CAREER: Hardware/Software Codesign for Secure Embedded Systems: Methods and Education

Patrick Schaumont, Bradley Department of ECE, Virginia Tech, Blacksburg, VA

Side-channel Analysis in Crypto Hardware

- Key Estimation based on observation of:
  - $P$: Simple Power Analysis (SPA)
  - $P$ and $out$: Differential Power Analysis (DPA)
  - $P$ and $(out)^n$: High Order DPA

Countermeasures using hiding or masking

**Hiding** $P(f(a)) \Rightarrow \text{const}$
- Dual-rail Encoded Circuits (WDDL, Tiri [2003])

**Masking** $f(a) \Rightarrow f_i(a \oplus r) \oplus f_j(r)$
- Dual-rail Masked Circuits (MDPL, Popp [2005])
- Random-switched Logic (RSL, Suzuki [2006])
- Boolean Masking (Oswald [2005])

Implementation Challenges: Deal with low-level electrical effects (unbalanced implementation, early propagation, glitches, memory effects) and logic-level effects (statistical bias on the mask, ...)

Approach: Develop systematic design methods for side-channel resistant circuits

Impact: Systematic design of trustworthy hardware is a basis for trustworthy software

Hiding-based Design Flow for Reconfigurable Hardware

Results: With DWDDL for reconfigurable logic, we demonstrate a methodology for hiding-based side-channel resistant circuits that offer protection from a **logical** and a **physical** perspective

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT