Journal of Electronic Testing (2022) 38:231
https://doi.org/10.1007/s10836-022-06015-w

Editorial

Vishwani D. Agrawal[1]

Received: 29 June 2022 / Accepted: 29 June 2022 / Published online: 20 July 2022

This issue contains seven articles. Three focus on hardware security, and one each on analog and mixed-signal test, software test and verification, soft errors, and built-in self-test.

The first among three hardware security papers provides a novel physical unclonable function (PUF). A PUF may have an application like authentication code or security key generation. Wang, Singh and Guin at Auburn University, Auburn, Alabama, USA, observe that some cells of a static random-access memory (SRAM) have reliable device-specific power up states. Their method of power ramping decisively identifies the definite-1 and definite-0 cells of a SRAM device.

Second paper addresses the security of configuration data of a field programmable gate array (FPGA), stored in SRAM. Zahid, from National University of Computer and Emerging Sciences, Islamabad, Pakistan, uses reverse engineering to detect the presence of any hardware Trojan (HT) that could have added path delays, malicious data outputs, or power fluctuations in the original design.

Third paper revisits PUF, examining several types of attacks and countermeasures, termed as self-PUF, cross-PUF, and DRILL-PUF. Authors are Kroeger and Karimi from University of Maryland Baltimore County, Baltimore, Maryland, USA, and Cheng, Danger and Guilley from Institut Polytechnique de Paris, France.

The fourth paper minimizes the number of test parameters for an analog circuit with little or no compromises on the defective parts per million (DPPM) and yield loss. This is achieved by a machine learning system, XGBoost, where decision tree traversal would rely on an entropy-based information criterion. Authors are Xiao, Zeng, Wu, Liu, and Li from University of Electronic Science and Technology of China, Chengdu, China, and Hu from Guilin University of Electronic Technology, Guilin, China.

Fifth paper discusses mutation testing of software. An artificial bee colony (ABC) algorithm, which mimics the natural behavior of bees tuned to optimize honey collection, identifies fault-prone paths in the control flow graph (CFG) of the software code. Once mutations are applied to instructions and data on those paths, testing shows higher efficiency when compared to other known mutation strategies. Contributors of this work are B. Arasteh and K. Arasteh from Istinye University, Istanbul, Turkey, Imanzadeh from Islamic Azad University, Tabriz, Iran, Gharehchopogh from Islamic Azad University, Urmia, Iran, and Zarei from Islamic Azad University, Shabestar, Iran.

Sixth paper focuses on soft errors resulting in silent data corruption (SDC). Because SDC does not produce immediately observable result, it is difficult to detect. For assessing reliability improvements due to radiation hardening, etc., identification of SDC-prone instructions of the system is required. This involves large-scale fault injection experiments. The paper defines an inductive learning framework called graph attention network, which can identify the SDC-prone instructions without fault injection. This contribution comes from Ma, Duan and Tang of Chang’an University, Xi’an, Shaanxi, China.

Seventh paper presents a built-in self-test (BIST) architecture for an asynchronous circuit. This work applies to circuits implemented with null convention logic (NCL). A simple NCL may use a dual-rail system, e.g., the dual state of a signal 1X could be interpreted as logic 1, 0X as logic 0, 00 as null, and 11 as illegal. Such a system is realizable with threshold logic components. A more advanced multi threshold null convention logic (MTNCL) is used in this work. Authors are Sparkman and Di from University of Arkansas, Fayetteville, AR, USA, and Smith from Texas A&M University-Kingsville, Kingsville, TX, USA. They enhance an existing BIST methodology of MTNCL circuits to reduce the test time by parallelization.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

✉ Vishwani D. Agrawal
agrawvd@auburn.edu

[1] Auburn University, Auburn, AL 36849, USA