Special Interest Group on Design Automation
ACM/SIGDA E-NEWSLETTER, Vol. 52, No. 5

SIGDA - The Resource for EDA Professionals

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

Online archive: http://www.sigda.org/newsletter

SIGDA News

1. U.S. Government, Chipmakers Renew Push for CHIPS Act

The U.S. government and domestic chipmakers strengthened separate efforts this week to pass the $52 billion CHIPS Act of stimulus measures. The CHIPS Act currently awaits congressional approval, warning of strategic vulnerabilities now and in the future.

2. NASA Joins Private SATCOM Providers to Upgrade Space Network

NASA last month selected six U.S. satellite communications (SATCOM) providers to develop and demonstrate near–Earth space services that may support future agency missions.

3. TSMC Expects $44 Billion in Capex Despite Slowdown Concerns

Taiwan Semiconductor Manufacturing Company (TSMC) reiterated its plan to spend more than $40 billion this year for capacity expansion despite concerns that overall demand for chips may wane.

4. Intel Invests $3 Billion in Oregon Fab to Regain Industry Leadership

Intel today opened a $3 billion expansion of D1X Mod3, an advanced technology fab in Hillsboro, Oregon; an investment that's aimed at recapturing leadership in semiconductor process technology.

5. Samsung Profit Soars on Memory Chip Demand

Samsung Electronics, the world's largest memory chipmaker, saw its profit in the first quarter of 2022 jump by more than 50% on strong demand for memory in data centers.

Messages from the EiCs

Dear ACM/SIGDA members,

We are excited to present to you May 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 the upcoming conferences to technical news and activities of our community. Get involved and contact us if you want to contribute articles or announcements.

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

Happy reading!

Debjit Sinha, Keni Qiu,
Editors-in-Chief,
SIGDA E-News

SIGDA EC

Yiran Chen,
Chair

Sudeep Pasricha,
Vice Chair and Conference Chair

X. Sharon Hu,
Past chair

6. [Streetlights Offer Path to Rapid mmWave 5G]

On my daily walks, I often look up at the streetlights and think about the potential they hold for deploying many different technology solutions, whether for environmental monitoring, surveillance, or for enhancing network infrastructure. So it was no surprise to see this week's announcement from Movandi and Ubicquia of their partnership to develop and deploy mmWave streetlight repeaters to enhance 5G and fixed wireless access coverage.

What Is

What is Needed for Secure Electronic Design Automation?

Contributing author: Kyle Juretus

Assistant Professor, Electrical and Computer Engineering Department, Villanova University

Editor: Xun Jiao <xun.jiao@villanova.edu>

Electronic design automation (EDA) tools have been critical to scaling the number of transistors in digital designs. For example, imagine the design effort needed for a team of engineers to manually layout a design with one billion transistors. While EDA tools have enabled the design scale and complexity of modern integrated circuits (ICs), the underlying optimization objectives of EDA tools largely focus on power, performance, and area (PPA). The focus on PPA has ultimately created some weaknesses that have been utilized as security vulnerabilities.

One major area for exploited vulnerability has been side-channel leakage. Where the power [1] or timing signatures of the device can leak sensitive data, such as an AES key [2]. Additionally, the complexity and cost of IC manufacturing has shifted the industry to a largely horizontal manufacturing flow [3], where production, testing, and verification may all be handled by untrusted third-party entities. Such security threats motivate not only new security solutions, but a re-imagining of the algorithms at the core of current EDA tools. Projects like the DARPA Automatic Implementation of Secure Silicon (AISS) program aim to do just this,

SIGDA E-News Editorial Board

pushing new design constraints of Power, Area, Speed, and Security (PASS).

To motive the need to change underlying algorithms in EDA, consider the research area of logic obfuscation where the goal is to make reverse engineering an IC design difficult [4]. Since traditional EDA tools have no security optimization criteria, the design alterations can often be localized and either removed or neutralized [5], leaving little to no security benefit. Ultimately, the underlying logic synthesis algorithms contribute to the security issues, where the graph cut and optimization flow [6] greedily tries to improve PPA based objectives. Such optimization strategies ultimately resemble the security alterations and original logic being optimized separately, rather than the needed combined optimization.

A variety of changes are required to create secure EDA tools. The first category of change needed is efficient and accurate measures of security. All too often measures of security tend to be based on an attack itself [7, 8], rather than a heuristic for attack complexity. Not only is it inefficient to run the attack to gauge security, it is also difficult to explore the wide range of parameters a given attack may employ [9]. Again, borrowing from the logic obfuscation research area, early work was very hard to quantify security for [4] but algorithm development has shifted towards quantifiable security against certain attacks [10, 11].

