LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

TECHNISCHE UNIVERSITÄT MÜNCHEN

Side Channel Attacks on Network-on-Chip

Johanna Sepulveda, Cezar Reindbrecht, Lilian Bossuet,
Guy Gogniat, Georg Sigl

La Grande
Motte – 23/06/2016

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

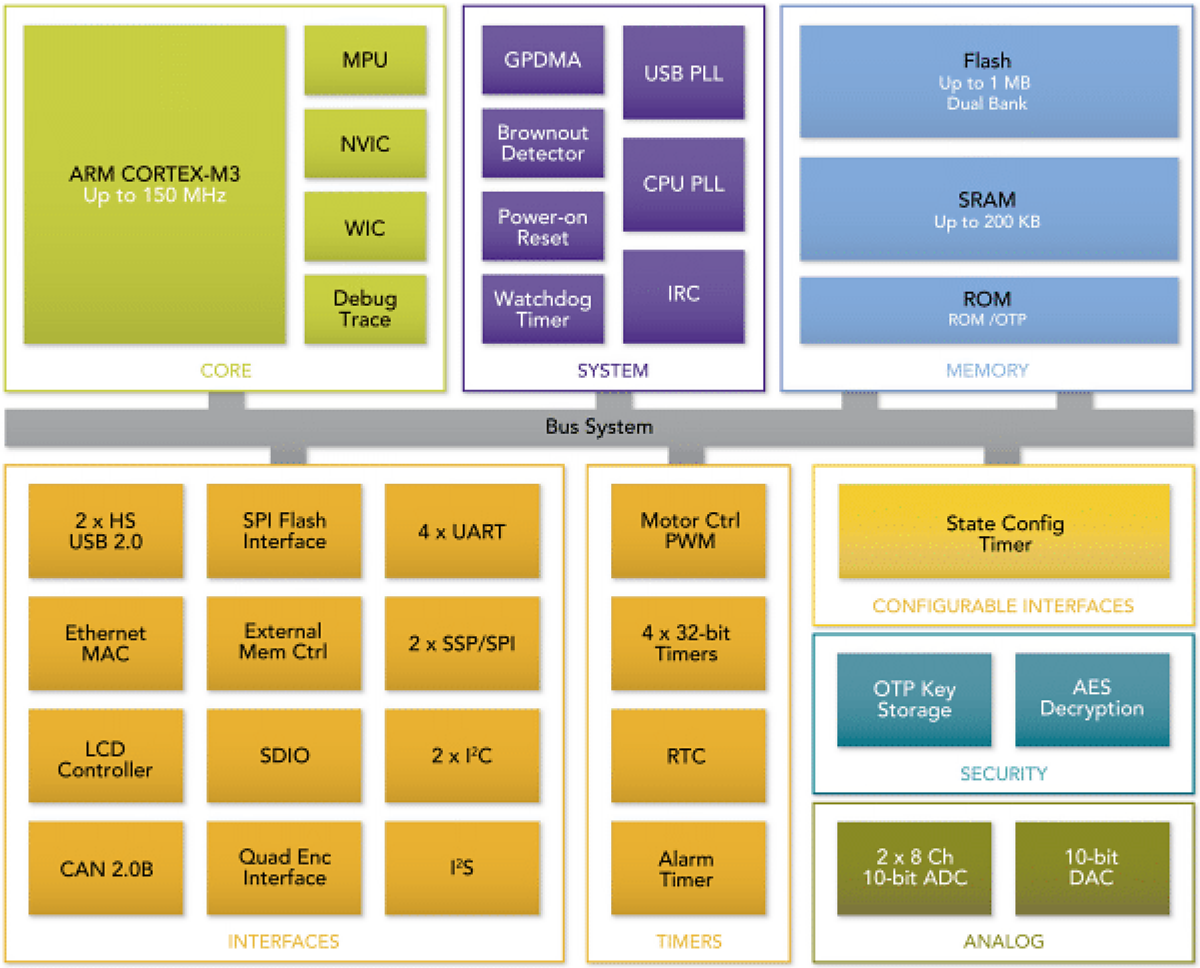
Membre de UNIVERSITÉ DE LYON

Lehrstuhl für Sicherheit in der Informationstechnik

TECHNISCHE UNIVERSITÄT MÜNCHEN

Motivation

- SoC System
  - 1 processor
  - Accelerators
  - Interfaces
  - Memories
  - Analog
  - Bus system



NXP LPC1800 – Used IPHONE 5S as Sensor Mng (M7)

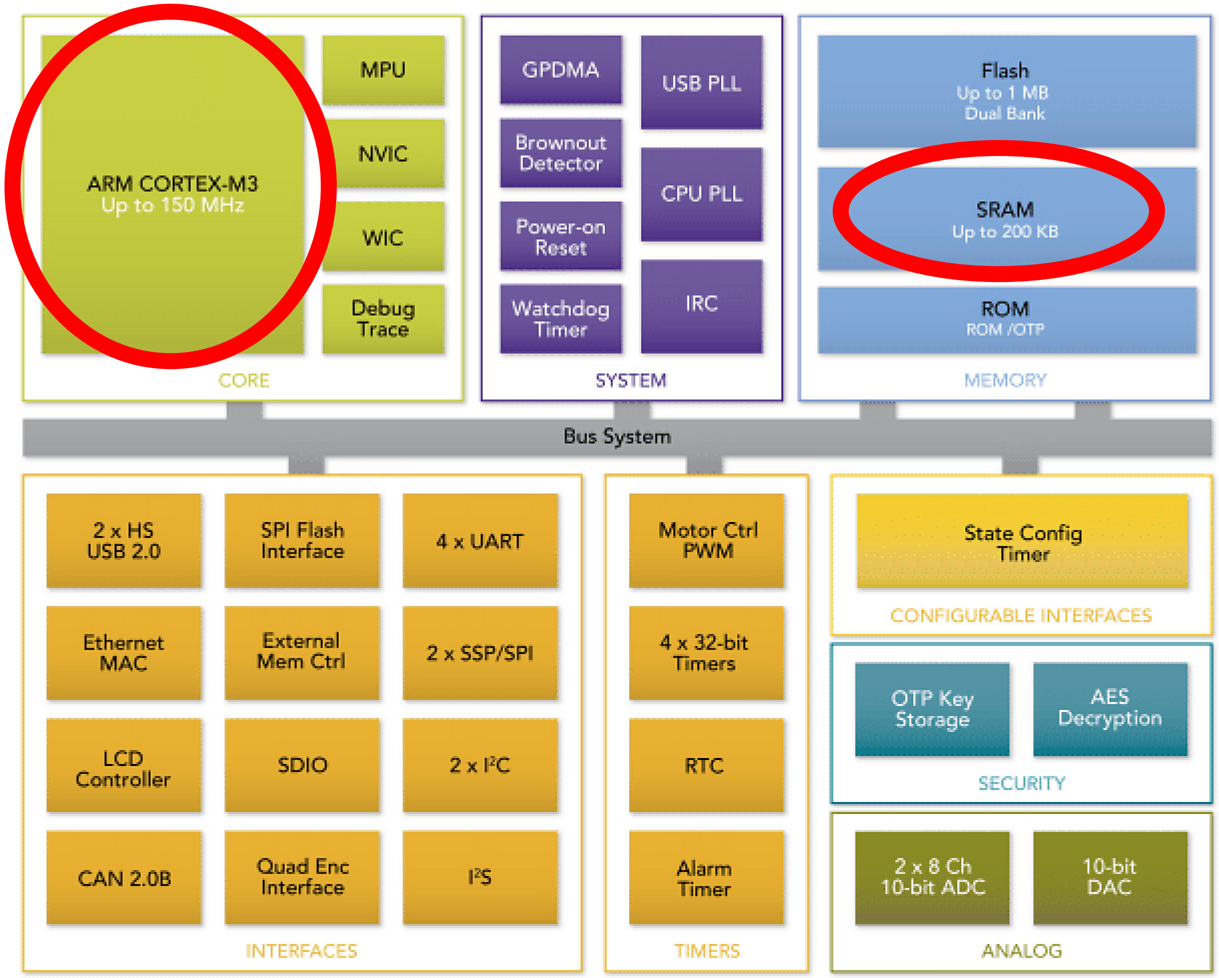
LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Lehrstuhl für Sicherheit in der Informationstechnik

