Current State of High-Precision EM Side-Channel Attacks and Implications on FPGA-Based Systems

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

16th November 2017
About Side-Channel Precision ...
Very Low-Precision Electromagnetic Field Measurements

Figure: De Mulder et al., 2007
Low-Precision Electromagnetic Field Measurements

- Recover Linux filesystem encryption key (AES) on a BeagleBone (500 MHz ARM Cortex)
- Coil diameters of 0.5 mm - 2.5 mm, bandwidth: $\approx 250 \text{MHz}$
Higher Precision Requires Invasion - Decapsulation

© Fraunhofer
Higher Precision Requires Invasion - Decapsulation
High-Precision EM Side-Channel Analysis
Measurement Setup for High-Precision EM SCA

- Best-case measurement setup for worst-case high-security evaluation
- Coil diameter: 0.1 mm - 0.25 mm, bandwidth: 3 GHz
Measurement Setup for High-Precision EM SCA
Measurement Setup for High-Precision EM SCA
Setup Details

- High resolution in location and time
  - Circuit parts instead of entire circuit (but no single gates / FFs!)
  - Less parasitics (low-pass filtering) for higher time-resolution
  - But: Smaller coils means less magnetic flux, more amplification, more noise

- Coil diameter: \(100 \mu m - 250 \mu m\), bandwidth: 3 GHz
- Amplification: 2 x 30 dB
- Oscilloscope: 1.5 GS/s minimum, 5 GS/s mostly; 2.5 GHz bandwidth; (8 bit resolution)
- (No EM shielding box)
Measurement Setup for High-Precision EM SCA

Setup Details

- Horizontal coil orientation
- Front-side measurement (because backside substrate leads to low signal e.g. -19 dB)
- Move coil over decapsulated die surface in x-y-grid
- Distance to surface: \(\approx 10 - 30 \mu m\) (touch down and lift slightly)
- Positioning of coil: \(\approx 0.5 \mu m\) resolution
- Time / memory depends on case: e.g. 4 days for \(40 \times 40\) grid, \(70 \mu m\) step size, 10k traces at 1600 positions total 33 GBytes, then e.g. 500k traces at \(\approx 10\) selected locations
Asymmetric Cryptography
Exponentiation Algorithms
CT-RSA 2012*

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

1: for \( i = D \) downto 1 do
2: if \( d_i = 1 \) then
3: \( c \leftarrow c^2 + a \)
4: \( a \leftarrow c \)
5: else
6: \( c \leftarrow c^2 + b \)
7: \( b \leftarrow c \)
8: end if
9: end for

Usual countermeasures: Constant time (e.g. Montgomery), randomized coordinates

Can be attacked using single traces (‘horizontal attacks’)

Single execution leakage: E.g. leakage from locations

Horizontal Attacks

CT-RSA 2012*

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

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

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 positions (posterior prob. for enumeration) ≈ $2^{22} - 2^{37}$
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 positions (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
Localized signal leakage: (1) Higher SNR (e.g. $\approx +4\text{dB}$), (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
- At position over s-box 1: mean and std dev above, extracted signal of s-box 1 below
- Time-precision: Detected leakage during time as short as critical path ($\approx 10\text{ns}$)
- *Heyszl, Merli, Heinz, De Santis, Sigl, ‘Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis’, CARDIS 2012
Latest DRP logic (FPGA) on Xilinx Spartan 6 (45 nm) (placement controlled, routing aut.)

- Power analysis: 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
Symmetric Crypto | Leakage Resilience
Leakage-Resilience

Re-Keying

- Goal is to prevent DPA (!)
- Alternative approach to more conventional masking or hiding

- Change key in every block-cipher execution
  - Even if attacker gets some leakage on one key, useless for next cipher execution
  - Prevent accumulating traces for DPA!
  - Change key by ‘mixing’ it completely (e.g. update through block cipher)

- Algorithmic level countermeasures - depends on application / protocoll:
  - Live authentication: Fresh random numbers (on both sides) can be chosen to generate new session key (e.g. CIPURSE)
  - If both sides synchronized, updated key can be overwritten synchronously (stateful)
  - But we are interested in stateless case!
Leakage-Resilience
Re-Keying

- FPGA receiving encrypted bitstreams:
  - We are looking into this application since years!
  - Must be decrypted from same longterm key always!
  - Bitstream cannot change (no fresh random numbers, no storing updated keys)
  - Attacker may even restart decryption to average noise!
  - How to have a longterm key and change it?