Once quantifiable measures of security are available, optimization strategies in EDA tools can be altered to include these new measures. For example, rather than using a look up table for Boolean matching based on measures like number of cells [6], resiliency or structural security scores can be evaluated to rate the structures under consideration. The weight of each optimization parameter should then be tunable based on the individual needs of the IC design.

The exposure of security to the designer also needs to be carefully considered. To achieve scalable security, it is important that the security decisions are not left entirely up to the designer. The knowledge and expertise in the area of hardware security is something that can be quickly undermined by one assumption and all designers should not be expected to be experts in security. Ultimately, significant analysis will be required to demonstrate how PPA constrained devices will alter security goals and the best ways to limit the security impact on the design.

In summary, security is needed as a design automation objective. To enable secure EDA tools, security solutions need to have efficient and accurate metrics for incorporation into EDA optimizers.

Paper Deadlines

NOCS'22 – IEEE/ACM Int'l Symposium on Networks-on-Chip
(co-located with ESWEEK 2022)
Hybrid Conference.
Shanghai, China
Deadline: May 6, 2022
(Abstracts due: April 29, 2022)
Oct 7-14, 2022
https://nocs2022.github.io

HOST'22 – IEEE Int'l Symposium on Hardware-Oriented Security and Trust
Washington DC
Deadline: May 11, 2021
(Abstracts due: April 27, 2021)
June 27-30, 2022
http://www.hostsymposium.org

ICCAD'22 – IEEE/ACM Int'l Conference on Computer-Aided Design
Hybrid in-person and virtual conference
Deadline: May 23, 2022
(Abstracts due: May 16, 2022)
Oct 30 - Nov 3, 2022
http://www.iccad.com

MEMOCODE'22 - IEEE/ACM Int'l Conference on Formal Methods and models for System Design
(co-located with ESWEEK 2022)
Hybrid Conference
Shanghai, China
Deadline: June 3, 2022
(Abstracts due: May 27, 2022)
Oct 13-14, 2022
https://memocode2022.github.io

Optimizers are going to need to be able to serve many different security constraints as well, and this exposure to IC designers needs to be carefully considered.

References

[1] Kocher, P., Jaffe, J., and Jun, B. Differential Power Analysis. In: Wiener, M. (eds) Advances in Cryptology — CRYPTO' 99. CRYPTO 1999. Lecture Notes in Computer Science, vol 1666. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48405-1_25

[2] Bonneau, J., Mironov, I. (2006). Cache-Collision Timing Attacks Against AES. In: Goubin, L., Matsui, M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11894063_16

[3] IARPA, "Trusted Integrated Chips (TIC) Program,"IARPA-BAA-11-09, October 2011.

[4] J. Roy, F. Koushanfar, and I. Markov, "EPIC: EndingPiracyofIntegrated Circuits," Proceedings of the IEEE/ACM Design, Automation and Test in Europe Conference, pp. 1069–1074, October 2008.

[5] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Removal Attacks on Logic Locking and Camouflaging Techniques," IEEE Transactions on Emerging Topics in Computing, August 2017.

[6] A. Mishchenko, S. Chatterjee and R. Brayton, "DAG-aware AIG rewriting: a fresh look at combinational logic synthesis," 2006 43rd ACM/IEEE Design Automation Conference, 2006, pp. 532-535, doi: 10.1145/1146909.1147048.

[7] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the Security of Logic Encryption Algorithms," Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust, pp. 137–143, May 2015.

[8] K. Juretus and I. Savidis, "Characterization of In-Cone Logic Locking Resiliency Against the SAT Attack," IEEE Transactions on Computer- Aided Design of Integrated Circuits and Systems, Vol. PP, pp. 1–14, 2019.

[9] K. Juretus and I. Savidis, "Importance of Multi-parameter SAT Attack Exploration for Integrated Circuit Security," 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2018, pp. 366-369, doi: 10.1109/APCCAS.2018.8605696.

[10] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. Rajendran, and O. Sinanoglu, "Provably-Secure Logic Locking: From Theory To Practice," Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 1601–1618, November 2017.

[11] K. Juretus and I. Savidis, "Increased Output Corruption and Structural Attack Resilience for SAT Attack Secure Logic Locking," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 1, pp. 38-51, Jan. 2021, doi: 10.1109/TCAD.2020.2988629.

