Full text available at: http://dx.doi.org/10.1561/3500000003

QED and Symbolic QED: Dramatic Improvements in Pre-Silicon Verification and Post-Silicon Validation

Other titles in Foundations and Trends® in Integrated Circuits and Systems

Recent Advances in Testing Techniques for AI Hardware Accelerators
Arjun Chaudhuri, Ching-Yuan Chen and Krishnendu Chakrabarty
ISBN: 978-1-63828-240-2

Of Brains and Computers
Jan M. Rabaey
ISBN: 978-1-63828-120-7

Emerging Trends of Biomedical Circuits and Systems
Mohamad Sawan, Jie Yang, Mahdi Tarkhan, Jinbo Chen, Minqing Wang, Chuanqing Wang, Fen Xia and Yun-Hsuan Chen
ISBN: 978-1-68083-906-7

Revisiting the Frontiers of Analog and Mixed-Signal Integrated Circuits Architectures and Techniques towards the future Internet of Everything (IoE) Applications
Rui P. Martins, Pui-In Mak, Sai-Weng Sin, Man-Kay Law, Yan Zhu, Yan Lu, Jun Yin, Chi-Hang Chan, Yong Chen, Ka-Fai Un, Mo Huang, Minglei Zhang, Yang Jiang and Wei-Han Yu
ISBN: 978-1-68083-892-3

Welcome to the World of Single-Slope Column-Level Analog-to-Digital Converters for CMOS Image Sensors
Albert Theuwissen and Guy Meynants
ISBN: 978-1-68083-812-1

QED and Symbolic QED: Dramatic Improvements in Pre-Silicon Verification and Post-Silicon Validation

Keerthikumara Devarajegowda
Clark Barrett
Florian Lonsing
Wolfgang Ecker
Mohammad R. Fadiheh
Wolfgang Kunz
Saranyu Chattopadhyay
Yanjing Li
David Lin
Dominik Stoffel
Srinivas Shashank Nuthakki
Subhasish Mitra
Eshan Singh

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Integrated Circuits and Systems

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

K. Devarajegowda *et al.*. *QED and Symbolic QED: Dramatic Improvements in Pre-Silicon Verification and Post-Silicon Validation*. Foundations and Trends® in Integrated Circuits and Systems, vol. 3, no. 2–3, pp. 51–218, 2024.

ISBN: 978-1-63828-399-7

Full text available at: http://dx.doi.org/10.1561/3500000003

Foundations and Trends® in Integrated Circuits and Systems
Volume 3, Issue 2–3, 2024

Editorial Board

Full text available at: http://dx.doi.org/10.1561/3500000003

Editorial Scope

Topics

Foundations and Trends® in Integrated Circuits and Systems survey and tutorial articles in the following topics:

- Analog, digital and mixed-signal circuits and systems
- RF and mm-wave integrated circuits and systems
- Wireless and wireline communication circuits and systems
- Data converters and frequency generation
- Power electronics and power management circuits
- Biomedical circuits and systems
- Sensor and imager circuits and cyber physical systems
- Security and resilient circuits and systems
- Circuits and systems in emerging non-CMOS technologies
- Circuit theory, modeling, analysis and design methods

Information for Librarians

Foundations and Trends® in Integrated Circuits and Systems, 2024, Volume 3, 4 issues. ISSN paper version 2693-9347. ISSN online version 2693-9355. Also available as a combined paper and online subscription.

Contents

QED and Symbolic QED: Dramatic Improvements in Pre-Silicon Verification and Post-Silicon Validation

Keerthikumara Devarajegowda[4], Florian Lonsing[1], Mohammad R. Fadiheh[1,2], Saranyu Chattopadhyay[1], David Lin[1], Srinivas Shashank Nuthakki[1], Eshan Singh[1], Clark Barrett[1], Wolfgang Ecker[3], Wolfgang Kunz[2], Yanjing Li[1], Dominik Stoffel[2] and Subhasish Mitra[1]

[1] *Stanford University, USA; keerthi.devraj@gmail.com*
[2] *Technische Universitaet Kaiserslautern, Germany*
[3] *Infineon Technologies AG, Germany*
[4] *Siemens EDA, Germany*

Keerthikumara Devarajegowda, Florian Lonsing, Mohammad R. Fadiheh, Saranyu Chattopadhyay, David Lin, Srinivas Shashank Nuthakki, Eshan Singh, Clark Barrett, Wolfgang Ecker, Wolfgang Kunz, Yanjing Li, Dominik Stoffel and Subhasish Mitra (2024), "QED and Symbolic QED: Dramatic Improvements in Pre-Silicon Verification and Post-Silicon Validation", Foundations and Trends® in Integrated Circuits and Systems: Vol. 3, No. 2–3, pp 51–218. DOI: 10.1561/3500000003.

