How to recognize a bad PUF

Vincent van der Leest, Intrinsic-ID

Berlin, November 3rd 2013

PUFFIN workshop

Presentation Outline

Introduction

PUFs and performed tests

Test results and analysis

Conclusions

Introduction

- During PUFFIN project measurements have been performed on many potential PUF instantiations
- PUFs are based on SRAM from different COTS devices
- Limited number of devices measured per PUF type
- Tests performed under limited different circumstances
- Data sets only allows for preliminary analysis

How can we make a first distinction between “good” and “bad” PUFs based on this limited amount of data?

PUFs and performed tests

Analysed devices:

- Tablets:
  - Ainol Novo 7
  - Pandaboard
- Microcontrollers:
  - Texas Instruments MSP430F5308
  - Microchip PIC16F1825
  - ST STM32F100R8/B
  - Atmel ATMega328p
- GPU: NVIDIA GeForce GTX 295 graphics cards

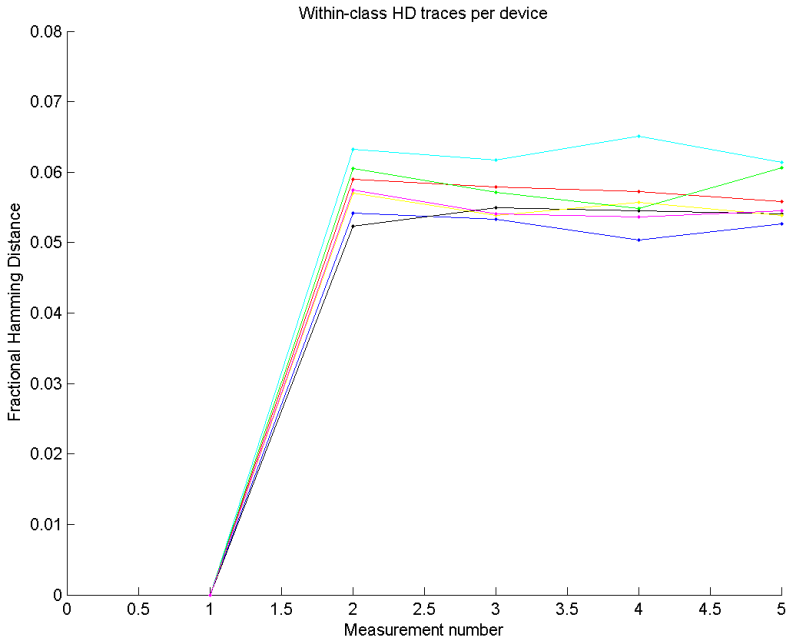
PUFs and performed tests

Performed tests:

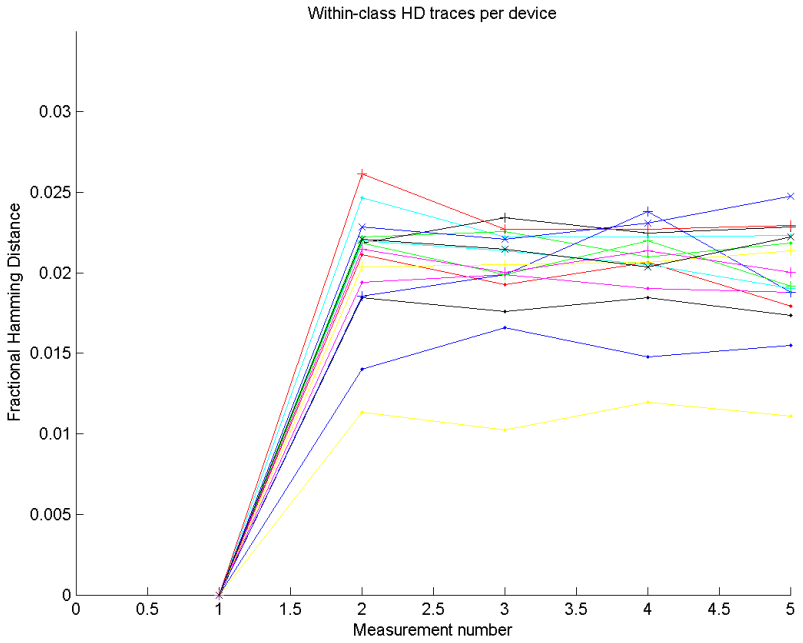
- Repeated Start-up Test
  - Measure PUFs multiple times under stable conditions
- Between-class Hamming Distance Test
  - Compare enrollment measurements from different devices
- Hamming Weight Test
  - Count number of 0's and 1's in PUF measurements
- Temperature Cycle Test
  - Measure PUFs multiple times at varying ambient temperatures