BioCAS'22 – Biomedical Circuits and Systems Conference
Taipei, Taiwan
Deadline: June 10, 2022
Oct 13-15, 2022
https://2022.ieee-biocas.org/

HiPC'22 – IEEE Int'l Conference on High Performance Computing, Data, And Analytics
Deadline: June 24, 2022
(Abstracts due: June 10, 2022)
Dec 18-21, 2022
http://www.hipc.org

MLCAD'22 - ACM/IEEE Workshop on Machine Learning for CAD
Snowbird, Utah
Deadline: Jul 1, 2022
Sep 12 - 13, 2022
https://mlcad-workshop.org/

FPT'22 - Int'l Conference on Field-Programmable Technology
Hybrid: Hong Kong, China
Deadline: Jul 15, 2022
(Abstracts due: Jul 8, 2022)
Dec 5-9, 2021
http://icfpt.org

ASP-DAC'23 - Asia and South Pacific Design Automation Conference
Miraikan, Tokyo, Japan
Deadline: Jul 29, 2022
(Abstracts due: Jul 24, 2022)
Jan 16-19, 2023
http://www.aspdac.com

SIGDA Awards

1. EDAA Outstanding Dissertations Award @ DATE 2022
https://www.date-conference.com/awards
Topic 1: Thesis: "High-level Synthesis of Dynamically Scheduled Circuits", Lana Josipovic, Ph.D., EPFL, CH.
Advisor: Prof. Paolo Ienne
Topic 3: Thesis: "Design for Manufacturability and Reliability through Learning and Optimization", Wei Ye, PhD., University of Texas at Austin, US.
Advisor: Prof. David Z. Pan
Topic 4: Thesis: "Revisiting Fault Analysis of Block Ciphers: Attacks, Defenses, and Vulnerability Assessment Frameworks", Sayandeep Saha, Ph.D., Indian Institute of Technology, Kharagpur, IN.
Advisor: Prof. Debdeep Mukhopadhyay and Prof. Pallab Dasgupta

2. DATE Best IP Award @ DATE 2022
https://www.date-conference.com/awards
"XST: A Crossbar Column-Wise Sparse Training For Efficient Continual Learning", by Fan Zhang, Li Yang, Jian Meng, Jae-sun Seo, Yu Cao, Deliang Fan, Arizona State University, US.

3. DATE Best Paper Awards @ DATE 2022
https://www.date-conference.com/awards
D Track: "FastGR: Global Routing on CPU-GPU with Heterogeneous Task Graph Scheduler", by Siting Liu[1,2], Peiyu Liao[1,2], Rui Zhang[3], Zhitang Chen4, Wenlong Lv[4], Yibo Lin[1], Bei Yu[2].
[1]Peking University, [2] The Chinese University of Hong Kong, [3] HiSilicon Technologies Co., [4] Huawei Noah's Ark Lab
A Track: "Algorithm-Hardware Co-Design for Efficient Brain-Inspired Hyperdimensional Learning on Edge", by Yang Ni[1], Yeseong Kim[2], Tajana Rosing[3], Mohsen Imani[1].
[1] University of California Irvine, [2] DGIST Republic of Korea, [3] University of California San Diego
T Track: "Self-Terminated Write of Multi-Level Cell ReRAM for Efficient Neuromorphic Computing", by Zongwu Wang, Zhezhi He, Rui Yang, Shiquan Fan, Jie Lin, Fangxin Liu, Yueyang Jia, Chenxi Yuan, Qidong Tang, Li Jiang.
Shanghai Jiao Tong University, China

Upcoming Conferences

RTAS'22 - IEEE Real-Time and Embedded Technology and Applications Symposium
Milano, Italy
May 4-6, 2022
http://2022.rtas.org

FCCM' 22 - IEEE International Symposium On Field-Programmable Custom Computing Machines
New York
May 15–18, 2022
https://www.fccm.org/

MDTS'22 – IEEE Microelectronics Design & Test Symposium
Virtual
May 23-26, 2022
http://natw.ieee.org

ISCAS'22 – IEEE Int'l Symposium on Circuits and Systems
Austin, TX
May 28 - June 1, 2022
http://iscas2022.org

GLSVLSI'22 – ACM Great Lakes Symposium on VLSI Orange County, CA
June 6-8, 2022
http://www.glsvlsi.org

OSCAR'22 - First Workshop on Open-Source Computer Architecture Research
New York (co-located with ISCA 2022)
June 11, 2022
https://oscar-workshop.github.io/

E Track: "Efficient Global Robustness Certification of Neural Networks via Interleaving Twin-Network Encoding", by Zhilu Wang[1], Chao Huang[2], Qi Zhu[1].
[1] Northwestern University, [2] University of Liverpool, Northwestern University

4.ACM SIGDA/CEDA/EDAA PhD Forum Prize @ DATE 2022
https://www.date-conference.com/awards
"Ultra-Fast Temperature Estimation Methods For Architecture-Level Thermal Modeling", Hameedah Sultan, Indian Institute of Technology Dehli, IN
"Dependable Reconfigurable Scan Networks", Natalia Lylina, University of Stuttgart, DE

