Master Thesis Topics

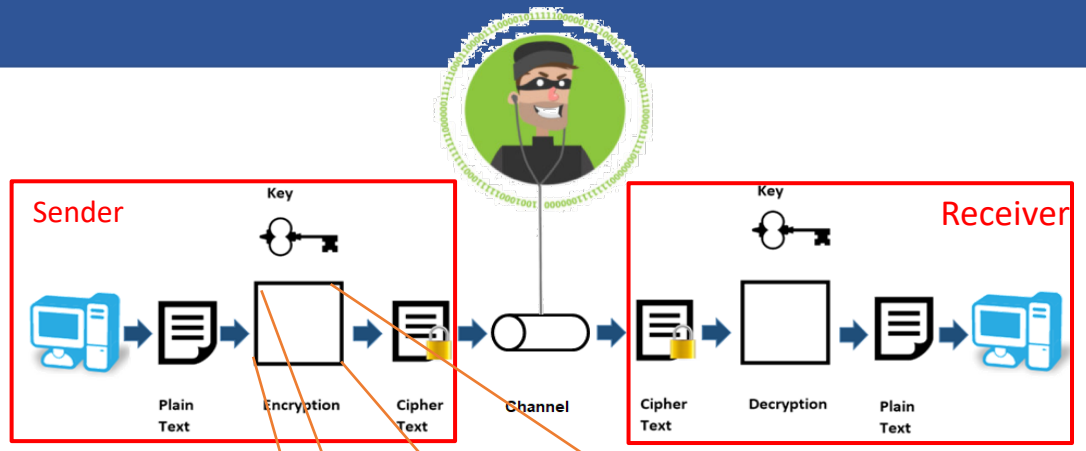
Hardware Security

Mottaqiallah Taouil (M.Taouil@tudelft.nl)
Cezar R. W. Reinbrecht (C.R.WedigReinbrecht@tudelft.nl)
14 May 2020

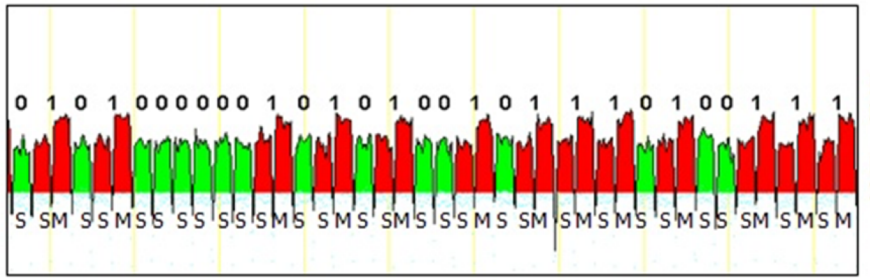
TU Delft
Delft University of Technology

Hardware Security

- Cybersecurity:
  - protection against attacks on computer systems
- Cryptography
  - AES: Internet communication, protect files
  - RSA: Bank communication, credit-card
- Hardware Vulnerabilities:
  - Technology
  - Design
  - Architecture



