Contact : Pirouz.Bazargan-Sabet@Lip6.fr

Laboratory of Computer Sciences of UPMC (Paris 6)
http://www.lip6.fr

http://spaces.enst.fr

LIP6 A research laboratory in computer science of University Pierre & Marie Curie (Paris 6) and CNRS (French National Center for Scientific Research)

188 Permanent researchers and 244 PhD Students

5 Departments: Scientific Computing, Decision, DataBases, Networks and Distributed Systems, Systems on Chips

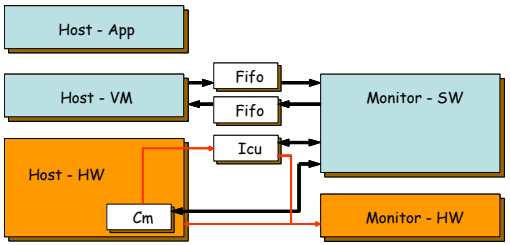
LIP6 activities in security of systems

ANR project 2008-2010 SoS – Smart on Smart
https://tokyo.emse.fr/trac/sos

Partners : CEA, Viaccess, TrustedLogic, Lip6

Context : Systems implementing security integrate a large number of sensors and counter-measures to face attacks. This may lead to a loose of performance in terms of computation time and energy.

Goal : Introduce a smart management of counter-measures via an independent processor based monitoring sub-system. The monitor analyzes the context and the history of events to adopt a security strategy and to switch on and off appropriate counter-measures in case of attack suspicion.



LIP6 involvement in SPACES project

Context : We aim at evaluating the robustness of cryptographic systems against SCA before fabrication.

Goal : Development of several simulation tools to evaluate EM field and instantaneous current at transistor, gate or functional description level.

SPACES simulators vs. Spice :

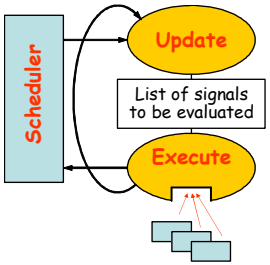
- ✓ Same input description
- ✓ Less accurate but comparable
- ✓ Orders of magnitude faster

SPACES vs. Digital Simulators :

- ✓ Same Event-Driven algorithm
- ✓ Higher accuracy

Dynamic timing evaluation
RC of interconnects
Current to Vss and to Vdd
Smooth signal transition
Slope change during transition
Incomplete transition - glitches

LIP6 targets the development of a unique Simulation Engine that can be customized into a specific simulator by plugging an Evaluation Engine.



Update signals' value. When Event resume the evaluation of dependent signals

The Evaluation Engine calculates signals' value (timing) and physical parameters (I or EM).

The evaluation may relay on an analytical expression or a tabular representation

Workshop on Cryptographic Hardware and Embedded Systems 2011 **(CHES 2011)**
Nara, Japan, from September 28th to October 1st 2011