Full text available at: http://dx.doi.org/10.1561/3500000003

Preface

System-on-Chips (SoCs) are an integral part of our lives. The complexity of SoCs requires sophisticated tools and methods for ensuring functional correctness, especially in critical domains such as automotive and healthcare applications. In addition, the prevalence of security features in SoCs and emerging threats such as Spectre and Meltdown underscore the need for advanced verification techniques to combat security vulnerabilities. Existing verification approaches consume over 50% of development effort. Pre-silicon verification ensures functional correctness before chip fabrication, while post-silicon validation detects bugs that escape pre-silicon verification. Existing pre-silicon and post-silicon approaches are inadequate resulting in skyrocketing bug escapes and respins. To address these challenges, this book presents pre-silicon verification and post-silicon validation methods based on Quick Error Detection (QED) principles: self-consistency checking to detect and localize design bugs.

Symbolic QED combines QED principles with model checking (a formal verification technique) for pre-silicon verification. Many studies, including industrial case studies, have demonstrated the effectiveness and practicality of Symbolic QED:

(1) Symbolic QED successfully detected every logic bug detected by traditional industrial verification flows, which included both simulation- and formal-based verification techniques. Symbolic

QED detected additional logic bugs that were not recorded as detected by industrial verification flows.

(2) Symbolic QED significantly boosts design productivity, achieving 8X reduction in verification efforts for new designs and 80X reduction for subsequent design revisions.

(3) Symbolic QED achieved rapid bug detection, with runtime at or below 20 seconds, and concise counterexamples of 10 or fewer clock cycles, facilitating swift debugging.

QED-based methods for post-silicon validation significantly reduce the error detection latency (the time elapsed between the occurrence of a bug and its manifestation as an observable failure) by several orders of magnitude, addressing the limitations of existing validation and debug approaches. Experimental results demonstrate the effectiveness and applicability of QED:

(1) QED approaches can be largely automated, enabling large productivity benefits.

(2) QED improves error detection latencies by up to 9 orders of magnitude, reducing it to very few clock cycles (generally fewer than 1,000 clock cycles for most bug scenarios).

(3) QED enables up to 4X improvement in bug coverage, detecting bugs that may be missed by traditional post-silicon validation approaches.

The book also discusses Unique Program Execution Checking (UPEC), a hardware security verification technique inspired by QED principles. UPEC systematically detects Transient Execution Side-channels (TES) in processor implementations and has demonstrated its ability to detect Spectre and Meltdown type security attacks on complex processor cores. UPEC is the first formal verification approach at the Register-Transfer Level (RTL) that comprehensively checks for TES vulnerabilities in microarchitectures without prior knowledge of specific attacks. This enables the detection of new or previously unknown TES threats through UPEC rather than depending on the insights of security researchers

and experts. The scalability of UPEC has been validated on complex out-of-order processors, such as BOOM, which features over 650,000 state bits.

Beyond the specific QED techniques described here, a new pre-silicon verification approach called G-QED (Generalized Quick Error Detection) is already demonstrating significant drastic benefits for pre-silicon verification of a wide variety of designs.

References

[1] M. Abramovici, "A reconfigurable design-for-debug infrastructure for SoCs," in *Proceedings of IEEE/ACM Design Automation Conference*, 2006.

[2] A. Adir *et al.*, "Threadmill: A post-silicon exerciser for multi-threaded processors," in *Proceedings of IEEE/ACM Design Automation Conference*, 2011.

[3] A. Aharon, D. Goodman, M. Levinger, Y. Lichtenstein, Y. Malka, C. Metzger, M. Molcho, and G. Shurek, "Test program generation for functional verification of powerPC processors in IBM," in *Proceedings of IEEE/ACM Design Automation Conference*, 1995.

[4] T. Aitch, *Aquarius: A pipelined RISC CPU*, 2003. URL: https://opencores.org/projects/aquarius.

[5] M. E. Amyeen, S. Venkataraman, and M. W. Mak, "Microprocessor system failures debug and fault isolation methodology," in *Proceedings IEEE International Test Conference*, 2009.

