RUHR-UNIVERSITÄT BOCHUM

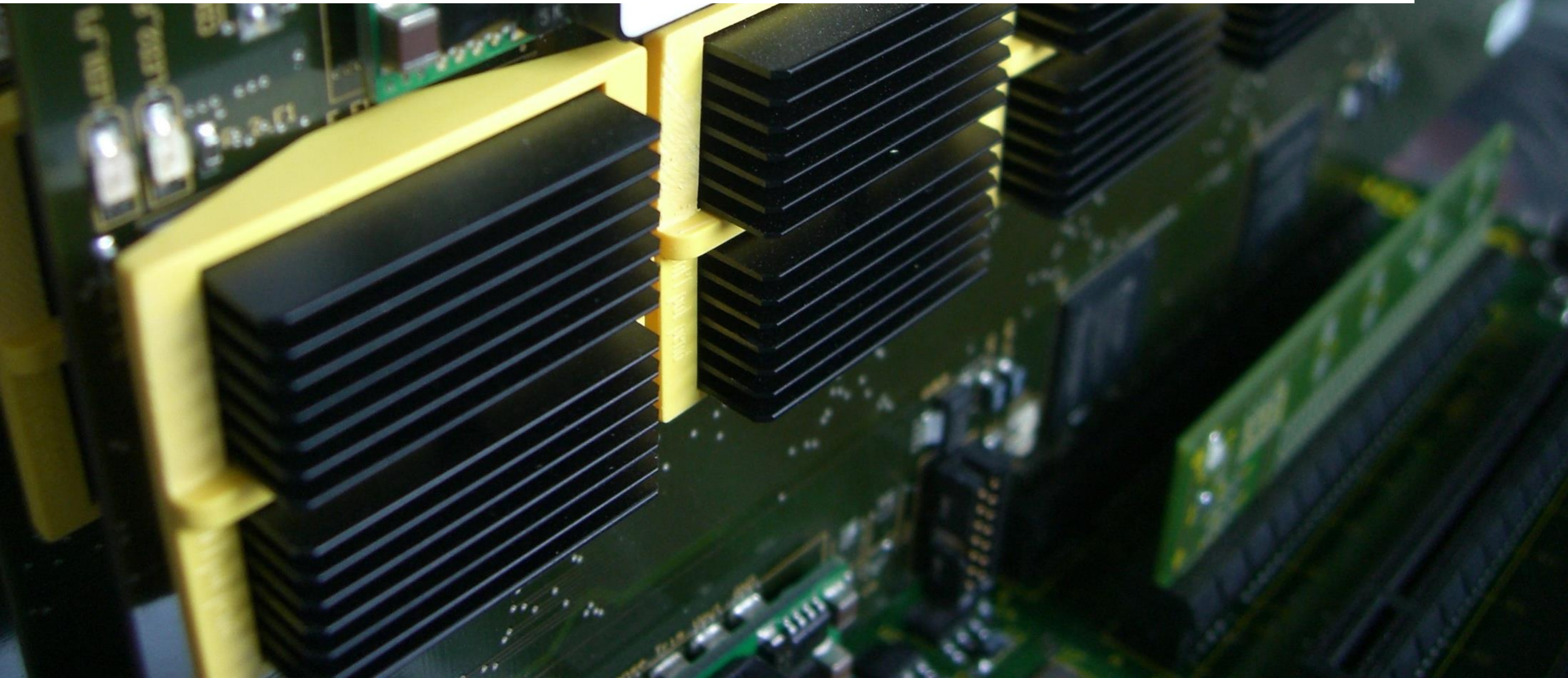
hgi SHA

RUB

ACHIEVING SIDE-CHANNEL PROTECTION WITH DYNAMIC LOGIC RECONFIGURATION ON MODERN FPGAS

PASCAL SASDRICH, AMIR MORADI, OLIVER MISCHKE, TIM GÜNEYSU

INT. SYMPOSIUM ON HARDWARE-ORIENTED SECURITY AND TRUST, MCLEAN, VA, USA MAY 6, 2015

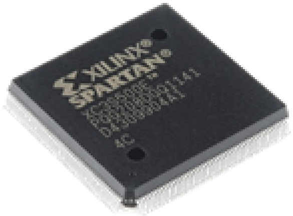


OUTLINE OF THIS TALK

- **INTRODUCTION**
  - MOTIVATION
  - CONTRIBUTION
- **PRELIMINARIES**
  - CONFIGURABLE LOOK-UP TABLE
  - RECONFIGURABLE FUNCTION TABLE
- **COUNTERMEASURES**
  - S-BOX DECOMPOSITION
  - BOOLEAN MASKING
  - REGISTER PRECHARGE
- **PRACTICAL EVALUATION**
  - LEAKAGE ASSESSMENT METHODOLOGY
  - NO COUNTERMEASURE
  - SINGLE COUNTERMEASURE
  - COMBINATION OF COUNTERMEASURES
- **CONCLUSION**

WHAT IS THE IDEA BEHIND THIS WORK?

- **FPGA**: *(re-)programmable logic device* popular for cryptographic implementations
- **Partial (runtime) reconfiguration**: exchange (partial) designs on demand
- **Observer:** hard to predict current operation and functionality

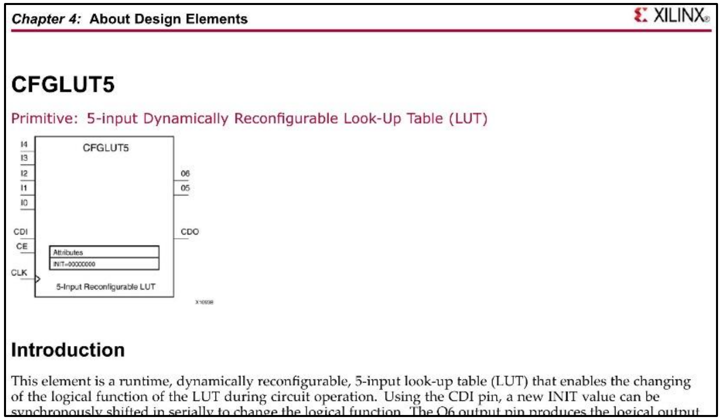


