IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 19, 2022, accepted February 6, 2022, date of publication February 14, 2022, date of current version February 22, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3151378

Locating Hardware Trojans Using Combinatorial Testing for Cryptographic Circuits

LUDWIG KAMPEL[1], PARIS KITSOS[2], (Senior Member, IEEE), AND DIMITRIS E. SIMOS[1], (Member, IEEE)

[1]SBA Research, 1040 Vienna, Austria
[2]Electrical and Computer Engineering Department, University of the Peloponnese, 26334 Patras, Greece

Corresponding author: Ludwig Kampel (lkampel@sba-research.org)

This work was supported in part by the Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK); in part by the Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW); in part by the Federal State of Vienna; in part by the European Union and Greek National Funds; and in part by the Regional Operational Program ''Western Greece 2014–2020,'' under the Call ''Financial Strengthening Research Development and Innovation Projects in the Priority Area of RIS3-ICT'' through the Project entitled Integrated Information and Communications Technology (ICT)-Based Active Living Support System 'MeACT' under Grant 5038641.

ABSTRACT This paper presents a novel method for locating combinational hardware Trojans (HT) based on fault location approaches used in combinatorial testing. This method relies exclusively on the combinatorial properties of the executed test vectors and the results of test execution. Under specific assumptions, the method is guaranteed to locate all combinational HTs with trigger patterns of length ℓ or less, with the location process itself consuming negligible time. We give a description of our method by devising suitable algorithms and provide the links to combinatorial fault location. Furthermore, we demonstrate our approach in a concrete case study where we locate HTs embedded in a circuit that implements the AES symmetric-key encryption algorithm with 128 bits key length. In these experiments, we demonstrate how any HT that is activated by a trigger pattern of length $\ell \leq 8$ can be located in an effective way. Our method compares particularly well against randomized approaches. Although instantiated for a specific circuit in our case study, the proposed approach is generic, due to its algorithmic description, and can be applied for testing other (cryptographic) circuits. We believe that our work presents an important first step in the development of more general logic testing methodologies for HT location using combinatorial testing methods.

INDEX TERMS Circuit testing, combinatorial testing, detection techniques, hardware trojans, fault location analysis.

I. INTRODUCTION

The security of information and communication technologies and electronic systems in general is often solely related to the security of its software part, leaving hardware security out. However, when treating the security of an electronic system holistically hardware security must be addressed as well. A reliable and secure piece of hardware is expected to implement and execute only what it is designed to and nothing else, even in the presence of an intentional attack. In modern society, the globalization of the semiconductor industry raises additional concerns regarding the authenticity and security of fabricated integrated circuits (ICs). IC design and manufacturing may involve multiple fabricators and circuits have to run through multiple stages until a final product reaches its customer. In each individual production stage, there is potential for malicious manipulation of an IC. This threat is recognized in the US not only by intelligence service agents [1], but also in reports of government institutions [2]. It has been the subject of scientific discussion and investigation for several [3]. For instance, rumors exist that in 2007, a Syrian radar failed to warn of an incoming air strike due to a backdoor in the system's chips [3]. Similarly, a German missile system located at the Turkish-Syrian border may have carried out ''unexplained commands'' in 2015, with rumors suggesting that the system had been hacked and tampered hardware might have been used as an entry point [4]. More concrete documentation of attacks based on HTs are difficult to find, possibly due to concerns regarding the impact on security, economy, and society. Regardless of whether these rumors are true or not, there exists scientific evidence that cybersecurity attacks based on vulnerable hardware are possible [5]. Thus, establishing a trustworthy supply chain for information technology equipment is of

The associate editor coordinating the review of this manuscript and approving it for publication was Porfirio Tramontana.