Polytech network form for PhD Research Grants from the China Scholarship Council

This document describes the PhD subject and supervisor proposed by the French Polytech network of 14 university engineering schools. Please contact the PhD supervisor by email or Skype for further information regarding your application.

Supervisor information

Family name	Benoit
First name	Pascal
Email	Pascal.benoit@lirmm.fr
Web reference	http://www.lirmm.fr/~pbenoit/
Lab name	LIRMM
Lab web site	www.lirmm.fr/
Polytech name	Polytech Montpellier
University name	University of Montpellier
Country	France

PhD information

Title	Main memory security vulnerabilities in the context of emerging technologies
Main topics regards to CSC list (3 topics at maximum)	I-13. Network information security.; I-14. IC Design; I-11. Structure of new computer systems

Required skills in science and engineering	We are looking for excellent candidates with a university degree on Electrical Engineering, Computer Sciences or equivalent. Any experience from computer architecture, embedded system architecture, and programming (C, C++, python) is a merit. You should have strong analytical skills and be highly motivated. French language is not required. Interest and some understanding of cybersecurity and cryptography would be appreciated

Subject description (two pages maximum)

The 4th industrial revolution is the one of cyber-physical systems marked by a huge increase of electronic systems. These ones include all kinds of electronic systems such as High performance, embedded or Internet of Things devices. To reach better performance with minimum power consumption, traditional memories (SRAM, DRAM) will be replaced by nonvolatile memories such as Magnetoresistive RAM (MRAM) [6]. This emerging technology allows reducing drastically the leakage power consumption with low penalty on dynamic power consumption.

Another particularity of modern electronic systems is the need of connectivity for exchanging data. To protect communications and data, information is ciphered. The cryptographic algorithm being known, the secret lies in encryption/decryption keys. These cryptography solutions are generally designed to withstand mathematical cryptanalysis. The past decade has seen the rise of micro-architectural and hardware vulnerabilities. A lot of examples exist such as Spectre and Meltdown or even side-channel attacks [1-3]. This kind of attacks collects leakages during encryption/decryption process to hack systems and retrieve secret keys. State-of-the-art reference vulnerabilities at all levels of a system: processors, caches and main memory… To neutralize these vulnerabilities, it is necessary to offer efficient countermeasures. A promising solution is the use of homomorphic ciphering. This kind of encryption allows computation directly on the ciphertext. The encryption/decryption keys are much less manipulated which reduce the exposure to attacks.

The main objective of the PhD will be to study security in the context of modern electronic systems. A special highlight will be put on the memory subsystem. The essential challenges to face are the following:

- First of all, state-of-the-art vulnerabilities resulting of the main memory subsystem will be evaluated: Rowhammer and cold boot attacks [4-5]. The student will set up an evaluation environment on a simulator (gem5, nvmain) and one or two real platforms (x86, ARM).

- State-of-the-art vulnerabilities will be evaluated in the context of nonvolatile memories as main memories. New vulnerabilities will be proposed.
- Countermeasures dedicated to such attacks will be assessed. One promising solution is the use of homomorphic ciphering.

The PhD thesis will take place at the Laboratory of Informatics, Robotics and Microelectronics of Montpellier. It is a public funded cross-faculty (CNRS/University of Montpellier) and more particularly in the Adaptive Computing group (ADAC) which is part of the Microelectronics department. It conducts research in a number of areas connected to computer architecture / computer sciences (Embedded, HPC, Pervasive), digital hardware (MPSoC, reconfigurable architectures and hardware security) and emerging technologies (design of hybrid MRAM / CMOS devices). The PhD will join a team composed of permanent researchers, post-doc, PhD and Master students working on architecture and hardware security at different levels.

References:
[1] Kocher, Paul, et al. "Spectre attacks: Exploiting speculative execution." *arXiv preprint arXiv:1801.01203* (2018).
[2] Lipp, Moritz, et al. "Meltdown." *arXiv preprint arXiv:1801.01207* (2018).
[3] Bruguier, Florent, et al. "Cost-effective design strategies for securing embedded processors." *IEEE Transactions on Emerging Topics in Computing* 4.1 (2016): 60-72.
[4] Seaborn, Mark, and Thomas Dullien. "Exploiting the DRAM rowhammer bug to gain kernel privileges." *Black Hat* 15 (2015).
[5] Halderman, J. Alex, et al. "Lest we remember: cold-boot attacks on encryption keys." *Communications of the ACM* 52.5 (2009): 91-98.
[6] Senni, Sophiane, et al. "Exploring MRAM technologies for energy efficient systems-on-chip." *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 6.3 (2016): 279-292.