Cryptographic Engineering Research Group
Presents

ECE DEPARTMENTAL SEMINAR

Fight Against Counterfeiting and Theft of Electronics Devices by Designing SALWARE

Cédric Marchand
Hubert Curien Laboratory
University of Lyon, Saint-Etienne, France

Wednesday, September 23, 2015
1:30–2:30pm, ENGR 3507

Abstract:

For many years, the microelectronic industry has been facing an increase in the costs of integrated circuits (ICs) production. This effect is due to the increasing complexity of systems and the expensive technology refinement. As a result, this industry has seen relocation of its production facilities and a sharp increase in the number of fabless companies (companies which do not produce ICs themselves). In addition, the time-to-market is increasingly tight. Thus, ICs manufactured today are produced with a high amount of added value in a highly competitive industry! All these changes have made electronic devices the target of counterfeiting, illegal cloning, theft and malicious hardware insertion (such as hardware trojans). The counterfeiting of ICs has become a major problem in recent years. For instance, the number of counterfeit electronic circuits seized by the U.S. Customs between 2001 and 2011 has increased around 700 times. Between 2007 and 2010, the U.S. Customs confiscated 5.6 million counterfeit electronic products. Overall, counterfeiting is estimated to account for about 7% of the semiconductor market, which represents a loss of around $22 billion for the lawful industry in 2014.
Designing salutary hardware (salware) is a way to protect IPs against these emerging threats. Salware is a small piece of hardware, hardly detectable and hard to circumvent (from the attacker's point of view), inserted in an integrated circuit or an IP, used to provide intellectual property information and/or to remotely activate the integrated circuit or IP after manufacturing and/or during authorized use. This PhD study is devoted to the investigation of three different SALWARE mechanisms: IP Watermarking, Physical Unclonable Functions (PUFs), and ultra-lightweight cryptography.

Short bio:

Cédric Marchand received an M.S. degree in Electrical Engineering (2013) from Ecole Nationale Suprieure des Mines de Saint-Etienne in France. During his master's internship at the Airbus Defence and Space: Cybersecurity, he worked on the implementation and detection of hardware trojans using side channel analysis. Since November 2013, he has been a Ph.D student at University of Lyon at Saint-Etienne in France. He is a member of the Hubert Curien Laboratory, and investigates salutary hardware for IP protection. His work is funded by the French ANR project SALWARE (http://www.univ-st-etienne.fr/salware/). His research focuses on three types of mechanisms required to effectively fight against counterfeiting and theft of electronic devices: IP Watermarking, Physical Unclonable Functions, and ultra-lightweight cryptography.
Personal website: http://www.cedric-marchand.fr/en_GB/