SIGDA Special Interest Group Design Automation
The resource for EDA Professionals

1 January 2020, Vol. 50, No. 1
Online archive: http://www.sigda.org/publications/newsletter

Comments from the Editors

Dear ACM/SIGDA member,

We are excited to present to you the January e-newsletter. We encourage you to invite your students and colleagues to be a part of the SIGDA newsletter. The newsletter covers a wide range of information from upcoming conference and funding deadlines, hot research topics to news from our community. Get involved and contact us if you want to contribute an article or announcement.

For this month, we are introducing two new Editor for "What is" column: Prof. Wanli Chang, and Prof.

Xunjiao.
Prof. Yuanhao Chang and Prof. Wenchao Li have been served for the "what is" editor for the last year. We thank them for their great contribution to the e-newsletter.

The newsletter is evolving, let us know what you think.

Happy reading!

Aida Todri-Sanial
Yu Wang
Editors-in-Chief, SIGDA E-News

To renew your ACM SIGDA membership, please visit http://www.acm.org/renew or call between the hours of 8:30am to 4:30pm EST at +1-212-626-0500 (Global), or 1-800-342-6626 (US and Canada). For any questions, contact acmhelp@acm.org

Back to Contents

SIGDA News

(1) "Supply Chain 2019: Breakups, Boycotts, and ‘a Whole Lotta’ Tariffs"
[https://www.eetimes.com/supply-chain-2019-breakups-boycotts-and-a-whole-lotta-ta...]

In one year, the electronics supply chain saw a level of disruption that once took decades to achieve. The 1990s were known for frenetic M&A activity in the channel; 2019 will be marked by breakups.

(2) "Newest Nvidia AV SoC boasts ‘7x Xavier Performance’"
[https://www.eetimes.com/newest-nvidia-av-soc-boasts-7x-xavier-performance/]

At the company’s GPU Technology Conference (GTC) in Suzhou, China, Nvidia CEO Jensen Huang took to the stage to introduce Drive AGX Orin, the next generation SoC in the company’s automotive portfolio.

(3) "Qualcomm 5G Snapdragons Fly in Hawaii"
[https://www.eetimes.com/qualcomm-5g-snapdragons-fly-in-hawaii/]

With 5G rollouts started, Tech Summit was the event for Qualcomm to roll out the first application processors specifically designed for 5G — the flagship Snapdragon 865 and the more highly integrated Snapdragon 765.

(4) "AWS Rolls Out AI Inference Chip"
[https://www.eetimes.com/aws-rolls-out-ai-inference-chip/]

A year after announcing its in-house designed AI accelerator chip, Amazon Web Services (AWS) is making instances based on its Inferentia chip available for customer workloads.

(5) "Quantum Computers on Path to Extinguish Current Encryption Techniques"
[https://www.eetimes.com/quantum-computers-on-path-to-extinguish-current-encrypti...]

In the coming years, large-scale quantum computers will make most current cryptography techniques insecure. To avoid this, two major global directions are being pursued.

(6) "Low-Power FPGA Enables High-Performance Space Systems"
[https://www.eetimes.com/low-power-fpga-enables-high-performance-space-systems/]

Space missions increasingly require robust and efficient solutions. Microchip’s Radiation Tolerant (RT) PolarFire FPGA offers lower costs and faster design cycles.

(7) "Researchers Present Latest AI Algorithms at NeurIPS 2019"
[https://www.eetimes.com/researchers-present-latest-ai-algorithms-at-neurips-2019...]

Advances will help machines identify objects and figure out how to work together, improve their ability to understand language, and improve their ability to learn.

(8) "Ultrasound Sensor Turns Any Surface into a Touch Button"
[https://www.eetimes.com/ultrasound-sensor-turns-any-surface-into-a-touch-button/]

Whatever the material, whatever the material thickness, the California-based startup UltraSense Systems claims it can turn any surface into a user interface.

(9) "Improving Energy Efficiency with a SiC Isolated Gate Driver"
[https://www.eetimes.com/improving-energy-efficiency-with-a-sic-isolated-gate-dri...]

Using silicon carbide gate drivers can reduce energy loss by 30 percent while maximizing system uptime.

