5.5 Hardware Obfuscation

Date: Wednesday 27 March 2019
Time: 08:30 - 10:00
Location / Room: Room 5

Chair:
Francesco Regazzoni, ALARI-USI, CH

Co-Chair:
Daniel Grosse, University of Bremen, DE

Obfuscation is becoming a popular technique to protect IPs and designs. This session reports the last advances in protection based on obfuscation and on methodology for attacking them.

Time	Label	Presentation Title Authors
08:30	5.5.1	**DESIGN OBFUSCATION THROUGH SELECTIVE POST-FABRICATION TRANSISTOR-LEVEL PROGRAMMING** **Speaker**: Yiorgos Makris, The University of Texas at Dallas, US **Authors**: Mustafa Shihab, Jingxiang Tian, Gaurav Rajavendra Reddy, Bo Hu, William Swartz Jr., Benjamin Carrion Schaefer, Carl Sechen and Yiorgos Makris, The University of Texas at Dallas, US ***Abstract*** *Widespread adoption of the fabless business model and utilization of third-party foundries have increased the exposure of sensitive designs to security threats such as intellectual property (IP) theft and integrated circuit (IC) counterfeiting. As a result, concerted interest in various design obfuscation schemes for deterring reverse engineering and/or unauthorized reproduction and usage of ICs has surfaced. To this end, in this paper we present a novel mechanism for structurally obfuscating sensitive parts of a design through post-fabrication TRAnsistor-level Programming (TRAP). We introduce a transistor-level programmable fabric and we discuss its unique advantages towards design obfuscation, as well as a customized CAD framework for seamlessly integrating this fabric in an ASIC design flow. We theoretically analyze the complexity of attacking TRAP-obfuscated designs through both brute-force and intelligent SAT-based attacks and we present a silicon implementation of a platform for experimenting with TRAP. Effectiveness of the proposed method is evaluated through selective obfuscation of various modules of a modern microprocessor design. Results corroborate that, as compared to an FPGA implementation, TRAP-based obfuscation offers superior resistance against both brute-force and oracle-guided SAT attacks, while incurring an order of magnitude less area, power and delay overhead.* Download Paper (PDF; Only available from the DATE venue WiFi)
09:00	5.5.2	**KC2: KEY-CONDITION CRUNCHING FOR FAST SEQUENTIAL CIRCUIT DEOBFUSCATION** **Speaker**: Yier Jin, University of Florida, US **Authors**: kaveh shamsi[1], Meng Li[2], David Z. Pan[3] and Yier Jin[1] [1]University of Florida, US; [2]University of Texas, Austin, US; [3]University of Texas at Austin, US ***Abstract*** *Logic locking and IC camouflaging are two promising techniques for thwarting an array of supply chain threats. Logic locking can hide the design from the foundry as well as end-users and IC camouflaging can thwart IC reverse engineering by end-users. Oracle-guided SAT-based deobfuscation attacks against these schemes have made it more and more difficult to securely implement them with low overhead. Almost all of the literature on SAT attacks is focused on combinational circuits. A recent first implementation of oracle-guided attacks on sequential circuits showed a drastic increase in deobfuscation time versus combinational circuits. In this paper we show that integrating the sequential SAT-attack with incremental bounded-model-checking, and dynamic simplification of key-conditions (Key-Condition Crunching or KC2), we are able to reduce the runtime of sequential SAT-attacks by two orders of magnitude across benchmark circuits, significantly reducing the gap between sequential and combinational deobfuscation. These techniques are applicable to combinational deobfuscation as well and thus represent a generic improvement to deobfuscation procedures and help better understand the complexity of deobfuscation for designing secure locking/camouflaging schemes.* Download Paper (PDF; Only available from the DATE venue WiFi)
09:30	5.5.3	**PIERCING LOGIC LOCKING KEYS THROUGH REDUNDANCY IDENTIFICATION** **Speaker**: Alex Orailoglu, University of California, San Diego, US **Authors**: Leon Li and Alex Orailoglu, UC San Diego, US ***Abstract*** *The globalization of the IC supply chain witnesses the emergence of hardware attacks such as reverse engineering, hardware Trojans, IP piracy and counterfeiting. The consequent losses sum to billions of dollars for the IC industry. One way to defend against these threats is to lock the circuit by inserting additional key-controlled logic such that correct outputs are produced only when the correct key is applied. The viability of logic locking techniques in precluding IP piracy has been tested by researchers who have shown extensive weaknesses when access to a functional IC is guaranteed. In this paper, we uncover weaknesses of logic locking techniques when the attacker has no access to an activated IC, thus exposing vulnerabilities at the earliest stage even for applications that seek refuge from attacks through functional opaqueness. We develop an attack algorithm that prunes out the incorrect value of each key bit when it introduces a significant level of logic redundancy. Throughout our experiments on ISCAS-85 and ISCAS-89 benchmark circuits, the attack deciphers more than half of the key bits on average with a high accuracy.* Download Paper (PDF; Only available from the DATE venue WiFi)