TECHNISCHE UNIVERSITÄT MÜNCHEN

Motivation

- SCA on SoC
  - Power
  - Electromag.
  - Faults
  - …
  - Timing
    - Processor
    - Memory



NXP LPC1800 – Used IPHONE 5S as Sensor Mng (M7)

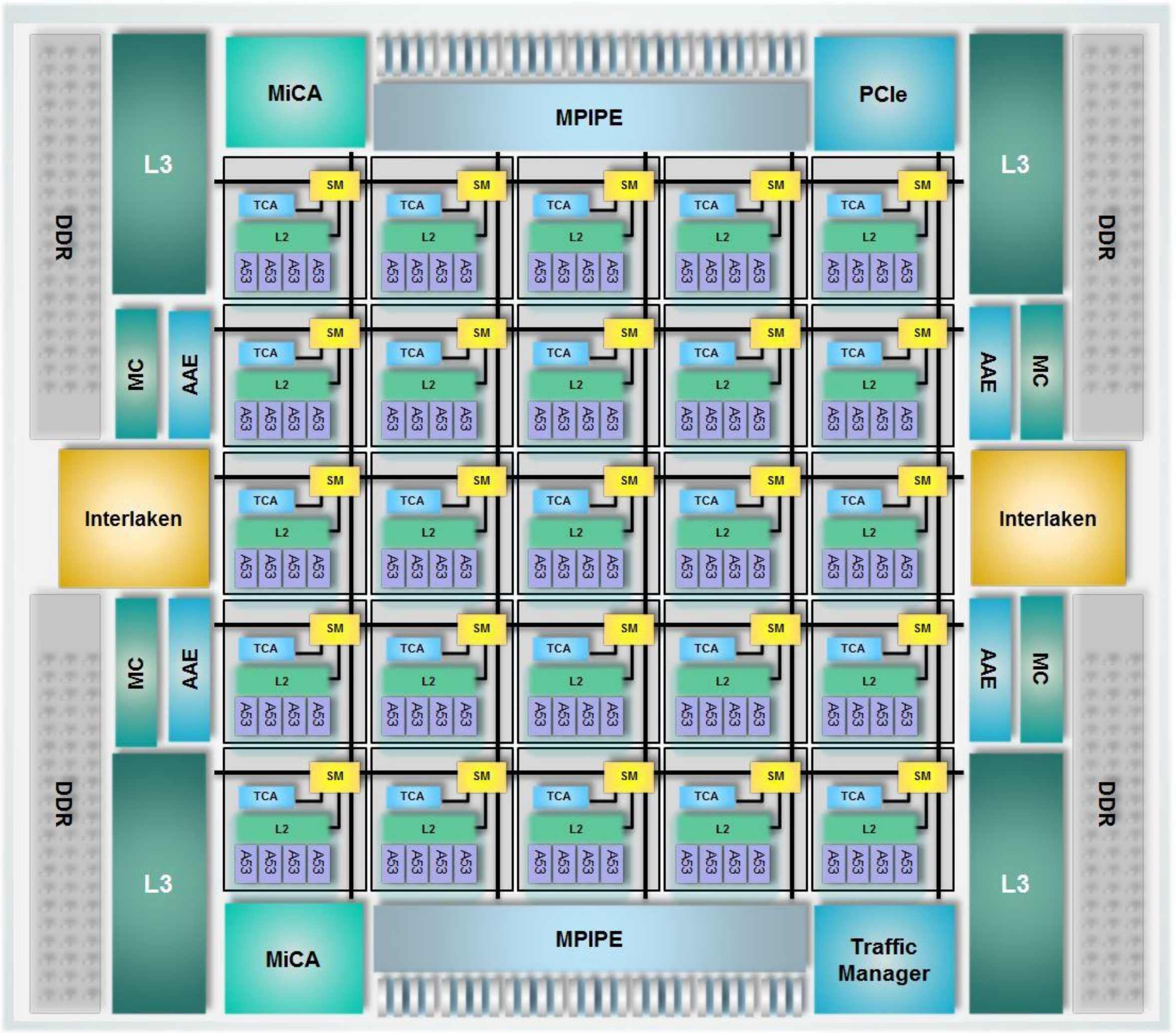
LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Lehrstuhl für Sicherheit in der Informationstechnik

TECHNISCHE UNIVERSITÄT MÜNCHEN

Motivation

- MPSoCs
  - 100 Processors
  - Accelerators
  - Interfaces
  - Shared Memory
  - Analog
  - NoC System