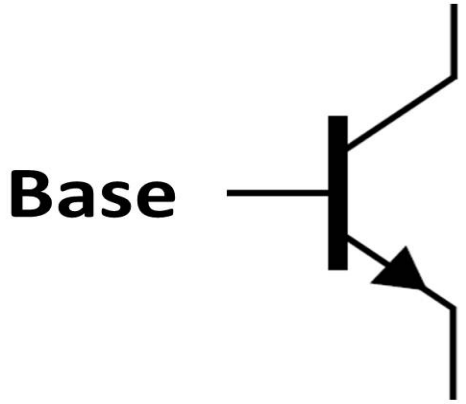

```
if (x == 1)
   f1()
end
```



OBSERVE POWER CONSUMPTION

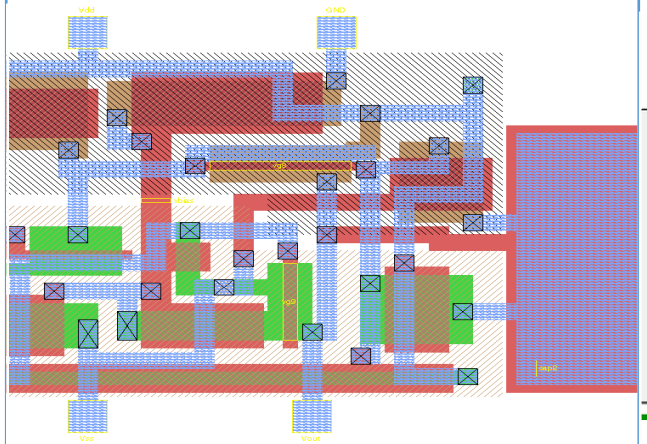
Hardware Vulnerabilities

Technology



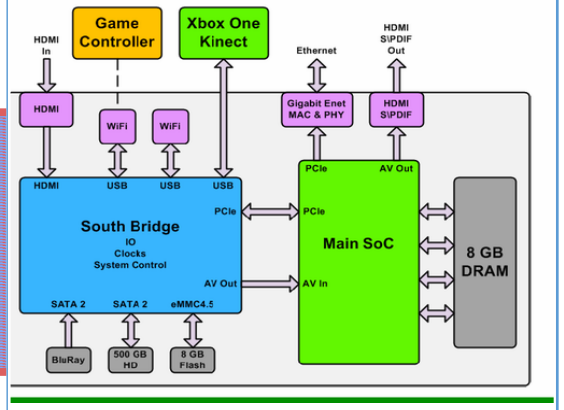
- Probe voltages/currents
- Change voltage/currents
- Current drain
- Heat observation
- EM emission
- Noise emission

Design



- Observation of RTL, netlist or layout
- Accessible test structures
- Presence of spare cells and empty routing area can be exploited

Architecture

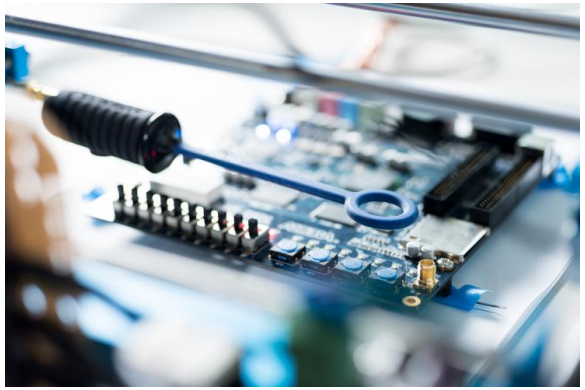


- Instructions and operations take different time
- Latency to memory depends on cache
- Configuration registers (privilege control)
- Observe hardware performance counters

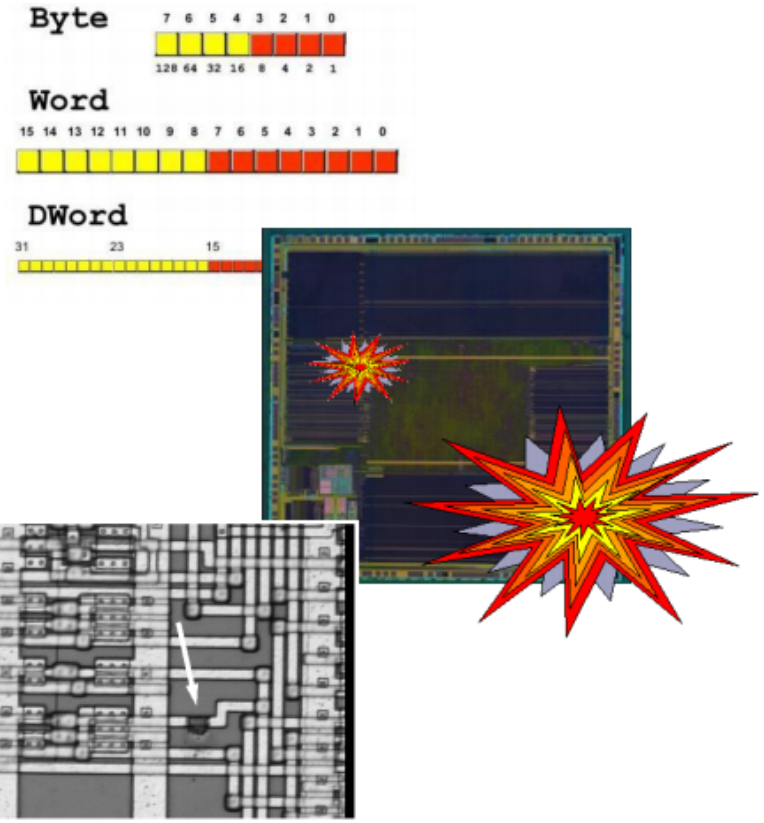
Hardware Vulnerabilities

- Examples:

