

2011 14th Euromicro Conference on Digital System Design

(DSD 2011)

Oulu, Finland

31 August - 2 September 2011



IEEE Catalog Number: CFP11291-PRT
ISBN: 978-1-4577-1048-3

2011 14th Euromicro Conference on Digital System Design

DSD 2011

Table of Contents

Message from the Program Chair.....	xvi
Conference Committees	xviii

Keynotes

Human++: Key Challenges and Trade-offs in Embedded System Design for Personal Health Care (Abstract)	3
<i>Harmke de Groot</i>	
Human++: Key Challenges and Trade-offs in Embedded System Design for Personal Health Care	4
<i>Harmke de Groot, Maryam Ashouei, Julien Penders, Valer Pop, Maja Vidojkovic, Bert Gyselinckx, and Firat Yazicioglu</i>	
Cryptographic Contests: Toward Fair and Comprehensive Benchmarking of Cryptographic Algorithms in Hardware (Abstract)	11
<i>Kris Gaj</i>	
The Future of Data-Parallel Embedded Systems (Abstract)	12
<i>Menno M. Lindwer</i>	

SCS-1: System and Circuit Synthesis (1)

Generalized If-Then-Else Operator for Compact Polynomial Representation of Multi Output Functions	15
<i>Ilya Levin and Osnat Keren</i>	
On the Cascade Implementation of Multiple-Output Sparse Logic Functions	21
<i>Václav Dvořák and Petr Mikušek</i>	
On Failure Rate Assessment Using an Executable Model of the System	29
<i>Mohammad Hossein Neishaburi and Zeljko Zilic</i>	

S&N(oC)-1: Systems and Networks on Chip (1)

A Cost Effective Centralized Adaptive Routing for Networks-on-Chip	39
<i>Ran Manevich, Israel Cidon, Avinoam Kolodny, Isask'har Walter, and Shmuel Wimer</i>	
Realization and Scalability of Release and Protected Release Consistency Models in NoC Based Systems	47
<i>Abdul Naeem, Axel Jantsch, Xiaowen Chen, and Zhonghai Lu</i>	
Numerical-Based Crosstalk Avoidance Coding to Reliable NoC Design	55
<i>Mansour Shafaei, Ahmad Patooghy, and Seyed Ghassem Miremadi</i>	
A Fast Congestion-Aware Flow Control Mechanism for ID-Based Networks-on-Chip with Best-Effort Communication	63
<i>Haoyuan Ying, Ashok Jaiswal, Thomas Hollstein, and Klaus Hofmann</i>	

RC: Reconfigurable Computing

Optimal Selection of Function Implementation in a Hierarchical Configware Synthesis Method for a Coarse Grain Reconfigurable Architecture	73
<i>Fahimeh Jafari, Shuo Li, and Ahmed Hemani</i>	
VMAP: A Variation Map-Aware Placement Algorithm for Leakage Power Reduction in FPGAs	81
<i>Behzad Salami, Morteza Saheb Zamani, and Ali Jahanian</i>	
PUMA: Placement Unification with Mapping and Guaranteed Throughput Allocation on an FPGA Using a Hardwired NoC	88
<i>Muhammad Aqeel Wahlah and Kees Goossens</i>	

SLEO: System-Level Energy Optimization of HW/SW Embedded Systems

Improved Power Modeling of DDR SDRAMs	99
<i>Karthik Chandrasekar, Benny Akesson, and Kees Goossens</i>	
Path-Based Dynamic Voltage and Frequency Scaling Algorithms for Multiprocessor Embedded Applications with Soft Delay Deadlines	109
<i>Alice M. Tokarnia, Pedro C. F. Pepe, and Leandro D. Pagotto</i>	
Power Minimisation for Real-Time Dataflow Applications	117
<i>Andrew Nelson, Orlando Moreira, Anca Molnos, Sander Stuijk, Ba Thang Nguyen, and Kees Goossens</i>	

