Guest Editorial: IEEE Transactions on Computer, Special Issue on Hardware Security

Simha Sethumadhavan and Srini Devadas

HARDWARE security is now widely recognized as an essential aspect of computer security, computer architecture, and VLSI design and testing due to developments over the last fifteen years. We have come a long way from questioning the validity of hardware threats to doubting the efficacy of attacks to accepting that attacks exist but arguing that solutions would be expensive to implement to developing solutions deployed in billions of devices. The set of papers in this special issue showcases the next stage of development of hardware security as a discipline.

The special issue includes 9 papers on various facets of hardware security, from foundational studies to industrial perspectives.

In the paper titled "High-Speed Hardware Architectures and FPGA Benchmarking of CRYSTALS-Kyber, NTRU, and Saber," the authors evaluate Post-Quantum Cryptography (PQC) finalists from the NIST competition and measure their performance with new architectures and an FPGA implementation.

"Revisiting Higher-Order Masked Comparison for Lattice-Based Cryptography: Algorithms and Bit-sliced Implementations" shows how one of the most expensive operations in side-channel secure lattice-based post-quantum cryptography – Masked comparison – can be optimized using novel algorithms and implementations.

The problem of hardware trojans is a core problem in hardware security that needs to be addressed to achieve any level of assurance. In the paper titled "Robust Hardware-Trojan Detection Based on Adversarial Training," the authors describe a machine learning-based method for detecting hardware trojans resilient to adversarial perturbation.

In "A Provably Secure Strong PUF based on LWE: Construction and Implementation," authors construct a "Lattice PUF," a PUF based on the hardness of the learning-with-errors (LWE) problem defined on integer lattices, and demonstrate provable security against ML attacks conducted by both classical and quantum computers.

Understanding complex systems and risks in their construction is a crucial aspect of hardware security. In "Reverse-engineering and Exploiting the Frontend Bus of Intel Processor," the authors perform a detailed characterization of the front-end bus in Intel processors to uncover policies determining how instructions flow from the cache through the processor front end to arrive at the back-end and use this to detect covert channels.

In "Preventing Coherence State Side Channel Leaks Using TimeCache," authors present a cache design that prevents side channels that result from the reuse of shared memory and show how the invention could also be resilient against attacks that exploit coherence states.

In the paper titled "A Framework for Design, Verification, and Management of SoC Access Control Systems," the authors describe a design and verification framework for on-chip access using a property-driven security verification methodology.

In "Generating Robust DNN with Resistance to Bit-Flip based Adversarial Weight Attack," authors show how DNNs can be protected against Rowhammer attack by obfuscating the bit order of model data to hide vulnerable bits with less vulnerable ones.

"(Adversarial) Electromagnetic Disturbance in the Industry" describes new capabilities that have emerged in the industry to cryptanalyze chips' resilience against non-invasive electromagnetic fault injection attacks.

We welcome comments and questions on this special issue. Thanks to all the reviewers for their service, the Editor in Chief, Dr. Louri, and Corresponding editors, Dr. Karanth and Dr. Abu-Ghazaleh, for making this special issue possible. Finally, thanks to all the authors who submitted their work for this special issue.

SIMHA SETHUMADHAVAN
SRINI DEVADAS

Digital Object Identifier no. 10.1109/TC.2022.3233145