ASIC Tools for DPA Prevention

Troy Hicks
VP of Engineering
Revere Security

Explosive Growth for Secure Devices

- Emerging markets
  - 16% smart card growth in China in 2012*
- Rapid adoption
  - Utilities
  - Tolling
  - Supply Chain
- Technology Improvements
  - AES acceleration in Intel Core i5

* RNCOS “Smart Card Market Forecast to 2012

Insecure Security

- Side-Channel Attacks
  - Timing Analysis Attacks
  - Power Analysis Attacks
  - Electromagnetic Analysis Attacks
  - Cache Attacks
  - Fault Analysis Attacks

Differential Power Analysis

- DPA Attacks
  - Premise: The key of a cryptographic device can be revealed simply by observing its power consumption
    - Low Cost
    - Minimum knowledge of implementation
    - Relatively simple algorithm
- Xilinx Virtex 4 & 5 bitstream encryption cracked*

* “On the portability of Side-Channel Attacks” Moradi et. al. Ruhr University

Current Prevention Methods

- Two Basic Approaches
  - Design in random power consumption
    - Many different approaches
      - *(Additional logic)*
  - Design for constant power consumption
    - Cell level techniques
      - DRP
      - SABL
      - WDDL
    - *(Larger cells)*

Conflicting Priorities

- Low Power
  - Quite inactive cells
    - Increasing Signal-Noise ratio makes DPA easier
- Low Cost
  - Reduce die area
    - Counter to typical DPA countermeasures

Nothing Unusual in EDA History

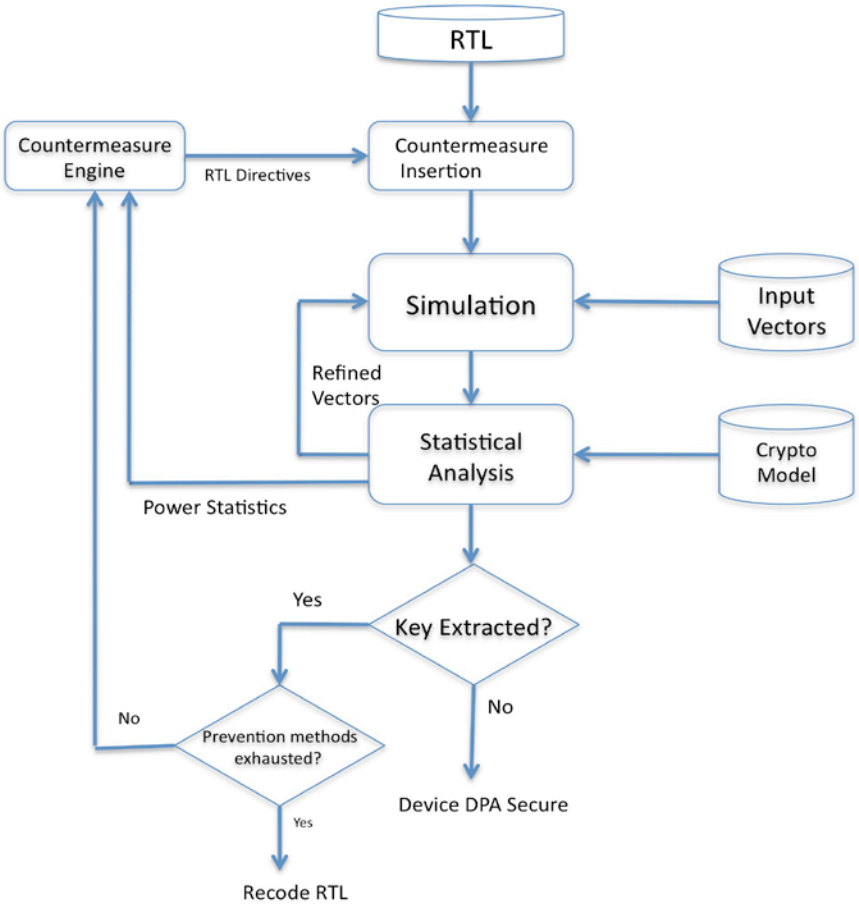
- Timing vs. SI
  - Timing = reduce RC delay
  - SI = reduce noise i.e. add cap
- BUT tools were available to make these tradeoffs
  - Timing analysis tools & SI analysis tools
  - Now integrated (SI-aware Timing & Placement)
- ASIC designers need DPA analysis and counter measure tools

