CCIT Report #897 May 2016

Exploiting the Scan Side Channel for Reverse Engineering of a VLSI Device

Leonid Azriel, Ran Ginosar, and Avi Mendelson

Technion, Israel Institute of Technology,
{leonida, ran, avi.mendelson}@technion.ac.il

Abstract. This paper presents a novel non-invasive method of reverse engineering of digital VLSI devices that exploits the scan chains originally inserted into the device for production test automation. The scan chains unfold the sequential logic of the device to form a combinational function. The device's logical functionality can then be discovered by examining this function. This potentially allows for the adversary to carry out a reverse engineering attack using simple off-the-shelf equipment for accessing the scan chains combined with Boolean function learning methods. To demonstrate the effectiveness of the method, we apply a set of heuristic learning algorithms that take advantage of common properties of digital circuits, in particular limited transitive fan-in of combinational logic and sub-circuit sharing properties. With these algorithms we achieve successful and fast reconstruction of popular cryptographic function implementations such as the AES cryptographic accelerator. The algorithm used for reconstruction of the AES is scalable and therefore can be used with significantly larger circuits. Finally, we discuss the existing countermeasures against scan-based side channel attacks and find that the presented method is immune to some of them.

Keywords: Side Channel Analysis, Scan Side Channel, Reverse Engineering

1 Introduction

Reverse engineering of a VLSI device is a complex task that traditionally requires tedious work and expensive equipment [25]. The ultimate goal of the reverse engineering process is, given the physical device, to discover its underlying algorithm; i.e., the device's behavioral definition. Roughly, we can represent the discovery task as a two-stage process: (1) Extraction of the circuit from the physical device and (2) Extraction of the behavioral model from the circuit.

The boundary between the two stages sometimes may be blurred; nevertheless, these are usually two distinct tasks. The first stage, as a rule, involves a sequence of invasive techniques, such as removing the package, performing cross-section, delayering, and imaging of nanoscale [18, 25]. The second stage is usually algorithmic [1, 14, 16, 22]. This paper addresses the first stage - circuit extraction. The complexity and cost of invasive circuit extraction methods commonly used