(10) "GPS Inventors Receive Top Engineering Prize at the Palace"
[https://www.eetimes.com/gps-inventors-receive-top-engineering-prize-at-the-palac...]

The four engineers who created GPS have been awarded a top engineering prize of £1 million in honor of their invention.

Back to Contents

"What is" Column

What is Fuzzing?

Yu Jiang
Associate Professor,
School of Software,
Tsinghua University, Beijing, CHINA

Fuzzing is one of the most popular software testing techniques for automated bug and vulnerability detection. The key idea of fuzzing is to generate plenty of inputs to execute the target application and monitor for any anomalies. It is easy to use and widely deployed in industry. For example, Google builds the OSS-Fuzz [1] platform to continuously test open source applications and found over one thousand bugs in five months. Microsoft develops a fuzzing cloud service Springfield [2] for developers to test their works.

While each fuzzer develops its own specific fuzzing strategy to generate inputs, there are in general two main types. One is a generation-based strategy which uses the specification of input format, e.g. grammar, to generate complex inputs. For example, IFuzzer [3] takes a context-free grammar specification to generate parse trees for code fragments. Radamsa [4] reads sample files of valid data and generates interesting different outputs from them. The other main strategy is mutation-based. This approach generates new inputs by mutating the existing seeds (good inputs contributing to improve the coverage). Recently, mutation-based fuzzers have been proposed to use coverage information of the target programs to further improve effectiveness for bug detection. For example, libFuzzer [5] mutates seeds by utilizing the Sanitizer-Coverage instrumentation to track block coverage, while AFL [6] mutates seeds by using static instrumentation to track edge coverage.

Fuzzing has attracted significant research interest in recent years. For example, by analyzing programs in source code or binary form, white-box fuzzers have more-detailed knowledge compared to the traditional generation- or mutation-based fuzzers. Symbolic execution-based white-box fuzzers [7] systematically explore the state space of a program by automatically constructing inputs exercising a predefined path. Taint analysis-based white-box fuzzers [8] infer bytes that impact more and limit mutation to those bytes accordingly. In addition to the efficiency improvement with more information on the traditional application software, other researchers also try to customize fuzzing to other domains, such as deep learning [9], block-chain [10] and industry control systems [11].

In real industry practice, it is common to integrate existing techniques for better performance. The approach of hybrid fuzzing is combing fuzzers together to play to their strengths. For example, supplying high-quality seeds which cover a large area of the target program is always good for improving the fuzzing coverage. SAFL [12] optimizes the fuzzer AFL widely used in industry by generating high-quality initial seeds with the white-box symbolic execution engine, and the optimization is integrated through the external input interface. Another example is the optimization combination of selecting input seeds and mutating seeds. Enfuzz [13] proposes a globally asynchronous and locally synchronous (GALS)-based seed synchronization mechanism to seamlessly ensemble those base fuzzers and obtain better performance.

In summary, fuzzing is a typical approach for automated system analysis and has been widely used in real industry practice. The main limitation is that it may not cover all paths and the customization to each type of software is time-consuming. More efforts should be paid to reduce the false negative rates and improve its scalability to different domains.

References

[1] Continuous fuzzing for open source software. https://opensource.googleblog.com/2016/12/announcing-oss-fuzz-continuous-fuzzing..., 2016
[2] Microsoft security risk detection. https://www.microsoft.com/en-us/research/project/project-springfield/, 2015
[3] Veggalms, S. et al. Ifuzzer: An evolutionary interpreter fuzzer using genetic programming. In ESORICS, pp. 581—601, Springer, 2016.
[4] HELIN, A. Radamsa. https://gitlab.com/akihe/radamsa, 2016.
[5] Libfuzzer. https://llvm.org/docs/LibFuzzer.html, 2017.
[6] ZALEWSKI, M. American fuzzy lop. https://github.com/mcarpenter/afl, 2015.
[7] Thanassis Avgerinos, et al. 2011. AEG: Automatic Exploit Generation. In NDSS 2011.
[8] Sanjay Rawat, et al. VUzzer: Application-aware Evolutionary Fuzzing. In NDSS 2017.
[9] Jianmin Guo, et al. 2018. DLFuzz: differential fuzzing testing of deep learning systems. In ESEC/SIGSOFT FSE, pages 739–743. ACM, 2018
[10] Ying Fu, et al. Evmfuzzer: detect evm vulnerabilities via fuzz testing. In ESEC/SIGSOFT FSE, pages 1110—1114. ACM, 2019
[11] Zhengxiong Luo, et al. Polar : Function code aware fuzz testing of ics protocol. In TECS, pages 93:1–93:22, ACM, 2019.
[12] Mingzhe Wang, et al. Safl: Increasing and accelerating testing coverage with symbolic execution and guided fuzzing. In ICSE-C, pages 61-64, IEEE, 2018
[13] Yuanliang Chen, et al. EnFuzz: Ensemble Fuzzing with Seed Synchronization among Diverse Fuzzers. Usenix Security, pages 1967–1983, 2019.

