Attack on DFA protected AES by Simultaneous Laser Fault Injections

Bodo Selmke[a], Johann Heyszl[a], Georg Sigl[b], 08/16/2016

[a]Fraunhofer Institue AISEC
[b]Technische Universität München

Fraunhofer
AISEC

- Laser Fault Injection
- Protected Hardware Implementation
- Symmetric algorithm (AES)

FA Countermeasures

1. Direct detection by specialized sensors
2. Handling of faults with various forms of redundancy (Time, Space)

Detection	Raise an alarm (interrupt signal) $\rightarrow$ Discard output of faulty ciphertext
Infection	Transform ("infect") ciphertext $\rightarrow$ Render analysis of output by DFA impossible

Our practical Investigation

Demonstrate successful attack against AES with duplication-based countermeasure using two simultaneous laser shots

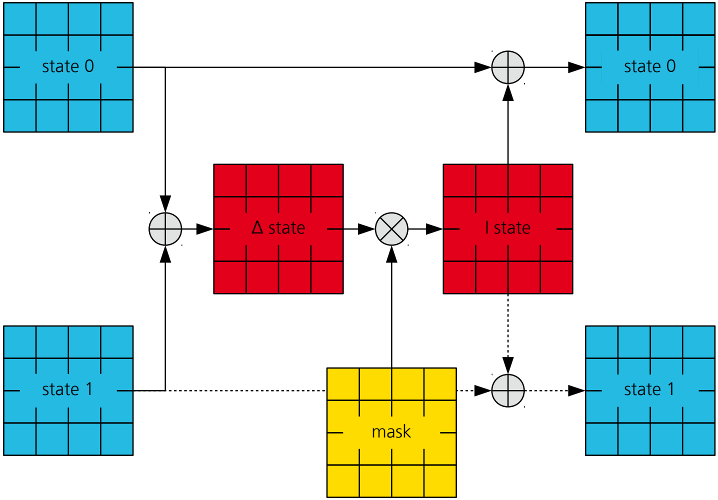
- AES on FPGA
- Protection by a countermeasure based on hardware duplication
- Determine locations for Laser Fault Injection
  $\rightarrow$ AES state registers
- Carry out Fault Injections into AES
- Apply DFA on record of output data
  $\rightarrow$ Determine if attack is feasible (We used the DFA by Saha et al.)

Redundant AES Design
Features

AES core

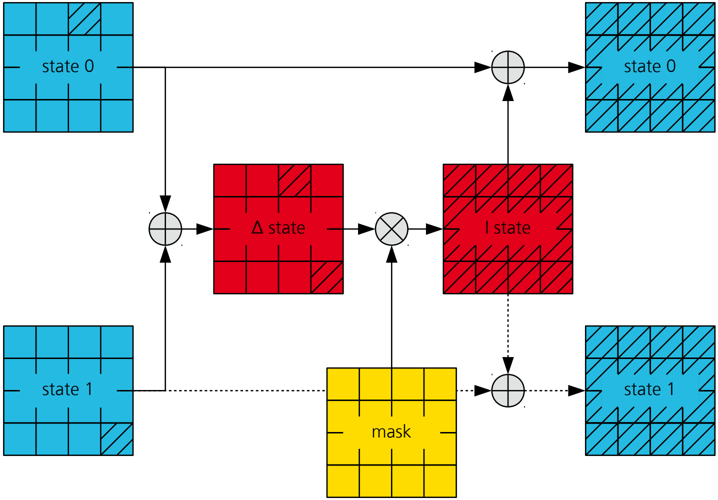
- 2 AES instances, one clock cycle per round
- Infection Countermeasure based on the design by Lomné et al.
- **48 MHz** clock frequency

