tesi di laurea magistrale

Mechanisms to Protect Intellectual Properties: the Physically Unclonable Functions Technology Approach

Anno Accademico 2014/2015

relatore
Ch.mo prof. Antonino Mazzeo

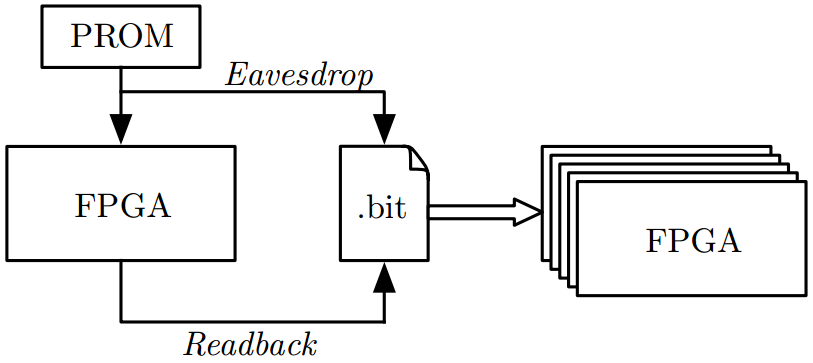
correlatore
Ing. Mario Barbareschi

candidato
Pierpaolo Bagnasco
Matr. M63/354

Introduction

- **Problems:**
  - Theft of Intellectual Property (IP)
  - Production of counterfeits components

- **Threats to hardware design:**
  - Reverse engineering
  - Cloning
  - Overbuilding
  - Tampering



Physically Unclonable Functions

- Physical(ly) Unclonable Functions (PUFs) exploit physical properties of imperfections which are randomly introduced by the manufacturing processes
- The function maps a set of inputs (**challenges**) to a set of outputs (**responses**), defining an unclonable and unique challenge/response pairs (CRPs) set
- The PUF concept can be used also in Integrated Circuits (ICs), with the introduction of Silicon PUFs
  - the process is the photolithography;
  - challenges are the applied electrical stimuli;
  - responses are the PUF's outputs.

PUF Quality Factors

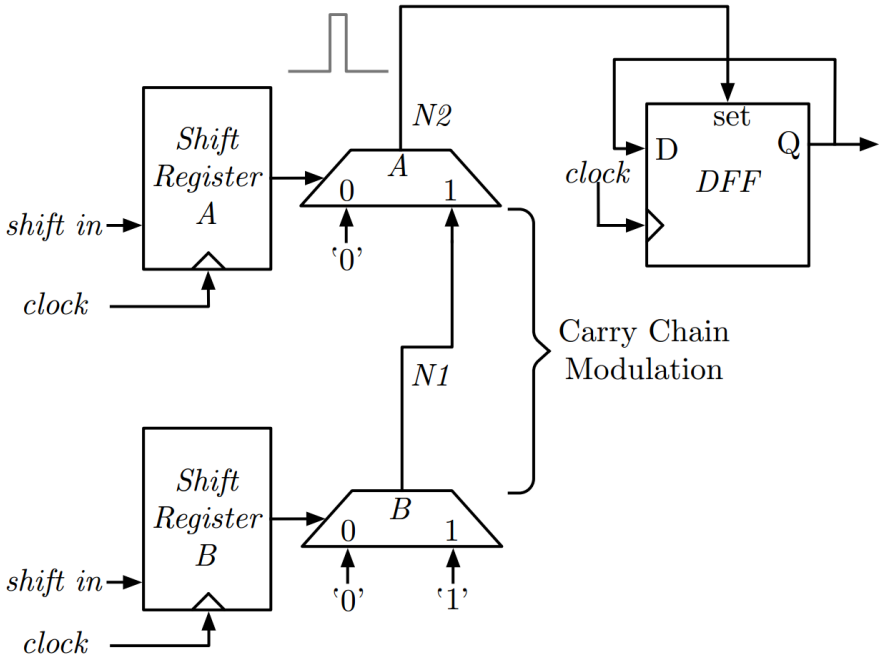
- **Uniqueness:** $$U = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \cdot 100\%$$

- **Uniformity:** $$RU(i) = \frac{1}{n} \sum_{t=1}^{n} R_{i,t} \times 100$$

- **Reliability:** $$HD_{intra} = \frac{1}{k} \sum_{j=1}^{k} \frac{HD(R_i, R'_{i,j})}{n} \times 100$$