Back to Contents

Paper Submission Deadlines

ICDCS'20 — IEEE Int'l Conference on Distributed Computing Systems
Singapore
Deadline: Jan 13, 2020 (Abstracts due: Jan 6, 2020)
Jul 8–10, 2019
https://icdcs2020.sg

NATW’20 — IEEE North Atlantic Test Workshop
Albany, NY
Deadline: Feb 7, 2020
May 18–20, 2020
http://natw.ieee.org

ISVLSI’20 — IEEE Computer Society Annual Symposium on VLSI
Limassol, Cyprus
Deadline: Feb 20, 2010
Jul 6–8, 2020
http://www.isvlsi.org

ISLPED’20 — ACM/IEEE Int’l Symposium on Low Power Electronics and Design
Boston, MA

Deadline: Mar 9, 2020 (Abstracts due: Mar 2, 2020)
Aug 10–12, 2020
http://www.islped.org

Back to Contents

Upcoming Symposia, Conferences and Workshops

VLSID'20 — Embedded and VLSI Design Conference
Bengaluru, India
Jan 4–8, 2020
http://www.vlsidesignconference.org

ASP-DAC'20 – Asia and South Pacific Design Automation Conference
Beijing, China
Jan 13–16, 2020
www.aspdac.com

HiPEAC'20: Int'l Conference on High Performance Embedded Architectures & Compilers
Balogna, Italy
Jan 20–22, 2020
https://www.hipeac.net

ISSCC'20 — IEEE Int'l Solid-State Circuits Conference
San Francisco, CA
Feb 16–20, 2020
http://isscc.org

FPGA’20 — ACM/SIGDA Int’l Symposium on Field-Programmable Gate Arrays
Seaside, CA
Feb 24–26, 2020
http://www.isfpga.org

DATE'20 – Design Automation and Test in Europe
Grenoble, France
Mar 9–13, 2020
http://www.date-conference.com

TAU’20 — ACM Int’l Workshop on Timing Issues in the Specification and Synthesis of Digital Systems
Monterey, CA
Mar 19–20, 2020
http://www.tauworkshop.com

ISQED'20 – Int'l Symposium on Quality Electronic Design
Santa Clara, CA
Mar 25–26, 2020
http://www.isqed.org

ISPD’20 — ACM Int’l Symposium on Physical Design
San Francisco, CA
Mar 29 – Apr 1, 2020
http://www.ispd.cc

HOST'20 — IEEE Int'l Symposium on Hardware-Oriented Security and Trust
San Jose, CA
May 4-7, 2020
http://www.hostsymposium.org

ASYNC'20 — IEEE Int'l Symposium on Asynchronous Circuits and Systems
Snowbird, UT
May 17-20, 2020
http://asyncsymposium.org

ISCAS'20 — IEEE Int'l Symposium on Circuits and Systems
Seville, Spain
May 17-20, 2020
http://iscas2020.org

GLSVLSI'20 — ACM Great Lakes Symposium on VLSI
Beijing, China
May 27-29, 2020
http://www.glsvlsi.org

ISCA'20 — Int'l Symposium on Computer Architecture
Valencia, Spain
May 30 — Jun 3, 2020
https://iscaconf.org

