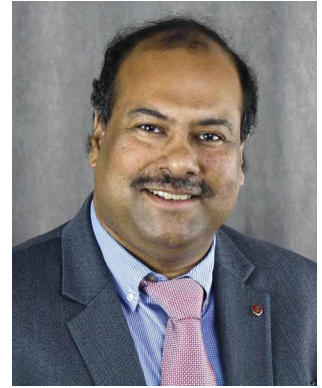


From the EIC

Special Issue on the 2021 Workshop on Top Picks in Hardware and Embedded Security



■ **THE ARTICLES IN** this issue are divided into three groups: 1) the first group are articles in the Special Issue on the 2021 Workshop on Top Picks in Hardware and Embedded Security; 2) the second group comprises general interest articles; and 3) additionally, we have two conference reports.

The highlight of this issue is the Special Issue on the 2021 Workshop on Top Picks in Hardware and Embedded Security. The Workshop on Top Picks on Hardware and Embedded System Security (Top Picks) was founded in 2018 with the goal of promoting the research that has made the greatest intellectual contributions. On 4 November 2021, 11 peer-reviewed articles were selected for presentation in the 4th Top Picks workshop (held virtually due to COVID-19). These presentations covered a broad range of problems in hardware and embedded system security. Each presenter reviewed the main contributions of their original article; summarized their work's impacts on academia, industry, and government; and discussed the future research directions.

This special issue comprises six invited articles from Top Picks presenters. The first two articles are on IC/IP protection. The third article addresses the protection of deep-learning models by leveraging hardware device-specific model finger-printing and a trusted execution environment. The fourth article reports the latest progress on the imbalance problem in evaluating the performance of machine-learning-based side-channel analysis. The next article

reveals timing-based side-channel and covert-channel attacks from the translation look-aside buffers (TLBs) and discusses how to design secure TLBs. The last article of this special issue describes a new specter-class attack that exploits the return stack buffer and does not rely on the branch predictor unit. We thank the Guest Editor Gang Qu for making this special issue possible.

The general interest articles are titled as follows: 1) "Cell-Aware Test on Various Circuits in an Advanced 3-nm Technology"; 2) "VioNet: A Hierarchical Detailed Routing Wire-Short Violation Predictor Based on a Convolutional Neural Network"; and 3) "Hard-Sign: A Hardware Watermarking Scheme Using Dated Handwritten Signature."

This issue also contains two conference reports: one on the 2023 Embedded Systems Week (ESWEEK) and the second one on the 42nd Edition of the International Conference on Computer-Aided Design (ICCAD 2023).

As always, many thanks to Scott Davidson for The Last Byte article "Predictions." I hope you enjoy reading this issue of *IEEE Design&Test*. ■

Partha Pratim Pande, *Editor-in-Chief*
Washington State University
Pullman, WA 99164-2752 USA

Digital Object Identifier 10.1109/MDAT.2024.3358221

Date of current version: 21 February 2024.