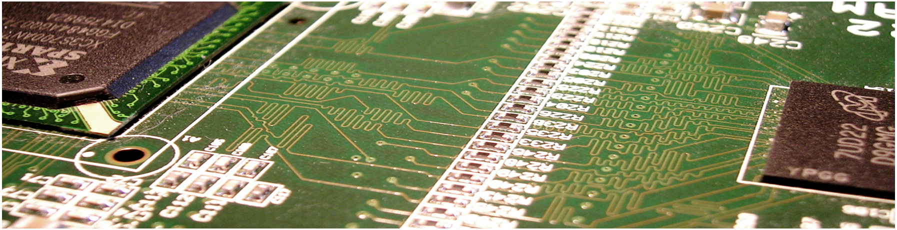
High-Precision Hardware Attacks - Crypto under High-Precision Laser Fire and EM Eavesdropping

Johann Heyszl, Head of Hardware Security Department
Fraunhofer-Institute for Applied and Integrated Security | FhG AISEC

29th September 2017

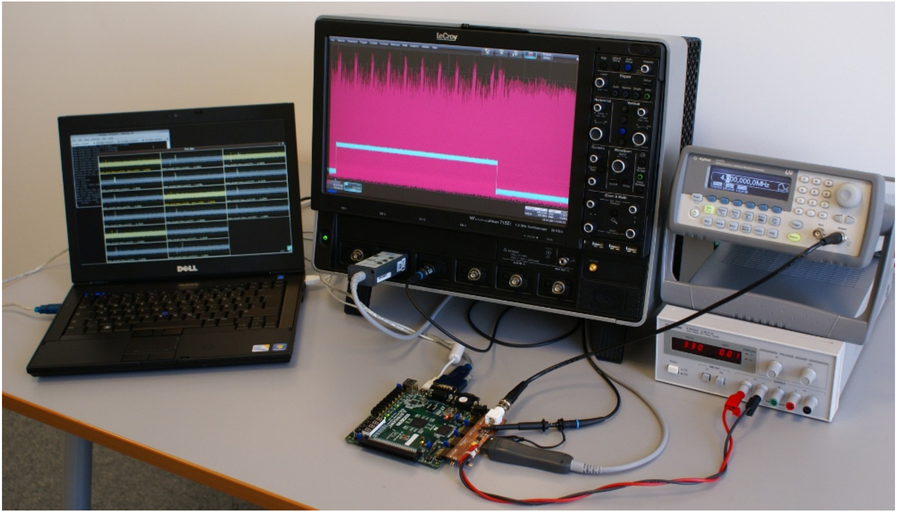
Fraunhofer
AISEC

High precision is invasive*

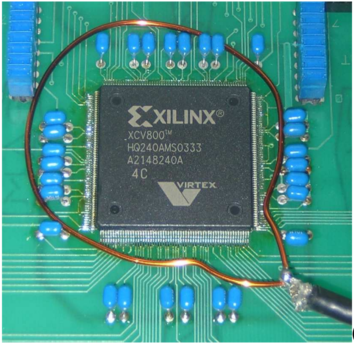


*Except for: Anceau et al., Nanofocused X-Ray Beam To Reprogram Secure Circuits, CHES 2017 :)

Low-Precision Power Measurements

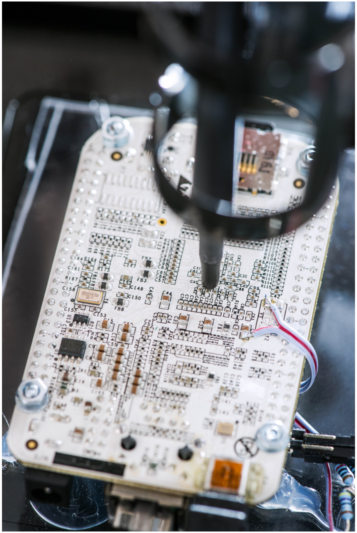


Low(est)-Precision Electromagnetic Field Measurements

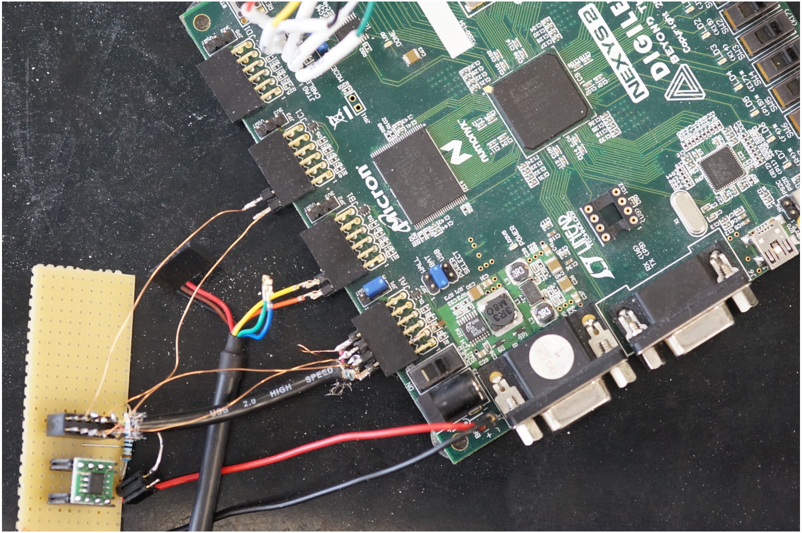


(from De Mulder et al., 2007)

