PHILIPS

FPGA Intrinsic PUFs and Their Use in IP Protection

Jorge Guajardo*, Sandeep S. Kumar*,
Geert-Jan Schrijen**, and Pim Tuyls**

* Philips Research Europe, Eindhoven, The Netherlands
** Business Line Intrinsic-ID, Philips Research, Eindhoven, The Netherlands

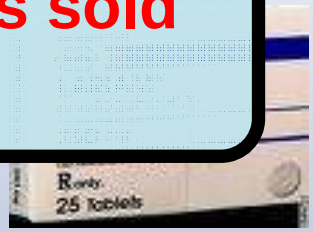
September 20, 2007

Contents

Intellectual Property Theft

- Annual value of trade in fake goods: $400 Billion
  - Spare parts
  - Clothing
  - Perfumes
  - Medicines
  - Audio & video
  - Software
  - Electronic Designs

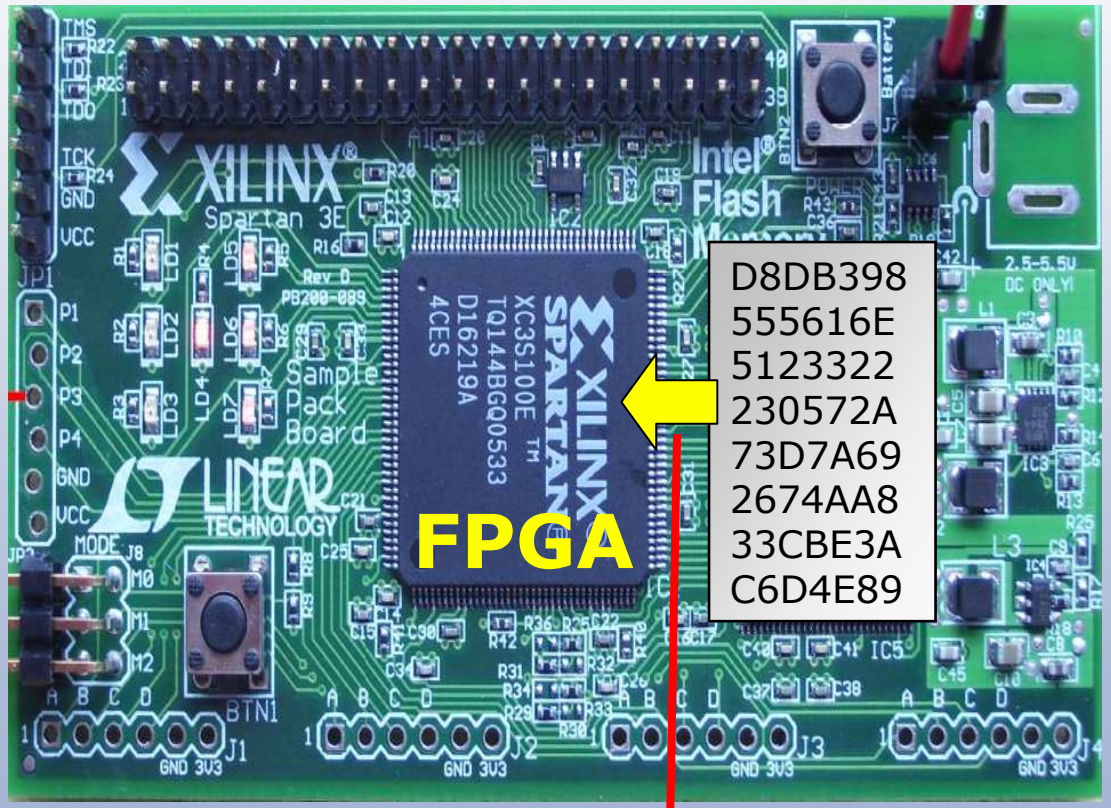
10% of all High Tech Products sold are Counterfeit!

