From the EIC

Robust Machine Learning

Machine learning techniques have become pervasive through many technical fields but an obstacle for employment is often the criterion of robustness. While machine learning can be a great means to improve upon the quality of traditional optimization techniques in uncritical scenarios (e.g., a customized online search result that proposes to a consumer a more or less well-fitting new product advertisement), it may be prohibitive to employ when directly embedded in critical decision flows (e.g., a self-driving car that needs to decide whether to engage an emergency brake). In the latter case, robustness is one mandatory constraint. Robustness can have many facets; some of them are covered by this timely special issue that represents the state of the art from a design and test point of view. Many thanks to the Guest Editors Theocharis Theocharides, Muhammad Shafique, Jungwook Choi, and Onur Mutlu for editing this special issue that includes two keynote articles, a survey on "Robust Machine Learning Systems: Challenges, Current Trends, Perspectives, and the Road Ahead," and six technical articles.

The General Interest section has one article by Gnad et al. titled "Remote Electrical-Level Security Threats to Multitenant Field-Programmable Gate Arrays," which shows that physical attacks can also be performed from within the FPGA itself since a high degree of freedom to design with FPGAs potentially jeopardizes security. The authors, therefore, suggest that, in the future, multitenant FPGA devices should have changes on the hardware side to enable isolation at the electrical level.

The 38th ACM/IEEE International Conference on Computer-Aided Design (ICCAD 2019) took place in Westminster (Denver area), CO, USA, on November 4–7, 2019. David Z. Pan, the General Chair, provides us a report on this major conference in CAD. As always, many thanks to Massimo Poncino, our Reports Editor, for acquiring this report.

Thanks to Theo Theocharides for the TTTC Newsletter.

Last but not least, many thanks to Scott Davidson for the Last Byte titled "Are You Sure You Love That Store?"

Enjoy reading! ■

Jörg Henkel
Editor-in-Chief
IEEE Design&Test

Digital Object Identifier 10.1109/MDAT.2020.2984228
Date of current version: 20 April 2020.