Low-Precision Electromagnetic Field Measurements

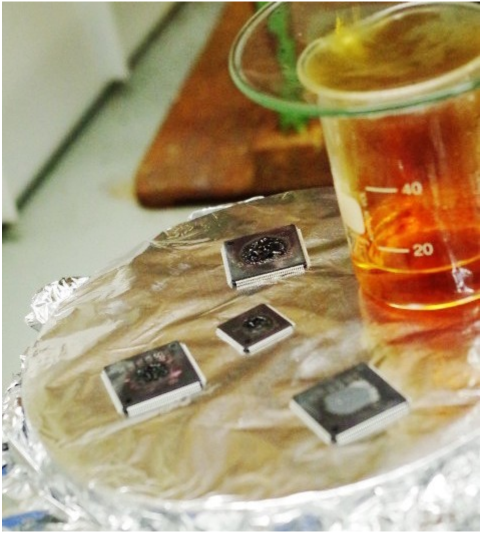


Low-Precision Fault Injection - Glitching



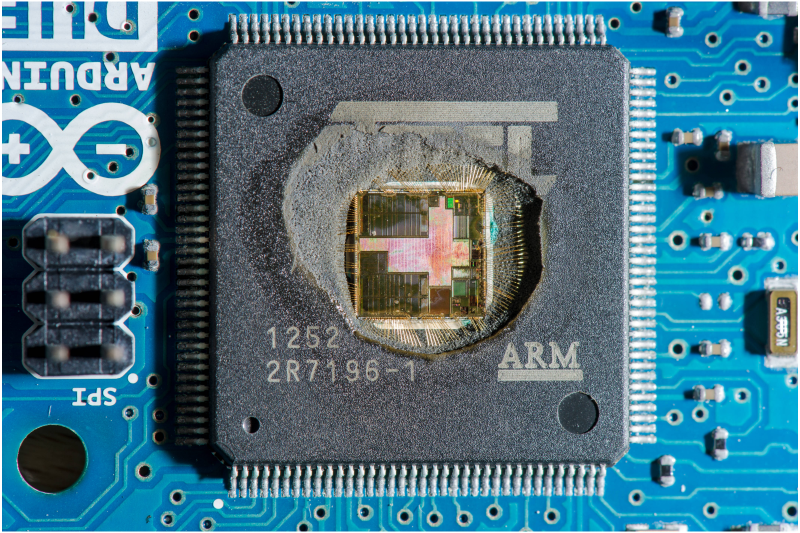
Fraunhofer AISEC

Chip Invasion - Decapsulation

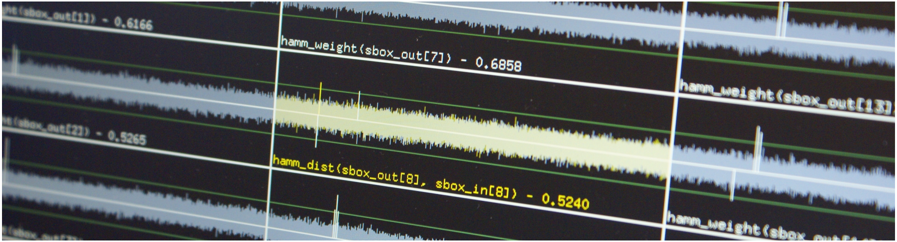


Fraunhofer
AISEC

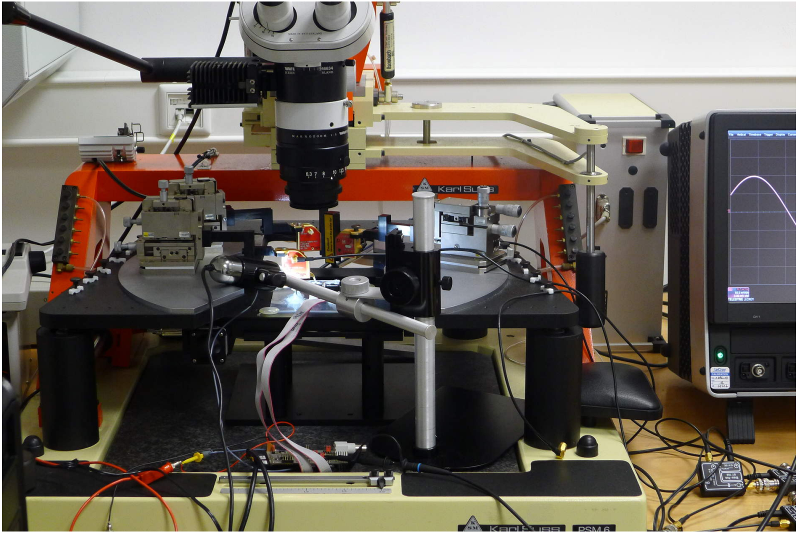
Chip Invasion - Decapsulation



High-Precision EM Side-Channel Analysis

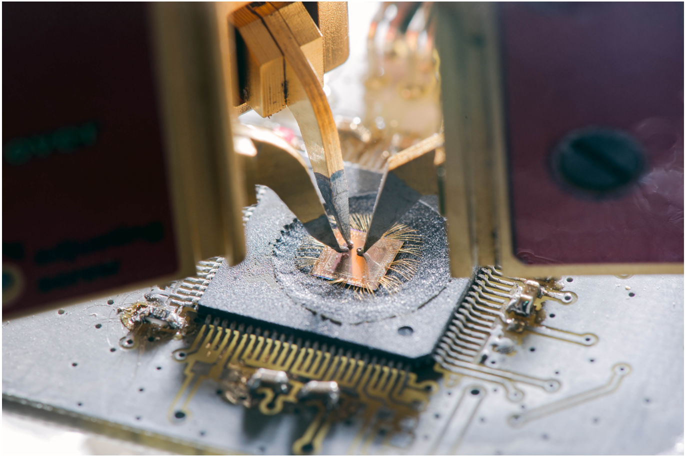


Measurement Setups for High-Precision EM SCA



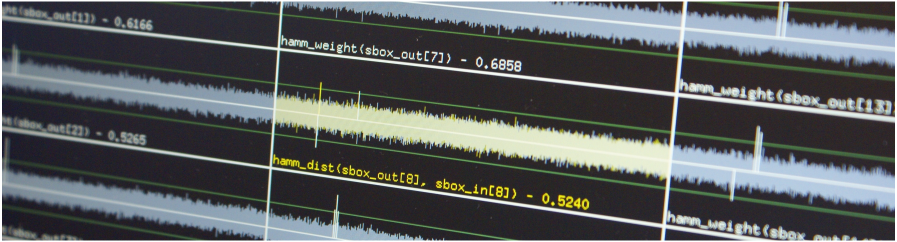
Fraunhofer
AISEC

Measurement Setups for High-Precision EM SCA



- Best-case measurement setup for worst-case high-security evaluation

Asymmetric Cryptography

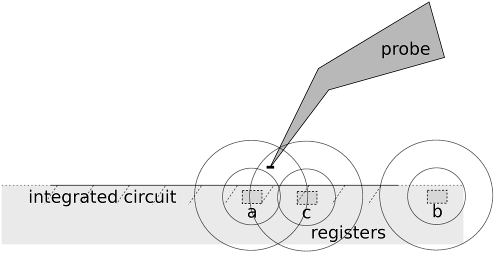


Exponentiation Algorithms

CT-RSA 2012*

- Example **pseudo**-algorithm: **Input:** Secret $d = d_D d_{D-1} \ldots d_2 d_1$ with $d_i \in \{0, 1\}$