Test results and analysis

Repeated Start-up Test



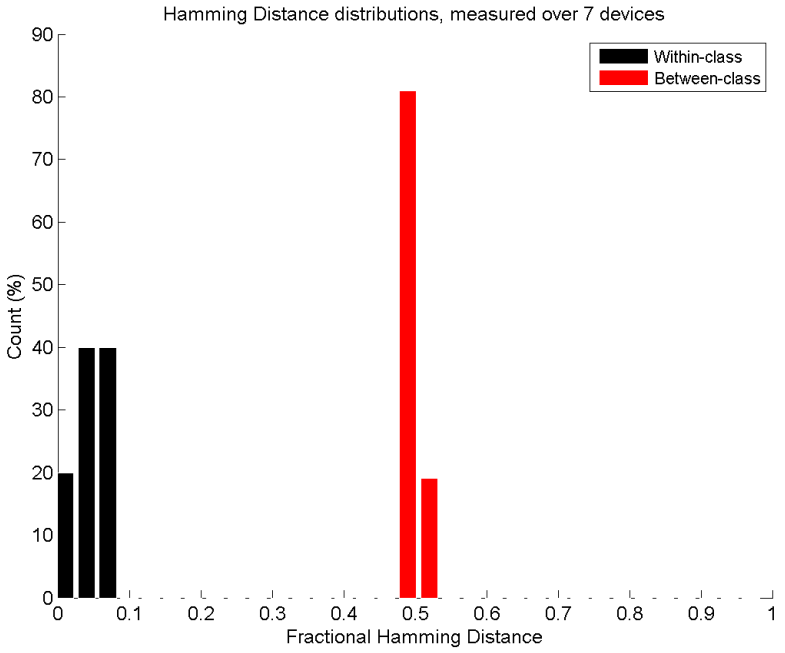
Good: Ainol Novo 7 tablet

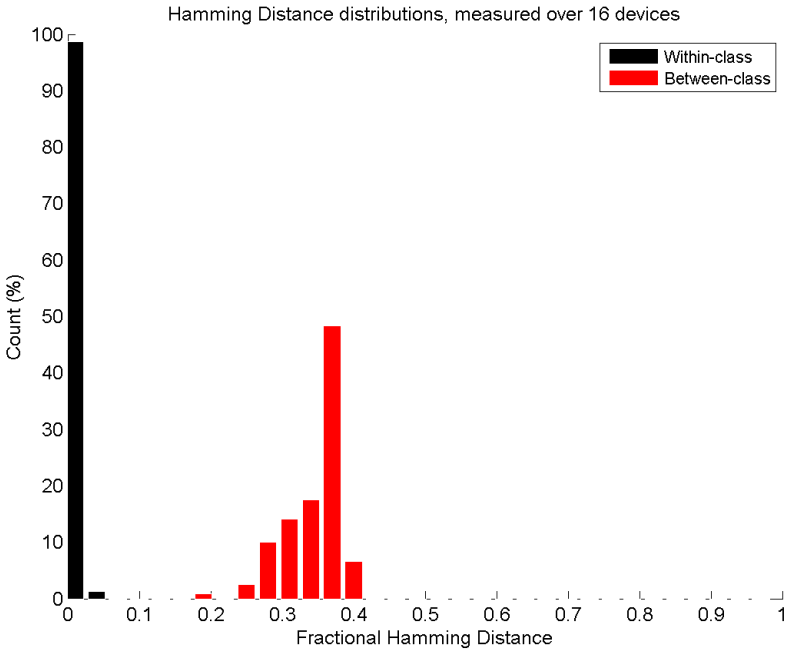


Good: PIC16F1825 microcontroller

Test results and analysis

Between-Class Hamming Distance Test



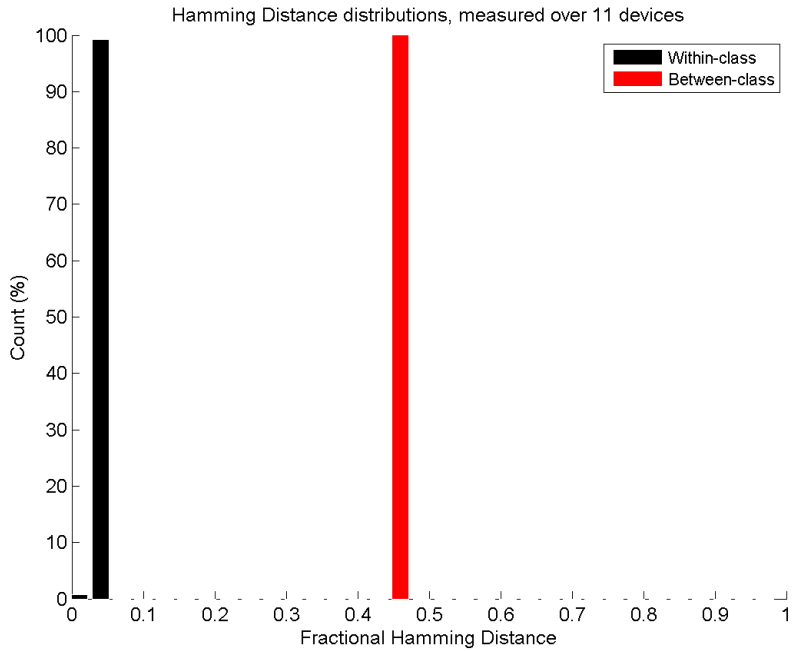


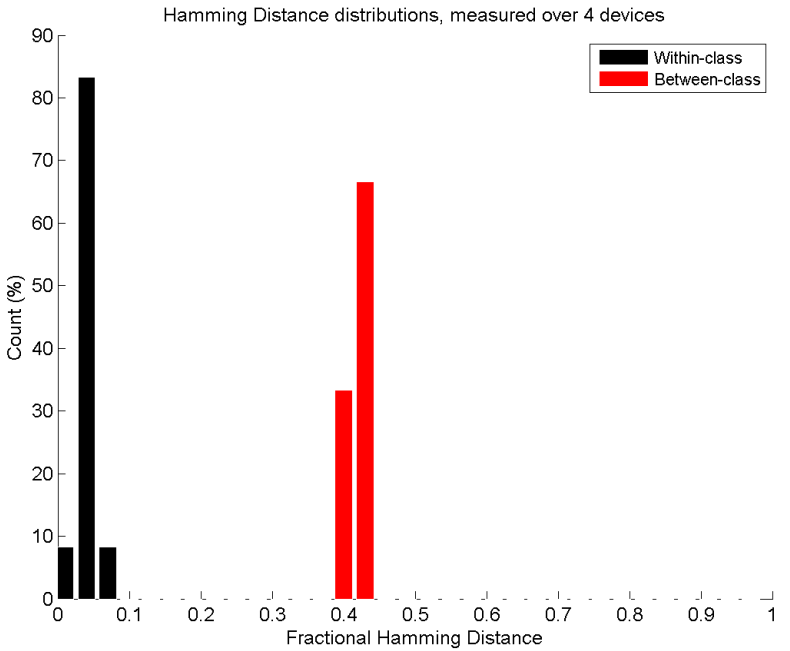
Good: Ainol Novo 7 tablet

Bad: PIC16F1825 microcontroller