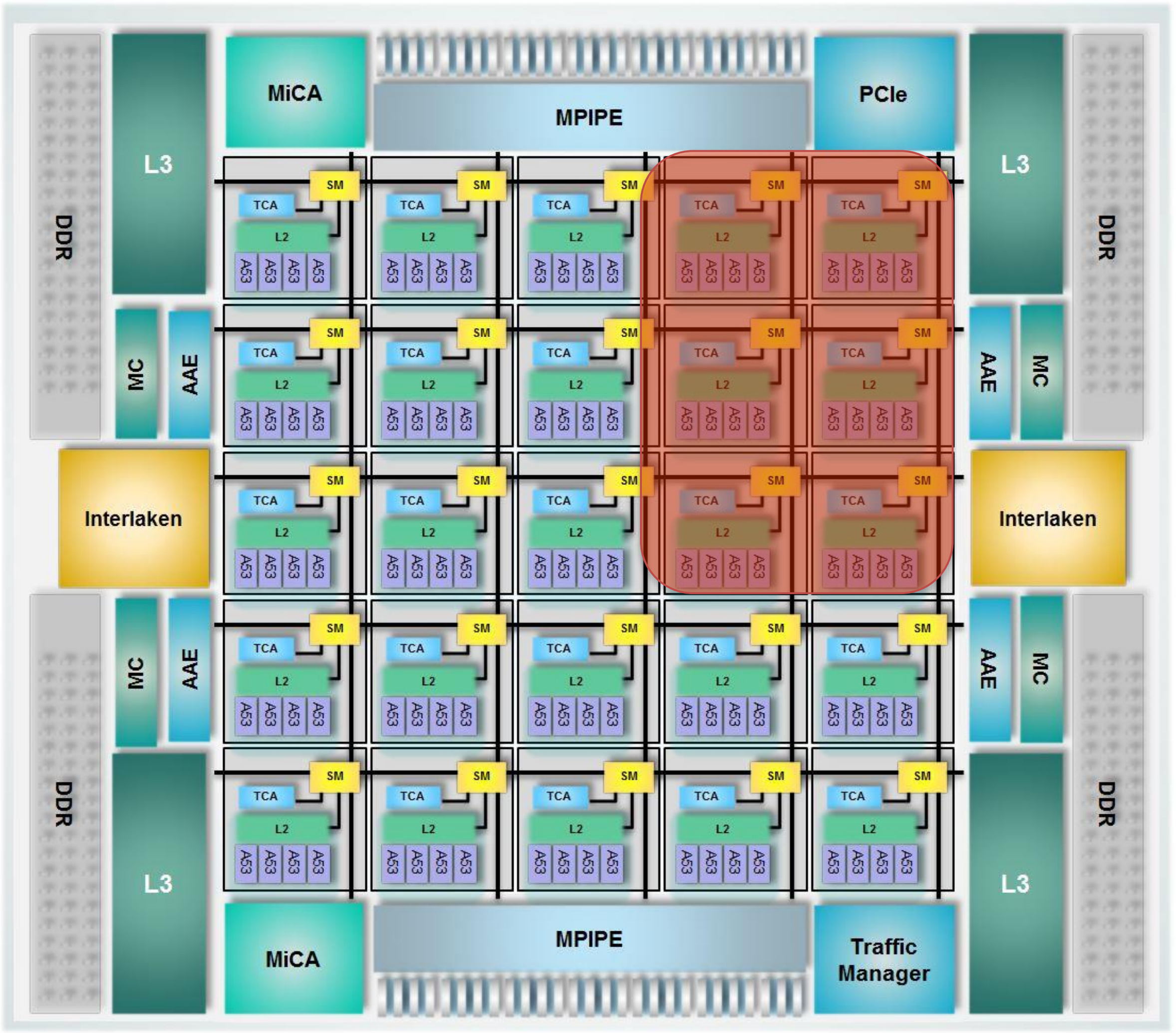


The Tile-Mx100. Source: EZchip

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Motivation

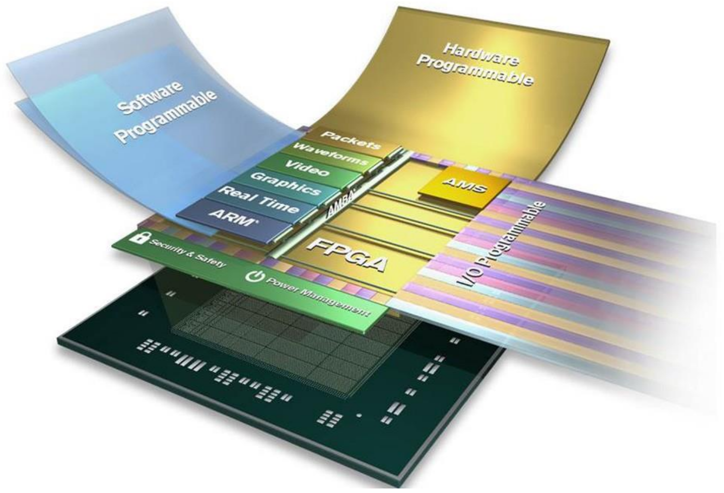
- SCA ?
- Challenges
  - Secure Zones
  - Firewalls
  - HW Complexity
    - DPA,...
- Opportunities
  - Shared resources
    - Memory
    - NoC



The Tile-Mx100. Source: EZchip

Outline

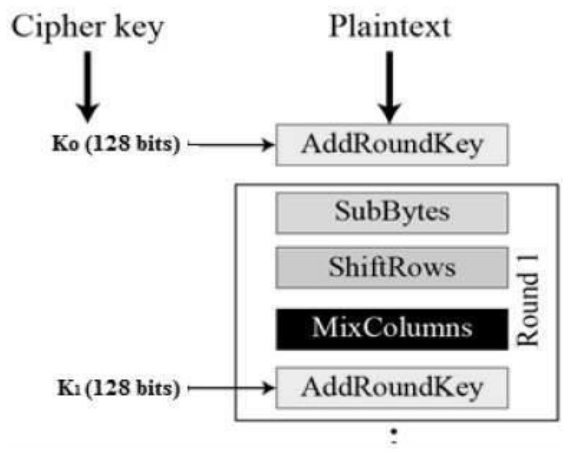
- Background
  - Cache Attack - Prime+Probe
- Timing Attacks on NoC
  - Single TA
  - Distributed TA
- NoC Prime+Probe Attacks
  - Firecracker
  - Arrow
- Countermeasure
- Experiments & Demonstration