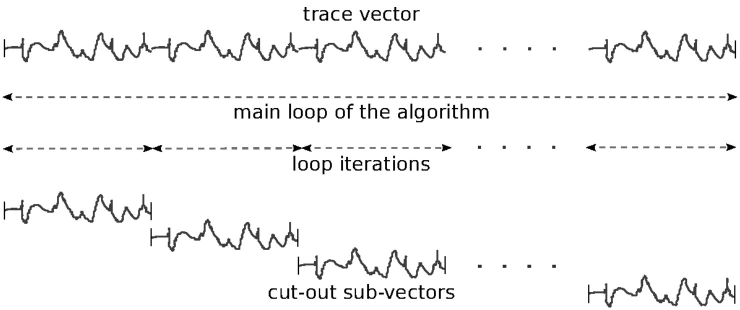
for $i = D$ downto 1 **do**
  if $d_i = 1$ **then**
    $c \leftarrow c^2 + a$
    $a \leftarrow c$
  else
    $c \leftarrow c^2 + b$
    $b \leftarrow c$
  end if
end for



- Usual countermeasures: Constant time (e.g. Montgomery), randomized coordinates
- Single execution leakage: E.g. Leakage from locations

- *Heyszl, Mangard, Heinz, Stumpf, Sigl, 'Localized Electromagnetic Analysis of Cryptographic Implementations', CT-RSA 2012

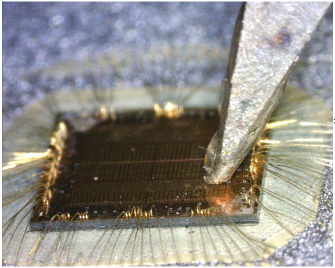
Horizontal Attacks
CT-RSA 2012*

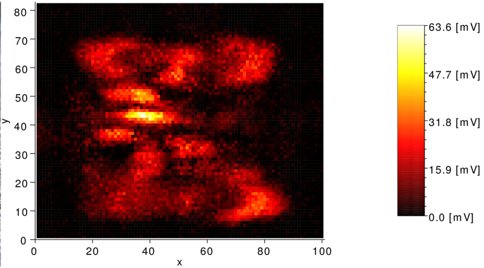


- Single-trace attack, e.g. EC scalar multiplication in ECDSA

- *Heyszl, Mangard, Heinz, Stumpf, Sigl, 'Localized Electromagnetic Analysis of Cryptographic Implementations', CT-RSA 2012