Idea: Use partial runtime reconfiguration for protection against an external observer or SCA-attacker.

Problem: Exchanging designs and circuits is very slow and can even can take up to *milliseconds*.

Solution: dynamic logic reconfiguration

- since Virtex-5 family Xilinx FPGAs offer 5-input **Configurable Look-Up Tables** (CFGLUT5)
- exchange logic configuration of CFGLUT5s but keep routing structure
- only few *clock cycles* rather than *milliseconds*
- older devices could use **Shift Registers** (SRL16E)



Chapter 4: About Design Elements XILINX®

CFGLUT5

Primitive: 5-input Dynamically Reconfigurable Look-Up Table (LUT)

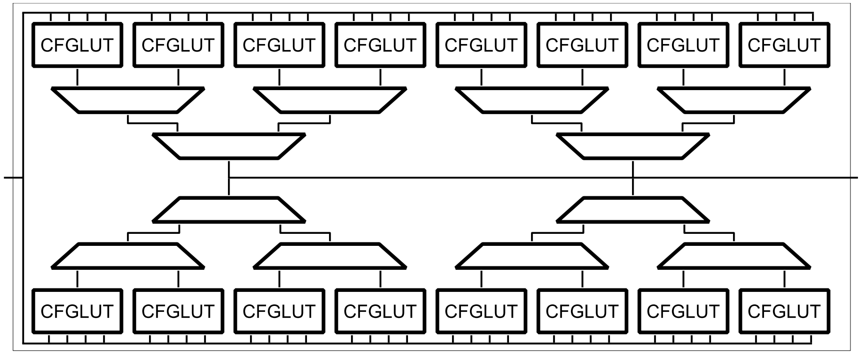
Introduction

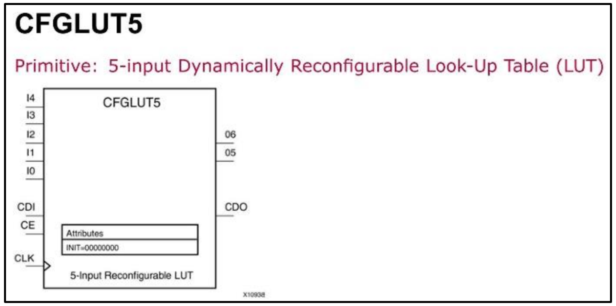
This element is a runtime, dynamically reconfigurable, 5-input look-up table (LUT) that enables the changing of the logical function of the LUT during circuit operation. Using the CDI pin, a new INIT value can be synchronously shifted in serially to change the logical function. The O6 output pin produces the logical output

Question: How can we use CFGLUT5 to build a side-channel countermeasure?