Test results and analysis

Between-Class Hamming Distance Test



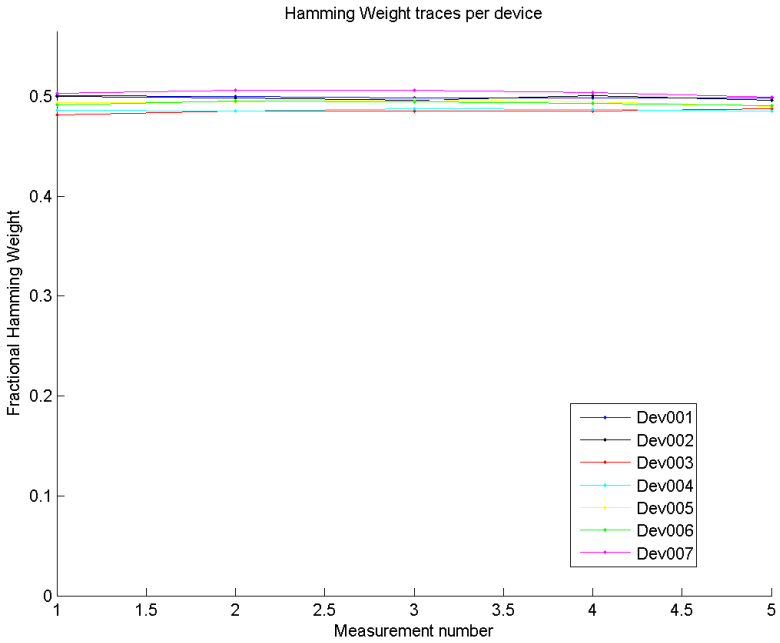


Reasonable: ST STM32F100R8

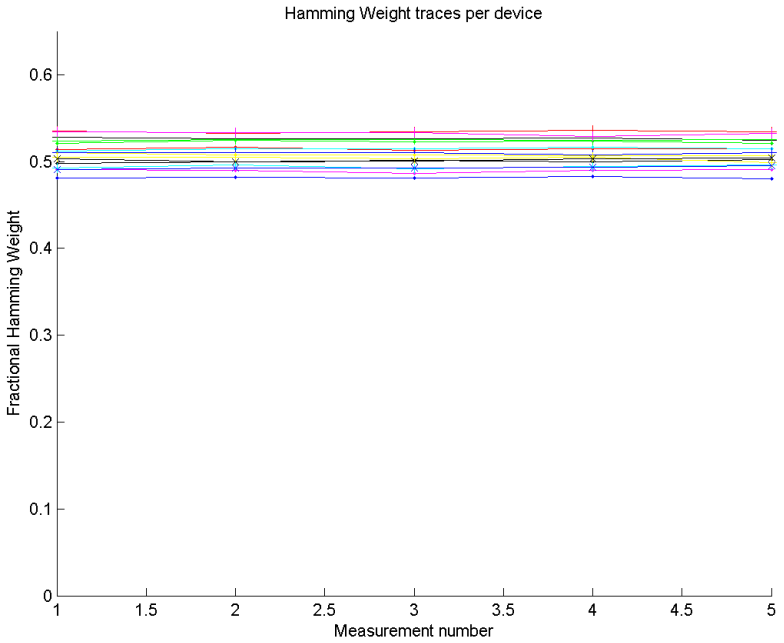
Reasonable: NVIDIA GeForce GTX 295

Test results and analysis

Hamming Weight Test



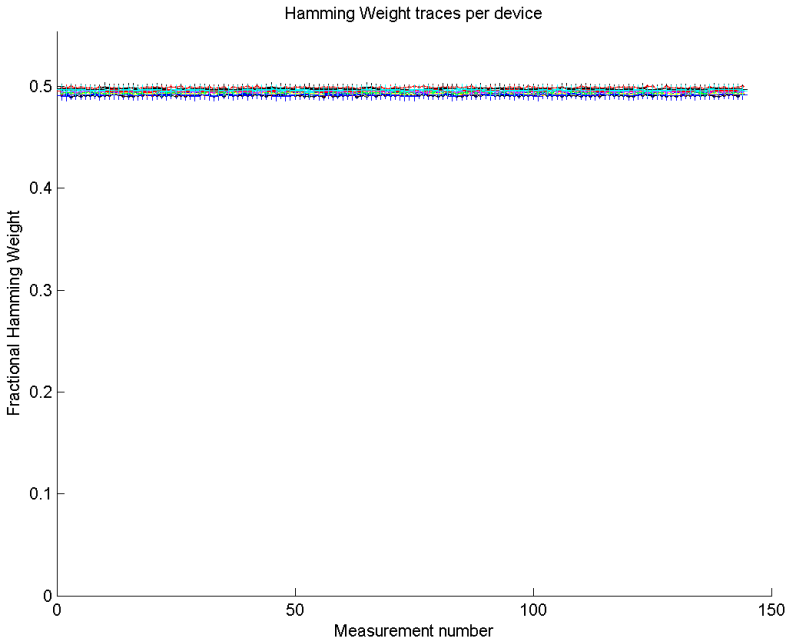
Good: Ainol Novo 7 tablet



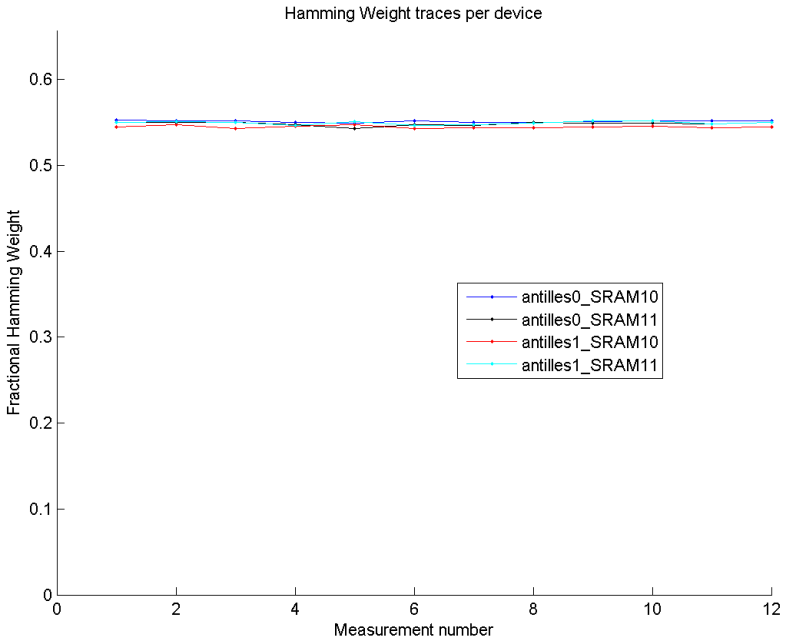
Good: PIC16F1825 microcontroller

Test results and analysis