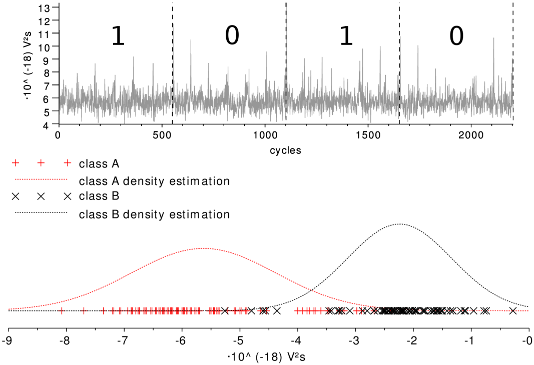
Profiled Attack
CT-RSA 2012*





- Xilinx Spartan 3A 90 nm
- Scan of surface, profiling, use best position with highest difference btw. 0 and 1
- Template attack successful - Exploiting single-execution leakage
- *Heyszl, Mangard, Heinz, Stumpf, Sigl, 'Localized Electromagnetic Analysis of Cryptographic Implementations', CT-RSA 2012

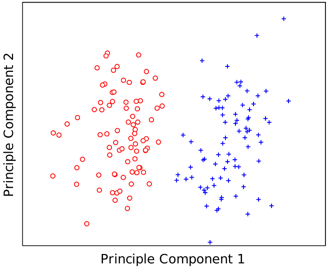
Attack w/o Profiling - Clustering-Based
CARDIS 2013*

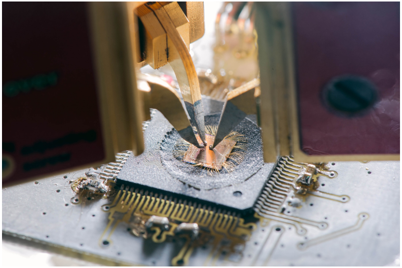


- No profiling → First horizontal attack based on unsupervised cluster classification
- Non-heuristic / state-of-art in pattern classification: e.g. k-means, Euclidean distance (contrary to hor. cross-corr. / Big Mac)
- Remaining entropy at some pos. (posterior prob. for enumeration) $\approx 2^{22} - 2^{37}$
- *Heyszl, Ibing, Mangard, De Santis, Sigl, 'Clustering Algorithms for Non-profiled Single-Execution Attacks on Exponentiations', CARDIS 2013

Multiple Probes

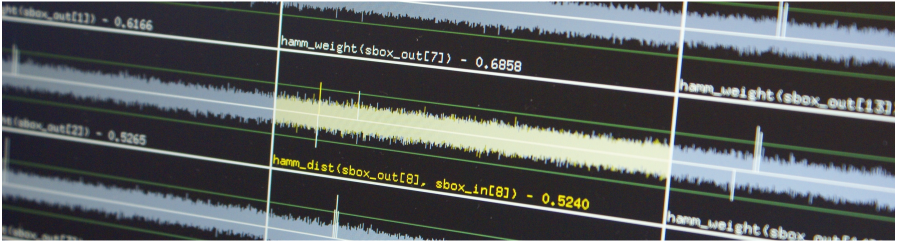
COSADE 2015*





- Improved algorithms: PCA for dim. reduction, expectation-maximization alg.
- PCA: most leakage in components e.g. 5 to 7, no leakage after 20
- Remaining entropy at some pos. (posterior prob. for enumeration) $\approx 2^0$
- Combining leakage of multiple probes: Better success probability from mult. locations, but quality 'better' only profiled - Helpful if single-shot attack with insufficient SNR
- *Specht, Heyszl, Kleinsteuber, Sigl, 'Improving Non-profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-channel High-Resolution EM Measurements', COSADE 2015