CONFIGURABLE LUTS AND RECONFIGURABLE FUNCTION TABLES

- **Configurable Look-Up Tables** were introduced with *Xilinx Virtex-5* and *Spartan-6* device families
- located in special slices called **SLICEM** and based on distributed memory / shift registers
- **CFGLUT5** can be used as:
  - single 5×1 LUT (32 cycles for reconfiguration)
  - two 4×1 LUTs with shared inputs (16 cycles for reconfiguration)
- combining multiple CFGLUTs with multiplexers stages we can build $(n \times m)$ ***reconfigurable function tables (RFT)***
- each RFT consists of $\boldsymbol{m \cdot \lceil 2^{n-4} \rceil}$ CFGLUTs
- for large structures this is inefficient, but for (4×4) functions (e.g. PRESENT S-box) this is an optimal choice





CFGLUT5

Primitive: 5-input Dynamically Reconfigurable Look-Up Table (LUT)

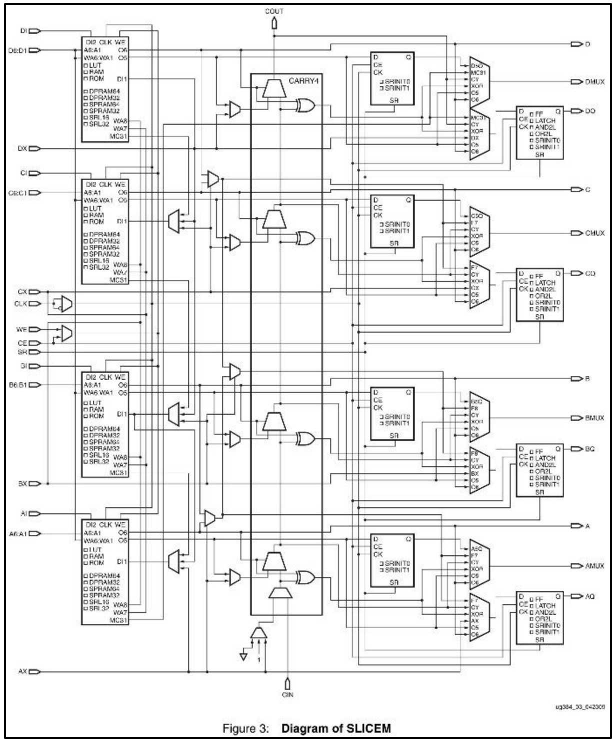
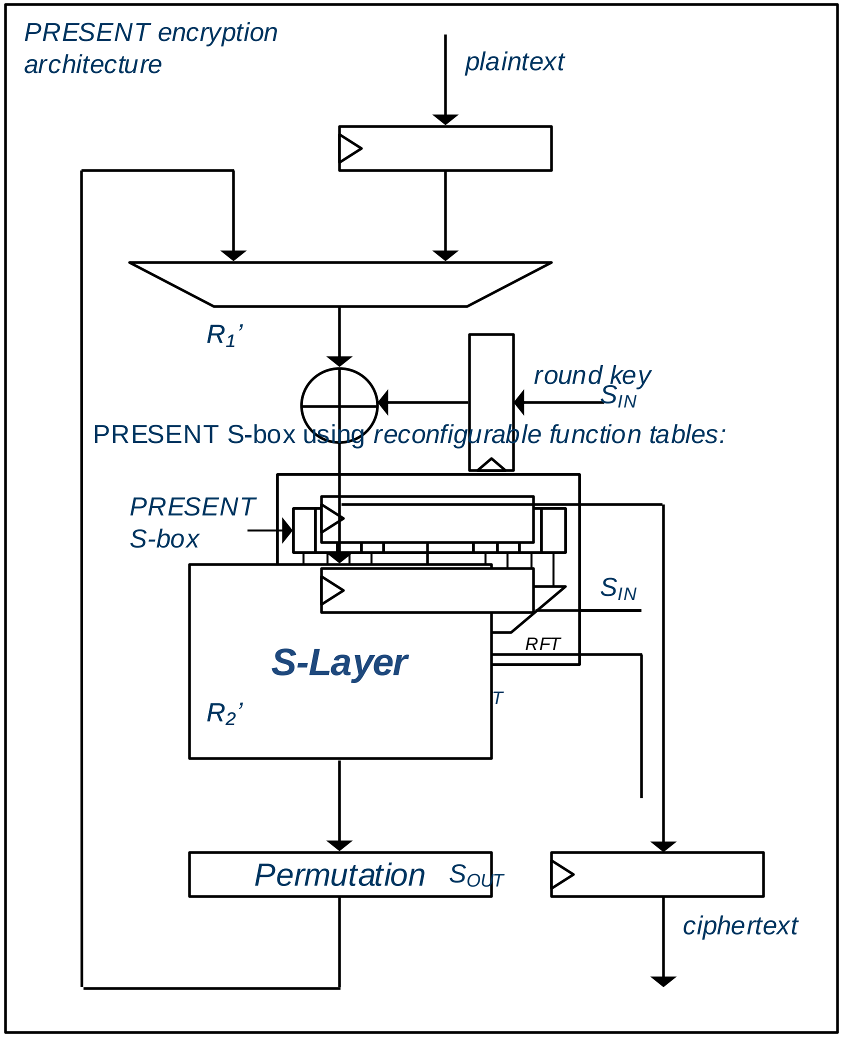


