Introduction to the Special Issue on CAD for Security: Pre-silicon Security Sign-off Solutions Through Design Cycle

Farimah Farahmandi, Ankur Srivastava, Giorgio Di Natale, Mark Tehranipoor

Introduction to the Special issue on CAD for Security: *Pre-silicon Security Sign-off Solutions Through Design Cycle*

This introduction welcomes all readers to this ACM JETC special issue on CAD for Security: Pre-silicon Security Sign-off Solutions Through Design Cycle. The articles published in this special issue reflect how computer-aided design (CAD) tools are developed to expand the notion of automated security verification throughout the system-on-chip (SoC) design cycle. This special issue aims to demonstrate how the semiconductor industry must look for security-oriented metrics and evaluation as part of automatic CAD solution development to aid analysis, identifying, root-causing, and mitigating SoC security problems. Throughout this introductory note, we first represent the need for such a security-oriented sign-off solution for the ASIC design flow, then it is followed by providing an overview of the articles published in this special issue and how they address such requirements.

CCS CONCEPTS • Security and privacy • Security and privacy ~ Systems security

Additional Keywords and Phrases: CAD for Security, Security Verification, SoC Security.

1. INTRODUCTION

The area of hardware security and trust has witnessed tremendous growth over the past decade. Despite the considerable investments in hardware security and trust research, there is still much required to provide comprehensive solutions for existing and emerging attacks as well as newly-exploited vulnerabilities. Security vulnerabilities in hardware designs are of major concern since it is almost impossible to patch them once the SoCs are fabricated and deployed in the field. Studies have revealed many vulnerabilities in SoC implementations, including side-channel leakage, information leakage, access control violations, and malicious changes. Ensuring the security of modern SoC designs is challenging due to their complexity, aggressive time-to-market demands, and the variety of attacks introduced during lifecycle. Given the wide usage of SoCs in mission-critical applications, it is critical to ensure their security before deployment. However, most of the existing solutions lack automation and rely on manual approaches and design reviews that are neither efficient nor scalable.

Considering the lack of automation for security-oriented evaluation, the semiconductor industry and system integrators are looking for a set of metrics, reusable security solutions, and automatic computer-aided design (CAD) tools to aid analysis, identifying, root-causing, and mitigating SoC security problems. Unfortunately, the existing tools do not alleviate these problems and the existing technologies are developed to optimize designs against power, performance, and area, while security is mostly ignored. In fact, in some cases, these tools unintentionally introduce additional vulnerabilities in the SoCs. Therefore, it is essential to have automatic CAD solutions to be able to analyze the security of SoCs comprehensively, at all levels of abstraction, and against all existing and known threats (e.g., information leakage, access control, fault-injection, side-channel, and hardware Trojan attacks).

The main purpose of these security-oriented CAD solution is to enable the possibility of verifying the security of the SoC designs at the pre-silicon stage (particularly at early stages such as behavioral design), and then they must be able to suggest possible countermeasures that address the potential vulnerabilities. Considering the above

challenges and potential solutions, the papers published in this special issue develop automatic CAD solutions for security sign-off in all levels of abstractions (i.e., C/C++, RTL, gate-level, and layout) for (i) (power/timing) side-channel vulnerability assessment and countermeasures, (ii) fault-injection vulnerability evaluation and countermeasures, (iii) security-oriented equivalency checking and verification, and (iv) automatic security property generation. One goal of this special issue is to offer the readers new research directions that aim at proposing CAD tools and frameworks for security verification and validation. Another goal is to demonstrate to readers how bringing CAD for security can present new avenues in research toward increasing the efficiency of automated security through CAD. This remains in effect for both chip design as well as run-time techniques. In particular, the special issue covers various abstraction layers. It demonstrates how CAD tools do enrich both design-time as well as run-time methodologies to significantly improve their security.

2. OVERVIEW OF THE ARTICLES FEATURED IN THIS ACM JETC SPECIAL ISSUE ON CAD FOR SECURITY

The first paper in this special issue, titled "*Reliable Constructions for the Key Generator of Code-Based Post-Quantum Cryptosystems on FPGA*", focuses on the impact of the environment and intentional faults on hardware implementations of code-based cryptography. Code-based cryptography is one feasible solution whose hardware architectures have become the focus of research in the NIST standardization process and has been advanced to the final round. Since previous studies have proved the vulnerability of hardware implementation of code-based cryptography, this study introduces efficient fault detection construction for the first time to account for such shortcomings. This work relies on regular parity, interleaved parity, and two different cyclic redundancy checks (CRC), i.e., CRC-2 and CRC-8, and shows their effectiveness on the McEliece cryptosystem (as well-known code-based cryptography). Here in this work, the presented fault detection techniques are employed in the distinct units of the key generator, which maximizes the likelihood of error detection. This work is a good illustration of how sets of formulations for the various finite field blocks of a cryptosystem can be constructed to be used for the automating fault detection.