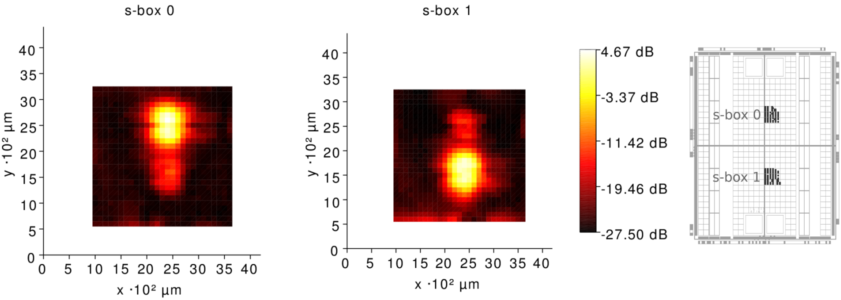
Symmetric Crypto



Fraunhofer AISEC

S-Box SNR

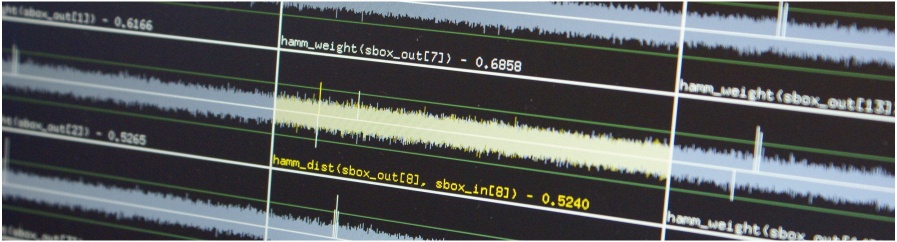
CARDIS 2012*



- Localized signal leakage: (1) Higher SNR (e.g. $\approx +4dB$), (2) two s-boxes distinctively
- 90 nm Xilinx Spartan-3A
- *Heyszl, Merli, Heinz, De Santis, Sigl, 'Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis', CARDIS 2012
- About probe size, positioning, distance, etc. also Specht, Heyszl, Sigl, 'Investigating measurement methods for high-resolution electromagnetic field side-channel analysis', ISIC 2014

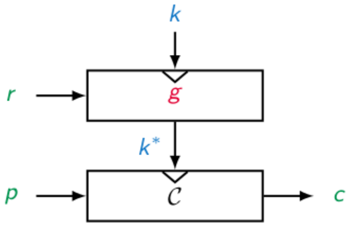
Fraunhofer AISEC

Symmetric Crypto | Leakage Resilience



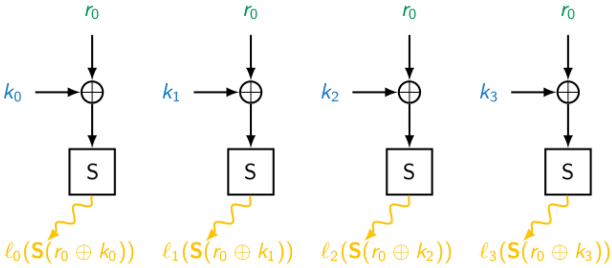
Fraunhofer AISEC

Leakage-Resilience
Re-Keying



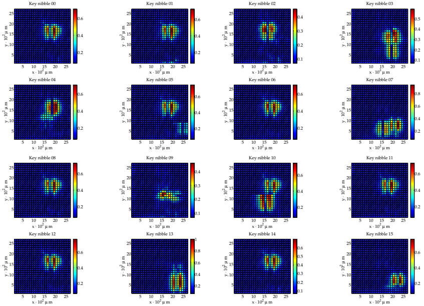
- Change key in every operation to limit leakage of one key
- Prevent attacker to accumulate traces for DPA
- Medwed et al. CHES 2012 (highly influencial): Leakage-resilient pseudo-random functions

Leakage-Resilience
Pseudo-Random Function



- Two main goals:
  1. Noise through parallel s-boxes (correlated because equal inputs)
  2. Limit data complexity (number of different traces for DPA)

Leakage-Resilient PRFs
PROOFS 2013, JCE 2014*



- Evaluation of PRF construction parameters:
  32 parallel PRESENT s-boxes. 2^4 data-complexity 2^4
- High-precision measurements, univariate profiled CPA
- S-boxes partly distinguished, reduced to $> 2^{80}$ after attack. OK, but threatening
- *Belaïd, De Santis, Heyszl, Mangard, Medwed, Schmidt, Standaert, Tillich, 'Towards fresh re-keying with leakage-resilient PRFs: cipher design principles and analysis', JCE 2014

Fraunhofer AISEC

Leakage-Resilience
COSADE 2017*

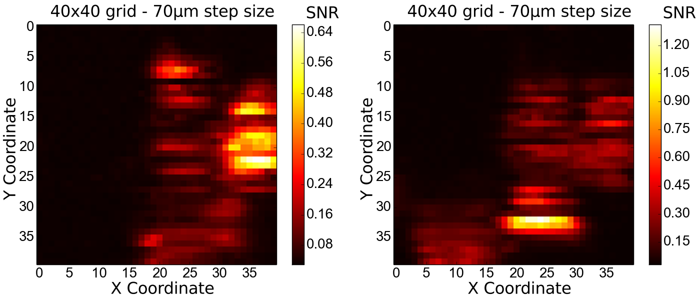
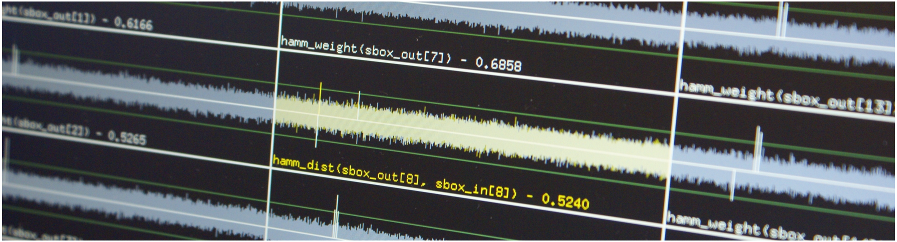