Background

Prime+Probe Attack

- Attack on Performance-oriented AES
- Targets the Tables T0, T1, T2, T3 in Cache
  - Pre-computed SubBytes, ShiftRows and Mix Columns
- Uses the relation of the indexes with the Key



$$\begin{cases}(x_0^{r+1},x_1^{r+1},x_2^{r+1},x_3^{r+1})=T_0[x_0^r]\oplus T_1[x_5^r]\oplus T_2[x_{10}^r]\oplus T_3[x_{15}^r]\oplus(K_0^r,K_1^r,K_2^r,K_3^r)\\(x_4^{r+1},x_5^{r+1},x_6^{r+1},x_7^{r+1})=T_0[x_4^r]\oplus T_1[x_9^r]\oplus T_2[x_{14}^r]\oplus T_3[x_3^r]\oplus(K_4^r,K_5^r,K_6^r,K_7^r)\\(x_8^{r+1},x_9^{r+1},x_{10}^{r+1},x_{11}^{r+1})=T_0[x_8^r]\oplus T_1[x_{13}^r]\oplus T_2[x_2^r]\oplus T_3[x_7^r]\oplus(K_8^r,K_9^r,K_{10}^r,K_{11}^r)\\(x_{12}^{r+1},x_{13}^{r+1},x_{14}^{r+1},x_{15}^{r+1})=T_0[x_{12}^r]\oplus T_1[x_1^r]\oplus T_2[x_6^r]\oplus T_3[x_{11}^r]\oplus(K_{12}^r,K_{13}^r,K_{14}^r,K_{15}^r)\end{cases}$$

Prime+Probe Attack

- Preconditions
  - Spy process running on Target CPU
  - Access to cache memory

- Treat Model
  1. Read an attacker information into cache (prime)
  2. Request the encryption of a random plaintext
  3. After encryption read again the attacker vector
  4. Observes when there is a cache miss (probe)
  5. Identify and annotate the accessed parts of the AES Table
  6. Analyze the data considering only the first/last round
  7. Repeat the process for several plaintexts

Lehrstuhl für Sicherheit in der Informationstechnik

Prime+Probe Attack

TECHNISCHE UNIVERSITÄT MÜNCHEN

- Related Works

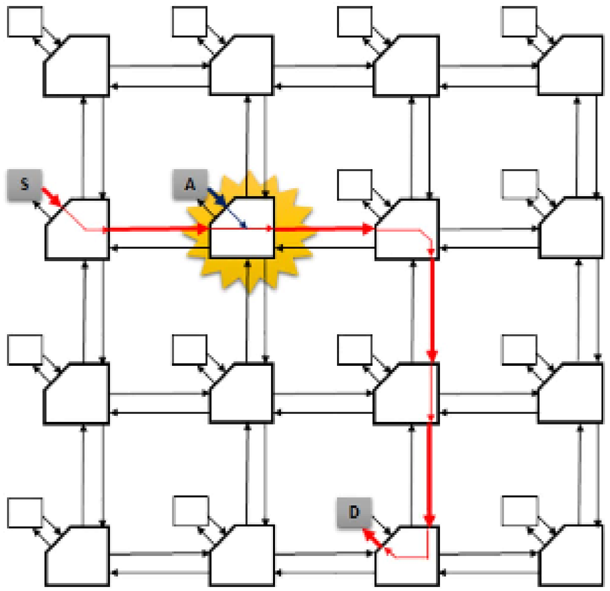
Work	Platform	Timing Leakage Source	Attacker Method	Traces Used
Osvik et al. [7]	SoC (single core)	L1 Cache	Spy process	16000
Xinjie et al. [8]	SoC (single core)	L1 Cache	Spy process	350
Liu et al. [10]	Bus-based MPSoC	LLC - L3 Cache	Spy process	33600
Oren et al. [11]	Bus-based MPSoC	LLC - L3 Cache	Browser process	5000

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Timing Attacks on NoC

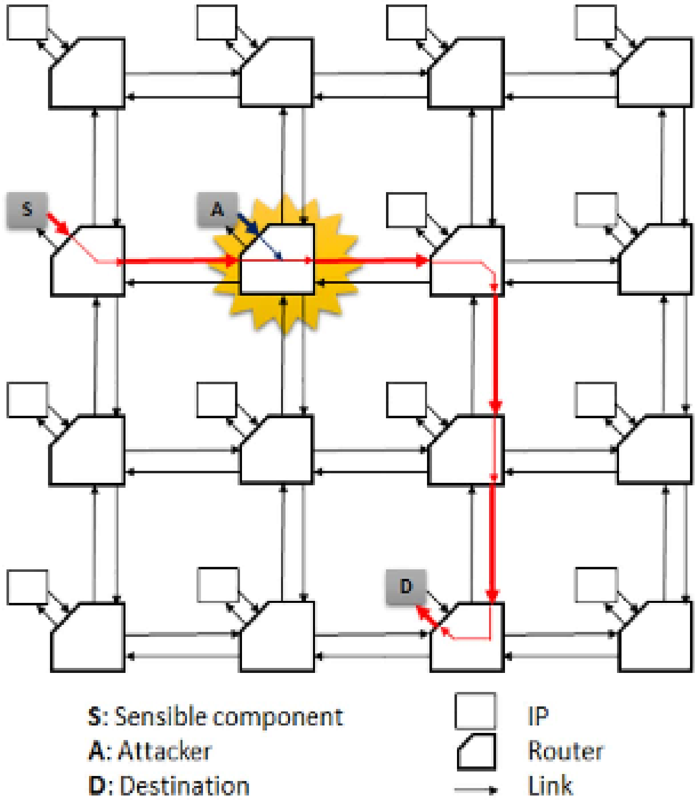
Timing Attacks on NoC

- Use the NoC to reveil sensitive information of the system
  - Access patterns
  - Core Mapping
  - Routing Algorithm
- Possible source of leakage:
  - Throughput
  - Arbiter/Scheduler