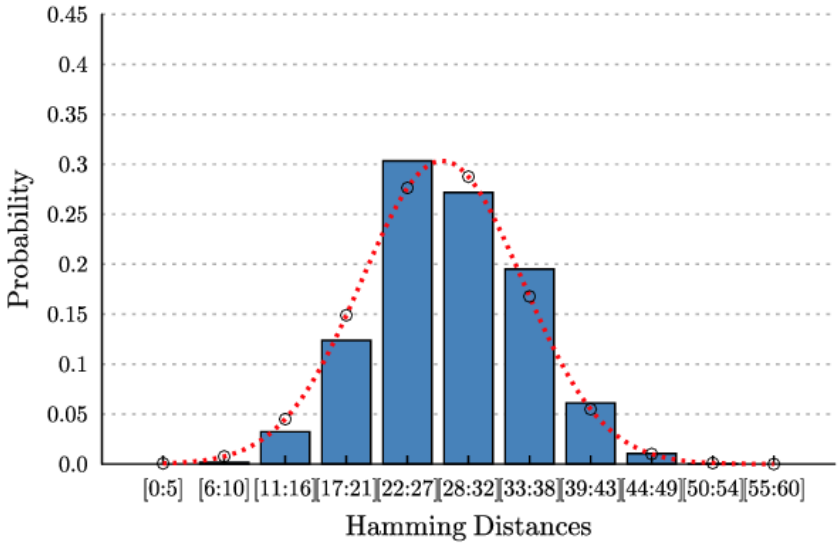
Anderson PUF Cell

- A glitch is generated trough 2 alternating sequences in counter-phase
- Due to manufacturing imperfections, the glitch has a different width for each cell
- The cell design perfectly matches the Xilinx Virtex-5 FPGA structure
- We ported the Anderson PUF on the Spartan-3E FPGA, enabling protection mechanisms even on low-cost devices



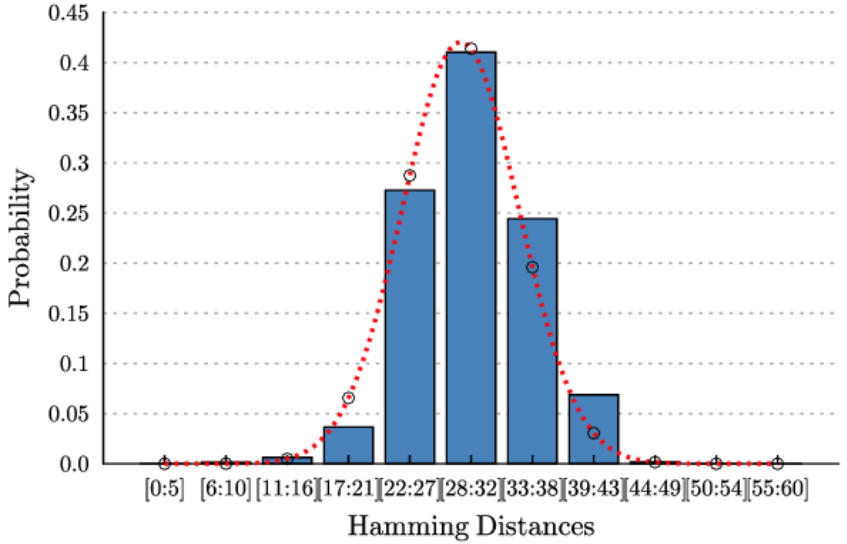
Anderson PUF Qualities

- **15 different FPGAs (XC3S1200E)**



Anderson PUF

Average Uniqueness value: 47.18%
Average Uniformity Value: 50.59%

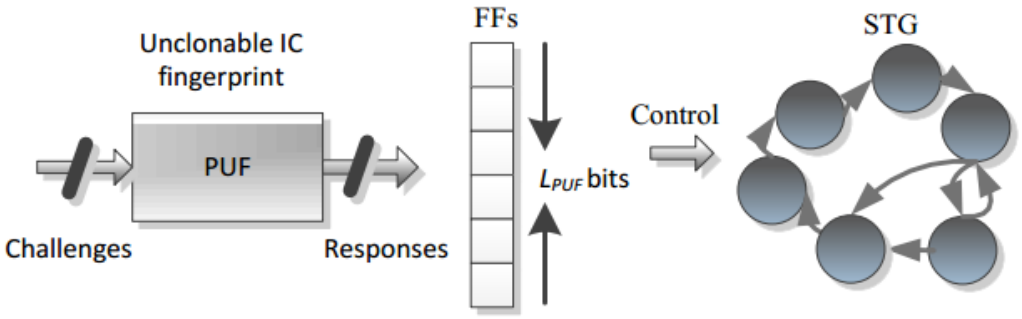


Enhanced Anderson PUF

Average Uniqueness value: 49.37%
Average Uniformity Value: 50.99%

FSM-Based IP Licensing Mechanism

- Enables a protection mechanism for low-cost FPGAs
- A *secure* FSM is added into the original IP core design
- The FSM enables the IP core only if the PUF response and the license are valid