5. DATE Fellow Award & CEDA Service Award @ DATE 2022
https://www.date-conference.com/awards
Franco Fummi, Università di Verona, IT

6. IEEE CS TTTC Outstanding Contribution Award @ DATE 2022
https://www.date-conference.com/awards
Franco Fummi, Università di Verona, IT
Cristiana Bolchini, Politecnico di Milano, IT

7. Lifetime Achievement Award @ ISPD 2022
https://ispd.cc/ispd2022/index.php?page=awards
Prof. Ricardo Augusto Da Luz Reis, Federal University of Rio Grande do Sul, Brazil

8. Best Paper Award @ ISPD 2022
https://ispd.cc/ispd2022/index.php?page=awards
"LEO: Line End Optimizer for Sub-7nm Technology Nodes", by Diwesh Pandey[1], Gustavo Tellez[2] and James Leland[3].
[1]IBM Systems, Bengaluru, India
[2]IBM T.J. Watson Research Center, Yorktown Heights, NY, USA
[3]IBM Systems, Poughkeepsie, NY, USA

9. Contest Winners @ ISPD 2022
https://ispd.cc/ispd2022/index.php
1st place: XDSecurity. Xidian University: Zhengguang Tang, Guangxin Guo, Benzheng Li, Hailong You, Jiangyi Shi); Giga Design Automation: Xiaojue Zhang
2nd place: NTUsplace. National Taiwan University: Jhih-Wei Hsu, Kuan-Cheng Chen, Yu-Hsiang Lo, Yan-Syuan Chen, Yao-Wen Chang

ISCA'22 – Int'l Symposium on Computer Architecture
New York City, USA
June 11-15, 2022
https://iscaconf.org/isca2022/

LCTES'22 – ACM Int'l Conference on Languages Compilers, Tools and Theory of Embedded Systems
San Diego, CA
June 14, 2022
https://pldi22.sigplan.org/home/LCTES-2022

HiPEAC'22: Int'l Conference on High Performance Embedded Architectures & Compilers
Budapest, Hungary
June 20-22, 2022
https://www.hipeac.net/2022/budapest/

ISVLSI'22 – IEEE Computer Society Annual Symposium on VLSI
Cyprus
July 4-6, 2022
http://www.ieee-isvlsi.org

ICDCS'22 – IEEE Int'l Conference on Distributed Computing Systems
Bologna, Italy
Jul 10 - 13, 2022
https://www.icdcs.org/

DAC'22 – Design Automation Conference
San Francisco, CA
July 10-14, 2022
http://www.dac.com/

IWLS'22 - International Workshop on Logic & Synthesis
Virtual conference
Jul 18-21, 2022
https://www.iwls.org

3rd place: CUEDA. The Chinese University of Hong Kong: Fangzhou Wang, Qijing Wang, Bangqi Fu, Shui Jiang, Xiaopeng Zhang, Tsung-Yi Ho, Evangeline F. Y. Young
3rd place: TalTech. Tallinn University of Technology: Tiago Perez, Mohammad Eslami, Felipe Almeida, Samuel Pagliarini

Who's Who

Kuan-Hsun Chen
Assistant Professor
University of Twente, the Netherlands
Research interests: Real-Time Embedded Systems, Non-Volatile Memories, Architecture-Aware Software Design, Resource-Constrained Machine Learning
Email: k.h.chen@utwente.nl
Webpage: https://people.utwente.nl/k.h.chen

ISLPED'22 – ACM/IEEE Int'l Symposium on Low Power Electronics and Design
Boston University, Boston, MA (Hybrid)
Aug 1-3, 2022
http://www.islped.org

VLSI-SoC'22 – IFIP/IEEE Int'l Conference on Very Large Scale Integration
Patras, Greece
Oct 3-5, 2022

http://www.vlsi-soc.com

ESWEEK'22 - Embedded Systems Week (CASES, CODES+ISSS, and EMSOFT)
Hybrid Conference. Shanghai, China
Oct 7-14, 2022
http://www.esweek.org

PACT'22 - Int'l Conference on Parallel Architectures and Compilation Techniques
Chicago, IL
Oct 10-12, 2022
http://www.pactconf.org

MICRO'22 – IEEE/ACM Int'l Symposium on Microarchitecture
Chicago, IL
October, 2022
http://www.microarch.org/micro55

EDAML - 1st IEEE International Workshop on Electronic Design Automation and Machine Learning
(Co-located with IPDPS 2022)
10AM-3PM ET, June 3, 2022
(Virtual Workshop)
http://www.ipdps.org/ipdps2022/2022-registration.html

Notice to authors