Single Timing Attack

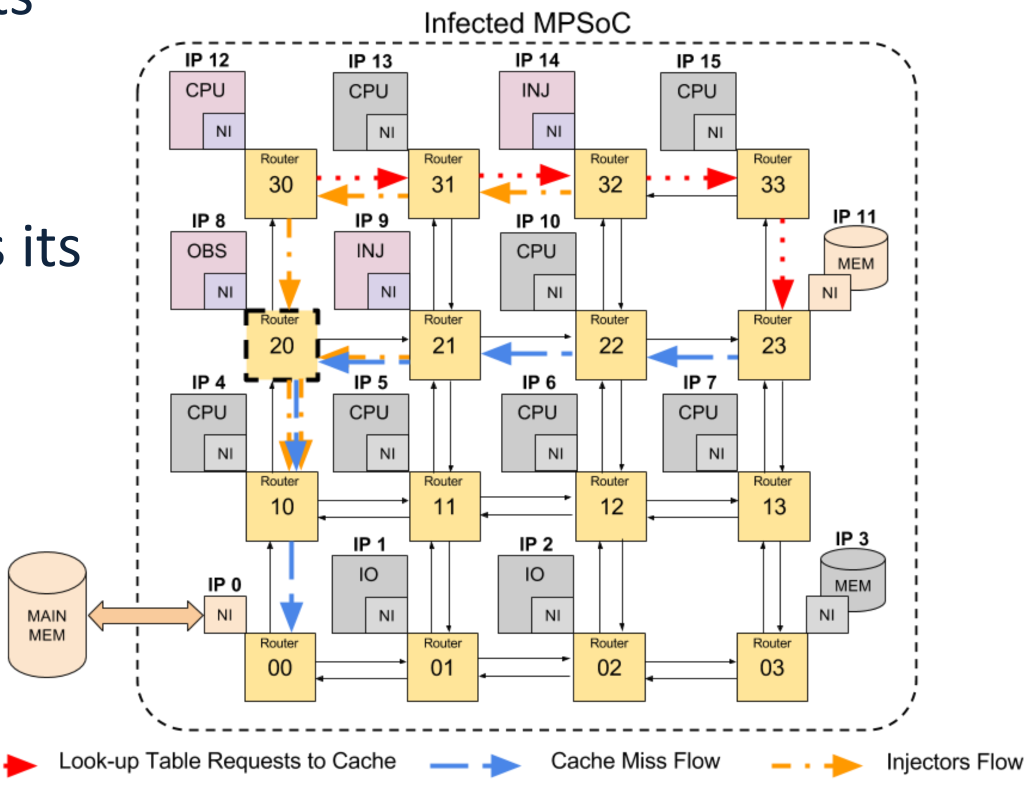
- Preconditions:
  - Logical Addresses
  - Routing Information
- Infection:
  - Download a malicious software
- Attack Model:
  - Malware injects data in the network, and observes its own throughput
  - When a sensitive data pass through, the throughput is degraded



NoC-Based Protection for SoC Time-Driven Attacks.
J. SEPULVEDA, J.P. DIGUET, M. STRUM, G. GOGNIAT.
IEEE ESL 2015

Distributed Timing Attack

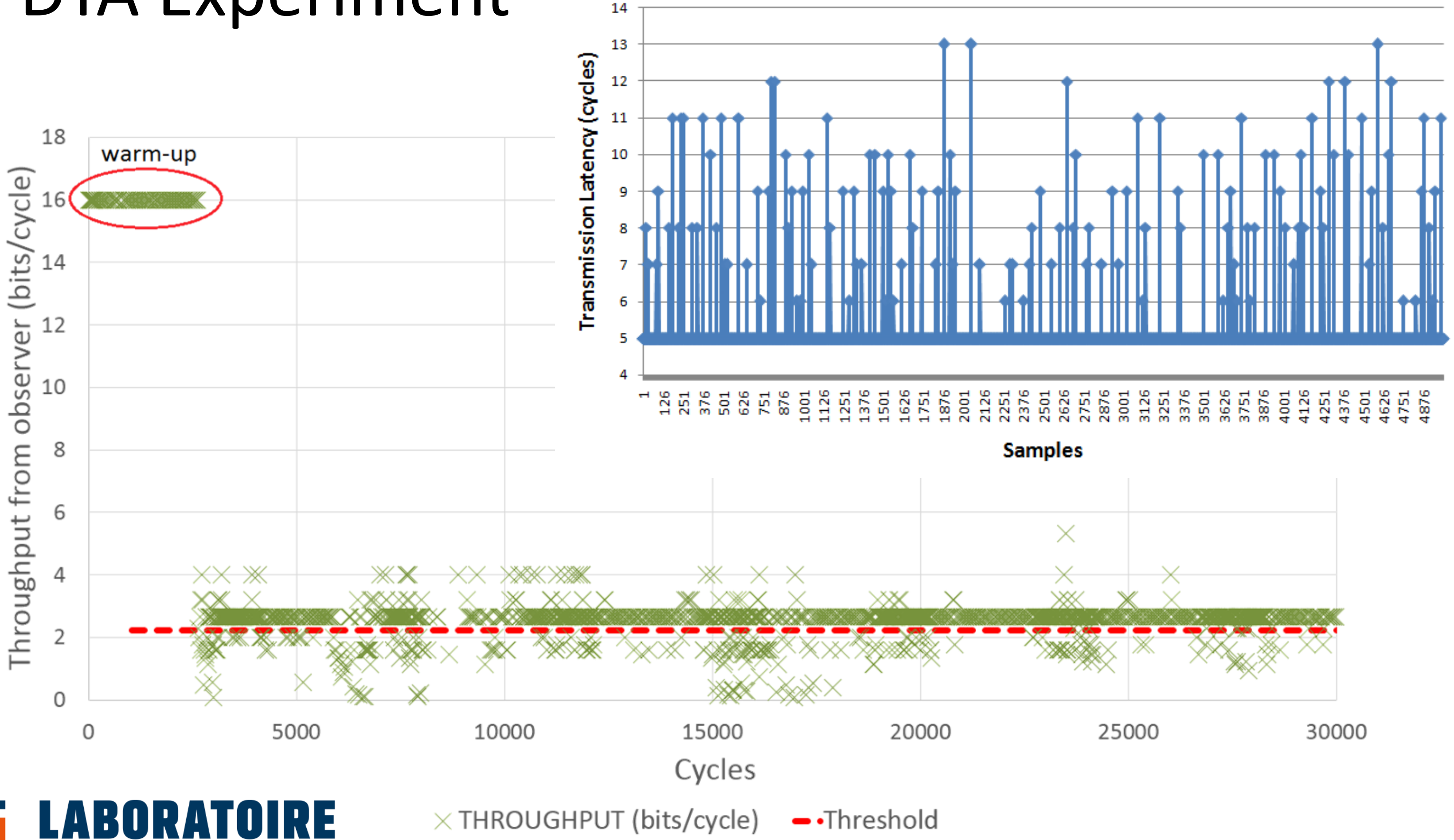
- Attack Model:
  - Injectors: Malware injects data in the network
  - Observers: Inject data at lower rates and observes its own throughput
  - Possible synchronization
  - Control traffic behavior



Gossip NoC - Avoiding Timing Side-Channel Attacks through Traffic Management.
C. REINBRECHT, A. SUSIN, L. BOSSUET, J. SEPULVEDA
ISVLSI 2016