IWBDA'20 – Int'l Workshop on Bio-Design Automation
Worcester, MA
Jun 8-10, 2020
http://www.iwbdaconf.org/2020

DAC'20 — Design Automation Conference
San Francisco, CA
Jul 19-23, 2020
http://www.dac.com/

Back to Contents

Research Spotlight

Best Paper Awards at ICCAD 2019: 2019 International Conference on Computer Aided Design, https://iccad.com/award_recipients

Front-End Award:
"Analyzing and Modeling In-Storage Computing Workloads On EISC — An FPGA-Based System-Level Emulation Platform" by Zhenyuan Ruan, Tong He and Jason Cong – Univ. of California, Los Angeles.

Back-End Award:
"Power Grid Fixing for Electromigration-Induced Voltage Failures" by Zahi Moudallal (Univ. of Toronto), Farid N. Najm (Univ. of Toronto) and Valeriy Sukharev (Mentor, A Siemens Business).

TEN YEAR RETROSPECTIVE MOST INFLUENTIAL PAPER AWARD:
"Nonvolatile Memristor Memory: Device Characteristics and Design Implications" by Yenpo Ho, Garng M. Huang and Peng Li – Texas A&M University.

Back to Contents

SIGDA Awards

Hello readers,
In this edition of Researcher spotlight, we meet Prof. Anirban Sengupta. He is an Associate Professor in the Department of Computer Science and Engineering at Indian Institute of Technology Indore, India. He is an elected Fellow of IET and Fellow of British Computer Society. He is an IEEE Distinguished Lecturer and IEEE Distinguished Visitor. He is the Editor-in-Chief of IEEE VLSI Circuits & Systems Letter, IEEE CS-TC on VLSI. He received his Ph.D. in Electrical and Computer Engineering from Ryerson University, Toronto, Canada. Excerpts from a recent conversation.

1. Can you share with us some of the research areas you are interested in?

Some of the research areas that I have been working on are:

□ Security of Hardware Accelerators
□ Forensic detective control of Hardware Accelerators
□ IP core Steganography
□ Functional obfuscation, logic encryption, structural obfuscation of DSP hardware
□ Hardware Trojan detection during High Level Synthesis
□ Multi-objective Optimization of Hardware Accelerators
□ Transient Fault Security of Hardware Accelerators
□ High Level Synthesis and Design Space Exploration

2. For readers unfamiliar with Hardware Security, could you help explain the significance of this discipline in the overall chip design space?

Hardware Security is the security deployed in the integrated circuits (soft IP, hard IP etc.) to secure against state-of-the-art threats. These threat models could be of several types depending on the intention of the adversary. For example, a popular hardware attack is backdoor insertion of malicious logic in a chip to induce unexpected behaviour. Hardware Security against such threats would mean employing techniques to prevent, detect and diagnose such malicious logics. Another popular hardware threat is IC/IP piracy where an original integrated circuit (or IP core) logic is counterfeited or cloned by an adversary to induce financial loss to an authentic IP owner, overbuilding and causing safety and reliability issues to a product. Hardware Security in this context would mean employing algorithms to detect (with highest probability) such pirated ICs/IPs and/or prevent manufacturing of such fake chips, as these causes safety hazards to the end consumers. Another popular hardware threat is reverse engineering of an IC where a chip is back-engineered (by an adversary in the untrustworthy regime) to gain access to its design netlist for either inducing malicious logic or copying. Hardware Security in this context would mean employing techniques to prevent (or at-least challenge) such malpractices from happening.
Thus, Hardware Security is defined in the context of the threat model and the target hardware. Different threat models have different hardware security solutions. Similarly, different hardware types (such as data-intensive hardware accelerator or application engine/dedicated IP core) vs. platform-based hardware (non-data intensive general-purpose cores) have different hardware security algorithms and implementation techniques. Further, the Hardware Security can be employed at all levels of VLSI design abstraction depending on the target hardware/application and threat model. This also means that this would dictate the design overhead, security/robustness achieved and energy-security trade-off from a chip designer's perspective.

3. In cases where a Hardware Trojan is activated only under very specific use case scenarios and is dormant in most other cases, can this be detected by RTL code coverage? Can this logic be removed away during synthesis and physical implementation phases?

