LIRMM

Séminaire sur l'Intégration en Microélectronique

Hardware-Security and Trust: Counterfeit and hardware Trojans

24 Mars 2016 - Salle de séminaire du LIRMM (Bat. 4)

9h30 : Accueil (Pascal Nouet) puis Introduction de la Journée (Philippe Maurine)

*9h45 : **Benedikt Gierlichs** (ESAT - Katholieke Universiteit Leuven)*

Electromagnetic Circuit Fingerprints for Hardware Trojan Detection

Integrated circuit counterfeits, relabeled parts and maliciously modified integrated circuits (so-called Hardware Trojan horses) are a recognized emerging threat for embedded systems in safety or security critical applications. We propose a Hardware Trojan detection technique based on fingerprinting the electromagnetic emanations of integrated circuits. In contrast to most previous work, we do not evaluate our proposal using simulations but we rather conduct experiments with an FPGA. We investigate the effectiveness of our technique in detecting extremely small Hardware Trojans located at different positions within the FPGA. In addition, we also study its robustness to the often neglected issue of variations in the test environment. The results show that our method is able to detect most of our test Hardware Trojans but also highlight the difficulty of measuring emanations of unrealistically tiny Hardware Trojans. The results also confirm that our method is sensitive to changes in the test environment.

*10h30: **David Hély** (LCIS-ESISAR)*

Enhancing side channel based HT detection methods with Logic Locking

Intellectual Property piracy and malicious alteration, named as Hardware Trojan (HT), are two increasing threats for modern system on chip. Logic locking techniques have been efficiently developed against IP piracy. It can also offer opportunities to facilitate power and path delay analysis based HT detection methods. In this work, we show how logic locking methods can be driven to make HT detection easier. We leverage these methods in order to increase the efficiency of both path delay and power analysis based HT detection techniques. Experimental results for several benchmarks show how the quality of logic locking is preserved while the detection quality is increased.

*11h15 : **Maxime Lecomte** (DPACA - CEA-TECH)*

Embedded Counterfeit and hardware Trojan detection

On-chip fingerprinting of IC topology for integrity verification The integrity of integrated circuits (ICs), in particular for detecting malicious add-ons like Hardware Trojans (HTs), have been studied in several recent researches. The main limit of the proposed techniques so far is that the bias induced by process variations restricts their efficiency and practicality. Most of those techniques compare two ICs' signatures while trying to get rid of the process variations. A novel approach, which in practice eliminates this limit is based on infection assumption and a new variation model. First, the assumption is that IC infection is done at a lot level, which is more realistic than models where infections are done on individual circuits. And a variation model for the performance of CMOS structures is introduced in real designs, which are different from test chips dedicated to the measure of process variations. This model is used to create signatures of lots, which are independent of the process variations and is used as a base to define methods allowing the detection of HTs and counterfeits in a straightforward way. The model and the method are validated experimentally on FPGA boards.

Séminaire sur l’Intégration en Microélectronique

Hardware-Security and Trust: Counterfeit and hardware Trojans

24 Mars 2016 - Salle de séminaire du LIRMM (Bat. 4)

12h00 : Repas (Cafet Bat 4)

*13h30 : **Jean-Luc Danger** (Telecom ParisTech)*

Logic Encoding against Hardware Trojan Horses and other Physical Attacks.

This talk presents a provable method to be robust against Hardware Trojan Horses (HTH) insertion in Integrated Circuit. As the HTH is composed of a probing part (Trigger) and a node modification part (Payload), the proposed method is effective against side-channel and fault injection attack. The principle relies on the use of linear codes to encode the sequential intermediate variables.

More specifically this provable method exploits code properties to give security parameters. It can be used to protect data, which is equivalent to the masking protection, but also the control part of any sensitive function. Some results, in terms of security gain and complexity, are given and discussed.

*14h15 : **Sophie Dupuis** (LIRMM - Université de Montpellier)*

Security against Hardware Trojan through logic testing and Design-For-Hardare Trust

With ever-shrinking transistor technologies, the cost of new fabrication facilities is becoming prohibitive and outsourcing the fabrication process to low-cost locations has become a major trend in Integrated Circuits (ICs) industry in the last decade. This raises the question about untrusted foundries in which the insertion of malicious circuitry or alterations, referred to as Hardware Trojans (HTs), is a possible threat. In this presentation, we summarize several detection techniques as well as prevention techniques. Firstly, we present a testing procedure dedicated to identifying where a possible HT may be easily inserted and generating the test patterns that are able to excite these sites. Secondly, we present several prevention techniques based on obfuscation, layout filling and duplication.

*15h00 : **Jérôme Rampon** (Algodone)*

Hardware Monetization Solutions

Algodone is a French start-up with strong relationships with the University of Montpellier and LIRMM. Algodone objective consists to build and to operate the first Silicon-as-a-Service business model enabling the semiconductor industry players to monetize throughout the complete life cycle and to increase total revenue. In practice, it is based on a HW license generator application with a Silicon Management System including an HW/SW framework suite. For those familiar with Software License Management (for example flexlm solution), a very simple analogy consists to classify our technology as hardware equivalent. Based on an elegant electronic DNA concept (Physical Unclonable Function), Algodone's technology allows to control, among others, the volume of chips integrating any IP block models or the configuration of a chip. Even though millions of chips of a given design are produced, each of them requires a dedicated license at runtime to enable its IPs or any feature designed under a HW license control. In any case, it drastically extends the flexibility of provider-customer relationships for any hardware embedded systems.

15h45 : Conclusions de la Journée (Philippe Maurine)

Contact organisation : Philippe.Maurine@lirmm.fr
Contact Inscription : communication@lirmm.fr