 10th Baltic Electronics Conf., BEC 2006 (Laulasmaa, Oct. 2006)*, pp. 199-202. Tallinn Univ. of Techn., 2006. doi: 10.1109/bec.2006.311097
- R. Ubar, A. Jutman, M. Kruus, H.-D. Wuttke. Applets for learning digital design and test. In *Proc. of 1st Int. Conf. on Interactive Mobile and Computer Aided Learning, IMCL 2006 (Amman, Apr. 2006)*, pp. 1-6?. Univ. Kassel, 2006.
- R. Ubar, M. Kruus. Success story of the Computer Engineering Department at the Tallinn University of Technology in EU projects. *The Parliament Magazine: European Politics and Policy*, n. 234, pp. 33, 2006.
- R. Ubar, J. Raik, T. Evartson, M. Kruus, H. Lensen. Diagnostic modelling of digital systems with multi-level decision diagrams. In R. Wamkeue, ed., *Proc. of 17th IASTED Int. Conf. on Modelling and Simulation, MS 2006 (Montréal, May 2006)*, pp. 207-212. Acta Press, 2006. article at publisher's website

- R. Ubar, J. Raik, A. Jutman, P. Ellervee. Digital electronics design and test at Computer Engineering Department of Tallinn University of Technology. *The House Magazine: The Parlamentary Weekly*, v. 32, n. 1198, p. 42, 2006.

- H.-D. Wuttke, A. Sudnitson, K. Henke. E-learning tools for teaching the design and validation of finite state machines. In *E-Learning and the Knowledge Society*, pp. 327-341. Communication and Cognition, Gent, 2006.

2007

- P. Ellervee, A. Arhipov, U. Reinsalu. Using emulation for system model analysis. In *Wksh. Digest of DATE 2007 Wksh. on Diagnostic Services in Network-on-Chips: Test, Debug and On-Line Monitoring (Nice, Apr. 2007)*, pp. 280-282. 2007.

- P. Ellervee, J. Raik, R. Ubar, K. Tammemäe. FPGA-based fault emulation of synchronous sequential circuits. *IET Computers and Digital Techniques*, v. 1, n. 2, pp. 70-76, 2007. doi: 10.1049/iet-cdt:20050065

- P. Ellervee, U. Reinsalu, A. Arhipov. Translating behavioral VHDL for emulation. In *Proc. of 25th IEEE NorChip Conf. 2007 (Aalborg, Nov. 2007)*, pp. ?-?. IEEE, 2007.

- G. Guglielmo, F. Fummi, M. Jenihhin, G. Pravadelli, J. Raik, R. Ubar. On the combined use of HLDDs and EFSMs for functional ATPG. In *Proc. of 5th IEEE East-West Design and Test Symp., EWDTS 2007 (Yerevan, Sept. 2007)*, pp. 503-509. IEEE, 2007.

- M. Jenihhin, J. Raik, A. Chepurov, R. Ubar. Assertion checking with PSL and high-level decision diagrams. In *Proc. of 8th IEEE Wksh. on RTL and High Level Testing, WRTLT '07 (Beijing, Oct. 2007)*, pp. ?-?. IEEE, 2007.

- M. Jenihhin, J. Raik, R. Ubar, W. A. Pleskacz, M. Rakowski. Layout to logic defect analysis for hierarchical test generation. In *Proc. of 10th IEEE Wksh. on Design and Diagnostics of Electronic Circuits and Systems, DDECS '07 (Kraków, Apr. 2007)*, pp. 35-40. IEEE, 2007. doi: 10.1109/ddecs.2007.4295251

- G. Jervan, H. Kruus, E. Orasson, R. Ubar. Hybrid BIST optimization using reseeding and test set compaction. In *Proc. of 10th Euromicro Conf. on Digital System Design, DSD 2007 (Lübeck, Aug. 2007)*, pp. 596-603. IEEE, 2007. doi: 10.1109/dsd.2007.4341529

- G. Jervan, H. Kruus, E. Orasson, R. Ubar. Optimization of memory-constrained hybrid BIST for testing core-based systems. In *Proc. of 2007 Int. Symp. on Industrial Embedded Systems, SIES '07 (Costa da Caparica, July 2007)*, pp. 71-77. IEEE, 2007. doi: 10.1109/sies.2007.4297319