[6] AQED-DAC-RESULTS, *Github*, 2020. URL: https://github.com/upscale-project/aqed-dac2020-results.

[7] A. Ardeshiricham, W. Hu, and R. Kastner, "Clepsydra: Modeling timing flows in hardware designs," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2017.

[8] ARM, *Arm A64 instruction set architecture*, 2018.

[9] K. Basu, D. Soni, M. Nabeel, and R. Karri, "NIST post-quantum cryptography—A hardware evaluation study," *IACR Cryptology ePrint Archive Report 2019/047*, 2019.

[10] A. A. Bayazit and S. Malik, "Complementary use of runtime validation and model checking," in *Proceedings of the 2005 IEEE/ACM International Conference on Computer-Aided Design*, USA, 2005.

[11] B. Bentley and R. R. Gray, "Validating the intel pentium 4 processor," *Intel Technology Journal*, vol. 5, no. 1, pp. 1–8, 2001.

[12] J. Bhadra, M. S. Abadir, L. Wang, and S. Ray, "A survey of hybrid techniques for functional verification," *IEEE Design Test of Computers*, vol. 24, pp. 112–122, 2007.

[13] M. Bohr, "The new era of scaling in an SoC world," in *Proceedings of IEEE Solid-State Circuits Conference*, 2009.

[14] J. Bormann, S. Beyer, A. Maggiore, M. Siegel, S. Skalberg, T. Blackmore, and F. Bruno, "Complete formal verification of TriCore2 and other processors," in *Design and Verification Conference (DVCon)*, 2007.

[15] D. Brand, "Verification of large synthesized designs," in *Proceedings of 1993 International Conference on Computer Aided Design (ICCAD)*, 1993.

[16] G. Cabodi, P. Camurati, F. Finocchiaro, and D. Vendraminetto, "Model checking speculation dependent security properties: Abstracting and reducing processor models for sound and complete verification," in *International Conference on Codes, Cryptology, & Information Security*, pp. 462–479, Springer, 2019.

[17] G. Cabodi, P. Camurati, S. F. Finocchiaro, F. Savarese, and D. Vendraminetto, "Embedded systems secure path verification at the HW/SW interface," *IEEE Design & Test*, vol. 34, no. 5, pp. 38–46, 2017.

[18] C. Cascaval, S. Chatterjee, H. Franke, K. J. Gildea, and P. Pattnaik, "A taxonomy of accelerator architectures and their programming models," *IBM Journal of Research and Development*, vol. 54, no. 5, 5:1–5:10, 2010.

[19] K. M. Chandy, J. Misra, and L. M. Haas, "Distributed deadlock detection," *ACM Transactions on Computer Systems*, vol. 1, no. 2, pp. 144–156, 1983.

[20] S. Chattopadhyay, K. Devarajegowda, B. Zhao, F. Lonsing, B. D'Agostino, I. Vavelidou, V. Bhatt, S. Prebeck, T. C. Ecker, C. Barrett, and S. Mitra, "G-QED: Generalized QED pre-silicon verification beyond non-interfering hardware accelerators," in *Design Automation Conference 2023*, San Fransisco, 2023.

[21] S. Chattopadhyay, F. Lonsing, L. Piccolboni, D. Soni, P. Wei, X. Zhang, Y. Zhou, L. Carloni, D. Chen, J. Cong, R. Karri, Z. Zhang, C. Trippel, C. Barrett, and S. Mitra, "Scaling up hardware accelerator verification using {A-QED} with functional decomposition," in *Formal Methods in Computer Aided Design (FMCAD)*, New Haven, CT, USA, 2021.

[22] W. Chen, S. Ray, J. Bhadra, M. Abadir, and L. Wang, "Challenges and trends in modern SoC design verification," *IEEE Design Test*, vol. 34, no. 5, pp. 7–22, 2017.

[23] Y. Chi, Y. Choi, J. Cong, and J. Wang, "Rapid cycle-accurate simulator for high-level synthesis," in *Proceedings of the 2019 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*, New York, USA, 2019.

[24] Y. Chi, Y. Choi, J. Cong, and J. Wang, "Rapid cycle-accurate simulator for high-level synthesis," in *FPGA*, 2019.

[25] E. Clarke, A. Biere, R. Raimi, and Y. Zhu, "Bounded model checking using satisfiability solving," *Formal Methods in System Design*, 2001.