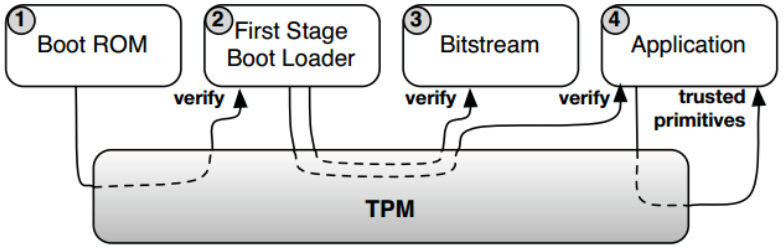


FPGA	Slices	Flip-flops
XC3S1200E	1.25%	0.43%
XC7Z020	0.26%	0.07%

60 bits case of study

Dynamic Hardware-IP Protection

- A *Security Module* (SM) is programmed into the device exploiting a secure boot procedure based on Trusted Platform Module (TPM)

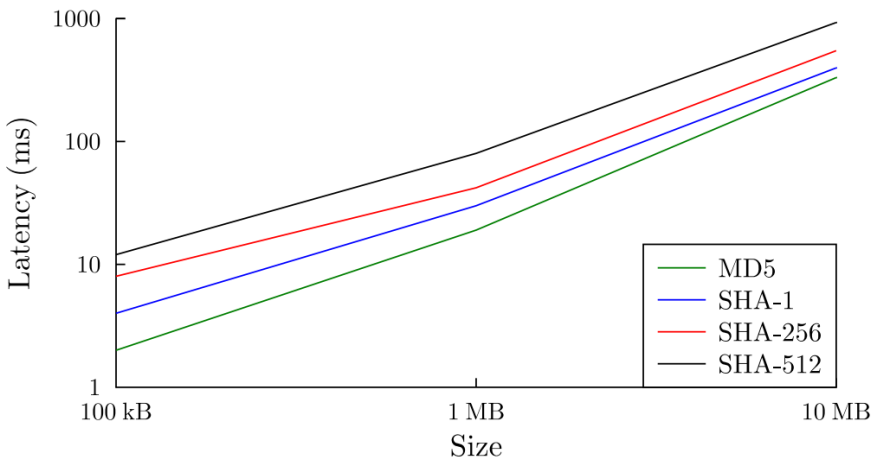


(Chain of trust)