The DPARTED

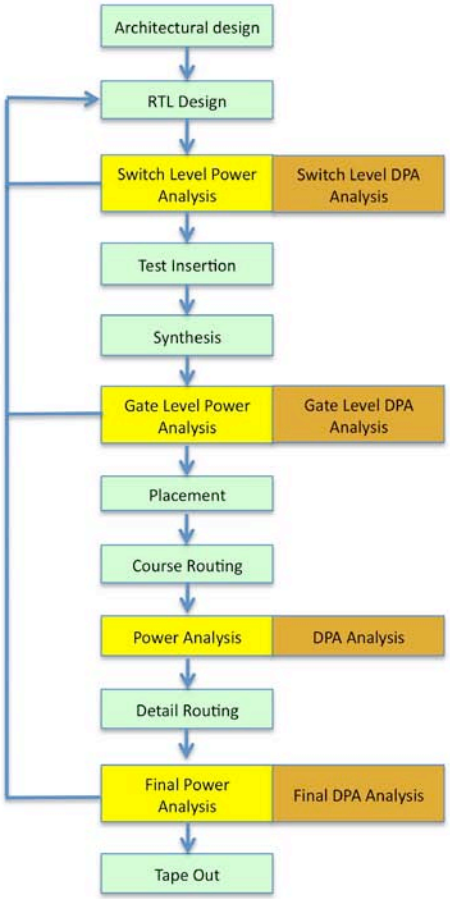
- DPA Resistant Tool for Electronic Design
- Being co-developed by Revere Security and Southern Methodist University

  - An EDA flow with built in DPA analysis and counter measures
    1) Flexible DPA analysis tool supporting varying levels of accuracy
    2) Enables counter measure insertion
    3) Standard tool flow

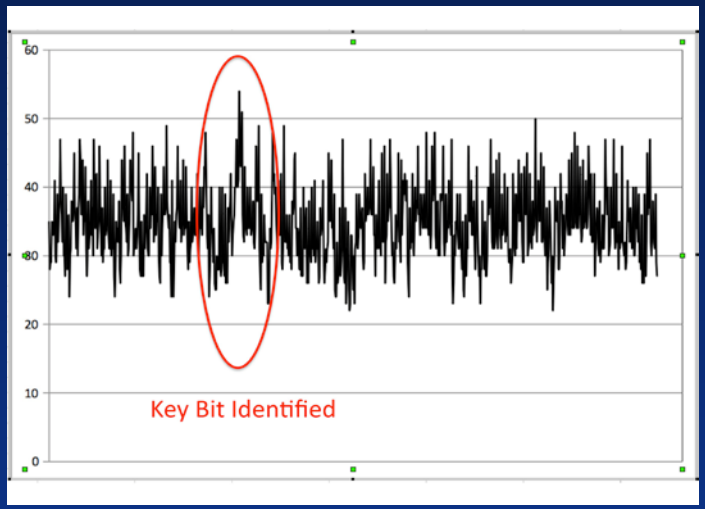
The DPARTED


RTL
Countermeasure Engine
RTL Directives
Countermeasure Insertion
Simulation
Input Vectors
Refined Vectors
Statistical Analysis
Crypto Model
Power Statistics
Yes
Key Extracted?
No
Device DPA Secure
No
Prevention methods exhausted?
Yes
Recode RTL

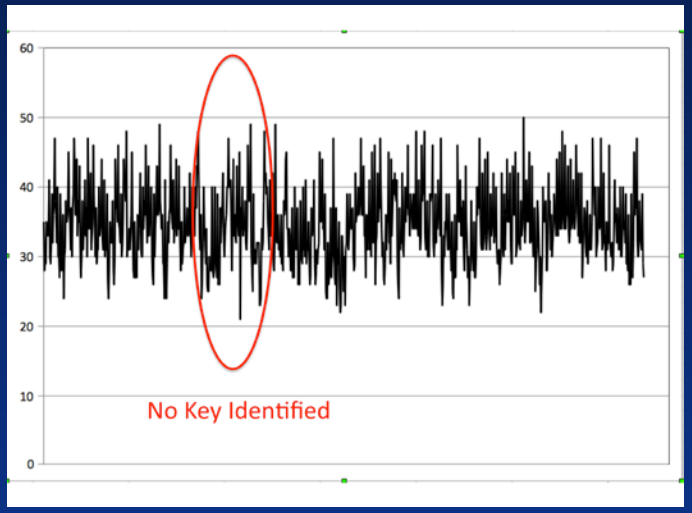
The DPARTED


Architectural design
RTL Design
Switch Level Power Analysis
Switch Level DPA Analysis
Test Insertion
Synthesis
Gate Level Power Analysis
Gate Level DPA Analysis
Placement
Course Routing
Power Analysis
DPA Analysis
Detail Routing
Final Power Analysis
Final DPA Analysis
Tape Out

The DPARTED



Hamming-Distance Analyses Before DPA Correction



Hamming-Distance Analyses After DPA Correction

Conclusions

- More and more sensitive information is being pushed to “edge” devices
- Adding security IP blocks alone does not make devices secure
- Side-channel attacks are very easy to perform and becoming very common place
- Designers need tools to help them make the right tradeoffs while implementing side-channel countermeasures
- Tools are in development at Revere Security and Southern Methodist University