[26] E. Clarke, O. Grumberg, and D. Peleg, *Model Checking*. Cambridge, MA, USA: MIT Press, 1999.

[27] *Common Weakness Enumeration*. URL: https://cwe.mitre.org/.

[28] J. Cong, M. A. Ghodrat, M. Gill, B. Grigorian, and G. Reinman, *Architecture Support for Accelerator-Rich CMPs*. San Fransisco, USA, 2012.

[29] J. Cong, P. Wei, C. H. Yu, and P. Zhou, *Bandwidth Optimization Through on-chip Memory Restructuring for HLS*. Austin, USA, 2017.

[30] E. G. Cota, P. Mantovani, G. Di Guglielmo, and L. P. Carloni, *An Analysis of Accelerator Coupling in Heterogeneous Architectures*. San Fransisco, CA, USA, 2015.

[31] F. M. De Paula, M. Gort, A. J. Hu, S. J. E. Wilton, and J. Yang, "BackSpace: Formal analysis for post-silicon debug," in *Proceedings Formal Methods in CAD*, 2008.

[32] F. M. De Paula, A. J. Hu, and A. Nahir, "nuTAB-backspace: Rewriting to normalize non-determinism in post-silicon debug traces," in *Proceedings International Conference on Computer Aided Verification*, 2012.

[33] S. Deng, D. Gümüşoğlu, W. Xiong, S. Sari, Y. S. Gener, C. Lu, O. Demir, and J. Szefer, "SecChisel framework for security verification of secure processor architectures," in *Proceedings of the 8th International Workshop on Hardware and Architectural Support for Security and Privacy*, 2019.

[34] G. Dessouky, D. Gens, P. Haney, G. Persyn, A. Kanuparthi, H. Khattri, J. M. Fung, and A. R. Sadeghi, "Hardfails: Insights into software-exploitable hardware bugs," in *USENIX Security*, 2019.

[35] S. Deutsch and K. Chakrabarty, "Massive signal tracing using on-chip DRAM for in-system silicon debug," in *Proceedings of IEEE International Test Conference*, 2014.

[36] K. Devarajegowda, M. R. Fadiheh, E. Singh, C. Barrett, S. Mitra, W. Ecker, D. Stoffel, and W. Kunz, "Gap-free processor verification by S2QED and property generation," in *2020 Design, Automation Test in Europe Conference Exhibition (DATE)*, Grenoble, 2020.

[37] K. Devarajegowda, E. Kaja, S. Prebeck, and W. Ecker, "ISA modeling with trace notation for context free property generation," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*, San Francisco, CA, USA, 2021.

[38] J. J. Dongarra, P. Luszczek, and A. P. Petitet, "The LINPACK benchmark: Past, present and future," *Concurrency and Computation: Practice and Experience*, vol. 15, 2003.

[39] W. Ecker, V. Esen, T. Steininger, and M. Zambaldi, "Memory models for the formal verification of assembler code using bounded model checking," in *Seventh IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, 2004. Proceedings*, 2004.

[40] W. Ecker, M. Velten, L. Zafari, and A. Goyal, "Metasynthesis for designing automotive SoCs," in *Proceedings of 51st ACM/EDAC/IEEE Design Automation Conference*, 2014.

[41] E. El Mandouh and A. G. Wassal, "Automatic generation of hardware design properties from simulation traces," in *Proceedings of IEEE International Symposium Circuits and System*, 2012.

[42] E. A. Emerson, "Temporal and modal logic," in *Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics*, 1990.

[43] E. A. Emerson and R. J. Trefler, "Parametric quantitative temporal reasoning," in *14th Symposium on Logic in Computer Science*, pp. 336–343, 1999.

[44] M. R. Fadiheh, J. Müller, R. Brinkmann, S. Mitra, D. Stoffel, and W. Kunz, "A formal approach for detecting vulnerabilities to transient execution attacks in out-of-order processors," in *2020 57th ACM/IEEE Design Automation Conference (DAC)*, 2020.

[45] M. R. Fadiheh, D. Stoffel, C. Barrett, S. Mitra, and W. Kunz, "Processor hardware security vulnerabilities and their detection by unique program execution checking," in *2019 Design, Automation and Test in Europe Conference and Exhibition (DATE)*, 2019.

[46] M. R. Fadiheh, J. Urdahl, S. Nuthakki, S. Mitra, C. Barrett, D. Stoffel, and W. Kunz, *Symbolic quick error detection using symbolic initial state for pre-silicon verification*, 2018.