The next article in this special issue, titled "*Automated Generation of Security Assertions for RTL Models*", introduces an automated vulnerability analysis of RTL models to generate security assertions for six classes of vulnerabilities. The assertion-based security validation provides the ability to check for vulnerabilities during execution. Therefore, the assertions at the pre-silicon level provide two opportunities: (i) runtime monitoring of security vulnerabilities, and (ii) fixing the vulnerabilities in the early stages of the design. The generated security assertions are primarily used for pre-silicon security verification. Once pre-silicon security sign-off is done, these security assertions can be removed from the pre-silicon models. Also, these assertions can be synthesized as runtime checkers for post-silicon validation. The proposed framework in this article attempts to reduce the effort needed for security assertion generation significantly compared to the manual development of such assertions. Automated generation of security assertions will enable assertion-based verification as one of the most promising pre-silicon security sign-off solutions.

The next article in this special issue, which is entitled "*Silicon-Correlated Simulation Methodology of EM Side-Channel Leakage Analysis*", proposes simulation-based power and EM side-channel leakage analysis (SCLA) techniques on a cryptographic integrated circuit (IC) chip in the system-level assembly. SCLA measures SC leakage metrics including T-score, SC leakage score (SLS), and the number of measurement traces to disclosure (MTD), leveraged

by a secure system-on-chip (SoC) design flow toward SC attack resiliency and SC leakage sign-off. Power SCLA features the tracking of security-sensitive registers within cryptographic logic paths and the automatic assignments of probe points on associated physical power nets. Power supply current traces are efficiently simulated for the large set of input payloads, with direct vector-based and vectorless random switching controls. EM SCLA evaluates magnetic fields created by every piece of metal wiring in metal stacks where the power supply current of cryptographic processing flows. The EM emission and EM SCLA from the backside Si surface of an IC chip in flip-chip packaging are experimentally examined with a 0.13 μm test chip. The proposed simulation-based SCLA exhibits the SC leakage metrics of on-chip location and direction dependency as accurately as in the measurements.

The next article, entitled "Survey of Approaches and Techniques for Security Verification of Computer Systems", surveys the landscape of security verification approaches and techniques for computer systems at various levels: from the software-application level all the way to the physical hardware level. Different existing projects are compared, based on the tools used and security aspects being examined. Since many systems require both hardware and software components to work together to provide the system's promised security protections, it is not sufficient to verify just the software levels or just the hardware levels in a mutually exclusive fashion. This survey especially highlights system levels that are verified by the different existing projects and present to the readers the state of the art in hardware and software system security verification. Few approaches come close to providing full-system verification, and there is still much room for improvement.

The last article of this special issue, entitled "ACCHASHTAG: Accelerated Hashing for Detecting Fault-Injection Attacks on Embedded Neural Networks", is another CAD framework for high-accuracy detection of fault-injection attacks on Deep Neural Networks (DNNs) with provable bounds on detection performance. Because recent literature on fault-injection attacks shows the severe DNN accuracy degradation caused by bit flips, the proposed framework in this article demonstrates how this can be detected by extracting unique signatures from the DNNs prior to deployment. This enables the designers to have a real-time fault detection on embedded platforms. Such an article again demonstrates how the attributes/features of the design/model can be acquired for the notion of security-oriented verification.

ACKNOWLEDGMENTS

We would like to thank all authors who contributed to this special issue, as well as those who submitted manuscripts that were not published in this issue, but whose important research we look forward to reading in future publications. And, of course, we want to thank all the reviewers who offered valuable input, feedback, and support for this special issue. We certainly hope you enjoy reading these excellent papers. Finally, we would like to thank all the staff members of ACM JETC, including the editors-in-chief, administrative, and editorial staff members for helping us develop this special issue.

FARIMAH FARAHMANDI
ECE Department, University of Florida, farimah@ece.ufl.edu

ANKUR SRIVASTAVA
ECE Department, University of Maryland, ankurs@umd.edu

GIORGIO DI NATALE
TIMA Laboratory, University of Grenoble, giorgio.di-natale@univ-grenoble-alpes.fr

MARK TEHRANIPOOR
ECE Department, University of Florida, tehranipoor@ece.ufl.edu