Figure 3: **Diagram of SLICEM**

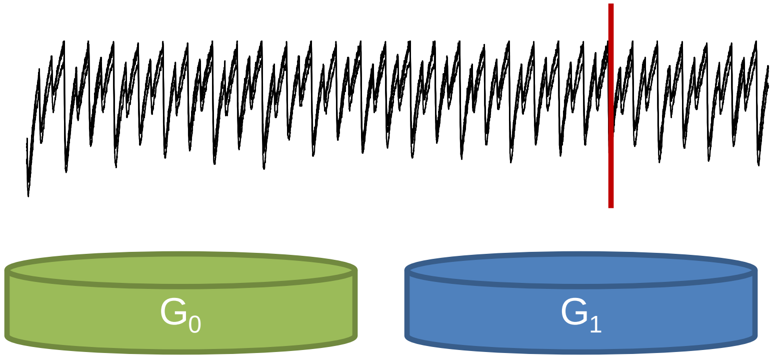
THE PROPOSED COUNTERMEASURES?

- **round-based architecture** with 16 S-boxes
- all countermeasures target **S-layer**
- implement S-boxes using *reconfigurable function tables*
- **decompose** the PRESENT S-box into two *reconfigurable function tables*
  - first *reconfigurable function table* R_1 is chosen randomly
  - second *reconfigurable function table* R_2 is computed using the original S-box such that: $R_2\big(R_1(x)\big) = S(x)$
  - place register stage in between R_1 and R_2 to only store (random) $R_1(x)$
- add **Boolean masking** to both *reconfigurable function tables* and recompute them as:
  $R_1'(x) = R_1(x \oplus m_1) \oplus m_2$
  $R_2'(x) = R_2(x \oplus m_2) \oplus P^{-1}(m_1)$
- insert a second register stage for random **register precharge** to avoid leakage based on the Hamming distance model:
  $HD(x \oplus m, y \oplus m) = HW(x \oplus y)$



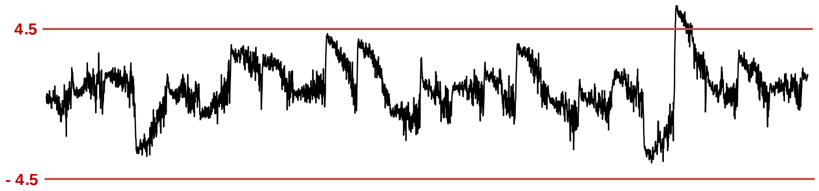
EVALUATION USING WELCH'S *t*-TEST

- measure power traces with digital oscilloscope
- determine distinguisher, e.g.:
  - fix vs. random plaintext (*non-specific t*-test)
  - bit of intermediate round result
  - multi-bit intermediate result
- group traces depending on distinguisher
- compute *sample mean* for each point in time
- compute *sample variance* for each point in time
- determine *t*-statistic for each point in time:



$$t = \frac{\mu(T \epsilon G_1) - \mu(T \epsilon G_0)}{\sqrt{\frac{\delta^2(T \epsilon G_1)}{|G_1|} + \frac{\delta^2(T \epsilon G_0)}{|G_0|}}}$$