[47] M. R. Fadiheh, A. Wezel, J. Mueller, J. Bormann, S. Ray, J. M. Fung, S. Mitra, D. Stoffel, and W. Kunz, "An exhaustive approach to detecting transient execution side channels in RTL designs of processors," *IEEE Transactions on Computers*, vol. 72, no. 1, pp. 222–235, 2023.

[48] H. D. Foster, "Trends in functional verification: A 2014 industry study," in *Proceedings of 52nd Design Automation Conference*, 2015.

[49] O. Friedler *et al.*, "Effective post-silicon failure localization using dynamic program slicing," in *Proceedings IEEE/ACM Design Automation Test in Europe*, 2014.

[50] K. Ganesan, F. Lonsing, S. S. Nuthakki, E. Singh, M. R. Fadiheh, W. Kunz, D. Stoffel, C. Barrett, and S. Mitra, "Effective pre-silicon verification of processor cores by breaking the bounds of symbolic quick error detection," *CoRR*, vol. abs/2106.10392, 2021.

[51] M. Giordano, K. Prabhu, K. Koul, R. M. Radway, A. Gural, R. Doshi, Z. F. Khan, W. Kustin, T. Liu, G. B. Lopes, V. Turbiner, W.-S. Khwa, Y.-D. Chih, M.-F. Chang, G. Lallement, B. Murmann, S. Mitra, and P. Raina, "CHIMERA: A 0.92 TOPS, 2.2 TOPS/W edge AI accelerator with 2 MByte on-chip foundry resistive RAM for efficient training and inference," in *VLSI*, 2021.

[52] S. Hangal, S. Narayanan, N. Chandra, and S. Chakravorty, "IODINE: A tool to automatically infer dynamic invariants," in *Proceedings IEEE/ACM Design Automation Conference*, 2005.

[53] Y. Hara, H. Tomiyama, S. Honda, H. Takada, and K. Ishii, "Chstone: A benchmark program suite for practical c-based high-level synthesis," in *Procedings of ISCAS*, 2008.

[54] Y. Hara-Azumi, H. Tomiyama, S. Honda, and H. Takada, "Proposal and quantitative analysis of the CHStone benchmark program suite for practical C-based high-level synthesis," *Journal of Information Processing*, vol. 17, pp. 242–257, 2009.

[55] J. L. Hennessey and D. A. Patterson, "Memory hierarchy design," in *Computer Architecture: A Quantitative Approach*, Morgan Kauffman, 2012.

[56] T. Hong, Y. Li, S. Park, D. Mui, D. Lin, Z. A. Kaleq, N. Hakim, H. Naemi, D. S. Gardner, and S. Mitra, "QED: Quick error detection tests for effective post-silicon validation," in *2010 IEEE International Test Conference*, 2010.

[57] W. Hu, L. Wu, Y. Tai, J. Tan, and J. Zhang, "A unified formal model for proving security and reliability properties," in *IEEE 29th Asian Test Symposium (ATS)*, 2020.

[58] B. Y. Huang, S. Ray, A. Gupta, J. M. Fung, and S. Malik, "Formal security verification of concurrent firmware in socs using instruction-level abstraction for hardware," in *IEEE/ACM Design Automation Conference*, 2018.

[59] IEEE-UVM, "IEEE standard for universal verification methodology language reference manual," in *IEEE Std 1800.2-2020 (Revision of IEEE Std 1800.2-2017)*, 2020, pp. 1–458.

[60] S. I. Inc., *The sparc architecture manual, version 8*, 1994.

[61] ISO, "ISO," in *26262-1:2018 road vehicles functional safety*, Geneva, Switzerland: International Organization for Standardization, 2021.

[62] T. Jauch, A. Wezel, M. R. Fadiheh, P. Schmitz, S. Ray, J. M. Fung, C. W. Fletcher, D. Stoffel, and W. Kunz, "Secure-by-construction design methodology for CPUs: Implementing secure speculation on the RTL," in *IEEE/ACM International Conference on Computer Aided Design (ICCAD)*, 2023.

[63] D. Josephson, "The good, the bad, and the ugly of silicon debug," in *Proceedings IEEE/ACM Design Automation Conference*, 2006.

[64] S. Katz, O. Grumberg, and D. Geist, "Have I written enough properties?—A method of comparison between specification and implementation," in *Correct Hardware Design and Verification Methods*, Berlin, Heidelberg: Springer, 1999, pp. 280–297.