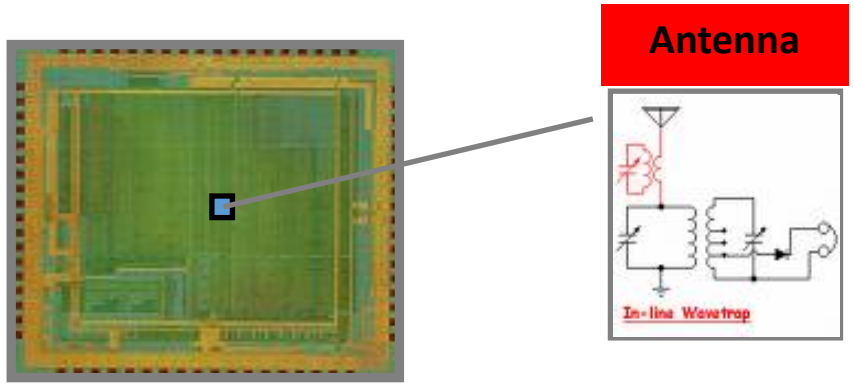
TECHNOLOGY – Side Channel Analysis



ARCHITECTURE – Fault Injection



DESIGN - Hardware Trojan



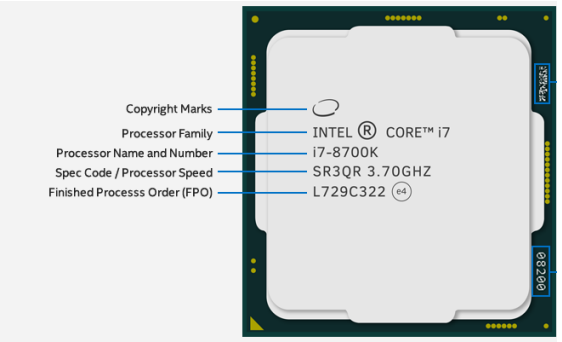
Hardware Countermeasures – IC Metering

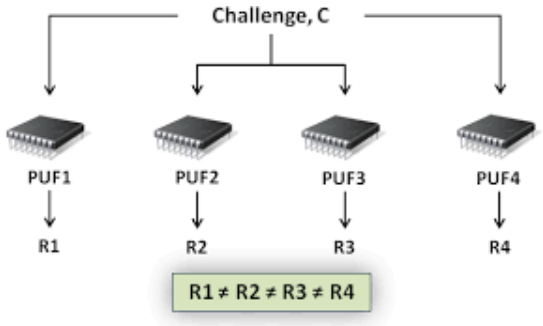
- **Passive Metering - identification**
  - Provides passive ways for designers to identify IC after manufacturing process

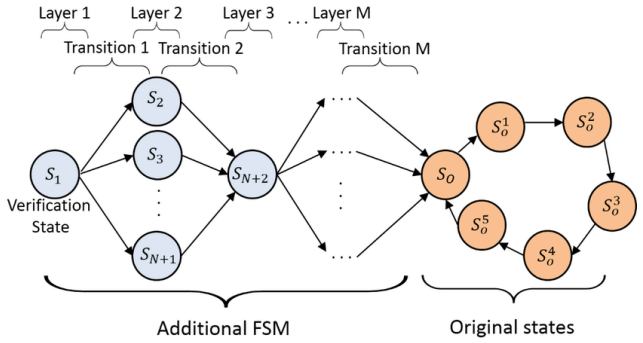
- **Active Metering – monitoring and control**
  - Provides active ways for designers to identify, enable, control, or disable IC after manufacturing process
  - Unlike passive metering, active metering requires communication between IP owner and the chip for proper activation

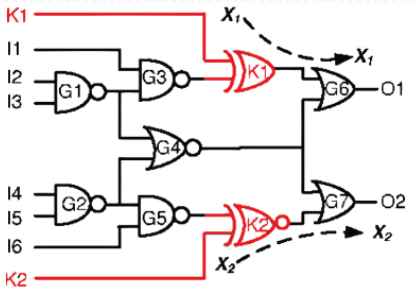
Passive (Identification):
- Reproducible: IDs/Watermark
- Unique: Fingerprint

Active:
- FSM obfuscation
- Gate obfuscation (Logic Locking)









