Detection and Prevention of Hardware Trojans in Integrated Circuits

Nowadays the manufacturing of integrated circuits is generally made by specialized companies called "founders" and not by the company who designed the circuit [3]. During the foundry stage, the design can be modified and internal data or secret could become accessible. This malevolent insertion is called "Hardware Trojan" (HT). This potential threat has been taken very seriously by DARPA who launched the Trust in IC program in 2007 [8] whose objectives was to design efficient procedures to detect Hardware Trojans. The impact of HT can be very large, the list below describes some potential effects which can wreak havoc on the trust of the device: -# To switch on remotely a device, as a missile launcher as described in [1]. -# To alter internal nodes to speed up the aging of the device [16]. -# To retrieve a secret like a ciphering key in cryptographic implementation [13]. -# To provide a backdoor which allows a malware to access protected resources [11]. The Hardware Trojans are activated by a trigger which corresponds to a specific state or sequence of states. Then they can change a net value or activate a parasitic element like a resistor to increase the power consumption. The current methods to detect HT are based either on the insertion of specific detection blocks (invasive method) or by using a reference model to compare with the manufactured circuit. For instance the invasive methods consist in adding obfuscating blocks [6], using the Q and Q of all the Flip-Flops [5], or inserting hidden Flip-Flops [12, 15, 9]. The non-invasive method can be employed during the test phase, as proposed in [10] and improved in [7] with a higher detection rate. Another non-invasive method consists in using side-channels and a reference model as presented in [2]. Other statistical techniques have been proposed which used many circuits to characterize its behaviour when the HT is activated, as in [14, 4]. All these techniques are perfectible, as it is impossible to get a detection rate of 100%, the detection is complex and statistical methods are sensitive to process variation. This PhD subject is part of the FUI14 collaborative project "HOMERE". The goal of this thesis is to find efficient ways to avoid malevolent actions from HT.

The challenges of the PhD subject are to thwart the impact of the Hardware Trojans: -# To find resilient methods to prevent a malevolent action of potential HT. That means that any inserted HT would be completely uncultivable when it is triggered by the adversary. -# To find better detection methods, as described in the context chapter. This detection can be performed during the test phase or the operating phase. The objective is to obtain a significant improvement compared to existing methods. In order to achieve these goals, many tasks should be carried out, among them: -# The coverage of all the HT techniques (generation and detection) which have been published. It has to described the principle along with advantages and limitations of each technique. -# The study of new and efficient techniques for both resiliency and detection. In this phase a few methods will be proposed. -# The validation of the proposed methods. Prototypes based on FPGA should be designed for this phase. An ASIC design could also be done for this purpose. -# The results analysis with a comparison of different studied methods.

This project is part of the FUI14 collaborative project "HOMERE" where there is a specific dissemination task. The research results should be submitted to international conferences about the security of embedded systems, as for instance CHES, DATE, HOST, COSADE among the most known conferences.