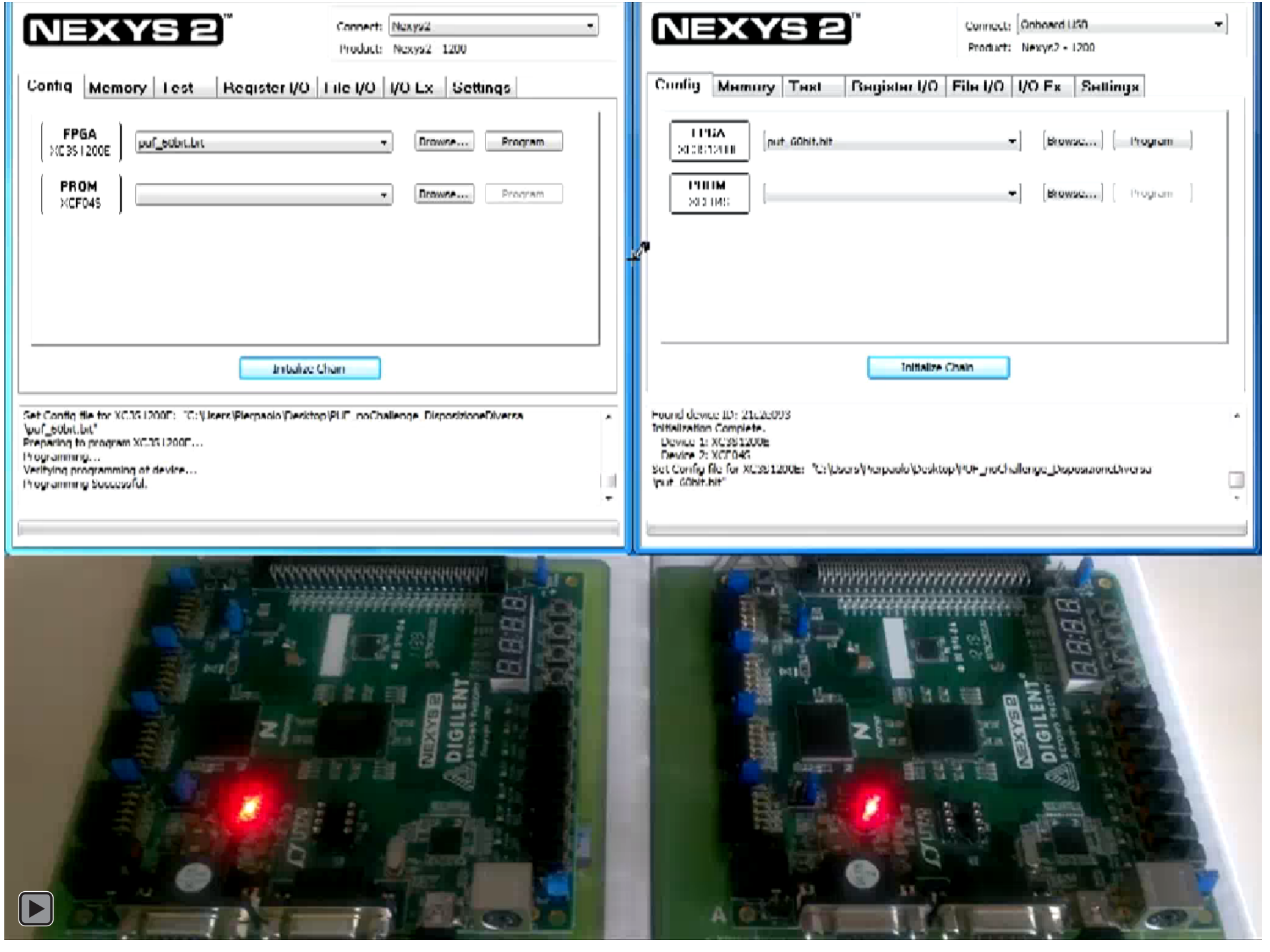
- The SM includes the Anderson PUF and a SW decryption engine
- The SM decrypts an encrypted partial bitstream (HWIP) using as key a specific PUF response, then partially re-configures the FPGA with the decrypted bitstream