SCS-2: System and Circuit Synthesis (2)

VHDL Code Generation from Formal Event-B Models	127
<i>Sergey Ostroumov and Leonidas Tsiopoulos</i>	
Process Variation Reduction for CMOS Logic Operating at Sub-threshold Supply Voltage	135
<i>Bo Liu, Hamid Reza Pourshaghghi, Sebastian Moreno Londoño, and José Pineda de Gyvez</i>	
Hardware Reuse in Modern Application-Specific Processors and Accelerators	140
<i>Alexandre S. Nery, Lech Jozwiak, Menno Lindwer, Mauro Cocco, Nadia Nedjah, and Felipe M.G. França</i>	
Quaternary High Performance Arithmetic Logic Unit Design	148
<i>A.N. Nagamani and S. Nishchai</i>	

S&N(oC)-2: Systems and Networks on Chip (2)

Low-Latency and Low-Overhead Mesochronous and Plesiochronous Synchronizers	157
<i>Jean Michel Chabloz and Ahmed Hemani</i>	
Towards an Efficient NoC Topology through Multiple Injection Ports	165
<i>Jesús Camacho, José Flich, José Duato, Hans Eberle, and Wlodek Olesinski</i>	
LastZ: An Ultra Optimized 3D Networks-on-Chip Architecture	173
<i>Amir-Mohammad Rahmani, Pasi Liljeberg, Juha Plosila, and Hannu Tenhunen</i>	
Comparison of Different Thread Scheduling Strategies for Asymmetric Chip MultiThreading Architectures in Embedded Systems	181
<i>Charly Bechara, Nicolas Ventroux, and Daniel Etiemble</i>	

DTDS-1: Dependability and Testing of Digital Systems (1)

SAT-Based Generation of Compressed Skewed-Load Tests for Transition Delay Faults	191
<i>Roland Dobai and Marcel Baláz</i>	
Adaptive Temperature-Aware SoC Test Scheduling Considering Process Variation	197
<i>Nima Aghaee, Zebo Peng, and Petru Eles</i>	
Chip Temperature Selfregulation for Digital Circuits Using Polymorphic Electronics Principles	205
<i>Richard Ruzicka and Vaclav Simek</i>	
A Technique for Accelerating Injection of Transient Faults in Complex SoCs	213
<i>Alireza Rohani and Hans G. Kerckhoff</i>	

FTDSD-1: Fault Tolerance in Digital System Design (1)

SEU Simulation Framework for Xilinx FPGA: First Step towards Testing Fault Tolerant Systems	223
<i>Martin Straka, Jan Kastil, and Zdenek Kotasek</i>	
Fault Tolerance of Multiple Logic Faults in SRAM-Based FPGA Systems	231
<i>Farid Lahrach, Abderrahim Doumar, and Eric Châtelet</i>	
Reliability-Aware Design Optimization for Multiprocessor Embedded Systems	239
<i>Jia Huang, Jan Olaf Blech, Andreas Raabe, Christian Buckl, and Alois Knoll</i>	
Design of Asynchronous Circuits on FPGAs for Soft Error Tolerance	247
<i>Yu Bai and Weidong Kuang</i>	

P-1: Poster Session (1)