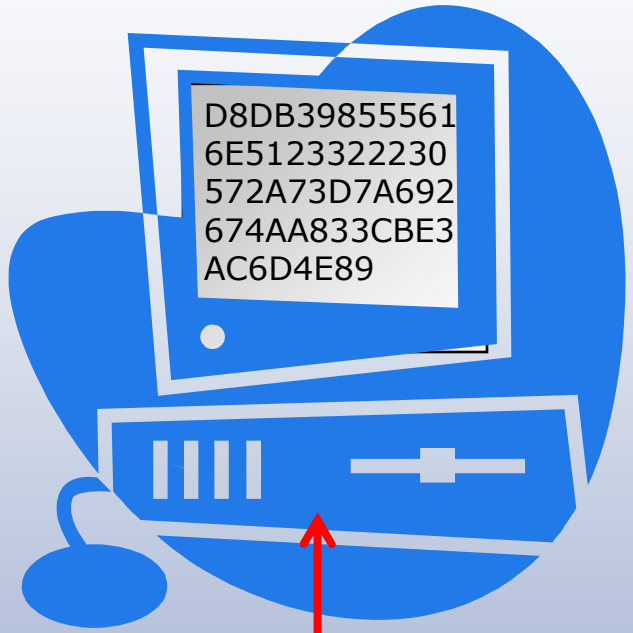


- IC designs
- Electronic circuitry
- Configuration data of programmable devices