Figure: S-box 0 left, S-box 1 right

- New evaluation of PRF construction: 16 parallel AES s-boxes, minimal data complexity **2**
- Multivariate profiled CPA: High SNRs of individual s-boxes on Xilinx Spartan-6 45 nm
- Reduces entropy to 2^0 $\rightarrow$ Working on fix currently
- *Unterstein, Heyszl, De Santis, Specht, 'Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks', COSADE 2017

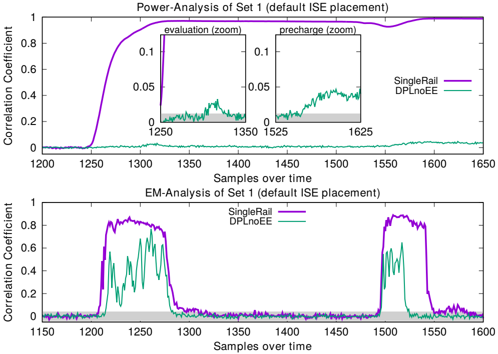
Fraunhofer AISEC

Symmetric Crypto | Dual-Rail Countermeasure



Fraunhofer AISEC

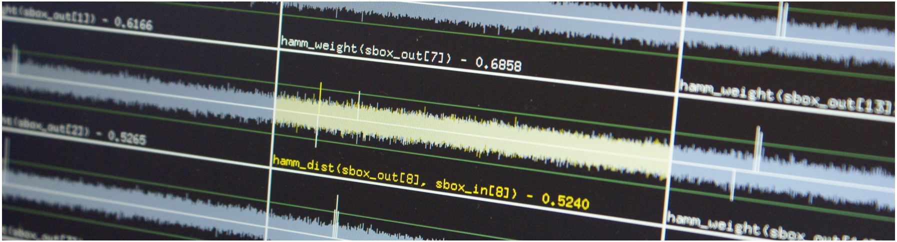
High-Resolution EM vs. Dual Rail Precharge Logic
CHES 2017*



- Latest DRP logic (FPGA) on Xilinx Spartan 6 (45 nm) (placement controlled, routing aut.)
- Power analisis: Security gain 425. Helpful. Similar with **3 mm** probe
- High-resolution EM: Security gain only 1.34 → Not helpful
- *Immler, Specht, Unterstein, 'Your Rails Cannot Hide from Localized EM: How Dual-Rail Logic Fails on FPGAs', CHES 2017

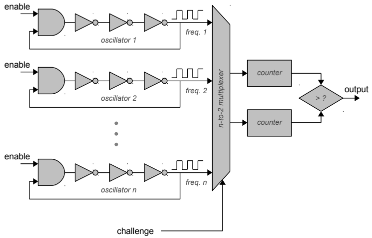
Fraunhofer AISEC

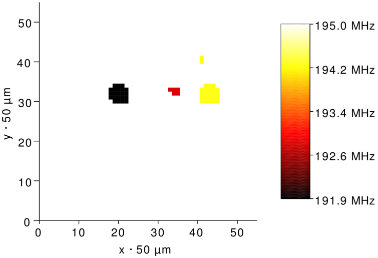
PUFs



Fraunhofer
AISEC

Attacking RO-PUFs
HOST 2013*

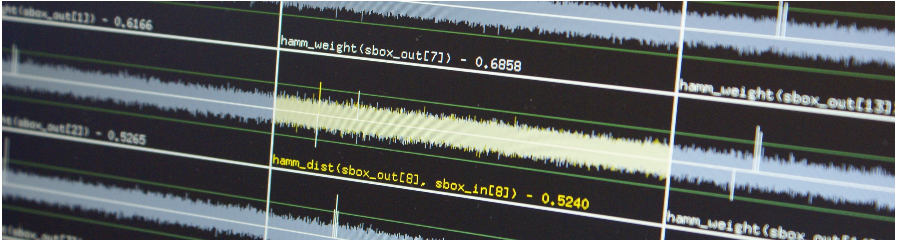




- Every RO assigned to one counter for comparison
- Attacker measures *RO frequency and sequence / counter assignement*
- Full characterization means full break

- *Merli, Heyszl, Heinz, Schuster, Stumpf, Sigl, 'Localized electromagnetic analysis of RO PUFs', HOST 2013

Protection?


hamm_weight(sbox_out[7]) - 0.6858
hamm_dist(sbox_out[8], sbox_in[8]) - 0.5240
0.6166
0.5265