- G. Jervan, M. Kruus, E. Rüstern. Graduate school in information and communication technologies: experiences at Tallinn University of Technology. In *Proc. of 2007 IEEE Int. Conf. on Microelectronic Systems Education, MSE '07 (San Diego, CA, June 2007)*, pp. 25-26. IEEE, 2007. doi: 10.1109/mse.2007.47

- A. Jutman, A. Tsertov, A. Tsepurov, I. Aleksejev, R. Ubar, H.-D. Wuttke. BIST analyzer: a training platform for SoC testing. In *Proc. of 37th ASEE/IEEE Frontiers in Education Conf., FIE '07 (Milwaukee, Oct. 2007)*, pp. SH3-8-SH3-13. IEEE, 2007. doi: 10.1109/fie.2007.4418125

- A. Mellik, J. Raik. Comparative mixed-signal test method and toolset. In *Proc. of IEEE Int. Wksh. on Open Source Test Technology Tools, IOST3 2007 (Berkeley, CA, May 2007)*, ? pp. 2007.

- E. Orasson. Hybrid built-in self-test: methods and tools for analysis and optimization of BIST. V. 35 of *Theses of Tallinn Univ. of Technology C*. Tallinn Univ. of Technology, 2007. thesis at TUT DL

- J. Raik, V. Govind, R. Ubar. An external diagnosis method for network-on-a-chip. In *Wksh. Digest of DATE 2007 Wksh. on Diagnostic Services in Network-on-Chips: Test, Debug and On-Line Monitoring (Nice, Apr. 2007)*, pp. ?-?. 2007.

- J. Raik, R. Ubar, V. Govind. Test configurations for diagnosing faulty links in NoC switches. In *Proc. of 12th IEEE European Test Symp., ETS '07 (Freiburg, May 2007)*, pp. 29-34. IEEE, 2007. doi: 10.1109/ets.2007.41

- J. Raik, R. Ubar, M. Jenihhin, A. Chepurov. PSL assertion checking with temporally extended high-level decision diagrams. In *Proc. of 9th IEEE Latin-American Test Wksh. (Puebla, Feb. 2008)*, IEEE, to appear.