[65] R. Keller, "Formal verification of parallel programs," *Communications of ACM*, 1976.

[66] J. Keshava, N. Hakim, and C. Prudvi, "Post-silicon validation challenges: How EDA and academia can help," in *Proceedings IEEE/ACM Design Automation Conference*, 2010.

[67] H. F. Ko and N. Nicolici, "Automated trace signals identification and state restoration for improving observability in post-silicon validation," in *Proceedings of IEEE/ACM Design Automation Test in Europe Conference*, 2008.

[68] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Y., "Spectre attacks: Exploiting speculative execution," *arXiv preprint arXiv:1801.01203*, 2018.

[69] W. Li, F. Alessandro, and S. A. Seshia, "Scalable specification mining for verification and diagnosis," in *Proceedings IEEE/ACM Design Automation Conference*, 2010.

[70] X. Li, V. Kashyap, J. K. Oberg, M. Tiwari, V. R. Rajarathinam, R. Kastner, T. Sherwood, B. Hardekopf, and F. T. Chong, "Sapper: A language for hardware-level security policy enforcement," in *ACM SIGARCH Computer Architecture News*, 2014.

[71] X. Li, M. Tiwari, J. K. Oberg, V. Kashyap, F. T. Chong, T. Sherwood, and B. Hardekopf, "Caisson: A hardware description language for secure information flow," *ACM SIGPLAN Notices*, vol. 46, pp. 109–120, 2011.

[72] D. Lin, S. Eswaran, S. Kumar, E. Rentschler, and S. Mitra, "Quick error detection tests with fast runtimes for effective post-silicon validation and debug," 2015.

[73] D. Lin, T. Hong, F. Fallah, N. Hakim, and S. Mitra, "Quick detection of difficult bugs for effective post-silicon validation," in *DAC Design Automation Conference 2012*, 2012.

[74] D. Lin, T. Hong, Y. Li, S. E, S. Kumar, F. Fallah, N. Hakim, D. Gardner, and S. Mitra, "Effective post-silicon validation of system-on-chips using quick error detection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 33, no. 10, pp. 1573–1590, 2014.

[75] M. Lipp, S. D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, and Y. Yarom, "Meltdown," *arXiv preprint arXiv: 1801.01207*,

[76] X. Liu and Q. Xiu, "Trace signal selection for visibility enhancement in post-silicon validation," in *Proceedings IEEE/ACM Design Automation Test in Europe Conference*, pp. 1338–1343, 2009.

[77] F. Lonsing, K. Ganesan, M. Mann, S. S. Nuthakki, E. Singh, M. Srouji, Y. Yang, S. Mitra, and C. Barrett, "Unlocking the power of formal hardware verification with CoSA and symbolic QED," in *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2019.

[78] F. Lonsing, S. Mitra, and C. Barrett, "A theoretical framework for symbolic quick error detection," *CoRR*, vol. abs/2006.05449, 2020.

[79] D. J. Lu, "Watchdog processors and structural integrity checking," *IEEE Transactions on Computers*, vol. 31, no. 7, pp. 681–685, 1982.

[80] M. M. K. Martin, D. J. Sorin, B. Beckmann, M. Marty, M. Xiu, A. R. Alameldeen, K. E. Moore, M. D. Hill, and D. A. Wood, "Multifacet's general execution-drive multiprocessor simulator (GEMS) toolset," *ACM SIGARCH Computer Architecture News*, vol. 33, no. 4, pp. 92–99, 2005.

[81] S. Mitra, S. A. Seshia, and N. Nicolici, "Post-silicon validation opportunities, challenges and recent advances," in *Proceedings of IEEE/ACM Design Automation Conference*, 2010.

[82] M. D. Nguyen, M. Thalmaier, M. Wedler, J. Bormann, D. Stoffel, and K. Kunz, "Unbounded protocol compliance verification using interval property checking with invariants," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp. 2068–2082, 2008.

[83] NVIDIA, *NVIDIA deep learning accelerator*, 2021. URL: http://nvdla.org/primer.html.

[84] J. Oberg, S. Meiklejohn, T. Sherwood, and R. Kastner, "Leveraging gate-level properties to identify hardware timing channels," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 33, no. 9, pp. 1288–1301, 2014.

