Guest Editorial

Kanad Basu¹ · Mingsong Chen² · Rubin Parekhji³

Published online: 15 November 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

With increase in circuit complexity, reduction in feature size and time to market, as well as distributed chip development environment, verification, testing and security have manifested themselves as serious challenges to Integrated Circuit (IC) design. New challenges are emerging in each of these domains, demanding novel solutions. In this special issue of *JETTA*, we have selected ten papers from the proceedings of the 32nd International Conference on VLSI Design and 18th International Conference on Embedded Systems, which took place in New Delhi, India during January 5–9, 2019. These papers address important challenges in IC verification, test and security and propose innovative solutions. Each paper underwent a set of peer reviews before inclusion in this special issue. Here, we introduce the papers appearing here.

1 Hardware Security Track

The first paper improves FPGA-based Physical Unclonable Function (PUF) by developing a novel randomized placement algorithm. PUFs find extensive use in both hardware and software security for performing cryptography protocols like generating keys, device authentication, etc. A big challenge in existing PUFs is reliability. The authors design a reliable, low-area overhead FPGA-based PUF for use in various cryptographic operations.

The second paper deals with power analysis attacks. Power analysis attacks are a form of side channel attacks used to leak secret keys from cryptographic hardware like AES. In this paper, the authors design a CAD-based methodology to perform pre-

silicon power analysis attack on a gate level netlist description of cryptographic hardware. The authors validate the model with PRESENT like cryptographic methods, where the authors show that they need few power traces to recover keys with high correlation. The paper is essentially an attack paper, which postulates the vulnerabilities in an existing cryptographic hardware design.

While the second paper illustrates power side channel attacks, the third paper provides defense against them. Existing defenses against power side channel attacks incur high area and power overheads, which are not affordable for low power IoT edge devices. The authors propose a novel Finite State Machine (FSM) encoding-based method that prevents power analysis attacks and reduces area overhead. The proposed methodology shows a reduction in power footprints by 40%.

The fourth and the last paper in this section designs a classical cryptanalysis attack against logic locking. Logic locking is an important IC protection mechanism against reverse engineering by malicious third-party entities in the design phase, like untrusted foundries. A design house “locks” the circuit with known keys, which are unknown to a reverse engineer and hence, the latter infers only an incomplete view of the circuit. In this paper, the authors develop a formal attack based on linear and differential approximations on logic locked circuits.

2 Verification Track

The first of two paper in this track tries to address the problem of determination of equivalence of two n -input majority terms for energy efficient circuit technologies like spintronics and domain wall magnets. Since majority gates implement more complex Boolean functions than traditional AND/OR gates, the equivalence problem is becoming a major bottleneck in the logic synthesis flow. Based on prime implicants, this paper provides a solution. Meanwhile, an efficient algorithm is presented that can compact an n -input majority term to an equivalent n -input majority term that has the smallest number of inputs. Experimental results show the efficiency of the proposed algorithms.

Due to factors such as lack of golden responses, highly restricted observability and irreproducible nature of bugs, error localization from post-silicon debug data is a highly

✉ Rubin Parekhji
parekhji@ti.com

Kanad Basu
kanad.basu@utdallas.edu

Mingsong Chen
mschen@sei.ecnu.edu.cn

¹ University of Texas at Dallas, Richardson, TX, USA

² East China Normal University, Shanghai, China

³ Texas Instruments, Bangalore, India

challenging problem. To deal with this problem, the second paper proposes a signal tracing methodology for SAT-based error localization in the post-silicon environment. A grouping-based methodology is introduced for signal selection and it is used with different observability enhancement schemes to obtain a smaller execution trace. Experimental results on a variety of benchmark circuits show that the proposed method succeeds in the post-silicon environment for two kinds of error scenarios.

3 Test Track

There are four papers in this track, with three from VLSI Design 2019 and one from VLSI Design 2018, submitted to *JETTA* in 2019.

The first paper, “RSBST: An Accelerated Automated Software-based Self-test Synthesis for Processor Testing,” describes new methods to synthesize efficient software based tests for high coverage of processor modules using code evolution techniques. This work establishes correlation between behavioral models and gate level netlists with respect to synthesis time, memory requirement and coverage benefits for MIPS and Leon3 processors.

The second paper, “A Binary Decision Diagram Approach to On-line Testing of Asynchronous Circuits with Dynamic and Static C-Elements,” proposes a new method for on-line test of asynchronous circuits using fault detection transitions to incorporate selective and partial replication. The method is circuit and function independent, and can work for larger circuits with signal transition graphs (STGs) and BDDs.

The third paper, “An Integrated Framework for Application Independent Testing of FPGA Interconnect,” presents a configuration independent method to test FPGAs. The tests cover all enumerated paths and hence verify all interconnect resources inside the FPGA. Opens and shorts are considered and SAT methods help derive constraints for different configurations. Xilinx Virtex FPGAs provide results.

Fourth and the last paper, “Identification of Random/Clustered TSV Defects in 3D IC during Pre-bond Testing,” describes two heuristic methods for testing under the assumption of unconstrained distribution of defects. Results show reduction in test times across multiple test sessions covering different partitions in the die. The paper examines the impact of variable defect distributions and fault formulations on test time.

We hope that the readers will find this special issue a valuable compilation for handy reference. In closing, we would like to thank all the authors and reviewers for their contributions, and the Editor-in-Chief and the Springer *JETTA* publication team for supporting this special issue. We welcome feedback and suggestions from the readers and others who would like to contribute to this journal.

Kanad Basu is an Assistant Professor at the University of Texas at Dallas. Prior to this, he was an Assistant Research Professor at New York University. Basu received his MS and PhD degrees from the University of Florida. After PhD, he spent several years in semiconductor industries like IBM and Synopsys. He is the author of several book chapters, peer reviewed journal and conference articles and two US patents. He has received several accolades for his works in both academia and industry, including the “Best Paper Award” at the International Conference on VLSI Design, 2011. Basu’s research interests include hardware security, verification and testing.

Mingsong Chen is a full Professor in the School of Software Engineering Institute at the East China Normal University. He received his BS and MEng degrees from Nanjing University in 2003 and 2006, respectively, and PhD from the University of Florida in 2010, all in Computer Science. His research interests include formal verification, design automation of smart cyber physical systems, and IoT. Chen has published 1 book, 20+ patents/copyrights, and more than 70 research articles in premier international journals and conferences. He currently serves as an Associate Editor of IET Computer and Digital Techniques and the Journal of Circuits, Systems and Computers. He serves on the technical program committees of several leading international conferences including DAC, DATE, and RTSS. He is a Senior Member of IEEE, a Senior Member of CCF, and a member of ACM.

Rubin Parekhji has been with Texas Instruments, Bangalore, since 1996, where he has led and mentored DFT teams on various design and test technology projects across multiple product groups, and is a Distinguished Member of Technical Staff. More recently, he has been a member of the Analog Engineering and Kilby Lab. teams at TI, working on low cost test methods and test entitlement targets. He has published regularly and delivered tutorials at leading conferences, has mentored a large number of students, has been a visiting faculty member, and has several issued patents. He has a PhD from Indian Institute of Technology, Bombay, India and he currently serves on the Editorial Board of *JETTA*.