- Standaert et al. 2009, Medwed et al. CHES 2012: Leakage-resilient Pseudo-Random Functions (PRFs)
- (Other proposal: Sponge-based ‘ISAP’ from TU GRAZ Debraunig et al. FSE 2017)
Leakage-Resilience
Pseudo-Random Function

- Medwed et al. CHES 2012 based on GGM (Goldreich, Goldwasser, Micali) tree

This is how to get from longterm key $k$ to updated key $\text{PRF}_k(\text{IV})$ using an IV:

- Attacker even allowed to make device repeat this (e.g. average-out noise)
- But: In every layer, only two different inputs $p_0$ or $p_1$
- Very interesting about this: No random numbers required! No masking with all its pitfalls!
Leakage-Resilience
Two Main Concepts in Medwed/Standaert Direction

- Additionally, algorithmic noise from parallel S-Boxes which cannot be averaged-out
- No divide-and-conquer if input to all s-boxes equal (carefully chosen inputs)

Summary of Medwed/Standaert et al. direction:

1. Algorithmic noise through parallel s-boxes
   (correlated because equal inputs; no averaging this out)
2. Limited data complexity (number of different traces for DPA)
Evaluation of PRF construction parameters:
32 parallel PRESENT s-boxes. $2^4$ data-complexity

High-precision EM 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
Leakage-Resilience

- Based on this, we wanted to make it work ... But unsuccessful (see COSADE 2017 later)

- Then, Medwed et al. ASIACRYPT 2016:
  - Use unknown inputs $p_x$ instead of $p_0$ and $p_1$ in GGM tree PRF
  - Improves security of tree: Inputs unknown, DPA impossible
  - AES-based, so 16 s-boxes, data-complexities $\geq 2$ in tree for increased performance
  - But unknown inputs must be derived somehow
  - Medwed et al. use PRG with (1) parallelism noise and (2) input limit 2 again ...

- They target ASICs, where s-boxes are closely packed (should work better)
- We looked into it again on FPGAs ...

Leakage-Resilience
COSADE 2017*

- New evaluation of PRF construction: 16 parallel AES s-boxes, minimal data complexity 2
- Multivariate profiled CPA incl. LDA: High SNRs of s-boxes on Xilinx Spartan-6 45 nm
- Reduces entropy to $2^{48}$ - not enough → Working on fixing currently (under review)
- *Unterstein, Heyszl, De Santis, Specht, ‘Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks’, COSADE 2017

Figure: S-box 0 left, S-box 1 right
PUFs
Attacking RO-PUFs
HOST 2013*

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

High resolution in the real world
■ High-precision leads to higher SNR, but at which measurement position?

■ **Finding position is very difficult under real-world circumstances!**
  - Looking for high signal strengths only helpful when exact time of execution known
  - (SNR computation or correlation-based leakage tests require many, aligned traces)

■ **But also time-alignement of traces w/o trigger difficult!**
  - All discussed results used perfect alignement from trigger and synchronized scope
  - E.g. align on significant peaks and hope that attacked part is near to such a peak
  - Different coils lead to different ‘looking’ signals (e.g. different alignement peaks)

■ Combination of misalignement and unknown positions is very demanding in practice!
Prediction and Modelling?

Is there a reasonable way of predicting leakage from high-precision EM (or position)?

- Data-dependent currents through different layers. Very DUT and technology-specific!
- Even after fully completed backend design (P&R etc.) difficult to predict exactly (opinion)
- Electric modelling in SPICE seems infeasible: Slow even for few transistors, but digital designs have e.g. $10^3 - 10^6$ ...

Open question

Figure: Left: Chipworks, TSMC 28 nm, Xilinx Kintex-7
Protection?

Real-world:
- For many e.g. IoT devices, chip decapsulation is not realistic
- Conventional countermeasures such as time-based hiding increase difficulty massively
- Prevent trace patterns that can be used for alignment
- Dedicated to location-based leakage (e.g. ECC): location-randomization

Research-world:
- We still work on leakage resilience :)
- EM sensor to detect equipment (Homma et al. CHES 2014)
Conclusion

- High-precision EM is very powerful, especially against FPGAs
- Not always ‘easy’ to perform, requires expensive setup and automation
- Currently, high-precision EM measurements seem required to assess security level
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