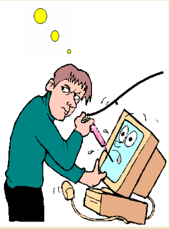
Power Analysis Attacks and Defenses

Leakage-Based Differential Power Analysis (LDPA) on Sub-90nm CMOS Cryptosystems[1]

Lang Lin, Wayne Burleson (University of Massachusetts Amherst)

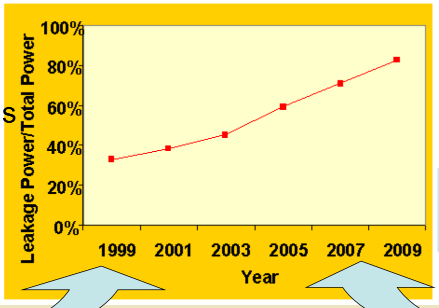
Abstract

Power analysis attacks keep threatening the security and privacy of CMOS cryptosystems in Smartcards and RFIDs. With the scaling down of supply voltage and CMOS technology below 90nm, leakage power plays an increasing role in the overall power dissipation. Accordingly, sub-90nm CMOS cryptosystems with conventional power-attack-resistant abilities may be vulnerable to a novel leakage-based differential power analysis (LDPA). We have demonstrated the feasibility of LDPA by SPICE simulation, and we are exploring several MOS logic styles to tolerate both DPA and LDPA attacks.



Conventional Differential Power Analysis (DPA): exploit *dynamic power* dependence on input patterns

Comprehensive studies on DPA-resistant logic styles for embedded cryptosystems



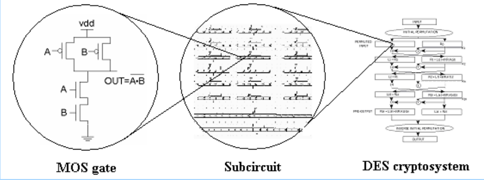
Projected leakage power as a fraction of the total power by ITRS

CMOS cryptosystems below 90nm technologies: *leakage power* becomes dominant and also input-dependent

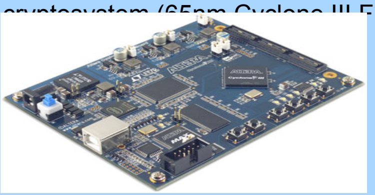
Will LDPA work and how to design LDPA-tolerant cryptosystems

Methodology

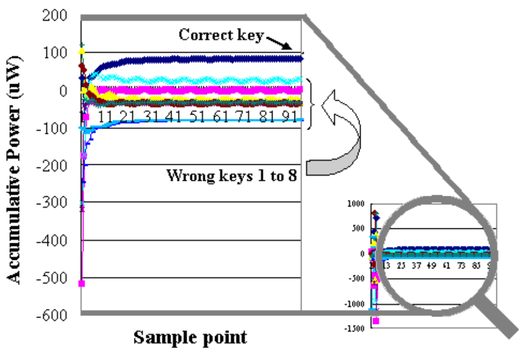
Stage 1: LDPA simulation in SPICE from the gate level to the system level



Stage 2: Practical LDPA on an FPGA-based cryptosystem (65nm Cyclone III FPGA)



Simulation results: a successful LDPA on a DES substitution box with standard CMOS logic style (see the left figure), where the key can be extracted by exploiting the leakage power part faster than by exploiting the dynamic power part



Future work:

- LDPA on an entire cryptosystem (DES, AES…)
- LDPA-tolerant MOS logic styles
- Practical LDPA and LDPA-tolerant cryptosystems

National Science Foundation
WHERE DISCOVERIES BEGIN

1.Lang Lin, Wayne Burleson, “Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems”, accepted by 2008 IEEE International Symposium on Circuits and Systems, May 2008. (This work is supported by an NSF Cyber Trust Program)