Hardware Attacks and Design for Security

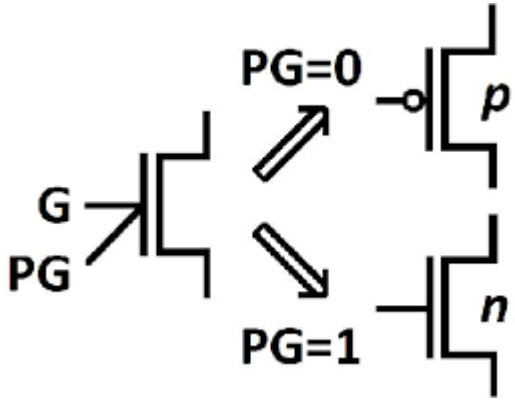
Research Topics

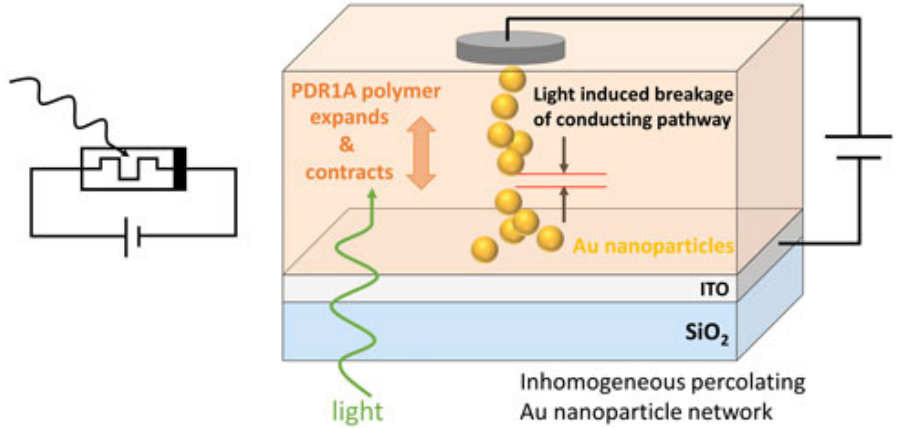
Passive Metering – Unique ID Generation

1. Use special circuits to create unique IDs
   - Polymorphic gates

2. Use emerging technologies to intentionally create IDs:
   - Memristors

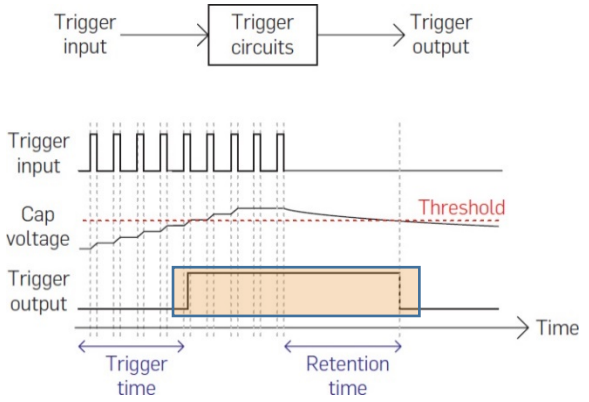
- Research
  - Generate unique signatures inside Chip
  - Elaboration of ID circuit
  - Electrical simulations

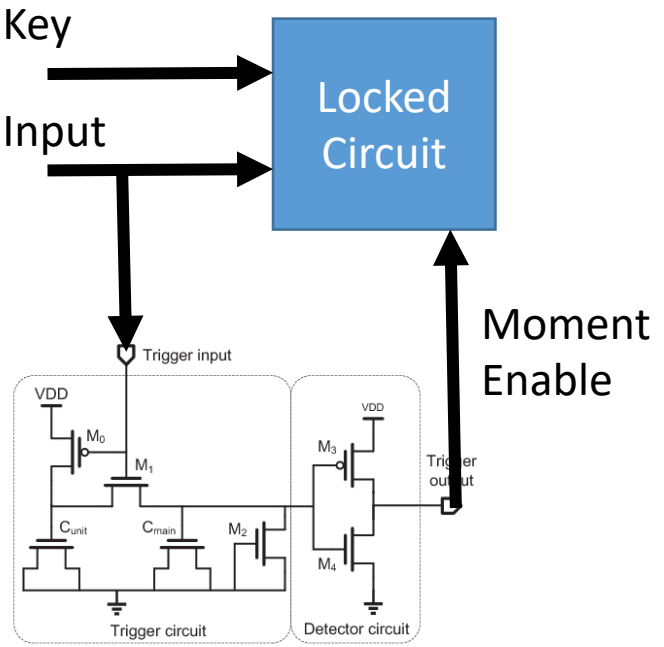




Active Metering – Time-Dependent Logic Locking

- Logic Locking Scheme will depend on:
  - Key
  - Input
  - Moment – "Exact time to unlock IC"

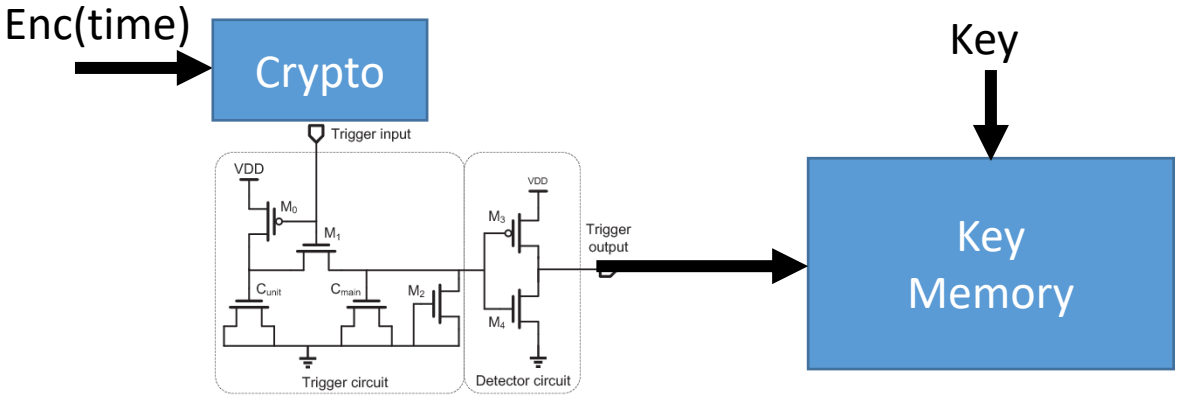




- Research
  - Design trigger circuit
  - Elaborate LL scheme that depends on time