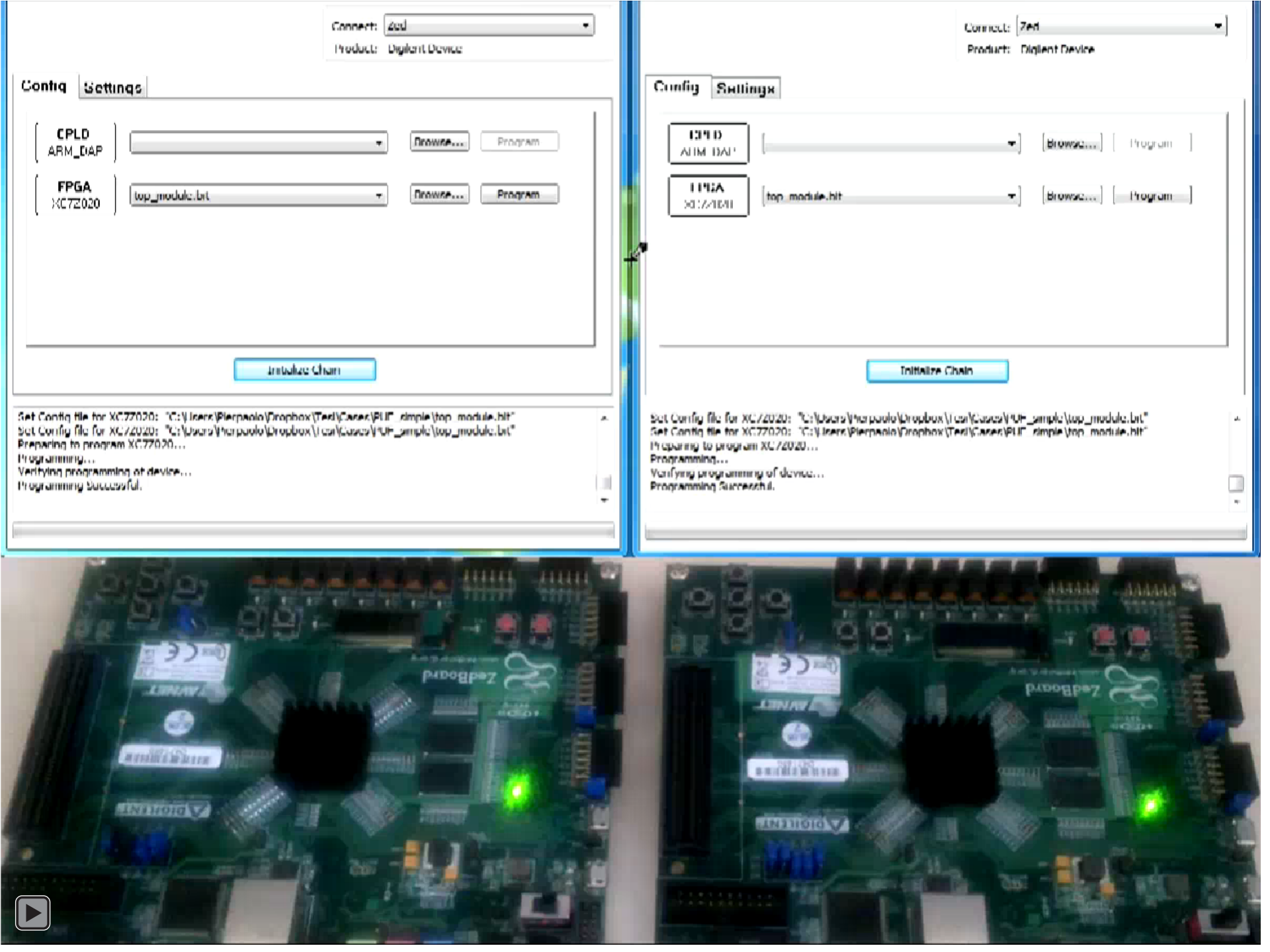
Primitive	Bitstream size (150 kBytes)	Bitstream size (600 kBytes)
AES-CBC	170 ms	682 ms
AES-GCM	280 ms	1122 ms

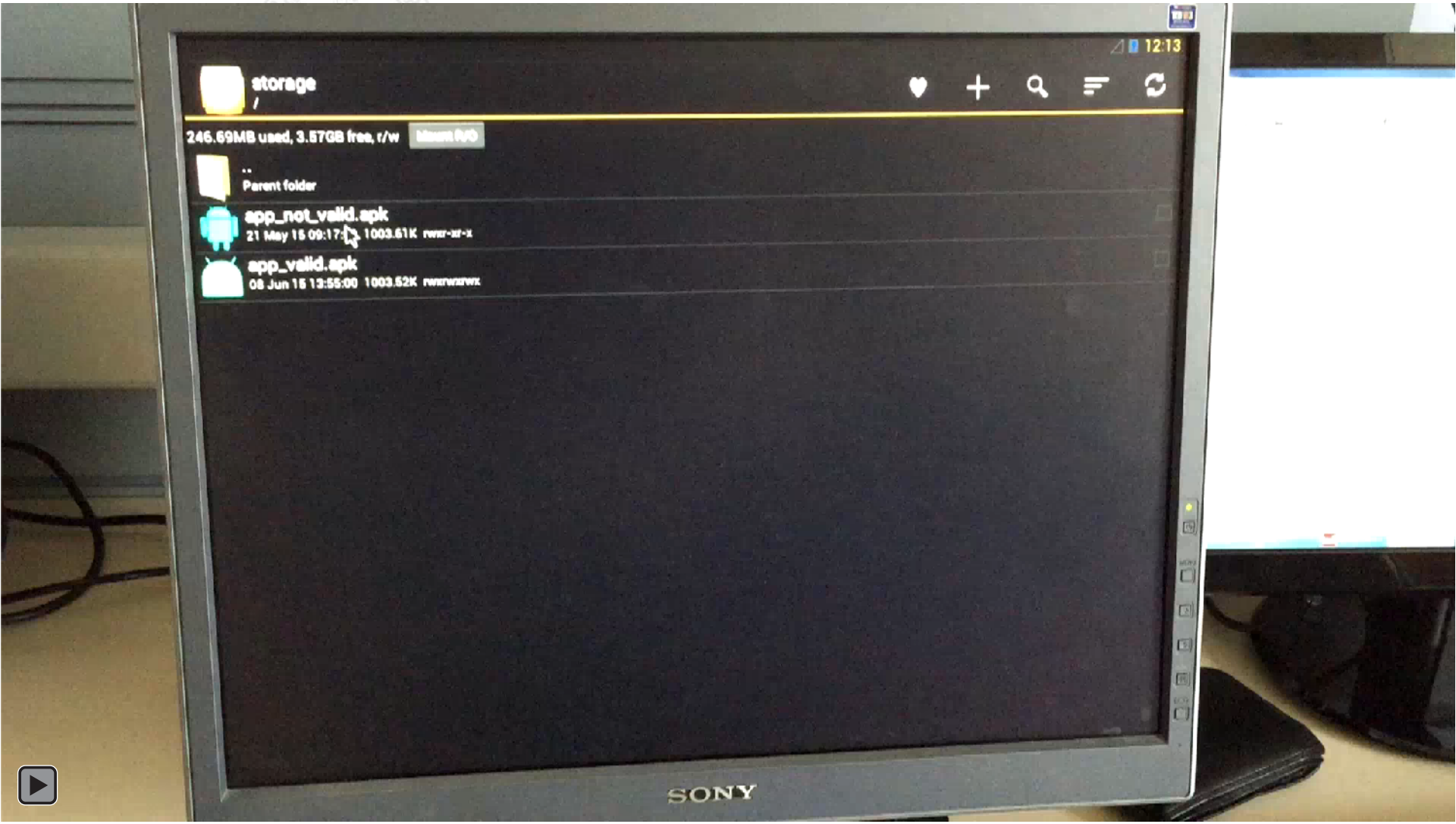
Implementation of a Trusted Platform Exploiting Android OS



