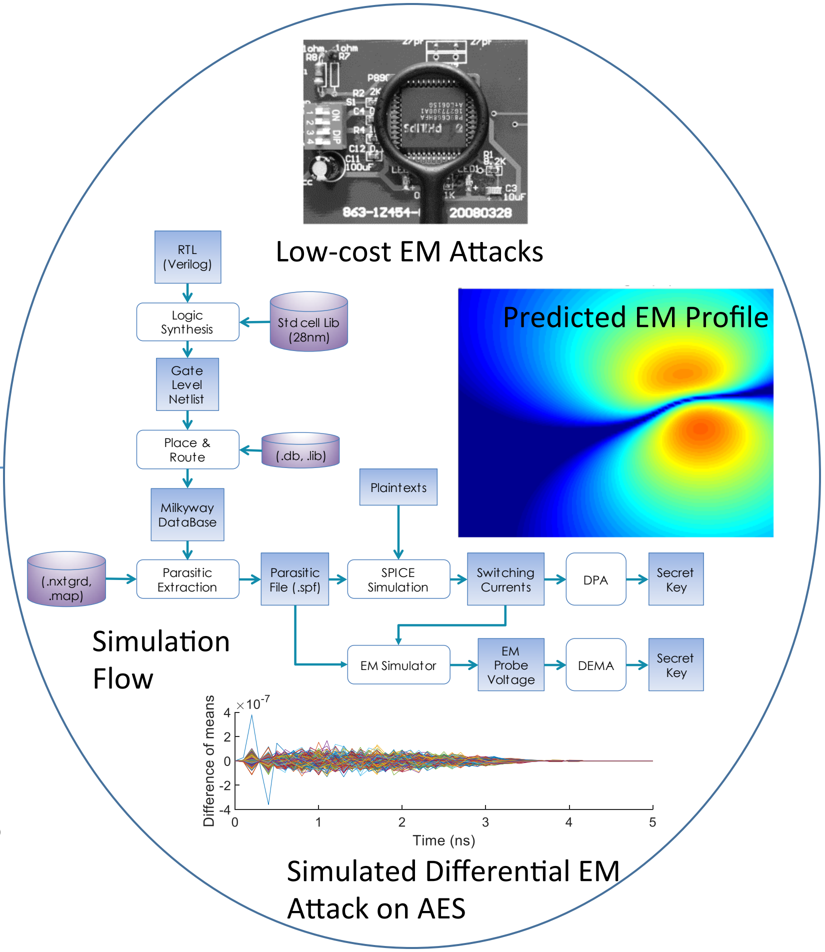
Simulation-Based Verification of EM Side-Channel Attack Resilience of Embedded Cryptographic System

Challenge:

- Electromagnetic (EM) side-channel can be easily exploited by attackers using low-cost measurement equipment
- More dangerous than the related power channel
- How to validate EM side-channel immunity before fabrication of cryptographic HW?

Solution:

- Simulation techniques and models for estimating information-carrying EM emissions
- Novel ways of dealing with computational complexity of security validation
- Customized EM simulators to capture emissions from complex interconnects



Low-cost EM Attacks

Predicted EM Profile

Simulation Flow

Simulated Differential EM Attack on AES

Scientific Impact:

- Efficiently relating crypto-algorithmic processes to EM information
- Methods to cope with simulation complexity with quantified accuracy-cost tradeoffs
- Efficiently modeling current space-time-shape properties

Broader Impact:

- Design-time validation of security is enabled
- Reduced cost of security certification
- Project is done in close interaction with industry: project co-sponsored by Semiconductor Research Corporation and its member companies

STARSS SaTC NSF-1527888; PIs: Michael Orshansky and Ali Yilmaz (University of Texas at Austin); Contact: Michael Orshansky (orshansky@utexas.edu)