Crypto is ubiquitous in today’s IT devices
• In smartphones for communication
• In hardware drives for storage
• In smartcards for authentication

How can these devices protect the secrets therein?
Attackers can often exfiltrate secret keys from devices!

A typical attack: differential power-analysis
Measure the power consumption during a crypto operation
Collect many traces and detect the consumption difference between processing a 0 or a 1 for each bit of the secret key.

The Threshold Implementation approach
• Share each secret-input bit into several random bits
• Probing any wire or tile will only reveal random bits

Protecting AES in hardware is of utmost importance!
AES is the Advanced Encryption Standard … pervasive in crypto circuits.

Two main categories of attacks:
• Leakage: derive secrets from side-channels
• Fault injection: interfere with the computation

Engaging with the community
Our positioning of the problem (NISTIR 8214A) led to a workshop (organized by KU-Leuven) focused on single-device threshold AES:

Online Workshop on Threshold Schemes for NIST-approved Symmetric Block Ciphers in a Single-Device Setting — July 7–9, 2020

Key take-aways / questions:
• Big differentiation between leakage-only and combined attacks
• What protective schemes are really relevant to the industry?
• Benchmarking is needed (how many traces to break a protection?)
• Need verification tools to check correctness of threshold design

Our approach to standardization
• Devise two reference attack models for evaluation of proposals
• Develop threshold guidelines with potential to improve best-practices
• Integrate proposed techniques in the crypto validation pipeline

Contact: threshold-crypto@nist.gov
TC forum: https://csrc.nist.gov/tc-forum
Webpage: https://csrc.nist.gov/Projects/Threshold-Cryptography
Poster produced for the NIST-ITL Virtual Science Day 2020 (October 29)