Detection by code coverage is not always possible. In some cases, sometimes RTL code coverage augmented with ATPG, redundant circuit removal etc. are sufficient to identify suspicious signals for detecting Hardware Trojans. There has been several approaches to prove this. However, key is that since Trojan only becomes visible at runtime (after triggering by an adversary through external means), thereby could remain completely ineffective before, thus being difficult to detect during RTL simulation/other lower level tests. Therefore, without detailed examination, few classes of Trojan may sometimes go unnoticed. This is applicable for both small and large size modules (as micro 3PIPs) present in HLS library during design of macro 3PIPs or hardware accelerators or application specific engines (peripheral hardware). Another possibility is some types of Trojans only induce delay (overhead) without affecting computational output. Hence even if RTL functional validation is performed for all 3PIPs, still it may go undetected. Similarly, other possibilities exist. Further, because there is no trustworthy golden IP model, therefore, the detection of Trojan in a 3PIP during HLS may not always be possible. Nevertheless, security aware High-Level Synthesis (HLS) using Dual Modular Redundancy (DMR) can be useful in some cases, in the context of reusable IP cores or hardware accelerators or application specific engines/processors (peripheral hardware)

Hence, the better way, than detective control of Trojan, is preventive control of Trojans using obfuscation and/or logic encryption methodologies — functional and/or structural obfuscation when the threat model considered is untrusted foundry (fabrication phase). In the case of 3PIP hardware Trojans, this would be not useful.

4. Typically, in products that acquire features by way of notable 3rd party IP integration, there are 'power roll-ups' for static power and dynamic power at each IP level and hierarchically as well. Do you foresee detecting dormant IPs through static power IP signatures? Can checksums of expected stimuli and outputs be created to detect Trojans?

Yes, it is possible in some cases. Using side channel parameters to detect hardware Trojan is a well-researched area in the community. Power signature of IPs can be one of them. Other side channel parameters such as current, voltage, energy signatures may also be useful depending on the IP. However, process variation (and parameters such as threshold voltage etc.) is an important factor, as these parameters may get affected by process variations. Sometimes unwanted noise due to process variation may be misunderstood as Trojan during side channel detection. So, this has to be taken care of during detection process. Further side channel-based detection may also become irrelevant when the hardware Trojan logic/circuit is very small. This results in very insignificant change in side channel parameter during analysis. Finally, best choice of the side channel parameter that provides accurate detection of hardware Trojan also becomes important.

5. In the case of Digital Watermarking, typical metrics like ownership coincidence, tamper-proofing, cost of embedding seem to offer a reasonable amount of integrity. However, increasing the logic complexity or register count to achieve one or more of these metrics seems increasingly challenging at advanced nodes with process variation. How do you envision an optimality in this space?
The most efficient digital IP watermarking techniques are those which do not offer overhead in register count and incurs minimal complexity. Further, the designed digital watermarking algorithms should be independent of process variations and/or technology scale. However, having said that, the register count overhead due to embedding watermark may also depend on the choice of the signature

combination, strength and devised encoding rule. Additionally, the register overhead also would depend on the size/complexity of the target application/IP core. For example, if the application engine is FIR filter, then choosing a large vendor signature for embedding watermark may incur storage overhead; while the same signature strength will not incur any overhead for large size IP such as image/video CODECs. This is sometimes beyond the control of the IC/IP vendor/designer. Hence signature-free watermark called as 'IP steganography' has been devised by researchers. This class of approaches remove the dependency on the signature characteristics. These are better than IP watermarking approaches in terms of controllability and overhead. Further being signature-free, there is no chance of ghost signature etc. to prove false claim of ownership. Moreover, in case signature and encoding rules gets compromised for digital IP watermarking, there is no way for a genuine IP vendor to prove ownership or authenticate himself/herself. This vulnerability is also removed by certain IP steganography approaches which additionally include crypto-logics/ciphers such as hashing, RSA etc. with large size vendor keys to generate secret constraints for embedding. Hence even if the signature and encoding rules get leaked/compromised, an adversary also would need to know the crypto-logics/ciphers (and key values) to scientifically prove IP ownership.
Hence, I envision the future is heading towards more efficient methodologies for invalidating IP ownership and/or piracy detection such as IP steganography and digital forensics (or forensic detective techniques, and these are usually independent of process variations and technology scale.