Redundant AES Design
Infection Scheme



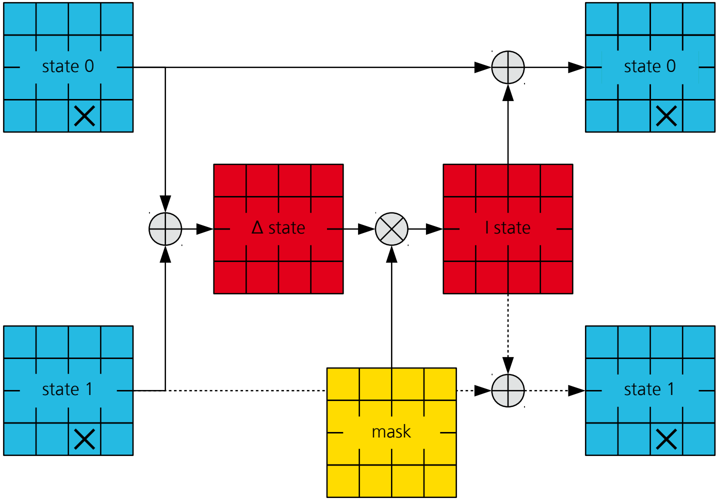
Fraunhofer AISEC

Redundant AES Design
Infection Scheme



Redundant AES Design

Infection Scheme



Fraunhofer AISEC

Redundant AES Design
Features cont'd

AES core

- 2 AES instances, one clock cycle per round
- Infection Countermeasure based on the design by Lomné et al.
- 48 MHz clock frequency

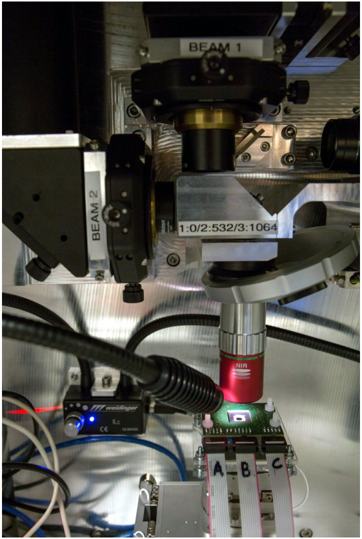
Generation of Trigger Signal

- Implemented on FPGA
- Adjustable delay counters, initiated with the start-signal of the AES

Device Under Test

- Xilinx Spartan-6 FPGA
- 45 nm feature size

Used Laser System



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

Fraunhofer AISEC

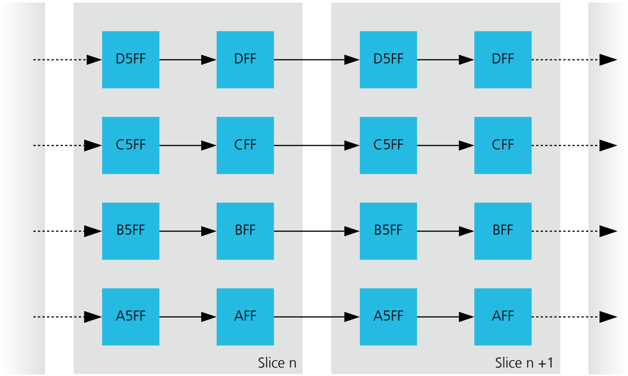
Preliminary Investigation
Locating the AES State Registers

- Attack requires knowledge of register location
- Use of dedicated FPGA-design to locate individual flip-flops
- Precision of the Laser sufficient to inject matching fault?

- 3-Step Approach to find the flip-flops of interest:
  1. Locate a BRAM near the area where the relevant slices are assumed
  2. Evaluate optimal focal plane for maximum precision
  3. Scan area to locate the specific flip-flops