- J. Raik, R. Ubar, A. Jutman, I. Aleksejev. A scalable test set compaction method for sequential circuits. In *Proc. of 9th IEEE Latin-American Test Wksh. (Puebla, Feb. 2008)*, IEEE, to appear.
- J. Raik, R. Ubar, A. Krivenko, M. Kruus. Hierarchical identification of untestable faults in sequential circuits. In *Proc. of 10th Euromicro Conf. on Digital System Design, DSD 2007 (Lübeck, Aug. 2007)*, pp. 668-671. IEEE, 2007. doi: 10.1109/dsd.2007.4341539
- J. Raik, R. Ubar, T. Viilukas, M. Jenihhin. Mixed hierarchical-functional fault models for targeting sequential cores. *J. of Systems Architecture*, to appear.
- U. Reinsalu, A. Arhipov, T. Evartson, P. Ellervee. HDLs for students with different background. In *Proc. of 2007 IEEE Int. Conf. on Microelectronic Systems Education, MSE '07 (San Diego, CA, June 2007)*, pp. 69-70. IEEE, 2007. doi: 10.1109/mse.2007.49
- A. Sudnitson, S. Devadze. Web-based computer aided design support of finite state machine additive decomposition for low power. In *Proc. of 5th IEEE East-West Design and Test Symp., EWDTS 2007 (Yerevan, Sept. 2007)*, pp. 494-498. IEEE, 2007.
- M. Tagel, G. Jervan. Deterministic traffic generator for NoC simulator. In *Wksh. Digest of DATE 2007 Wksh. on Diagnostic Services in Network-on-Chips: Test, Debug and On-Line Monitoring (Nice, Apr. 2007)*, pp. 288-290. 2007.
- R. Ubar, S. Devadze, M. Jenihhin, J. Raik, G. Jervan, P. Ellervee. Hierarchical calculation of malicious faults for evaluating the fault-tolerance. In *Proc. of 4th IEEE Int. Symp. on Electronic Design, Test and Applications, DELTA '08 (Hongkong, Jan. 2008)*, IEEE, to appear.
- R. Ubar, S. Devadze, J. Raik, A. Jutman. Ultra fast parallel fault analysis on structurally synthesized BDDs. In *Proc. of 12th IEEE European Test Symp., ETS '07 (Freiburg, May 2007)*, pp. 131-136. IEEE, 2007. doi: 10.1109/ets.2007.43
- R. Ubar, S. Devadze, J. Raik, A. Jutman. Parallel fault backtracing for calculation of fault coverage. In *Proc. of Int. Conf. on Microelectronics, Devices and Materials and Wksh. on Electronic Testing, MIDEM '07 (Bled, Sept. 2007)*, pp. 165-170. MIDEM, 2007.
- R. Ubar, S. Devadze, J. Raik, A. Jutman. Parallel Fault Backtracing for Calculation of Fault Coverage. In *Proc. of 13th Asia and South Pacific Design Automation Conf., ASP-DAC 2008 (Seoul, Jan. 2008)*, IEEE, to appear.
- R. Ubar, T. Evartson, H. Lensen, M. Aarna. Hierarchical fault diagnosis in embedded digital systems with multi-level decision diagrams. In *Proc. of 5th Int. Conf. on Industrial Automation (Montréal, July 2007)*, pp. 1-6. 2007.
- R. Ubar, G. Jervan, J. Raik, M. Jenihhin, P. Ellervee. Dependability evaluation in fault-tolerant systems with high-level decision diagrams. In *Proc. of 52nd Int. Scientific Coll., IWK 2007 (Ilmenau, Sept. 2007)*, v. 2, pp. 147-152. Universitätsverlag Ilmenau, 2007.
- R. Ubar, A. Jutman, S. Devadze, H.-D. Wuttke. Bringing research issues into lab scenarios on the example of SoC testing. In *Proc. of 2007 Int. Conf. on Engineering Education, ICEE 2007 (Coimbra, Sept. 2007)*, pp. ?-?. 2007.
- R. Ubar, A. Jutman, M. Kruus, E. Orasson, S. Devadze, H.-D. Wuttke. Learning digital test and diagnostics via Internet. *Int. J. of Online Engineering*, v. 3, n. 1, 2007, 9 pp., 2007. article at journal's website
- R. Ubar, S. Kostin, J. Raik. Built-in self diagnosis with multiple signature analyzers in digital systems. In *Proc. of 9th IEEE Latin-American Test Wksh., LATW 2008 (Puebla, Feb. 2008)*, IEEE, to appear.
- R. Ubar, S. Kostin, J. Raik. Embedded diagnosis in digital systems. In *Proc. of 26th Int. Conf. on Microelectronics, MIEL 2008 (Nis, May 2008)*, IEEE, to appear.
- R. Ubar, S. Kostin, J. Raik, T. Evartson, H. Lensen. Fault diagnosis in intergrated circuits with BIST. In *Proc. of 10th Euromicro Conf. on Digital System Design, DSD 2007 (Lübeck, Aug. 2007)*, pp. 604-610. IEEE, 2007. doi: 10.1109/dsd.2007.4341530

- R. Ubar, S. Kostin, J. Raik, M. Kruus. Experimental comparison of different diagnosis algorithms in the BIST environment. In F. de Felice, ed., *Proc. of 16th IASTED Int. Conf. on Applied Simulation and Modelling, ASM 2007 (Palma de Mallorca, Aug. 2007)*, pp. 88-92. Acta Press, 2007. article at publisher's website

- R. Ubar, J. Raik, H. Kruus, H. Lensen, T. Evartson. Diagnostic modelling of digital systems with binary and high-level decision diagrams. In L. L. Bonilla, M. Moscoso, G. Platero, J. M. Vega, eds., *Progress in Industrial Mathematics at 14th Europ. Conf. for Mathematics in Industry, ECMI 2006 (Madrid, July 2006)*, v. 12 of *Mathematics in Industry*, pp. 902-907. Springer, 2008. doi: 10.1007/978-3-540-71992-2_158

- H.-D. Wuttke, R. Ubar, K. Henke, A. Jutman. Assessment of student's design results in e-learning-scenarios. In *Proc. of 8th Int. Conf. on Information Technology Based Higher Education and Training, ITHET 2007 (Kumamoto, July 2007)*, pp. 1-6. IEEE, 2007.