Back to Contents

Call for Papers: IEEE Design and Test - Special issue on Open-Source EDA

Aim and Scope:
In the 80s the academic community produced several very high-quality EDA tools that spawned the EDA industry. Tools like Spice, Espresso, and SIS became the foundation of EDA companies. Open-source tools enable rapid innovation and create an ecosystem for scientific development. In recent years, the cost and difficulty of IC design in advanced nodes have stifled hardware design innovation and have raised unprecedented barriers to bringing new design ideas to the marketplace. Unlike the thriving software community, which enjoys a large number of open-source operating systems, compilers, libraries and applications, the hardware community lacks such a modern ecosystem. With the advent of Open Silicon IP Ecosystems like RISCV, Chips Alliance, and Free Silicon Foundation, the time has come to reinvigorate the open-source movement in EDA tools. The EDA open-source landscape is fragmented and a full open-source EDA flow is lacking. Recent programs from governmental agencies aim to jump-start development of open-source EDA tools to reduce the cost and turnaround time of hardware design. Open-source development also leads to special challenges such as physical design kit support and tool maintenance and support.
Topics of Interest:

Specific topics of interest include but are not limited to the following:
SoC architecture and design tools
Simulation tools
Automatic accelerator and high-level synthesis
Tools for security and system verification
Logic synthesis
P & R tools (Floorplanning, Placement, Physical synthesis, Clock tree synthesis, Global and detailed Routing and Layout finishing)
Analysis tools: parasitics, timing, power, IR drop and thermal
Pervasive machine learning for EDA flows
Automated analog design
Design for emerging technologies

Submission Guidelines:
Prospective authors should follow the submission guidelines for IEEE Design & Test. All manuscripts must be submitted electronically to IEEE Manuscript Central at https://mc.manuscriptcentral.com/dandt

A specific special issue category will be available and selectable from a menu. All articles will undergo the standard IEEE Design & Test review process. Submitted manuscripts must not have been previously published or currently submitted for publication elsewhere.

Manuscripts must not exceed 5,000 words, including figures (with each average-size figure counting as 200 words) and a maximum of 12 references (50 for surveys). This amounts to about 4,000 words of text and a maximum of five small to medium figures. Accepted articles will be edited for clarity, structure, conciseness, grammar, passive to active voice, logical organization, readability, and adherence to style. Please see IEEE Design & Test Author Resources for links to Submission Guidelines Basics and Electronic Submission Guidelines and requirements.

Accepted articles must meet the following three criteria:
Technical novelty: all articles must meet the standard criteria of technical contribution, in terms of novel methodologies and algorithms with demonstrated superiority over existing methods.
Open-source and interoperability: all submissions must include a link to their open-source code. All open-source tools must use standard input and output file formats or databases to ensure interoperability in EDA flow.
High impact on EDA flows: acceptance priority will be given to articles that address missing or critical needs within the existing open-source ecosystem.

Submissions that heavily overlap with prior conference publications by the same authors will be given low acceptance priority.

Schedule:
Initial Submission Deadline: 15 January 2020
Notification First Round: 1 March 2020
Revision Submission: 1 April 2020
Final Notification: 1 May 2020
Final Version Due: 15 May 2020

Guest Editors:
Sherief Reda, Brown University, sherief_reda@brown.edu
Leon Stok, IBM, leonstok@us.ibm.com
Pierre-Emmanuel Gaillardon, University of Utah, pierre-emmanuel.gaillardon@utah.edu

Back to Contents

Tools announced at WOSET 2019

ACT: Asynchronous Digital Flow
http://github.com/asyncvlsi/act

AMC: Asynchronous Memory Compiler
https://github.com/asyncvlsi/AMC

BLASYS: A Tool for Approximate Logic Synthesis
https://github.com/scale-lab/BLASYS

CirKit: A logic synthesis framework
https://github.com/msoeken/cirkit

EvoApproxLib: Extended Library of Approximate Arithmetic Circuits
https://ehw.fit.vutbr.cz/evoapproxlib/