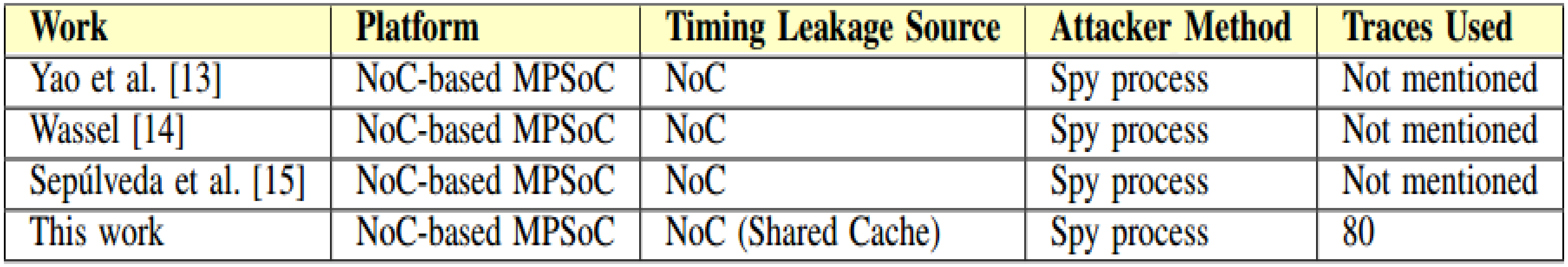
Distributed Timing Attack

- DTA Experiment



Timing Attacks on NoC

- Related Works:



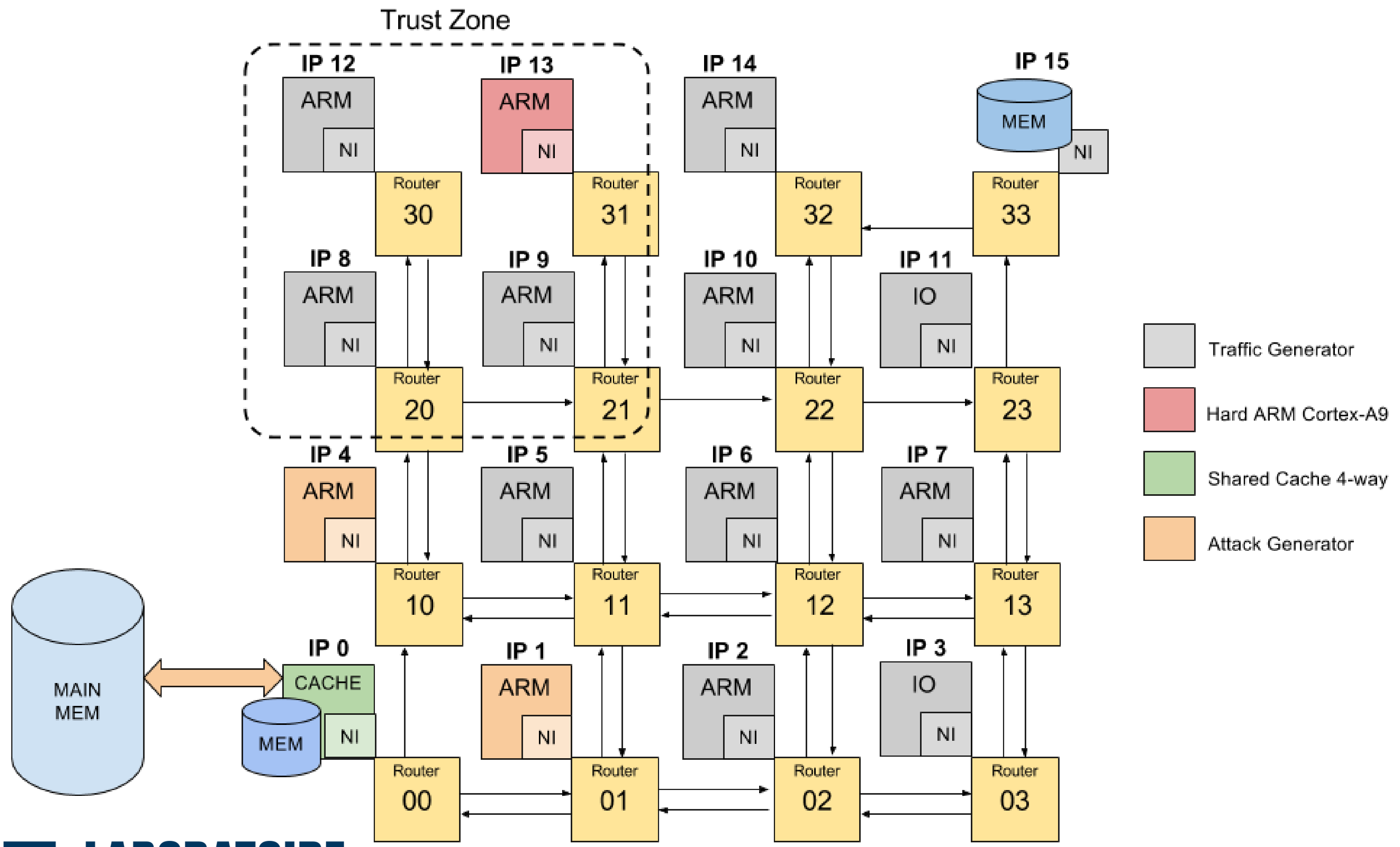
Work	Platform	Timing Leakage Source	Attacker Method	Traces Used
Yao et al. [13]	NoC-based MPSoC	NoC	Spy process	Not mentioned
Wassel [14]	NoC-based MPSoC	NoC	Spy process	Not mentioned
Sepúlveda et al. [15]	NoC-based MPSoC	NoC	Spy process	Not mentioned
This work	NoC-based MPSoC	NoC (Shared Cache)	Spy process	80

NoC Prime+Probe Attack

NoC P+P: Preconditions

- AT knows MPSoC Mapping
- AT knows NoC Routing
- AT knows Cache Configuration
- AT generates encryption plaintext
- AT knows residence of AES tables in memory
- AT can access shared Cache
- AT can control one IP core

NoC P+P: Target Environment



LABORATOIRE
HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Lehrstuhl für Sicherheit in der Informationstechnik

TECHNISCHE UNIVERSITÄT MÜNCHEN

NoC P+P: Firecracker & Arrow

- Firecracker
  - To attack small shared caches (tables shares sets)
  - Observes all 1st round access, then read cache
    - Tolerate low precision in NoC observation
  - Annotate the non-accessed sets to eliminate candidates
- Arrow
  - To attack big shared caches (tables do not share Sets)
  - Observes at least one access in four during 1st round
    - High precision required in NoC observation
  - Annotate the specific sets accessed to analyze directly