HMMER Performance Model for Multicore Architectures	257
<i>Sebastian Isaza, Ernst Houtgast, and Georgi Gaydadjiev</i>	
Kactus2: Environment for Embedded Product Development Using IP-XACT and MCAPI	262
<i>Antti Kamppi, Lauri Matilainen, Joni-Matti Määttä, Erno Salminen, Timo D. Hämäläinen, and Marko Hännikäinen</i>	
10-Gigabit Throughput and Low Area for a Hardware Implementation of the Advanced Encryption Standard	266
<i>Paolo Maistri and Régis Leveugle</i>	
Multicore Cache Simulations Using Heterogeneous Computing on General Purpose and Graphics Processors	270
<i>Georgios Keramidas, Nikolaos Strikos, and Stefanos Kaxiras</i>	
Power Spectral Density Side Channel Attack Overlapping Window Method	274
<i>Philip Hodggers, Kean Hong Boey, and Maire O'Neill</i>	
Dynamic Power Estimation for Motion Estimation Hardware	279
<i>Caglar Kalaycioglu and Ilker Hamzaoglu</i>	
A Module for Packet Hijacking in NetFPGA Platform	283
<i>Alfio Lombardo, Carla Panarello, Diego Reforgiato, Enrico Santagati, and Giovanni Schembra</i>	
Fault Models Usability Study for On-line Tested FPGA	287
<i>Jaroslav Borecký, Martin Kohlík, Pavel Kubalík, and Hana Kubátová</i>	

ET: Important Issues Introduced by Emerging Technologies

Hardware Implementation of a Flexible Tag Platform for Passive RFID Devices	293
<i>Thomas Plos and Martin Feldhofer</i>	
Design of a Low Power, Sub-Threshold, Asynchronous Arithmetic Logic Unit Using a Bidirectional Adder	301
<i>Jiaoyan Chen, Dilip Vasudevan, Emanuel Popovici, and Michel Schellekens</i>	
An Overlapped Block Motion Compensation Hardware for Frame Rate Conversion	309
<i>Tevfik Zafer Ozcan, Cagla Cakir, Mert Cetin, and Ilker Hamzaoglu</i>	
Cost of Sparse Mesh Layouts Supporting Throughput Computing	316
<i>Martti Forsell, Ville Leppänen, and Martti Penttonen</i>	

FDR: Flexible Digital Radio

An Environment for (re)configuration and Execution Management of Flexible Radio Platforms	327
<i>Pierre-Henri Horrein, Christine Hennebert, and Frédéric Pétrot</i>	
FBMC and GFDM Interference Cancellation Schemes for Flexible Digital Radio PHY Design	335
<i>Rohit Datta, Gerhard Fettweis, Zsolt Kollár, and Péter Horváth</i>	
A Novel Architecture for Scalable, High Throughput, Multi-standard LDPC Decoder	340
<i>Muhammad Awais, Ashwani Singh, Emmanuel Boutillon, and Guido Masera</i>	

DTDS-2: Dependability and Testing of Digital Systems (2)

A Non-Intrusive Online FPGA Test Scheme Using a Hardwired Network on Chip	351
<i>Muhammad Aqeel Wahlah and Kees Goossens</i>	
Techniques for SAT-Based Constrained Test Pattern Generation	360
<i>Jiří Balcárek, Petr Fišer, and Jan Schmidt</i>	
On RTL Testability and Gate-Level Stuck-At-Fault Coverage Correlation for Scan Circuits	367
<i>Michal Rumlík and Josef Strnadel</i>	
An Enhanced Path Delay Fault Simulator for Combinational Circuits	375
<i>P. Manikandan, Bjørn B. Larsen, and Einar J. Aas</i>	

FTDSD-2: Fault Tolerance in Digital System Design (2)

Dynamic Soft Error Hardening via Joint Body Biasing and Dynamic Voltage Scaling	385
<i>F. Firouzi, A. Yazdanbakhsh, H. Dorosti, and S. M. Fakhraie</i>	
Design of Fault Tolerant Network Interfaces for NoCs	393
<i>Leandro Fiorin, Laura Micconi, and Mariagiovanna Sami</i>	
Designing Robust Asynchronous Circuits Based on FinFET Technology	401
<i>Fataneh Jafari, Mahdi Mosaffa, and Siamak Mohammadi</i>	
Analyzing Area Penalty of 32-Bit Fault Tolerant ALU Using BCH Code	409
<i>Vahid Khorasani, Bijan Vosoughi Vahdat, and Mohammad Mortazavi</i>	