Fault: An Open Source DFT Toolchain
https://github.com/Cloud-V/Fault

LiveHD: A Productive Open-Source Hardware Development Flow
https://github.com/masc-ucsc/livehd

LSOracle: Automated AIG/MIG-based Logic Synthesis
https://github.com/LNIS-Projects/LSOracle

OGRE: Open-Source LEF/DEF Global Router
https://github.com/Cloud-V/OGRE

OpenDB: Physical Database for EDA tool development
https://github.com/The-OpenROAD-Project/OpenDB

OpenFPGA: An Open-source FPGA IP Generator
https://github.com/LNIS-Projects/OpenFPGA

OpeNPDN: Neural networks for automated synthesis of Power Delivery Networks
https://github.com/The-OpenROAD-Project/OpeNPDN

RTLog: A HDL together with a Compiler to create Relative Timing circuits.
https://github.com/VLSI-UTN-FRBA/RTLog

Skeletor: A tool for generating RTL templates from specification
https://github.com/jaquerinte/Skeletor

The EPFL logic synthesis libraries: A collection of modular open-source C++ libraries for logic synthesis
https://github.com/lsils/lstools-showcase

TherMOS: A thermal model for self-heating in advanced MOS devices
https://github.com/VidyaChhabria/TherMOS

Verible: A SystemVerilog parser, linter and formatter.
https://github.com/google/verible

Xyce: A parallel, SPICE-compatible analog circuit simulator
https://xyce.sandia.gov

Back to Contents

Call for Participant: ASP-DAC 2020 @Beijing

25th Asia and South Pacific Design Automation Conference
Date:January 13-16,2020
Place: China National Convention Center/Beijing ,China

Early-bird Registration Deadline: December 15, 2019
https://aspdac2020.github.io/aspdac20/registration/index.html

ASP-DAC is the largest conference in Asia and South-Pacific regions on Electronic Design Automation (EDA) area for VLSI and systems. ASP-DAC has been started in 1995 and this ASP-DAC 2020 is the 25th conference. ASP-DAC 2020 offers you an ideal opportunity to touch the recent technologies and the future directions on the LSI design and design automation areas by technical papers and tutorials. ASP-DAC also holds Designers' Forum to make presentations about the latest designs for designers. Please do not miss ASP-DAC 2020.

Keynote Speeches:
Keynote Speeches From Academia
1. Jan.14: Takao Someya, the University of Tokyo
2. Jan.15: Jason Cong, University of California, Los Angeles
Keynote Speeches From Industry
1. Jan.14: Synopsys,Inc
2. Jan.15: GigaDevice
3. Jan.16: Empyrean Software
4. Jan.16: Alibaba

Tutorials:
Registered tutorial participants can attend any of the following 9 topics taught by world-class experts.
tutorial-1: AI Chip Technologies and DFT Methodologies
tutorial-2: A Journey from Devices to Systems with FeFETs and NCFETs
tutorial-3: Comparison and Summary of Impulse-Sensitivity-Function (ISF) Extraction for Oscillator Phase Noise Optimization
tutorial-4: General Trends of Security Engineering for In-vehicle Network Architecture in Modern Electric Vehicle
tutorial-5: Model Compression and Neural Architecture Search for Efficient Deep Learning
tutorial-6: Hardware-based Security Solutions for the Internet of Things
tutorial-7: Machine Learning for Reliability of ICs and Systems
tutorial-8: Designing Application-Specific AI Processors
tutorial-9: An Emerging Trend in Post Moore Era: Monolithic 3D IC Technology

Designers'Forum:
ASP-DAC2020 is strongly supported by the local industry. Designers' Forum is conceived as a unique program that shares the design experience and solutions of real product developments among LSI designers and EDA academia/developers. The topics discussed in this forum include “Trends in EDA”, “Emerging Design”, and “AI Accelerators”.

University LSI Design Contest:
In University LSI Design Contest,state-of-the-art LSI designs compete on their design excellence and implementation quality. 6 high-quality designs will be introduced by presentation.

