Guest Editorial
Special Section on Hardware Security and Trust

Creating backdoors in integrated circuits (ICs), stealing hardware intellectual property, counterfeiting electronic components, reverse engineering ICs, and injecting malware in ICs are no longer nation state acts requiring specialized, expensive, and unlimited resources. Democratization of IC design has created numerous opportunities for rogues throughout the IC supply chain to inflict these attacks with aplomb and for a variety of reasons: personal gain, economic harm, economic gain, bringing disrepute, and sheer fun among others.

Traditionally, authenticity, integrity, and confidentiality of information stored and processed in ICs, hardware platforms and large-scale systems were being protected by using security primitives and protocols in software with the underlying hardware assumed to be secure and trustworthy. However, this assumption is no longer true; an increasing number of attacks are being reported on the hardware root of trust. There is a growing concern involving the security and trustworthiness of the hardware underlying the information systems on which modern society is reliant for mission- and safety-critical functions. To see why, let us consider a few aspects of IC design and test, and the security vulnerabilities that they engender.

First, IC and system designs have been traditionally optimized for performance, power, and reliability. Regardless of how secure an algorithm is, its physical implementation on hardware is prone to leak information through side channels that have been left unprotected, and attacks based on various side channels have emerged as major concerns for security-enabled applications. Power optimizations create power side channels and performance optimization yields timing side channels. So, reducing the side-channel leakages of sensitive circuits should be amongst the main goals of IC designers side-by-side power, performance, and reliability.

Second, modern ICs incorporate a large variety and amount of instrumentation/infrastructure to support post-silicon validation and debug, volume test and diagnosis, as well as in-field system monitoring and maintenance. This infrastructure, while enhancing access into deeply embedded logic, can be repurposed and misused to leak sensitive information from an IC. Design-for-test and design-for-debug efforts must, therefore, beware of the potential security holes they may create, and design-for-secure-test and design-for-secure-debug techniques and infrastructures should be developed to replace the traditional ones.

Another security vulnerability is an artifact of the new design and manufacturing flow that has been practiced for the last decade or two. In this new paradigm, mandated by the increased design complexity, stringent time-to-market deadlines, and unaffordable fabrication costs, complex system-on-chips (SoCs) include design blocks, aka cores, from third-party vendors, and fabrication is typically outsourced to third-party IC foundries. More and more design companies go fabless for obvious financial reasons at the expense of relinquished control over the design and manufacturing flow, which now spans companies, countries, and even continents. Such a distributed flow leads to security and trust vulnerabilities inevitably. Designers have been exploring on-chip defenses against a variety of threats ranging from hardware Trojans to reverse engineering and intellectual property (IP) piracy, resulting in recent design-for-trust efforts in various forms such as logic encryption, split manufacturing, and IC camouflaging.

Among the aforementioned security threats, one of the more prominent ones has been the counterfeit ICs. Aged, rejected, or cloned parts, which take a major share of counterfeit chips, find their way into the supply chain and pose a big threat to profitability, security, and reliability of electronic products. Among the various sources of counterfeit ICs, the mostly encountered one is the class of resold ICs; these are used ICs that are stripped from the boards, sorted by size and/or lead count, and reprocessed to look like brand new. A natural end result is reduced reliability and loss of reputation to the brand name, as the expected remaining lifetime of the resold IC is shorter than that of a brand-new part. Other forms of counterfeit ICs include those that are overproduced by an untrusted fab, in addition to reverse engineered, remarked, or cloned ones. Significant research efforts have been invested into counterfeit IC detection techniques such as age estimation and side-channel analysis methods, and prevention techniques such as traceable IDs built into the design, and the use of unclonable design structures.

From a different perspective, security of systems is becoming important. Consider the new industrial revolution that is underway in the manufacturing industry. Manufacturing is quickly moving to "connecting the unconnected," resulting in an "industrial Internet" enabling new services and experiences, including improved customer value through individualization and efficient production by taking advantage of machine-to-machine communication and by integrating production and business IT. On the flipside, these systems will become appealing targets of attacks. Attacks on the cyber-part of such industrial Internet of things can have disastrous consequences in the physical world. Complexity of these interconnected systems and the scope and variety of attacks on them present design challenges that span embedded hardware, software, networking, and system design.

Date of current version May 20, 2015.
Digital Object Identifier 10.1109/TCAD.2015.2432680

Overall, secure and trustworthy hardware components and platforms, and design and distribution supply chains are vital to all domains including financial, healthcare, transportation, and energy. However, whereas security and trust risks are better understood in software, understanding, and addressing the security threats to the hardware root of trust is an emerging challenge.

We exhort the IC and system designers, computer aided design tool developers, and test, verification and validation engineers to consider security side-by-side performance, and low-power and reliability as a metric for optimization. Important outstanding research problems that one may want to address include: hardware security primitives including physical unclonable functions, and true random number generators, hardware-enabled security protocols for IC usage metering, watermarking and obfuscation; hardware-based attacks, detection, recovery, and compensation; reverse engineering ICs at the transistor level, gate level, RT level, and system level; hardware Trojans: insertion and defenses; side channel attacks and countermeasures; security implications of split manufacturing; IC counterfeiting and securing the semiconductor supply chain; VLSI test, verification, and validation for trust; FPGA security; computer aided design (CAD) techniques for secure ICs and systems; interplay between security, trust, and reliability of emerging nanotechnologies; trustworthy hardware-based system security; trustworthy micro-architectures and benchmarks; and red team blue team trust assessment.

The CAD community is beginning to address these challenges and develop impactful solutions. Leading conferences such as the IEEE/ACM HOST, the IEEE/ACM DAC, the IEEE ICCAD, ASP-DAC, ITC, VTS, and ICCD are all focusing on hardware security. Recognizing this trend, the IEEE Transactions on CAD organized a call for a special section on hardware security. The response from the community was overwhelming and undoubtedly a record for any TCAD special section. We received 56 high-quality submissions. To handle this high volume, the special section will span three issues (June, July, and August). Beyond the special section, it is clear that hardware security has emerged as a key field in EDA. TCAD welcomes the submission of high-quality papers on hardware security for publication throughout the year.

Lastly, we would like to thank the contributors to this special section. There were a lot more papers than qualified reviewers. Thanks to all the authors. Our sincere and heartfelt thanks to all the reviewers that took on the extra load. We also convey our thanks to the TCAD Editor-in-Chief, Deputy Editor-in-Chief, and especially Ms. S. Dailey for managing the large number of papers and reviews.

RAMESH KARRI, *Guest Editor*
New York University

FARINAZ KOUSHANFAR, *Guest Editor*
Rice University

OZGUR SINANOGLU, *Guest Editor*
New York University Abu Dhabi

YIORGOS MAKRIS, *Guest Editor*
The University of Texas at Dallas

KEN MAI, *Guest Editor*
Carnegie Mellon University

AHMAD REZA SADEGHI, *Guest Editor*
Technische Universität Darmstadt

SWARUP BHUNIA, *Guest Editor*
University of Florida