[85] N. Oh, S. Mitra, and E. J. McCluskey, "Ed4I: Error detection by diverse data and duplicated instructions," *IEEE Transaction on Reliability*, vol. 51, no. 2, pp. 180–199, 2002.

[86] N. Oh, P. P. Shirvani, and E. J. McCluskey, "Control-flow checking by software signatures," *IEEE Transactions on Reliability*, vol. 51, no. 1, pp. 111–122, 2002.

[87] Onespin solutions, *Onespin 360 DV*. URL: https://www.onespin.com/.

[88] S.-B. Park, T. Hon, and S. Mitra, "Post-silicon bug localization in processors using instruction footprint recording and analysis (IFRA)," 2009.

[89] S. Patel and W.-M. W. Hwu, "Accelerator architectures," pp. 4–12, July 2008.

[90] P. Patra, "On the cusp of a validation wall," *IEEE Design & Test of Computers*, vol. 24, no. 2, pp. 193–196, 2007.

[91] F. M. de Paula *et al.*, "TAB-BackSpace: Unlimited-length trace buffers with zero additional on-chip overhead," in *Proceedings IEEE/ACM Design Automation Conference*, 2011.

[92] L. Piccolboni, G. Di Guglielmo, and L. P. Carloni, "KAIROS: Incremental verification in high-level synthesis through latency-insensitive design," in *Proceedings of FMCAD*, 2019.

[93] R. Raina and R. Molyneaux, "Random self-test method applications on powerPCTM microprocessor cache," in *Proceedings of ACM/IEEE Great Lakes Symposium on VLSI*, 1983.

[94] K. Reick, "Post-silicon debug—DAC workshop on post-silicon debug: Technologies, methodologies, and best-practices," in *IEEE/ACM Design Automation Conference*, 2012.

[95] A. Reid, R. Chen, A. Deligiannis, D. Gilday, D. Hoyes, W. Keen, A. Pathirane, O. Shepherd, P. Vrabel, and A. Zaidi, "End-to-end verification of ARM® processors with ISA-formal," in *28th International Conference on Computer Aided Verification*, 2016.

[96] RIDECORE, *Github*, 2017. URL: https://github.com/ridecore/ridecore.

[97] RIDECORE-BUGS, *Github*, 2017. URL: https://tinyurl.com/y8otzyxb.

[98] Rocket chip generator. Github. URL: https://github.com/chipsalliance/rocket-chip.

[99] S. K. Roy and S. Ramesh, "Functional verification of system on chips—Practices, issues and challenges," in *Proceedings of ASP-DAC/VLSI Design 2002. 7th Asia and South Pacific Design Automation Conference and 15th International Conference on VLSI Design*, 2002.

[100] J. Ruf, D. W. Hoffmann, T. Kropf, and W. Rosenstiel, "Simulation-guided property checking based on multi-valued ar-automata," in *Proceeding of the International Conference on Design, Automation and Test in Europe (DATE)*, 2001.

[101] G. Schelle, J. Collins, E. Schuchman, P. Wang, X. Zou, G. Chinya, R. Plate, T. Mattner, F. Olbrich, P. Hammarlund, R. Singhal, J. Brayton, S. Steibl, and H. Wang, "Intel nehalem processor core made FPGA synthesizable," in *Proceedings ACM/SIGDA International Symposium Field Programmable Gate Arrays*, 2010.

[102] Semiconductor Engineering, "Challenges in using ai in verification," 2020. URL: https://semiengineering.com/challenges-in-using-ai-in-verification/.

[103] J. P. Shen, "On-line monitoring using signatured instruction streams," in *Proceedings of IEEE International Test Conference, Oct. 1983*, pp. 275–282, 1983.

[104] E. Singh, K. Devarajegowda, S. Simon, R. Schnieder, K. Ganesan, M. R. Fadiheh, D. Stoffel, W. Kunz, C. Barrett, W. Ecker, and S. Mitra, "Symbolic QED pre-silicon verification for automotive microcontroller cores: Industrial case study," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Florence, Italy, 2019.

[105] E. Singh, D. Lin, B. Barrett, and S. Mitra, "Logic bug detection and localization using symbolic quick error detection," *Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2018.

[106] E. Singh, F. Lonsing, S. Chattopadhyay, M. Strange, P. Wei, X. Zhang, Y. Zhou, D. Chen, J. R. P. Cong, Z. Zhang, C. Barrett, and S. Mitra, "A-QED verification of hardware accelerators," in *57th ACM/IEEE Design Automation Conference (DAC)*, San Fransisco, CA, USA, 2020.