Time	Label	Presentation Title Authors
10:00	IP2-15, 595	**DEEP LEARNING-BASED CIRCUIT RECOGNITION USING SPARSE MAPPING AND LEVEL-DEPENDENT DECAYING SUM CIRCUIT REPRESENTATION** **Speaker**: Massoud Pedram, University of southern california, US **Authors**: Arash Fayyazi[1], Soheil Shababi[2], Pierluigi Nuzzo[2], Shahin Nazarian[2] and Massoud Pedram[1] [1]University of southern california, US; [2]University of Southern California, US ***Abstract*** *Efficiently recognizing the functionality of a circuit is key to many applications, such as formal verification, reverse engineering, and security. We present a scalable framework for gate-level circuit recognition that leverages deep learning and a convolutional neural network (CNN)-based circuit representation. Given a standard cell library, we present a sparse mapping algorithm to improve the time and memory efficiency of the CNN-based circuit representation. Sparse mapping allows encoding only the logic cell functionality, independently of implementation parameters such as timing or area. We further propose a data structure, termed level-dependent decaying sum (LDDS) existence vector, which can compactly represent information about the circuit topology. Given a reference gate in the circuit, an LDDS vector can capture the function of the gates in the input and output cones as well as their distance (number of stages) from the reference. Compared to the baseline approach, our framework obtains more than an-order-of-magnitude reduction in the average training time and 2× improvement in the average runtime for generating CNN-based representations from gate-level circuits, while achieving 10% higher accuracy on a set of benchmarks including EPFL and ISCAS'85 circuits.* Download Paper (PDF; Only available from the DATE venue WiFi)
10:01	IP2-16, 762	**PARTIAL ENCRYPTION OF BEHAVIORAL IPS TO SELECTIVELY CONTROL THE DESIGN SPACE IN HIGH-LEVEL SYNTHESIS** **Speaker**: Farah Taher, The University of Texas at Dallas, US **Authors**: Zi Wang and Benjamin Carrion Schaefer, The University of Texas at Dallas, US ***Abstract*** *Abstract—Commercial High-Level Synthesis(HLS) tool vendors have started to enable ways toprotect Behavioral IP (BIPs) from being unlawful used.The main approach is to provide tools to encrypt these BIPs which can be decrypted by the HLS tool only. The main problem with this approach is that encrypting the IP does not allow BIP users to insert synthesis directives into the source code in the form of pragmas (comments), and hence cancels out one of the most important advantages of C-based VLSI design: The ability to automatically generate micro-architectures with unique design metrics,e.g.area, power and performance.This work studies the infect to the search space when synthesis directives are not able to be inserted in to the encrypted IP source code while other options are still available to the BIP users (e.g.setting global synthesis options and limiting the number and type of functional units) and proposes a method that selectively controls the search space by encrypting different portions of the BIP. To achieve this goal we propose a fast heuristic based on divide and conquer method.Experimental results show that our proposed method works well compared to an exhaustive search that leads to the optimal solution.* Download Paper (PDF; Only available from the DATE venue WiFi)
10:00		End of session **Coffee Break** in Exhibition Area

Coffee Breaks in the Exhibition Area

On all conference days (Tuesday to Thursday), coffee and tea will be served during the coffee breaks at the below-mentioned times in the exhibition area.

Lunch Breaks (Lunch Area)

On all conference days (Tuesday to Thursday), a seated lunch (lunch buffet) will be offered in the Lunch Area to fully registered conference delegates only. There will be badge control at the entrance to the lunch break area.

Tuesday, March 26, 2019

- Coffee Break 10:30 - 11:30
- Lunch Break 13:00 - 14:30
- Keynote Lecture "Leonardo da Vinci, Humanism and Engineering between Florence and Milan" by Claudio Giorgione in room 1 13:50 - 14:20
- Coffee Break 16:00 - 17:00

Wednesday, March 27, 2019

- Coffee Break 10:00 - 11:00
- Lunch Break 12:30 - 14:30
- Keynote Lecture "Heterogeneous, High Scale Computing in the Era of Intelligent, Cloud-Connected" by David Pellerin, Amazon, US in room 1 13:50 - 14:20
- Coffee Break 16:00 - 17:00

Thursday, March 28, 2019

- Coffee Break 10:00 - 11:00
- University Booth Best Demo Award Presentation at the University Booth 10:30
- Lunch Break 12:30 - 14:00
- Keynote Lecture "A Fundamental Look at Models and Intelligence" by Edward A. Lee, University of California, Berkeley, US in room 1 13:20 - 13:50
- Coffee Break 15:30 - 16:00

Source URL: https://past.date-conference.com/conference/session/5.5