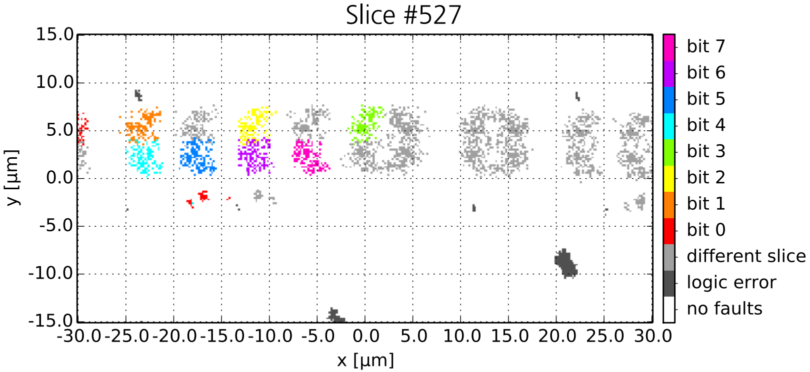
Fraunhofer AISEC

Preliminary Investigation
FF-Verification Design



Fraunhofer AISEC

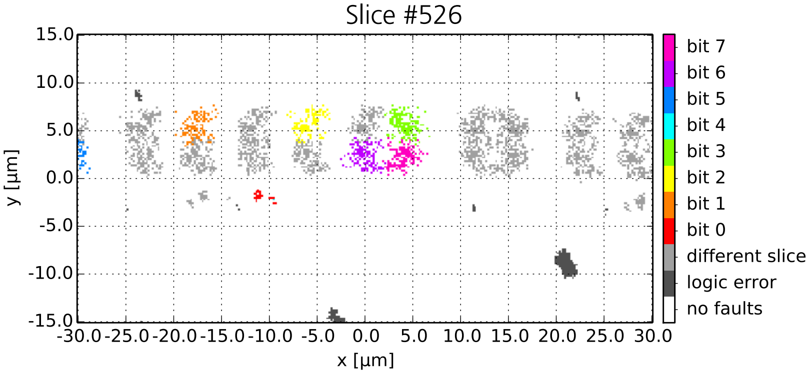
Preliminary Investigation
FF-Verification Design



- scan field **60 µm** × **30 µm**
- step size **200 nm**
- 2 laser shots per location: flip-flops initialized to **0** and **1**

Fraunhofer AISEC

Preliminary Investigation
FF-Verification Design

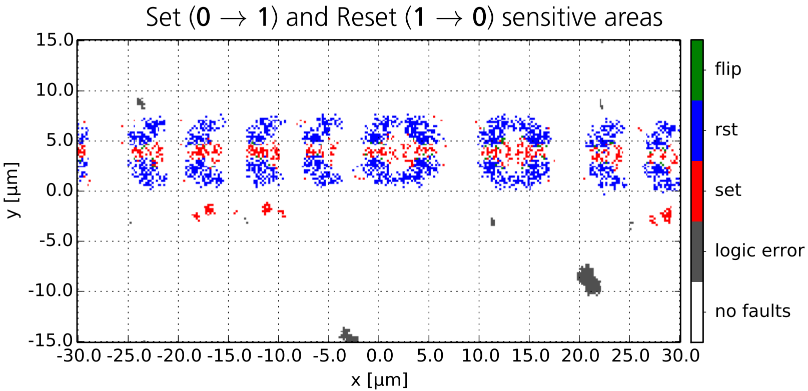


- scan field **60 µm** × **30 µm**
- step size **200 nm**

- 2 laser shots per location: flip-flops initialized to **0** and **1**

Fraunhofer AISEC

Preliminary Investigation
FF-Verification Design



- scan field **60 μm × 30 μm**
- step size **200 nm**
- 2 laser shots per location: flip-flops initialized to **0** and **1**

Fraunhofer AISEC

Performing the attack on the AES
Procedure

Preparation

- Positioning of both lasers according to the previous results
- Evaluation of correct timing for the fault injection

Attack

- Start AES computation
- Inject fault into state registers during round 7
- Record output
- Test if attack was successful (Perform DFA based on ciphertext pair)

Performing the attack on the AES
Results

Shots	Non-Exploitable Faults	Exploitable Faults	Attack Success Ratio
80000	21845	229	**0.29 %**

- Low success rate
- Single successful FI is sufficient
- Time to success: $\approx$ **5**min

Problems:

- Jitter of laser shot
- Drift of laser spot location

Performing the attack on the AES
Feasibility of the Attack in practice

- The attack required knowledge of the location of the state registers
  - Activity-Analysis can reveal location of the AES cores
  - Reverse-Engineering Methods can identify locations of registers
- Matching flip-flops can be found by exhaustive search (128 combinations)
- Stress on the device is low enough (All FI on single DUT)

Discussion
Countermeasures

Prevent this attack on state registers:

- *Fault Space Transformation (Patranabis et al.[a])*
  - Add an additional MixColumns / InvMixColumns Operation to one branch
  - The associated state register stores MixColumns-transformed version of state
  - FI in the combinatorial path might be feasible
- Parity Check for altered register contents

Raising attack complexity:

- Scrambling of the flip-flop locations
- Varying timing between both AES cores

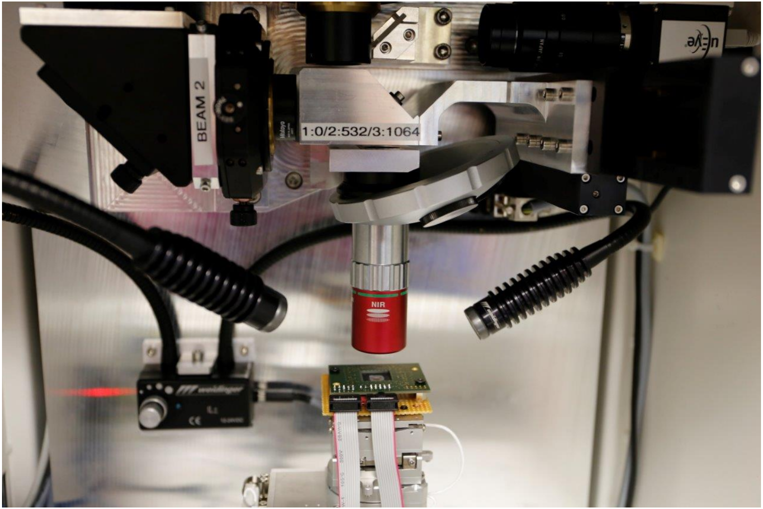
[a] Using State Space Encoding To Counter Biased Fault Attacks on AES Countermeasures, 2015

Conclusion

- We successfully show how two lasers can be used in an attack
- As example, broke duplication-based infective countermeasures
- Results principally affect most hardware duplication-based countermeasures!

Fraunhofer AISEC

Thank your for your attention
Questions?



Contact Information

Dipl.-Ing. Bodo Selmke

Department Hardware Security (HWS)

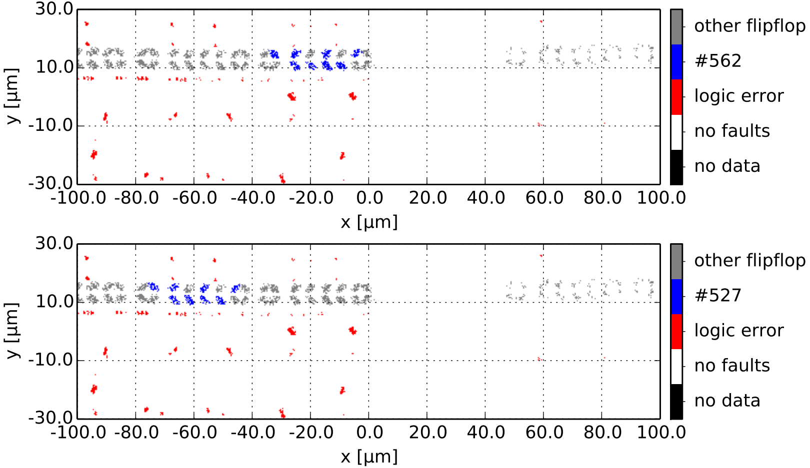
Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