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Lehrstuhl für Sicherheit in der Informationstechnik

Firecracker Attack

- Prime
  - Prepare all Sets used for all tables
- Probe
  - Starts after the 16th access
  - Read all Sets and annotate where occurs hits and misses
  - No need to avoid collisions during cache reading
- Analysis
  - Use the non-accessed Sets to eliminate candidates for all tables during 1st round
  - Optional: Second round analysis is possible too

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Arrow Attack

- Prime
  - Attacks the table separately (one per encryption)
  - Prepare only the Sets of one Table (T0,T1,T2 or T3)
- Probe
  - Each 4 access perform a reading until finish 1st round
  - Reads only the sets of current target table
  - Avoid collisions during cache read. Redo P+P with the same plaintext if there is no sufficient time.
- Analysis
  - Compute used sets for each plaintext to reveil the key

Countermeasure

Countermeasure: Traffic Mng

- Objectives:
  - Consider traffic anomalies as possible attacks
  - Distributed monitoring
  - Distributed decision
  - Light-weigth solution

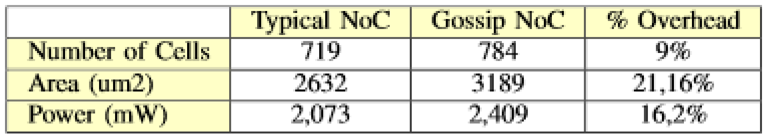
- Proposal 1:
  - Gossip NoC

Lehrstuhl für Sicherheit in der Informationstechnik

Gossip NoC

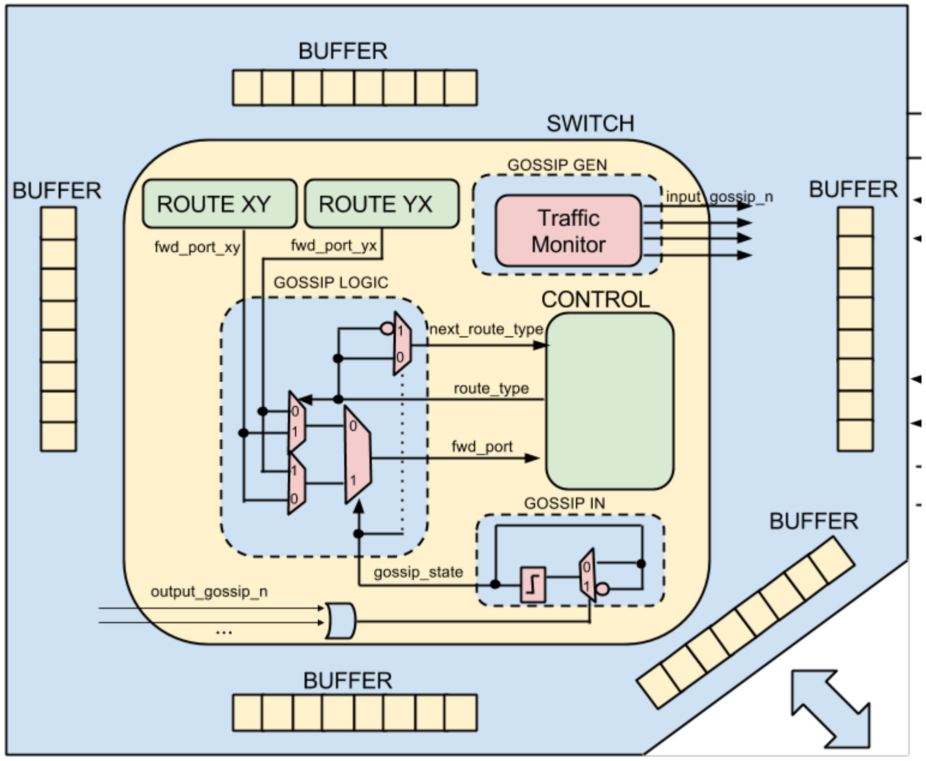
TECHNISCHE UNIVERSITÄT MÜNCHEN

- To detect traffic anomalie
- To inform neighbor routers about anomalie
- To change traffic algorithm for next packets



	Typical NoC	Gossip NoC	% Overhead
Number of Cells	719	784	9%
Area (um2)	2632	3189	21,16%
Power (mW)	2,073	2,409	16,2%

Synthesis results for a 65nm ASIC tech @1GHz.



LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Lehrstuhl für Sicherheit in der Informationstechnik

TECHNISCHE UNIVERSITÄT MÜNCHEN

Experiments & Demonstration

LABORATOIRE HUBERT CURIEN

UMR • CNRS • 5516 • SAINT-ETIENNE

Lehrstuhl für Sicherheit in der Informationstechnik

TECHNISCHE UNIVERSITÄT MÜNCHEN

Experimental Environment

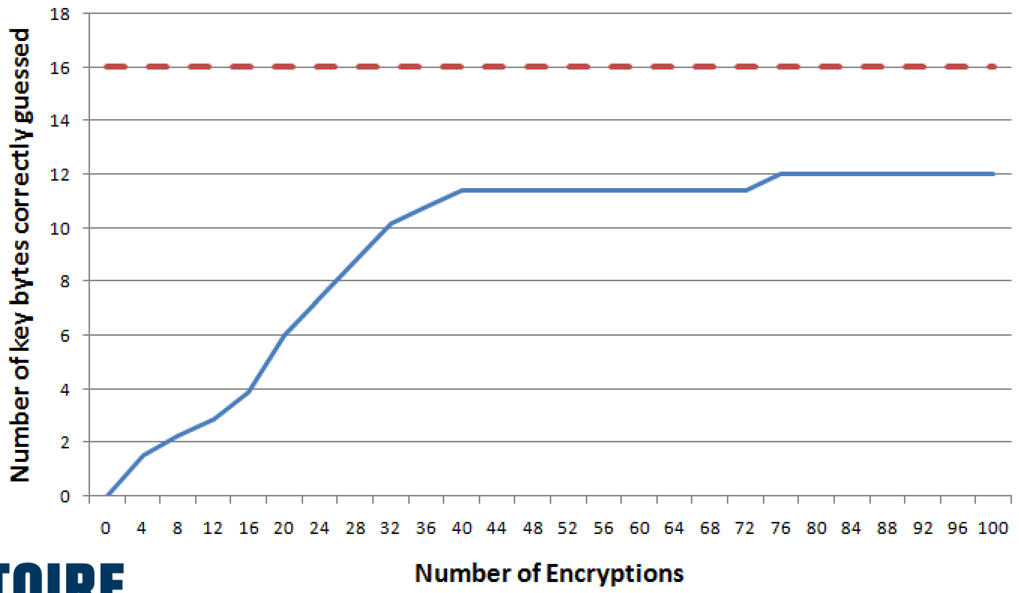
- Simulation Model
  - System C / VHDL (not synthesizeble)
  - To test insights and understand behavior
- Hardware Development System
  - MPSoC on FPGA
    - HPS (ARM Hard Core)
    - NIOS Processors
    - IO (UART)
    - Shared Cache Set Associative 16-way
    - Traffic Generators (General and Attacker)
- Host PC Software
  - Python script – MPSoC comm. and Analysis