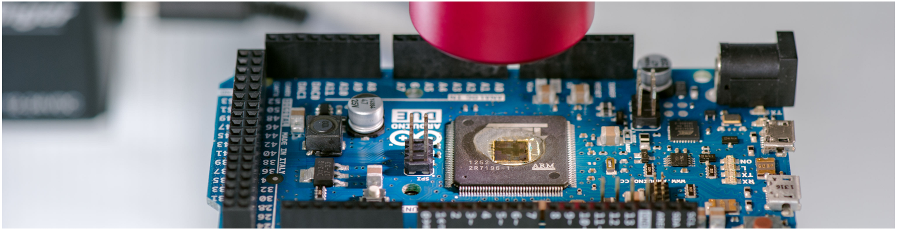
Protection

High-Precision EM Side-Channel Analysis

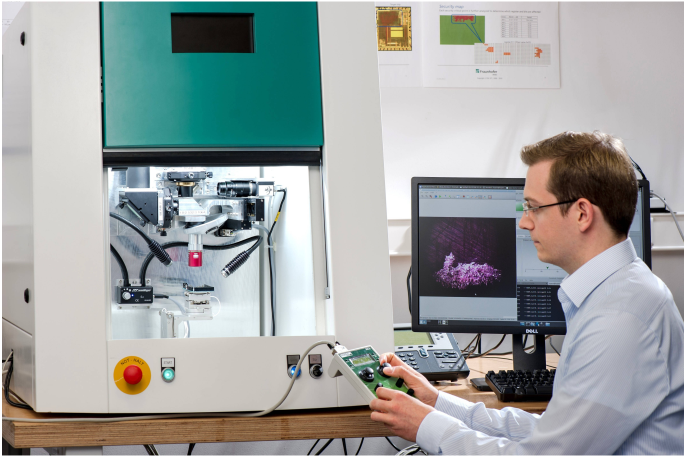
- High-precision leads to higher SNR (e.g. when PA fails)
- But requires finding a position (difficult under real-world circumstances)

- Conventional countermeasures (masking, time-based hiding, ..)
- EM sensor to detect equipment (ask Naofumi Homma)
- Dedicated to localized EM: location-randomization

High-Precision Laser Fault Injection



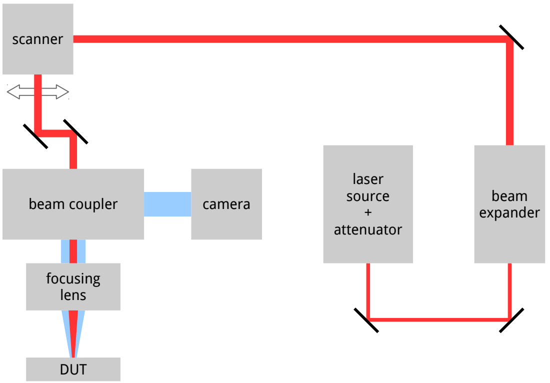
Laser-Based Fault Injection



- High-precision setup allows systematic evaluation

Fraunhofer
AISEC

Laser-Based Fault Injection

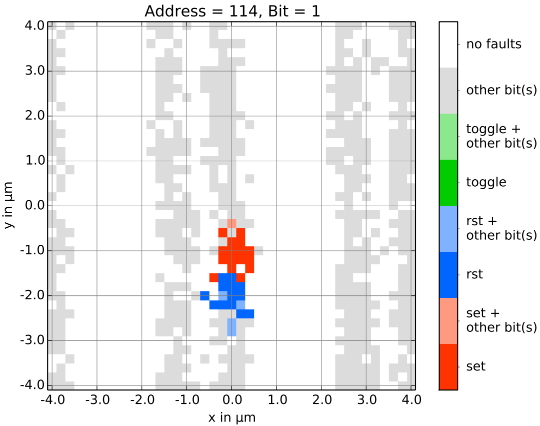


- **2×** infrared (**1064 nm**) laser with **800 ps** pulse length
- Beams independently positionable by laser scanners
- **4 µm** spot size

Fraunhofer AISEC

LFI Precision against 90 nm FPGAs

CARDIS 2015*

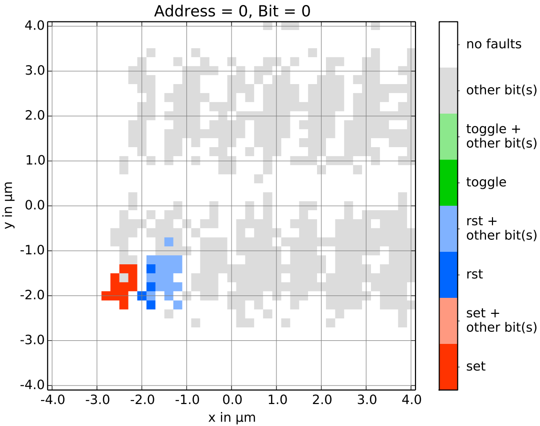


- Manipulates single bits (set to 0 or 1) in BRAM of 90 nm Xilinx Spartan-3A
- *B. Selmke, S. Brummer, J. Heyszl, G. Sigl, 'Precise laser fault injections into 90 nm and 45 nm SRAM-cells', CARDIS 2015