1. Internal:
   - Only when Moment Enable is 1, Key enters unlocking

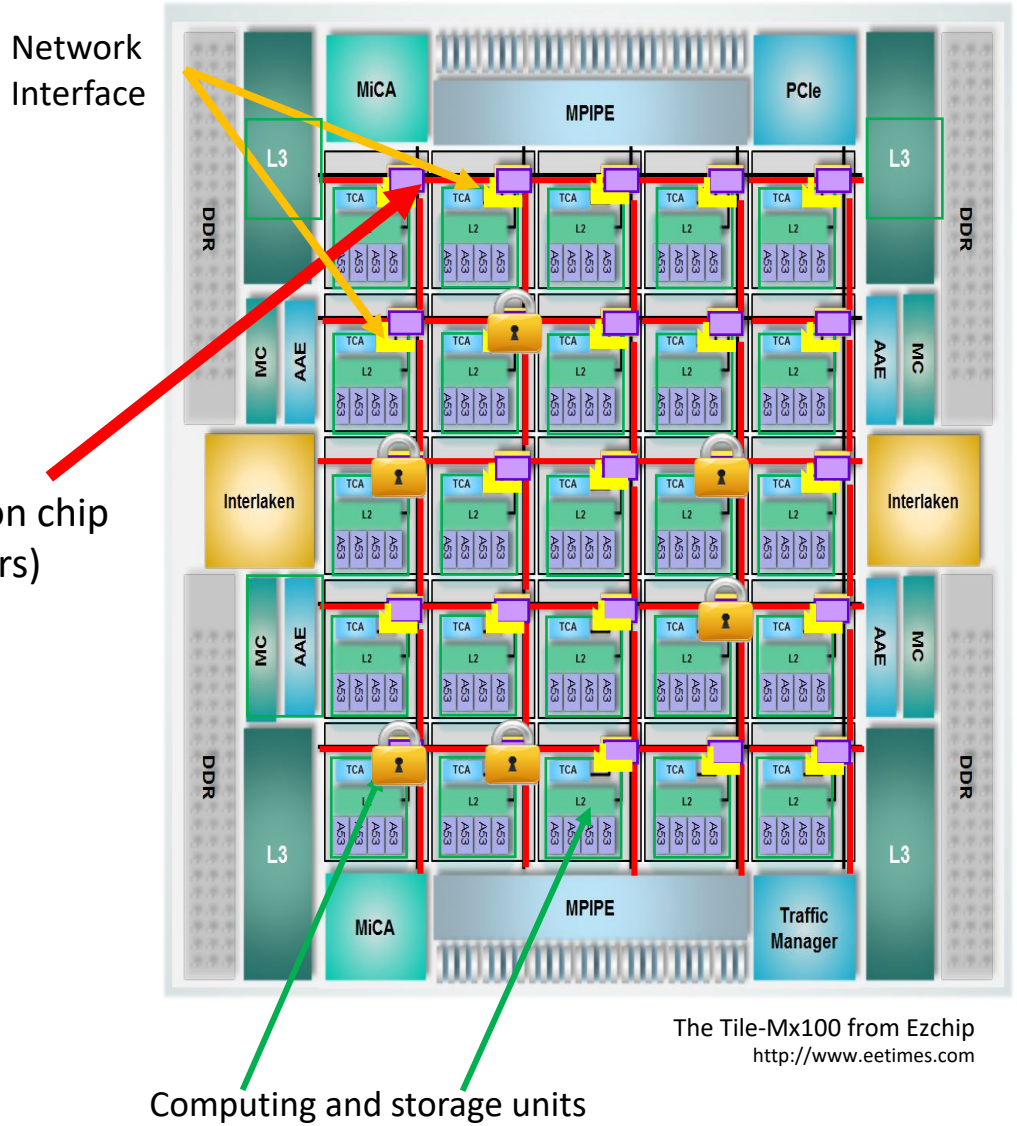
2. External:
   - Crypto used to establish time of unlocking
   - Key must be applied at specific time to be stored



Active Metering – Net-Lock

- Network-on-Chip Logic Locking
  - NoC integrates many elements
  - Lock routers means Lock IPs

- Research
  - Integrate Logic Locking scheme in a NoC Router
  - Elaborate online logic locking scheme
    - Activate/Deactivate IPs in the field
    - Cryptography and Protocols