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

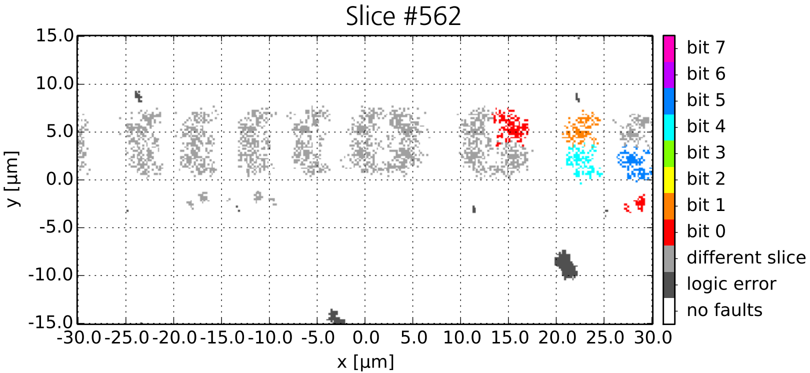
Phone: +49 89 3229986-132
Fax: +49 89 3229986-222
E-Mail: bodo.selmke@aisec.fraunhofer.de

Fraunhofer
AISEC

Backup Slides

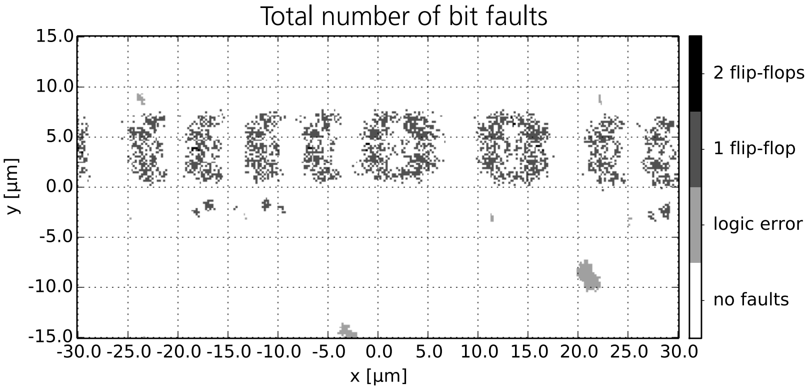


Backup Slides

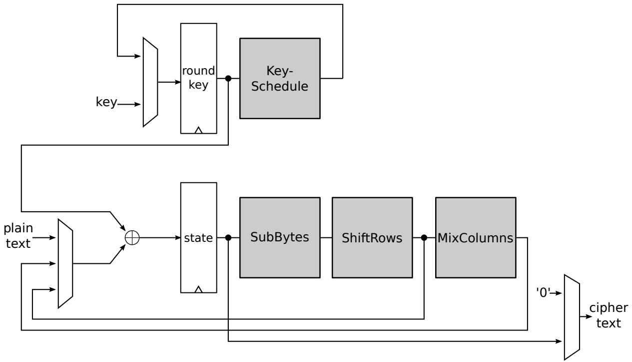


Fraunhofer AISEC

Backup Slides



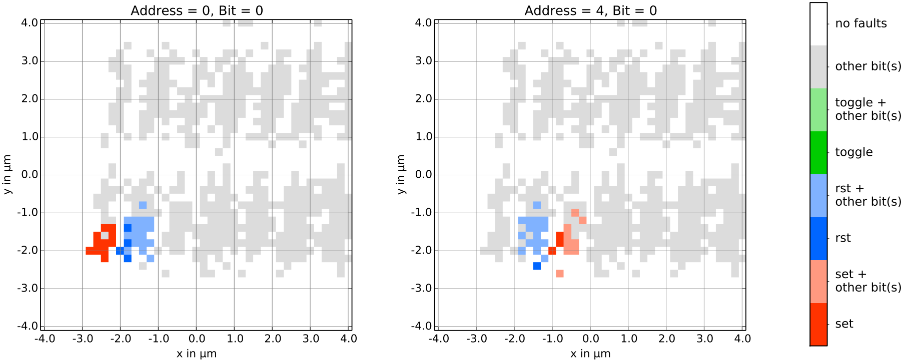
Backup Slides



Fraunhofer AISEC

Backup Slides

Backup Slides



Pulse energy **1.0 nJ**

Fraunhofer AISEC