Fraunhofer AISEC

LFI Precision against 45 nm FPGAs

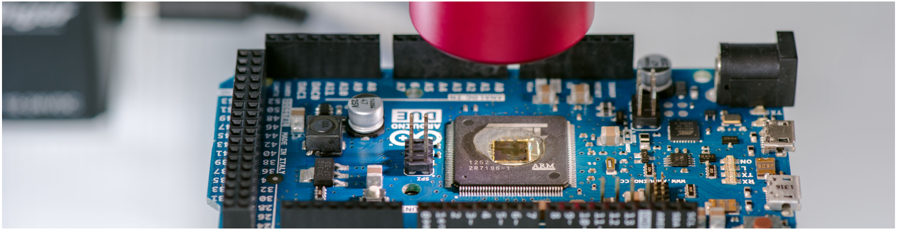
CARDIS 2015*



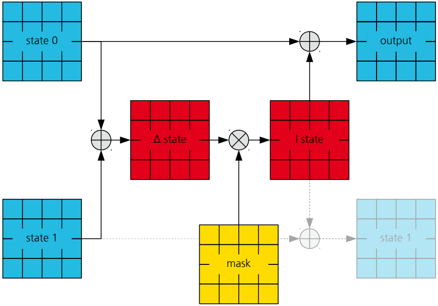
- Manipulates single bits (set to 0 or 1) in BRAM of 45 nm Xilinx Spartan-6
- *B. Selmke, S. Brummer, J. Heyszl, G. Sigl, 'Precise laser fault injections into 90 nm and 45 nm SRAM-cells', CARDIS 2015

Fraunhofer AISEC

High-Precision Dual-Beam LFI | Redundand AES



Dual Laser against Duplication Countermeasures
FDTC 2016*

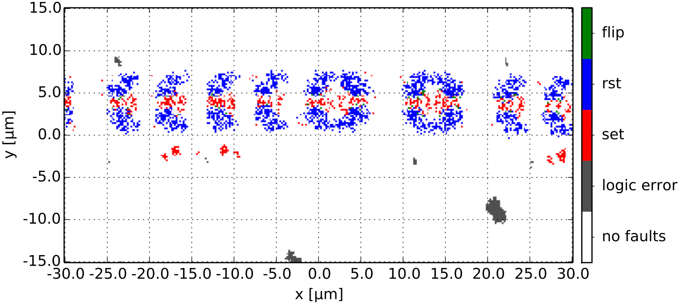


- Double redundancy + infection Scheme
- *B. Selmke, J. Heyszl, G. Sigl, 'Attack on a DFA Protected AES by Simultaneous Laser Fault Injections', FDTC 2016

Fraunhofer AISEC

Dual Laser against Duplication Countermeasures

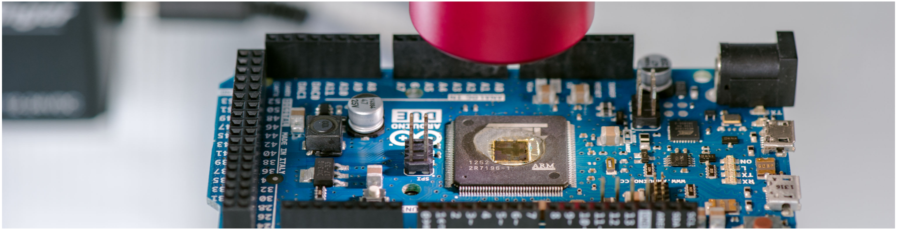
FDTC 2016*



- 45 nm Xilinx Spartan-6 (48 MHz); Dual beam laser
- Inject two equal faults into AES-state in round 7 of two FF-based designs
- Single successful FI is sufficient for DFA (time to success: ≈ **5**min)
- *B. Selmke, J. Heyszl, G. Sigl, 'Attack on a DFA Protected AES by Simultaneous Laser Fault Injections', FDTC 2016

Fraunhofer AISEC

Protection?



Fraunhofer
AISEC

Protection
High-Precision Laser Fault Injection

- High-precision is hurtful
- But precise locations must be found $\rightarrow$ Reverse-engineering is difficult
- But timing of LFI is critical $\rightarrow$ Time-jitter by construction is very effective

- Conventional countermeasures (redundancy e.g. parity / coding, laser-light sensors, jitter)

Fraunhofer AISEC

Conclusion

- What to do? Provable security possible?
- Laser fault injection
  - Fault model device-dependent / technology dependent, but precise!
  - Fault model $\approx$ equals worst case, quantifiable
  - Simulation / emulation of faults possible without LFI testing
  - Guarantees at design time (exhaustive emulation difficult however)
- EM side-channel
  - Very noisy, e.g. not possible to detect specific values
  - Attack success depends on available SNR
  - SNR extremely hard to predict in case of magnetic fields :(
- High-precision attacks are mostly relevant for protected devices
- Simple non-invasive FA (glitching, EM FI) an PA for regular IoT devices

Contact Information

Dr.-Ing. Johann Heyszl

Hardware Security Department

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Parkring 4
85748 Garching (near Munich)
Germany
Internet: http://www.aisec.fraunhofer.de

Phone: +49 89 3229986-172
Fax: +49 89 3229986-299
E-Mail: johann.heyszl@aisec.fraunhofer.de

Fraunhofer
AISEC