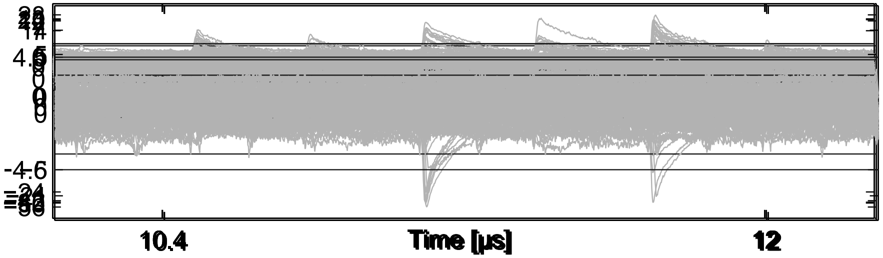
where μ denotes the *sample mean* and δ denotes the *sample variance*.



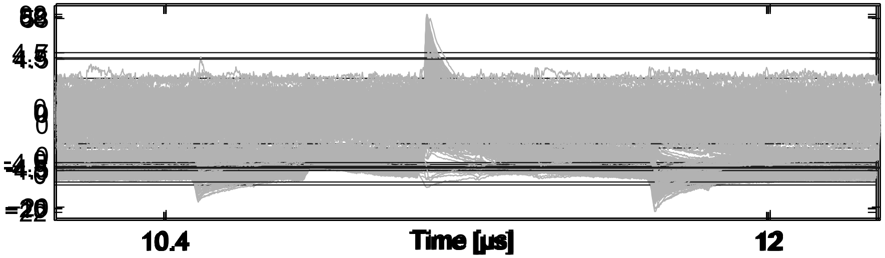
Fail/Pass Criteria: If there is any point in time for which the t-statistic exceeds a threshold of ± 4.5 the device under test fails.

WHAT ARE THE RESULTS?

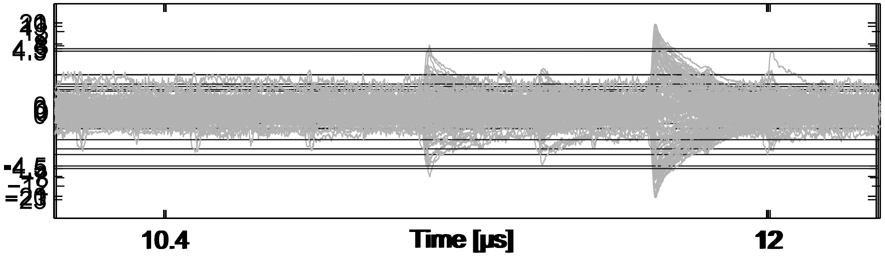
- distinguisher: intermediate values of round 16 (bits / nibbles)
- 3 different groups of test:
  - S-box output bits (64 models)
  - XOR of round in and out (64 models)
  - output value of S-box S_0 (16 models)
- 8 different test cases:
  - all countermeasures disabled
  - S-box decomposition
  - Boolean masking
  - register precharge
  - S-box decomposition and register precharge
  - Boolean masking and register precharge
  - S-box decomposition and masking
  - S-box decomposition, masking and register precharge
- 1 million power traces except for last test case: measured 10 million



Group 1: S-box output bits (64 models)



Group 2: XOR of round in and round out (64 models)



Group 3: Output value of S-box S_0 (16 models)

WHAT IS THE CONCLUSION OF THIS WORK?