P-2: Poster Session (2)

Low Power FPGA Implementations of JH and Fugue Hash Functions	417
<i>George Provelengios, Nikolaos S. Voros, and Paris Kitsos</i>	
Mutant Fault Injection in Functional Properties of a Model to Improve Coverage Metrics	422
<i>Ali Abbasinasab, Mehdi Mohammadi, Siamak Mohammadi, Svetlana Yanushkevich, and Michael Smith</i>	
A Unified Architecture for BCD and Binary Adder/Subtractor	426
<i>V. Chetan Kumar, P. Sai Phaneendra, Syed Ershad Ahmed, Sreehari Veeramachaneni, N. Moorthy Muthukrishnan, and M.B. Srinivas</i>	
Synthesizing Concurrent Synchronous Computing Machines from Interrupt-Driven Binaries	430
<i>Michael D. Wilder and Robert E. Rinker</i>	
Architectures for Fast Modular Multiplication	434
<i>Ahmet Aris, Berna Ors, and Gokay Saldamli</i>	
Transaction Level Modeling of a Networked Embedded System Based on a Power Line Communication Protocol	438
<i>Takieddine Majdoub, Sébastien Le Nours, Olivier Pasquier, and Fabienne Nouvel</i>	
Nexus: Hardware Support for Task-Based Programming	442
<i>Cor Meenderinck and Ben Juurlink</i>	
Evaluation of Fault-Tolerant Routing Methods for NoC Architectures	446
<i>Mojtaba Valinataj</i>	

AUD: Arithmetic Unit Design

On the Design of Modulo 2^{n+1} Multipliers	453
<i>Constantinos Efstathiou, Kiamal Pekmestzi, and Nicholas Axelos</i>	
Binary-to-RNS Conversion Units for moduli $\{2^n \pm 3\}$	460
<i>Pedro Miguens Matutino, Ricardo Chaves, and Leonel Sousa</i>	
Modulo 2^{n+1} Arithmetic Units with Embedded Diminished-to-Normal Conversion	468
<i>Evangelos Vassalos, Dimitris Bakalis, and Haridimos T. Vergos</i>	

SMVT-1: System, Hardware and Embedded-Software Specification, Modeling Verification and Test (1)

Automated Design Debugging in a Testbench-Based Verification Environment	479
<i>Mehdi Dehbashi, André Sülflow, and Görschwin Fey</i>	
Efficient Fault Simulation of SystemC Designs	487
<i>Weiyun Lu and Martin Radetzki</i>	
Higher-Order Abstraction in Hardware Descriptions with ClaSH	495
<i>Marco Gerards, Christiaan Baaij, Jan Kuper, and Matthijs Kooijman</i>	
Thermal Effect of TSVs in 3D Die-Stacked Integrated Circuits	503
<i>Hadrien A. Clarke and Kazuaki Murakami</i>	

ASC: Applications-Specific Computing

A Parallel Ray Tracing Architecture Suitable for Application-Specific Hardware and GPGPU Implementations	511
<i>Alexandre S. Nery, Nadia Nedjah, Felipa M.G. França, and Lech Jozwiak</i>	
Dynamic Flow Reconfiguration Strategy to Avoid Communication Hot-Spots	519
<i>Romain Prolonge, Fabien Clermidy, Leonel Tedesco, and Fernando Moraes</i>	
Microthreading as a Novel Method for Close Coupling of Custom Hardware Accelerators to SVP Processors	525
<i>Jaroslav Sykora, Leos Kafka, Martin Danek, and Lukas Kohout</i>	

AHSA-1: Architectures and Hardware for Security Applications (1)

Pre-silicon Characterization of NIST SHA-3 Final Round Candidates	535
<i>Xu Guo, Meeta Srivastav, Sinan Huang, Dinesh Ganta, Michael B. Henry, Leyla Nazhandali, and Patrick Schaumont</i>	