Exhibition:
In the exhibition, around 10 top enterprises in the field display and

demonstrate their latest products and systems.

SIGDA Student Research Forum:
The Student Research Forum is for PhD and MS students to discuss their dissertations and establish contacts with experts in the design automation community and for companies and academic institutes to discover extraordinary candidates. Limited funds are available for travel assistance.

Technical Sessions:
There are 86 high quality papers selected from 279 submissions. We also plan the following special sessions: “Emerging Memory Enabled Computing in The Post-Moore’s Era”, "AI Enhanced Simulation and Optimization in Back-End EDA Flow”, “Computation-in-Memory Based on Emerging Non-volatile Memories: Technology, Design, and Test and Reliability”, “Designing Reliable and Robust Circuits and Systems in the Nanometer Era”, “CMOS Annealing Hardware: Pursuing Efficiency for Solving Combinatorial Optimization Problems”, “Emerging Technologies across the Abstraction Layers”, “Resilience in Integrated Systems”.

Welcome to register!

http://www.aspdac.com
Contact: lishuolh@126.com

Back to Contents

Call for Papers and Demos: ACM/IEEE DESTION 2020

The 2nd Workshop on Design Automation for CPS and IoT
April 21, 2020 in Sydney, Australia (part of CPS-IoT Week 2020)
https://cps-vo.org/group/DESTION20
Overview:
Cyber-Physical Systems (CPS) such as autonomous vehicles, industrial robots, medical devices, and Internet-of-Things (IoT) applications, promise relevant economic and societal benefits. The design and operation of CPS and IoT, however, face serious challenges from the fast increase of system scale and complexity, the close interaction with physical environment and human activities, the adoption of multicore and distributed architectural platforms, and the stringent and diverse requirements on performance, safety, security, fault tolerance, extensibility, and energy consumption. In addition, incorporation of Learning Enabled Components (LEC) in CPS and IoT architectures is leading to new challenges in design flows that require re-thinking the fundamentals of assurance and certification. Many key engineering processes in current CPS and IoT design practices are ad-hoc (and often manual), and have been shown to be incapable of coping with such challenges. It is thus critical to have a new set of design automation methodologies, algorithms and tools for improving the quality, scalability, reliability, and productivity of CPS and IoT design processes. Emerging research directions investigate the development of AI-based co-design tools that take advantage of machine learning and artificial intelligence technologies in design flows. The new vision is a symbiotic design automation process that fuses human ingenuity with machine intelligence.

ACM/IEEE DESTION provides a premier forum for researchers and engineers from academia, industry, and government to present and discuss pressing challenges, promising solutions, and applications in design automation for CPS and IoT. The workshop has a broad scope covering tools for modeling, simulation, synthesis, validation and verification of CPS and IoT, and their applications in a variety of domains, such as automotive and transportation systems, avionics, buildings, grid, and medical devices.

The program of the workshop includes a keynote, presentations of contributed and invited papers, demonstrations, and posters.

We invite contributions in the following main topics:

§ Model and tool integration methodologies
§ Design space construction and exploration
§ Generative design approaches
§ Mining design repositories and design analytics
§ Human-machine symbiosis in design phases
§ Benchmark proposals for tool comparisons
Submissions:
Papers: All submissions must be in English. Only original papers that have not been submitted or published in other conferences or journals will be considered. Manuscripts should have no more than 10 pages. Shorter position papers are welcome.

Demos: DESTION 2020 seeks high-quality demos showing design automation benchmarks, tools, and applications for CPS and IoT. A 2-page abstract in English (including references) should be submitted.

Please submit your papers and demo abstracts at https://destion20.hotcrp.com/. The submission must be in the ACM two-column conference style, US Letter (8.5 inch x 11 inch) paper size, and 10pt text font size. All accepted papers and demo abstracts will be published in IEEE Xplore and ACM Digital Library as part of the DESTION 2020 proceedings.
Important Dates:
§ January 20 AoE, 2020: Submission deadline
§ February 10, 2020: Author notification
§ February 14, 2020: Camera-ready due

Back to Contents

Notice to Authors

This newsletter is a free service for current SIGDA members and is added automatically with a new SIGDA membership.
Circulation: 2,700