Hamming Weight Test



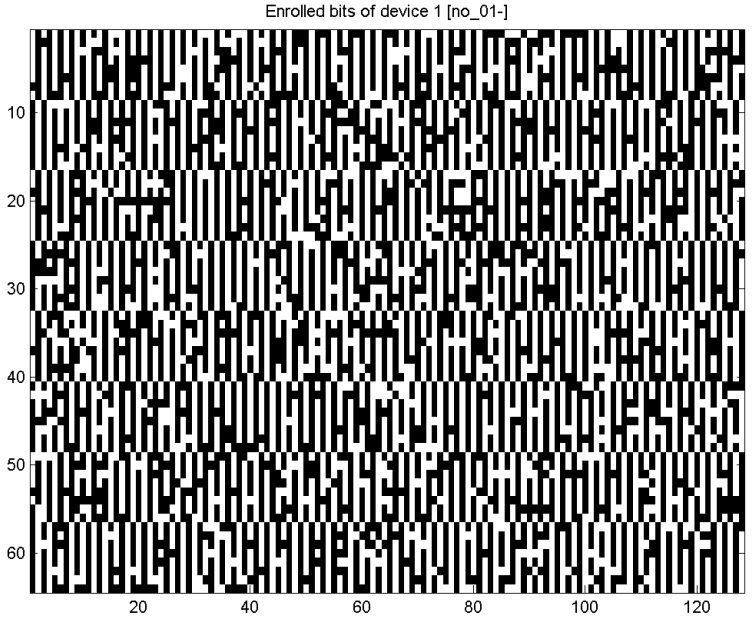
Good: ST STM32F100R8



Reasonable: NVIDIA GeForce GTX 295

Test results and analysis

Examples of start-up patterns

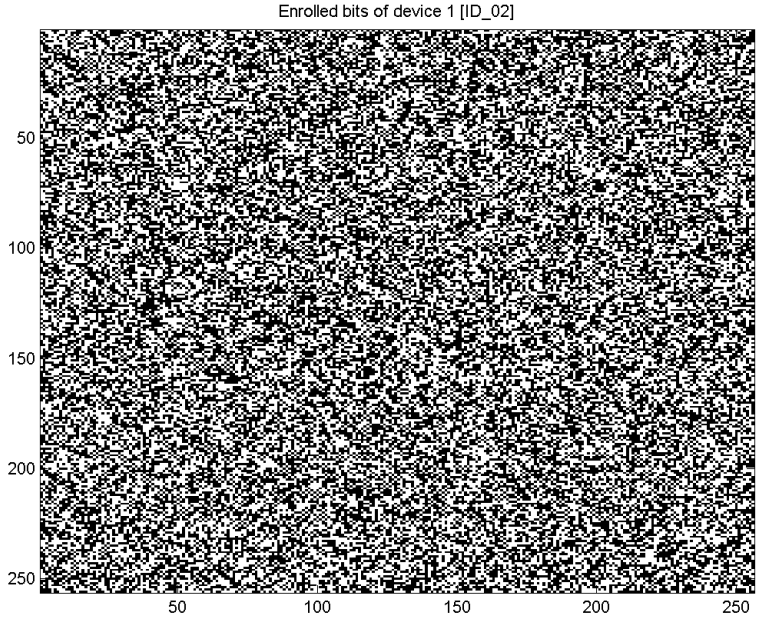


Good: Ainol Novo 7 tablet

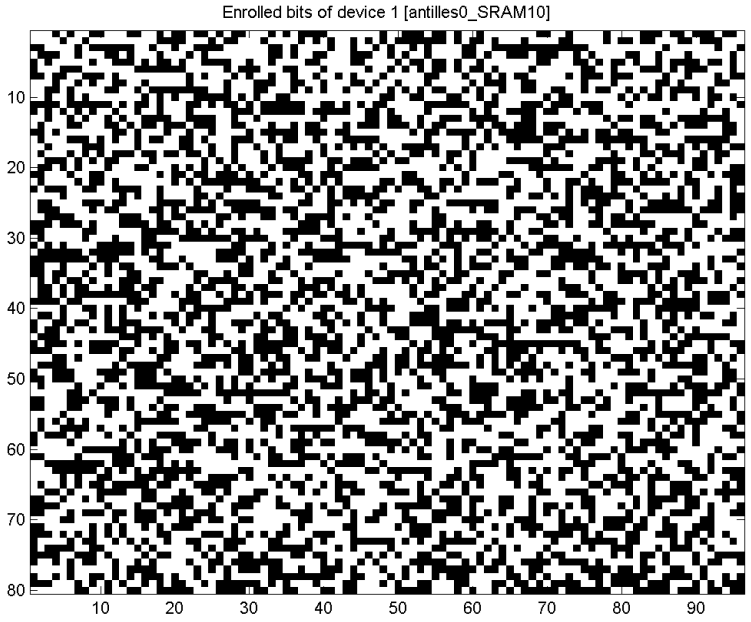
Bad: PIC16F1825 microcontroller

Test results and analysis

Examples of start-up patterns



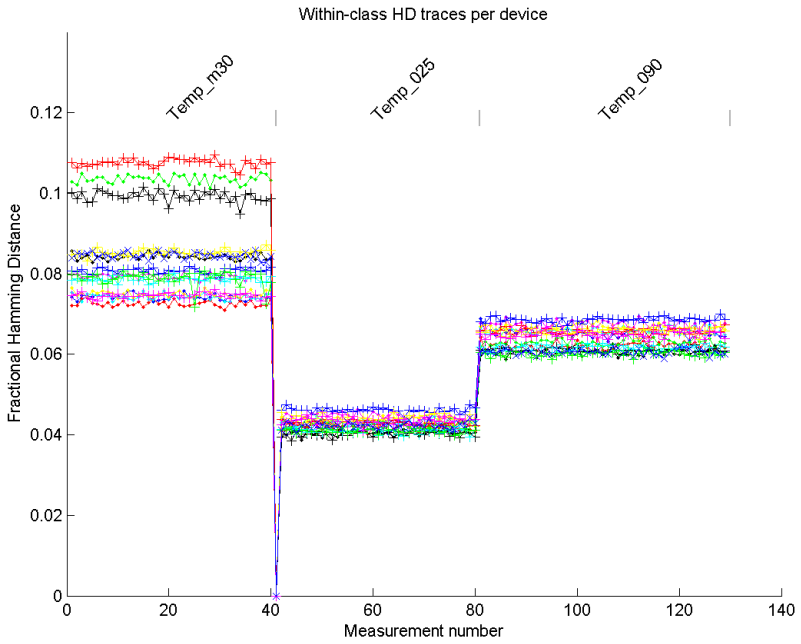