LABORATOIRE HUBERT CURIEN

UMR • CNRS • 5516 • SAINT-ETIENNE

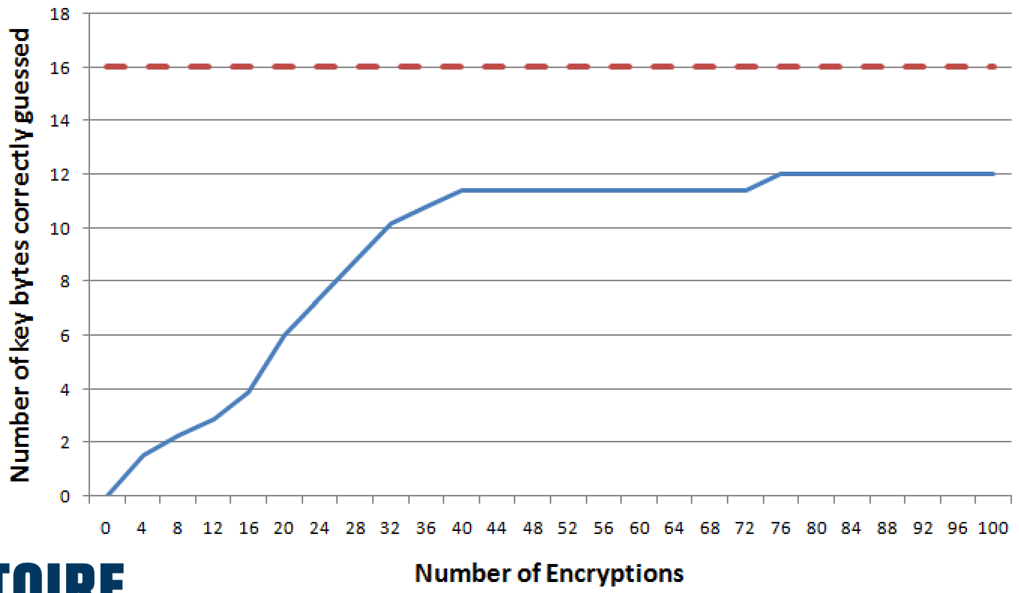
Firecracker Analysis

- Considering 12 cache access identifications
- Running 4 times each plaintext
- We reduced the search space 2^{128} *to* 2^{32} with only 20 different plaintext (80 encryptions)



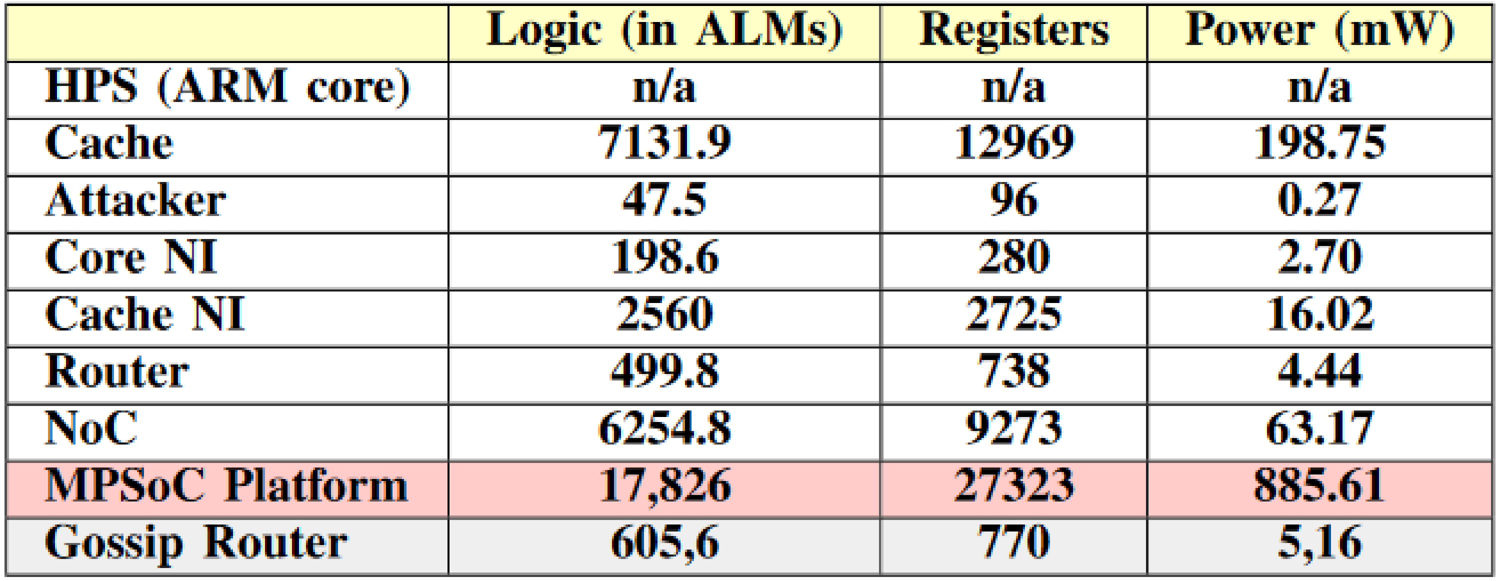
Arrow Analysis

- Considering 12 cache access identifications
- Running 4 times each plaintext
- We reduced the search space 2^{128} to 2^{32} with only 20 different plaintext (80 encryptions)



Hardware Costs

- FPGA Synthesis



	Logic (in ALMs)	Registers	Power (mW)
HPS (ARM core)	n/a	n/a	n/a
Cache	7131.9	12969	198.75
Attacker	47.5	96	0.27
Core NI	198.6	280	2.70
Cache NI	2560	2725	16.02
Router	499.8	738	4.44
NoC	6254.8	9273	63.17
MPSoC Platform	17,826	27323	885.61
Gossip Router	605,6	770	5,16

Lehrstuhl für Sicherheit in der Informationstechnik

TECHNISCHE UNIVERSITÄT MÜNCHEN

Demonstration

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Thank you