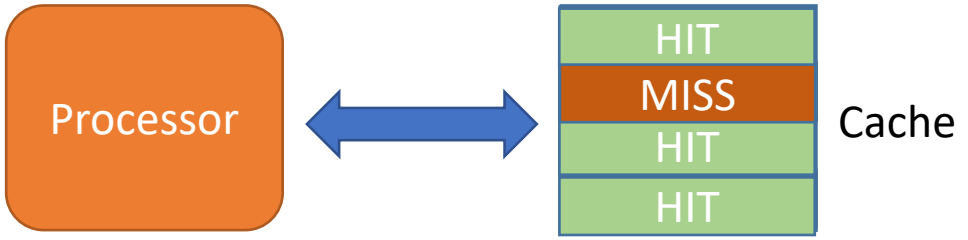
The Tile-Mx100 from Ezchip
http://www.eetimes.com

Design-for-Security – Attack Models and Countermeasures

- Caches are vulnerable to attacks
  - Several popular attacks
  - Attacks can be modeled

In collaboration with University of Technology of Talinn

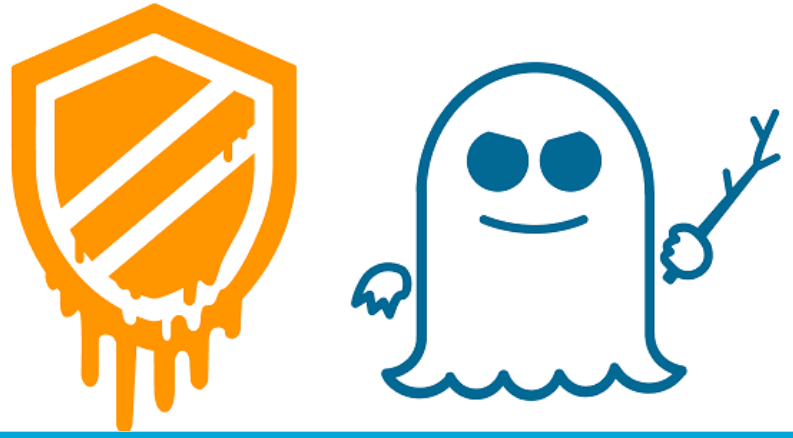
- Research
  - Evaluate existing attack models
  - Elaborate new attack models
  - Develop methodologies to verify/evaluate security of designs
  - Develop new countermeasures based on attack models



1) Attacker prepares the Cache
2) Victim uses the Cache
3) Attacker access the Cache

ID	attack $formula$	ID	attack $formula$	*
1	$Vx \to Ar \to Vx$	15	$Vx \to Vx \to Ar$	d
2	$Vx \to Vr \to Vx$	16	$Ar \to Vx \to Vr$	d
3	$Ar \to A1 \to Vx$	17	$Vr \to Vx \to Vr$	d
4	$Vr \to A1 \to Vx$	18	$Vx \to Vx \to Vr$	d
5	$A1 \to A1 \to Vx$	19	$Ar \to Vx \to A1$	e
6	$V1 \to A1 \to Vx$	20	$Vr \to Vx \to A1$	e
7	$Vx \to A1 \to Vx$	21	$A1 \to Vx \to A1$	f
8	$Vx \to A1 \to Vx$	22	$V1 \to Vx \to A1$	-
9	$Vr \to V1 \to Vx$	23	$Vx \to Vx \to A1$	e
10	$A1 \to V1 \to Vx$	24	$Ar \to Vx \to V1$	b
11	$V1 \to V1 \to Vx$	25	$Vr \to Vx \to V1$	b
12	$Vx \to V1 \to Vx$	26	$A1 \to Vx \to V1$	-
13	$Ar \to Vx \to Ar$	27	$V1 \to Vx \to V1$	c
14	$Vr \to Vx \to Ar$	28	$Vx \to Vx \to V1$	b

