Resource-efficient Cryptography against Physical Attacks

Elif Bilge Kavun

(University of Sheffield)

- Standard cryptography: DES, AES, RSA, etc.

- Lightweight cryptography – Resource-efficiency
  - Low-area, low-power, low-latency, …
  - HW/SW-oriented
  - Examples: PRESENT, PRINCE, PRIDE
  - Search for efficient building blocks

- Physical attacks
  - DPA, SPA, fault injection, etc.
  - Countermeasures required for algorithms: Costly

- Resource-efficient algorithms become costly again due to countermeasures

- Security by design
  - Design algorithms with attacks & countermeasures in mind
  - Feedback: Theory - HW/SW
  - Search for efficient and “secure” building blocks
  - Learnings from industry: Real-life problems
  - Existing work
    - SKINNY (Beierle et al)
    - Strong 8-bit Sboxes with Efficient Masking in HW (Boss et al, De Meyer et al)

- Security analysis
  - Mathematical attacks: Linear, differential, etc.
  - Side-channel attacks: Power attacks, timing attacks, etc.
  - Fault injection
  - Use deep-learning principles

- Tools
  - Synthesis flow & Power simulation flow
    - Area utilization and power consumption
  - FPGA
    - Secure and efficient layer search
    - Side-channel attacks: SASEBO board
    - Fault injection
  - Side-channel setup: Oscilloscope, probes, etc.
    - DPA, SPA

- Plan
  - First target: Symmetric crypto
  - Asymmetric crypto
  - Post-quantum crypto…