- We developed a customized version of Android OS which checks and installs only valid applications (*apks)*
- The TPM boot procedure is exploited in order to build a secure and trusted platform
- The validity check is based on the XML manifest of an Android *app*, which comprises the enciphered digest of the application executable


NEXYS 2
Connect: Nexys2
Product: Nexys2 1200
Config
Memory
Test
Register I/O
File I/O
I/O Ex
Settings
FPGA
XC3S1200E
puf_60bit.bit
Browse...
Program
PROM
XCF04S
Initialize Chain
Set Config file for XC3S1200E: "C:\Users\Pierpaolo\Desktop\PUF_proChallenge_DispositiviDiversi\puf_60bit.bit"
Preparing to program XC3S1200E...
Programming...
Verifying programming of device...
Programming Successful.
NEXYS 2
Connect: Onboard USB
Product: Nexys2 + 1200
Config
Memory
Test
Register I/O
File I/O
I/O Ex
Settings
FPGA
XC3S1200E
put_60bit.bit
Browse...
Program
PROM
XCF04S
Initialize Chain
Found device ID: 21c2c093
Initialization Complete.
Device 1: XC3S1200E
Device 2: XCF04S
Set Config file for XC3S1200E: "C:\Users\Pierpaolo\Desktop\PUF_proChallenge_DispositiviDiversi\put_60bit.bit"
DIGILENT
NEXYS 2


Config
Settings
CPLD
ARM_DAP
FPGA
XC7Z020
top_module.bit
Browse...
Program
Initialize Chain
Set Config file for XC7Z020: "C:\Users\Pierpaolo\Dropbox\Test\Cases\PIP_simple\top_module.bit"
Preparing to program XC7Z020...
Programming...
Verifying programming of device...
Programming Successful.
Config
Settings
Initialize Chain
Set Config file for XC7Z020: "C:\Users\Pierpaolo\Dropbox\Test\Cases\PIP_simple\top_module.bit"
Preparing to program XC7Z020...
Programming...
Verifying programming of device...
Programming Successful.


12:13
storage
/
246.69MB used, 3.57GB free, r/w
Mount R/O
..
Parent folder
app_not_valid.apk
21 May 15 09:17:
1003.61K rwxr-xr-x
app_valid.apk
08 Jun 15 13:55:00 1003.62K rwxrwxrwx
SONY

Future Work

- Defining a model for the glitch generation of the Anderson PUF by varying the supply voltage
- Analyzing the impact on responses of the logic surrounding a PUF in order to mitigate its effect
- Implementing low-weight mechanisms to enhance PUFs reliability
- Implementing the Android check mechanism on the most recent Android version and on other operating systems