28 Attacks Modeled



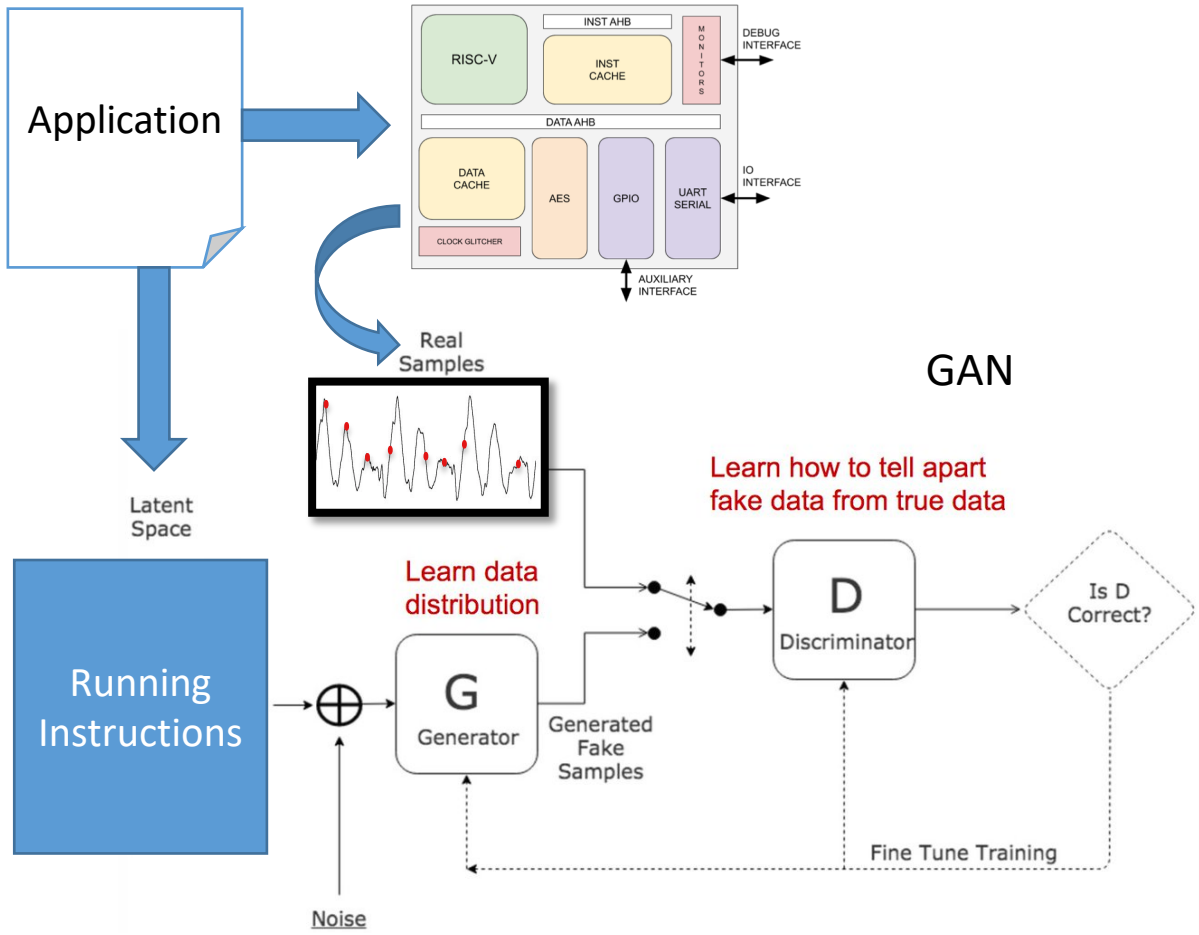
Design-for-Security – ORGANICS

- Generate power traces as they were "real"
  - Uses Generative Adversarial Networks (GAN)
  - Train the GAN to generate traces of a processor running applications

- Research:

1. Leakage Analysis or Attack Evaluations
   - Real power traces are used to train GAN
   - To be used when there is no physical access

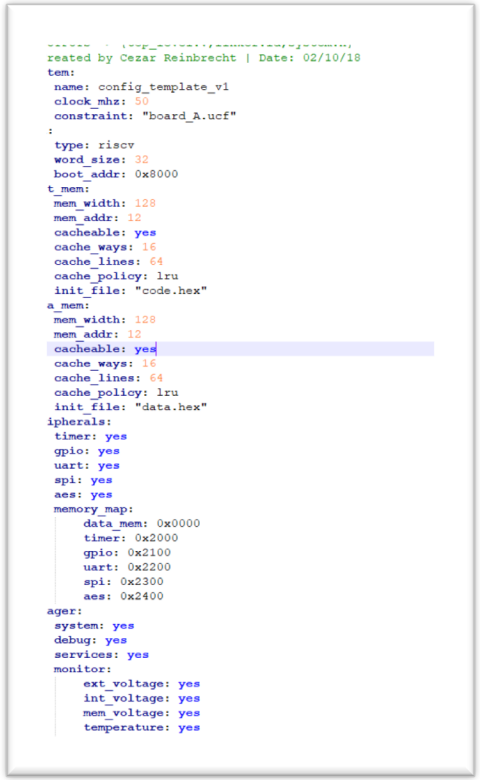
2. Secure IC design
   - Electrical Simulations train GAN
   - Security Evaluation of IC at design-time (new EDA tools?)