[107] M. J. Srouji, "(master thesis) AUTO-SQED: Automated symbolic quick error detection (SQED) for formal verification," Department of Computer Science, Stanford University, US, 2020.

[108] D. Stoffel, M. Wedler, P. Warkentin, and W. Kunz, "Structural FSM traversal," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 23, no. 5, pp. 598–619, 2004.

[109] P. Subramanyan and D. Arora, "Formal verification of taint-propagation security properties in a commercial SoC design," in *Design, Automation and Test in Europe Conference (DATE)*, 2014.

[110] T. Tambe, E. Yang, G. G. Ko, Y. Chai, C. Hooper, M. Donato, P. N. Whatmough, A. M. Rush, D. Brooks, and G.-Y. Wei, "A 25 mm^2 for IoT devices with 18 ms noise-robust speech-to-text latency via bayesian speech denoising and attention-based sequence-to-sequence DNN speech recognition in 16 nm FinFET," in *ISSCC*, 2021.

[111] A. Tang, S. Sethumadhavan, and S. Stolfo, "CLKSCREW: Exposing the perils of security-oblivious," in *26th fUSENIXg Security Symposium (USENIX Security 17)*, 2017.

[112] S. Vasudevan, D. Sheridan, S. Patel, D. Tcheng, B. Tuohy, and D. Johnson, "GoldMine: Automatic assertion generation using data mining and static analysis," in *Proceedings IEEE/ACM Design Automation Test in Europe*, 2010.

[113] B. Vermeulen and S. K. Goel, "Design for debug: Catching design errors in digital chips," *IEEE Design Test Computers*, vol. 19, no. 03, pp. 37–45, May 2002.

[114] Vscale, *Github*, 2017. URL: https://github.com/ucb-bar/vscale.

[115] I. Wagner and V. Bertacco, "Reversi: Post-silicon validation system for modern microprocessors," in *Proceedings of IEEE International Conference on Computer Design*, 2008.

[116] A. Waterman and K. Asanovic, *The RISC-V instruction set manual, volume I: User-level ISA*, 2017.

[117] P. N. Whatmough, S. K. Lee, M. Donato, H. Hsueh, S. L. Xi, U. Gupta, L. Pentecost, G. G. Ko, D. M. Brooks, and G. W., "A 16 nm 25 mm^2 SoC with a 54.5x flexibility-efficiency range from dual-core arm cortex-A53 to eFPGA and cache-coherent accelerators," in *VLSI*, 2019.

[118] B. Wile, J. Goss, and W. Roesner, *Comprehensive Functional Verification*. Elsevier, 2005.

[119] S. C. Woo, M. Ohara, E. Torrie, J. P. Singh, and A. Gupta, "The SPLASH-2 programs: Characterization and methodological considerations," in *The SPLASH-2 Programs: Characterization and Methodological Considerations*, 1995, pp. 24–36.

[120] Y. Yarom and K. Falkner, "FLUSH + RELOAD: A high resolution, low noise, L3 cache side-channel attack," in *23rd USENIX Security Symposium USENIX Security 14*, 2014.

[121] S. Yerramilli, "Addressing post-silicon validation challenges: Leverage validation & test synergy," in *IEEE International Test Comference*, 2006.

[122] D. Zhang, Y. Wang, G. E. Suh, and A. C. Myers, "A hardware design language for timing-sensitive information-flow security," *ACM SIGPLAN Notices*, vol. 50, no. 4, pp. 503–516, 2015.

[123] X. Zhang, H. Lu, C. Hao, J. Li, B. Cheng, Y. Li, K. Rupnow, and J. Xiong, "SkyNet: A hardware-efficient method for object detection and tracking on embedded systems," in *Proceedings of Machine Learning and Systems*, 2020.

[124] Y. Zhou, U. Gupta, S. Dai, R. Zhao, N. Srivastava, H. Jin, J. Featherston, Y.-H. Lai, G. Liu, G. A. Velasquez, W. Wang, and Z. Zhang, *Rosetta: A Realistic High-Level Synthesis Benchmark Suite for Software Programmable FPGAs*. Monterey, CA, USA, 2018.

[125] C. S. Zhu, G. Weissenbacher, and S. Malik, "Post-silicon fault localisation using maximum satisfiability and backbones," in *Proceedings IEEE/ACM Formal Methods Computer-Aided Design*, 2011.