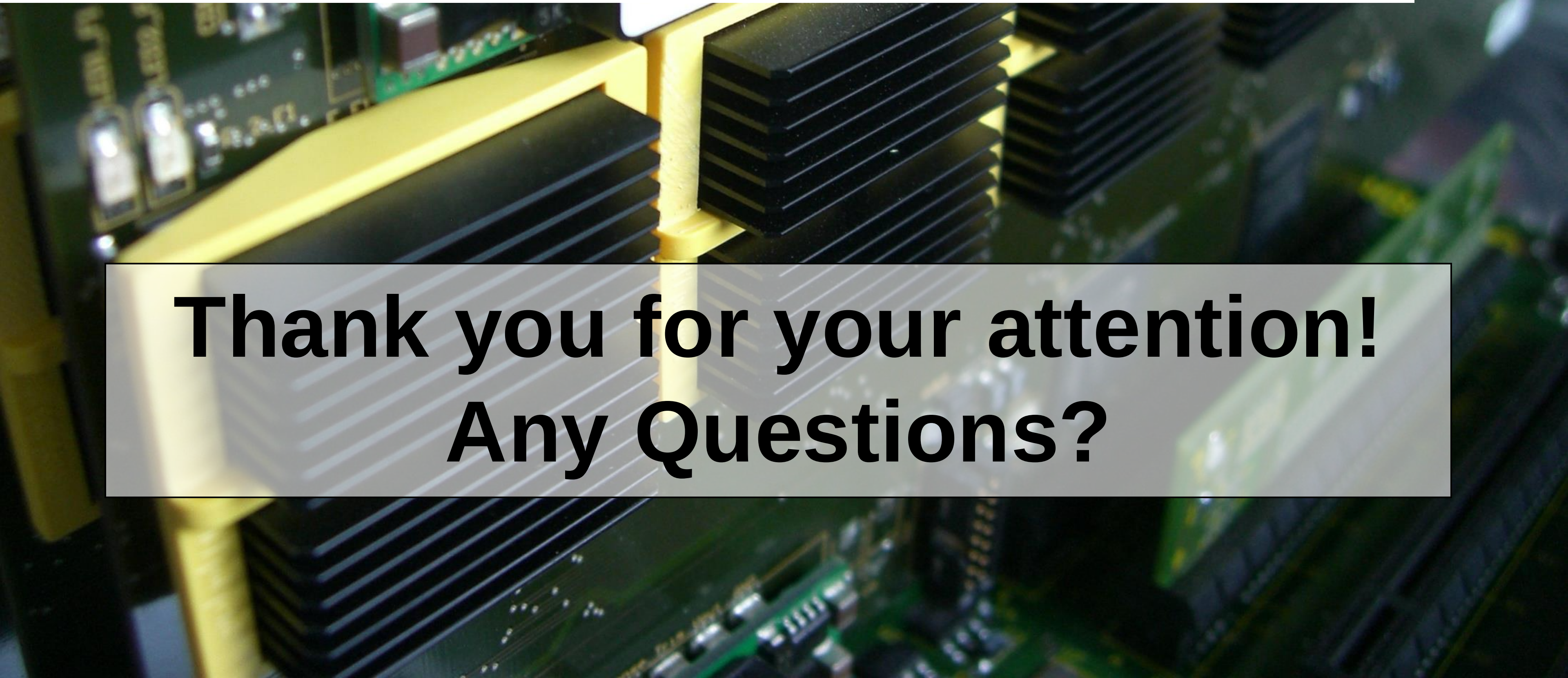
- first application of **dynamic logic reconfiguration** to realize a first-order-resistant masking scheme
- **Configurable Look-Up Tables** are not affected by known issues of masked hardware implementations, e.g. as *glitches*
- we provide **practical examination** of all countermeasures and their combinations
- used state-of-the-art **leakage assessment methodology** (specific *t*-test)
- design is first-order resistant even after measuring **10 million** power traces

EFFECTIVE TECHNIQUE TO ACHIEVE FIRST-ORDER SCA RESISTANCE ON FPGA-BASED PLATFORMS!

ACHIEVING SIDE-CHANNEL PROTECTION WITH DYNAMIC LOGIC RECONFIGURATION ON MODERN FPGAS

pascal.sasdrich@rub.de

INT. SYMPOSIUM ON HARDWARE-ORIENTED SECURITY AND TRUST, MCLEAN, VA, USA MAY 6, 2015



Thank you for your attention!
Any Questions?