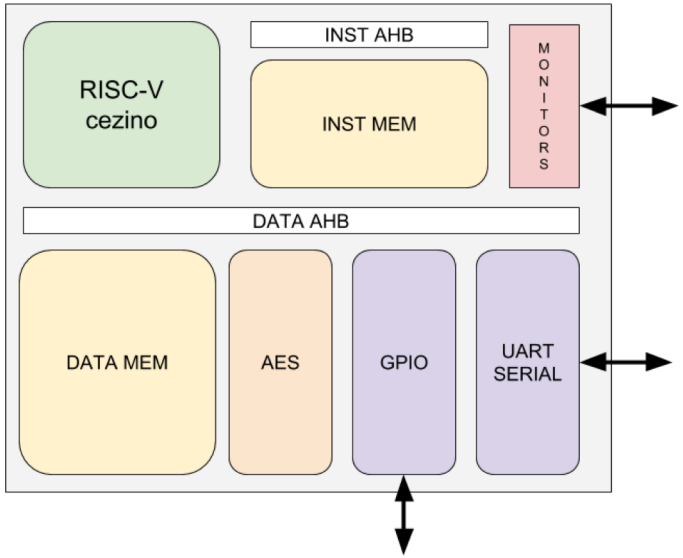


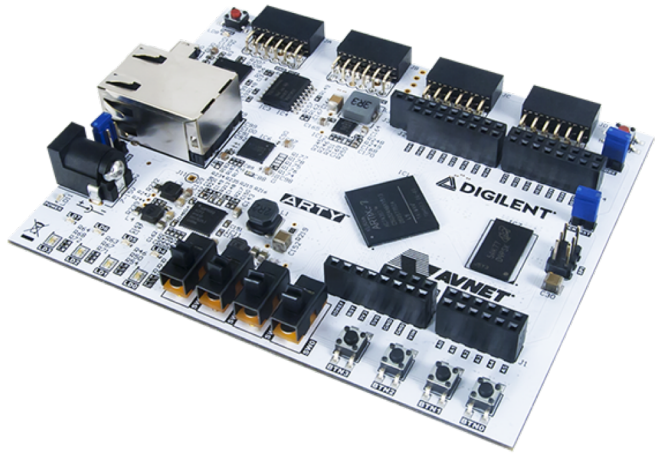
Design-for-Security – Hardware Security Platform

- Features:
  - IP-based flow – Customizable SoC
  - Top-level generation based on configuration file
  - Easy to simulate or emulate in FPGA (automated scripts)
  - Vendor-independent design
  - Use popular processors (mainly RISC-V)

- Objectives:
  - Perform Attacks:
    - Physical Side Channel Analysis
    - Logical Side Channel Analysis
    - Fault Injection
    - HW Trojans
  - Evaluates Countermeasures
    - Software
    - Hardware

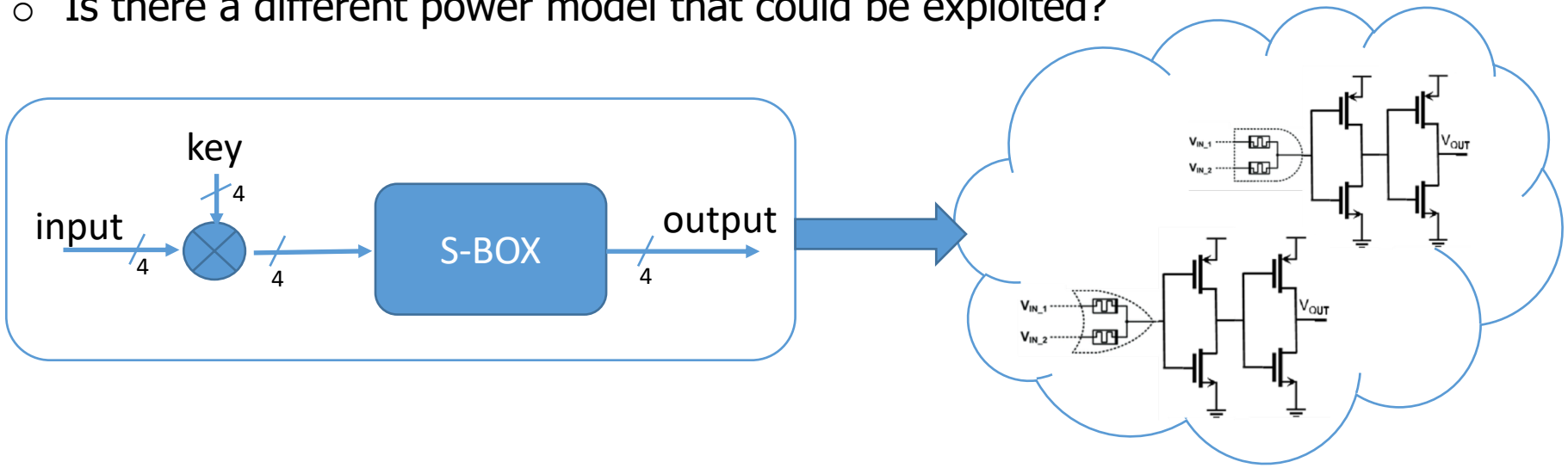






Emerging Technologies – Security Aspects of Memristors

- Research
  - Use MRL circuit to design a small cipher block (based on S-Box)
  - Perform electrical simulations
  - Evaluate with different cryptanalysis methods how difficult is to attack
  - Understand the power behaviour and leakage behaviour
    - Is there a different power model that could be exploited?



Master Thesis Topics

Thank you

Mottaqiallah Taouil (M.Taouil@tudelft.nl)
Cezar R. W. Reinbrecht (C.R.WedigReinbrecht@tudelft.nl)
14 May 2020