Good: ST STM32F100R8

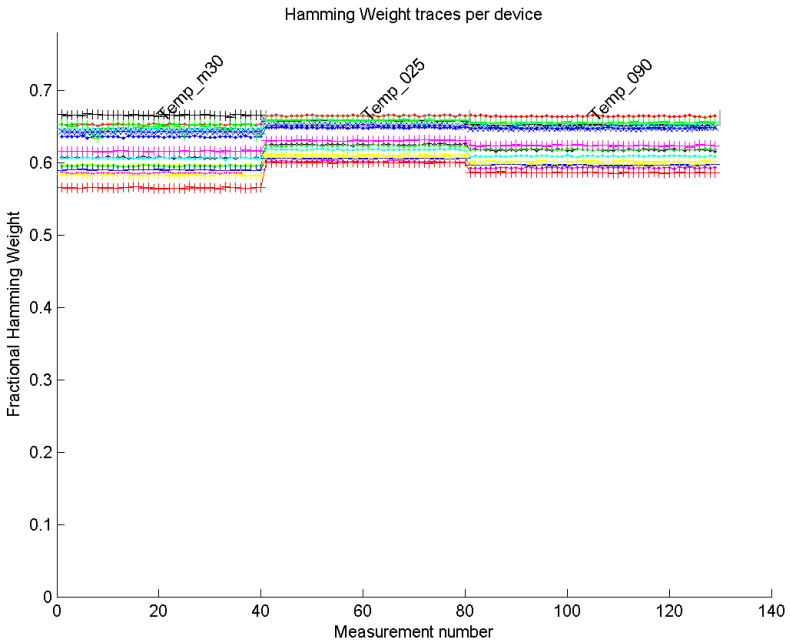


Reasonable: NVIDIA GeForce GTX 295

Test results and analysis

Temperature Cycle Test





Good: TI MSP430F5308

Hamming Weight Test: **Biased**

Test results and analysis

Type	Device	Quantity	RST	BCHDT	HWT	Remark
Tablets	Ainol Novo 7	7	Pass	Pass	Pass	Good PUF!
	Pandaboard	5	Pass	Pass	Pass	Good PUF!
Micro-controllers	TI MSP430F5308	15	Pass	(Weak) Pass	(Weak) Pass	Biased PUF
	PIC16F1825	16	Pass	Fail	Fail	Bad PUF!
	ST STM32F-100R8/B	11	Pass	(Weak) Pass	Pass	Correlation b/t devices
	Atmel ATMega328p	16	Pass	(Weak) Pass	(Weak) Pass	Biased PUF
GPU	NVIDIA GTX 295	4	Pass	(Weak) Pass	(Weak) Pass	Biased PUF

Conclusions

Conclusions:

- PUFs have been found in (SRAMs of) many different COTS devices
- Most measured SRAMs show promising results and could be suitable for PUF implementations
- Amount of pre-processing required will vary between PUFs
- **Note:** Temperature Cycle Test only performed on microcontrollers, since other devices will not survive extreme temperatures

- PIC16F1825 only device where SRAM definitely not usable as PUF
- This is due to severe (bytewise) biasing of the PUF responses, which is most likely caused by issues with power-up circuitry of SRAM