Novel Hardware Architecture for Implementing the Inner Loop of the SHA-2 Algorithms	543
<i>Ignacio Algreto-Badillo, Claudia Feregrino-Uribe, René Cumplido, and Miguel Morales-Sandoval</i>	
Modular Fault Injector for Multiple Fault Dependability and Security Evaluations	550
<i>Johannes Grinschgl, Armin Krieg, Christian Steger, Reinhold Weiss, Holger Bock, and Josef Haid</i>	
Breaking Hitag2 with Reconfigurable Hardware	558
<i>Petr Štembera and Martin Novotný</i>	

SoC: System-on-Chip Design

Iteration-Based Trade-Off Analysis of Resource-Aware SDF	567
<i>Yang Yang, Marc Geilen, Twan Basten, Sander Stuijk, and Henk Corporaal</i>	
SoC and Board Modeling for Processor-Centric Board Testing	575
<i>Anton Tsertov, Raimund Ubar, Artur Jutman, and Sergei Devadze</i>	
Hybrid Code-Data Prefetch-Aware Multiprocessor Task Graph Scheduling	583
<i>Morteza Damavandpeyma, Sander Stuijk, Twan Basten, Marc Geilen, and Henk Corporaal</i>	

SMVT-2: System, Hardware and Embedded-Software Specification, Modeling Verification and Test (2)

Efficient CRT RSA with SCA Countermeasures	593
<i>Apostolos P. Fournaris and Odysseas Koufopavlou</i>	
Control-Flow-Driven Source Level Timing Annotation for Embedded Software Models on Transaction Level	600
<i>Daniel Mueller-Gritschneider, Kun Lu, and Ulf Schlichtmann</i>	
HDL-Mutation Based Simulation Data Generation by Propagation Guided Search	608
<i>Tao Xie, Wolfgang Mueller, and Florian Letombe</i>	

M2APS: Monitoring Methods for Adaptive Parallel Systems

On-chip Monitoring: A Light-Weight Interconnection Network Approach	619
<i>Pablo Ituero, Marisa López-Vallejo, Miguel Ángel Sánchez Marcos, and Carlos Gómez Osuna</i>	
Enhancing Performance Sustainability of Fault Tolerant Routing Algorithms in NoC-Based Architectures	626
<i>Khalid Latif, Amir-Mohammad Rahmani, Kameswar Rao Vaddina, Tiberiu Seceleanu, Pasi Liljeberg, and Hannu Tenhunen</i>	

Formal Modeling of Multicast Communication in 3D NoCs	634
<i>Maryam Kamali, Luigia Petre, Kaisa Sere, and Masoud Daneshtalab</i>	
Thermal Analysis of Job Allocation and Scheduling Schemes for 3D Stacked NoC's	643
<i>Kameswar Rao Vaddina, Amir-Mohammad Rahmani, Khalid Latif, Pasi Liljeberg, and Juha Plosila</i>	

AHSA-2: Architectures and Hardware for Security Applications (2)

A Configurable Ring-Oscillator-Based PUF for Xilinx FPGAs	651
<i>Xin Xin, Jens-Peter Kaps, and Kris Gaj</i>	
A Unified Multiply/Accumulate Unit for Pairing-Based Cryptography over Prime, Binary and Ternary Fields	658
<i>Tobias Vejda, Johann Großschädl, and Dan Page</i>	
A Novel Architecture of Implementing Error Detecting AES Using PRNS	667
<i>Junfeng Chu and Mohammed Benaissa</i>	
How a Symmetry Metric Assists Side-Channel Evaluation - A Novel Model Verification Method for Power Analysis	674
<i>Annelie Heuser, Michael Kasper, Werner Schindler, and Marc Stöttinger</i>	

EAD: Energy-Aware Design

Rapid and Accurate Leakage Power Estimation for Nano-CMOS Circuits	685
<i>Michał Bryk, Lech Jóźwiak, and Wiesław Kuźmicz</i>	
An Energy Aware Design Space Exploration for VLIW AGU Model with Fine Grained Power Gating	693
<i>Ittetsu Taniguchi, Mitsuya Uchida, Hiroyuki Tomiyama, Masahiro Fukui, Praveen Raghavan, and Francky Catthoor</i>	
A Design Method for Programmable Two-Variable Discrete Function Generators Using Spline and Bilinear Interpolations	701
<i>Satoru Nakano, Yoichi Wakaba, Shinobu Nagayama, and Shin'ichi Wakabayashi</i>	
Exploiting Inter and Intra Application Dynamism to Save Energy	708
<i>Martijn Koedam, Sander Stuijk, and Henk Corporaal</i>	

MSDA: Multicore Systems: Design and Applications

Model Driven Cache-Aware Scheduling of Object Oriented Software for Chip Multiprocessors	719
<i>Tolga Ovatman and Feza Buzluca</i>	
Compiling Esterel for Multi-core Execution	727
<i>Simon Yuan, Li Hsien Yoong, and Partha S. Roop</i>	

Phase-Guided Scheduling on Single-ISA Heterogeneous Multicore Processors	736
<i>Lina Sawalha, Sonya Wolff, Monte P. Tull, and Ronald D. Barnes</i>	
Energy Behaviour of NUCA Caches in CMPs	746
<i>Alessandro Bardine, Pierfrancesco Foglia, Francesco Panicucci, Marco Solinas, and Julio Sahuquillo</i>	

APP: Applications of (Embedded) Digital Systems

A Wearable Intelligent System for the Health of Expectant Mom's and of Their Children	757
<i>Giovanni Danese, Francesco Leparati, Alessandra Majani, Giulia Matrone, and Enrico Merlino</i>	
Embedded System for Camera-Based TV Power Reduction	764
<i>Choong Geun Lee, Vasily G. Moshnyaga, and Koji Hashimoto</i>	
An Embedded Video Sensor for a Smart Traffic Light	769
<i>Guido Matrella and Davide Marani</i>	
On the Efficiency of Design Time Evaluation of the Resistance to Power Attacks	777
<i>Alessandro Barengi, Guido Bertoni, Fabrizio De Santis, and Filippo Melzani</i>	

P-3: Poster Session (3)

Soft Error Detection Technique in Multi-threaded Architectures Using Control-Flow Monitoring	789
<i>Mohammad Maghsoudloo, Hamid R. Zarandi, Saadat Pour Mozafari, and Navid Khoshavi</i>	
Automatic Interface Generation for Component Reuse in HW-SW Partitioning	793
<i>Nicola Bombieri, Franco Fummi, Sara Vinco, and Davide Quaglia</i>	
A Scalable Distributed Asynchronous Control Network for High Level Synthesis of Digital Circuits	797
<i>Tom van Leeuwen and Rene van Leuken</i>	
A Process-Variation-Adaptive Network-on-Chip with Variable-Cycle Routers	801
<i>Yohei Nakata, Yukihiro Takeuchi, Hiroshi Kawaguchi, and Masahiko Yoshimoto</i>	
Faster Processor Allocation Algorithms for Mesh-Connected CMPs	805
<i>Luka B. Daoud, M. El-Sayed Ragab, and Victor Goulart</i>	
Compatibility Study of Compile-Time Optimizations for Power and Reliability	809
<i>Ghazaleh Nazarian, Christos Strydis, and Georgi Gaydadjiev</i>	
An FPGA Implementation of the ZUC Stream Cipher	814
<i>Paris Kitsos, Nicolas Sklavos, and Athanassios N. Skodras</i>	

A Unified Execution Model for Data-Driven Applications on a Composable MPSoC	818
<i>Ashkan Beyranvand Nejad, Anca Molnos, and Kees Goossens</i>	
Author Index	823