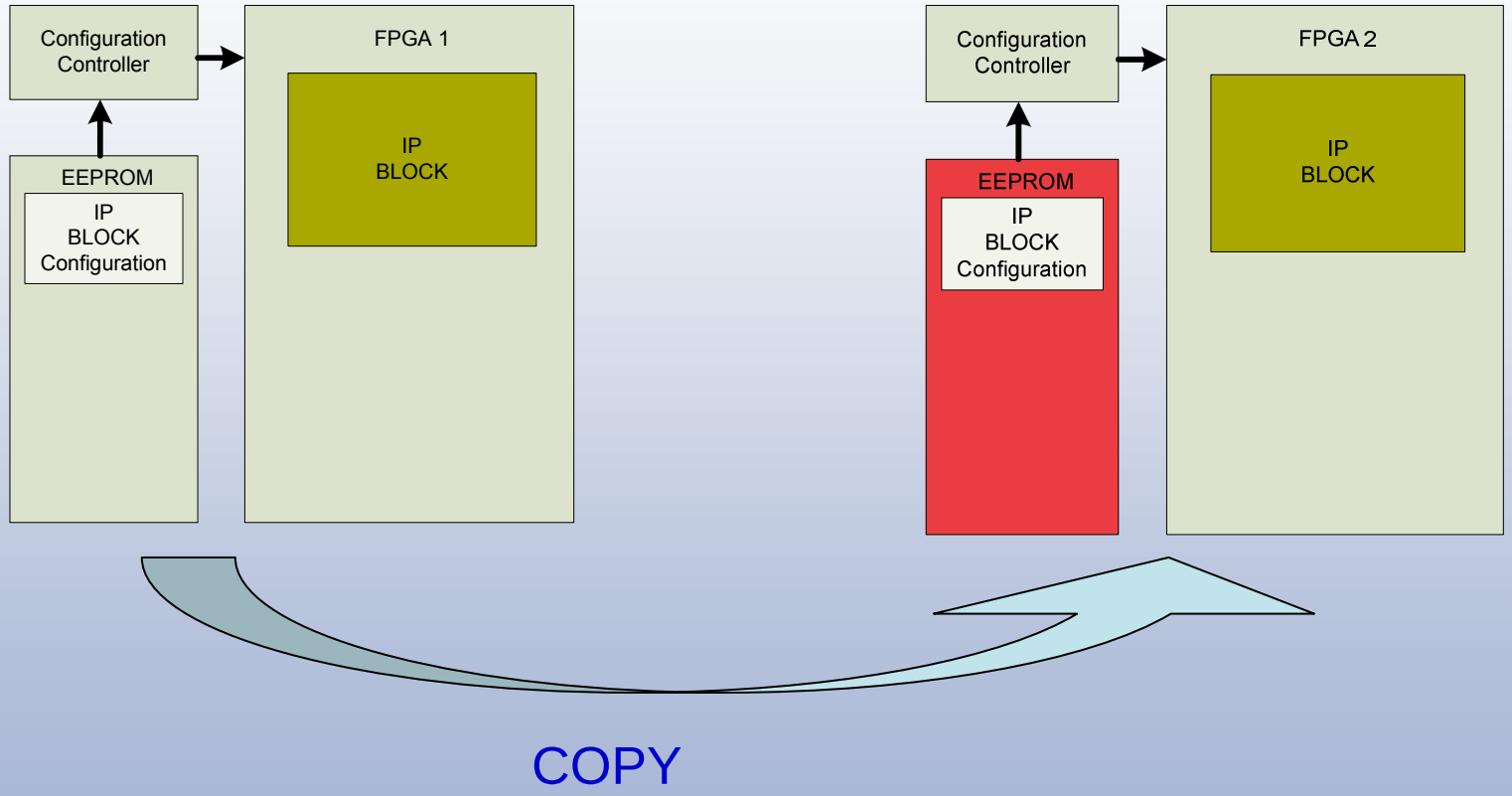
Contents

FPGA Design Cloning

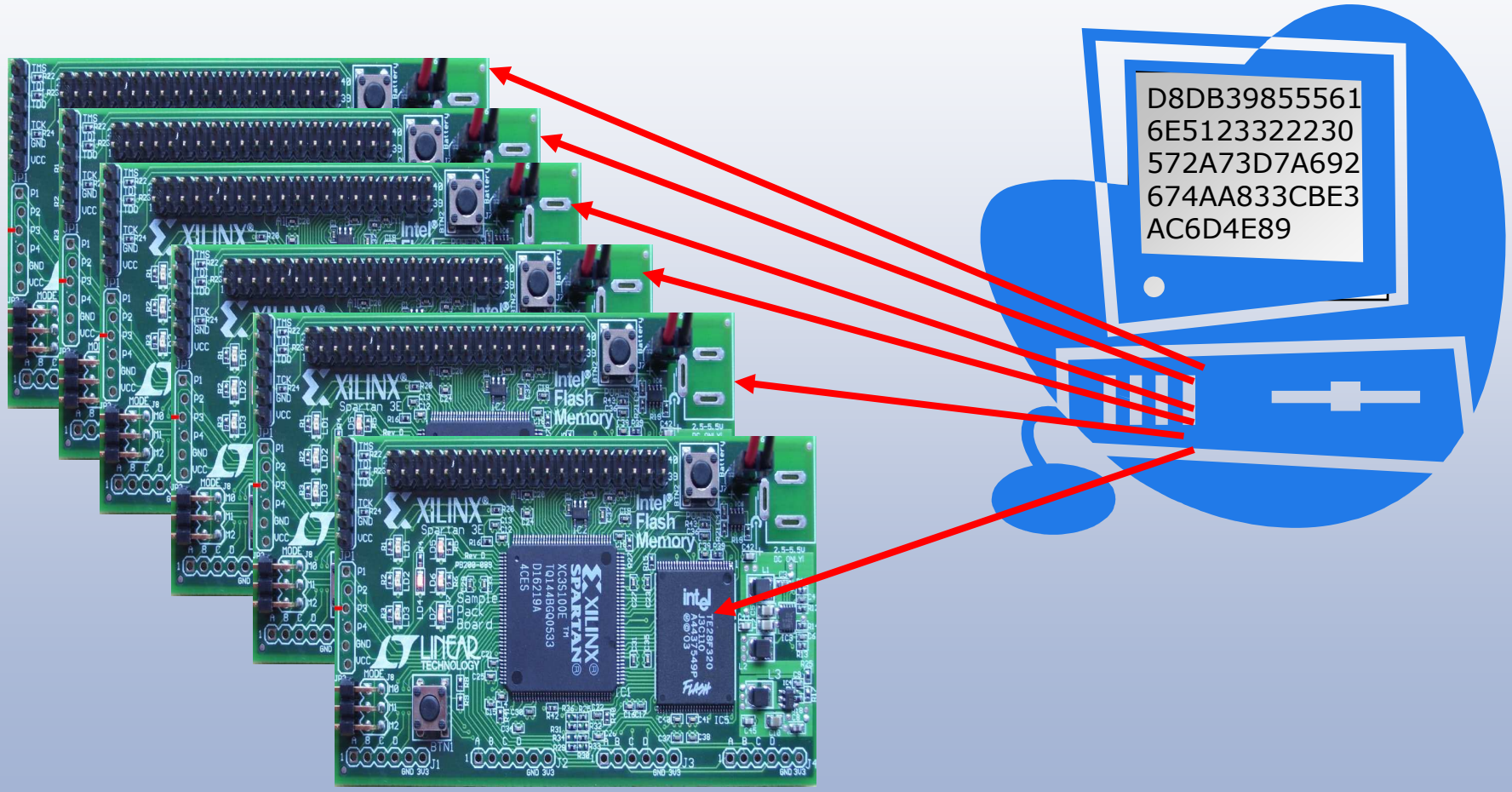




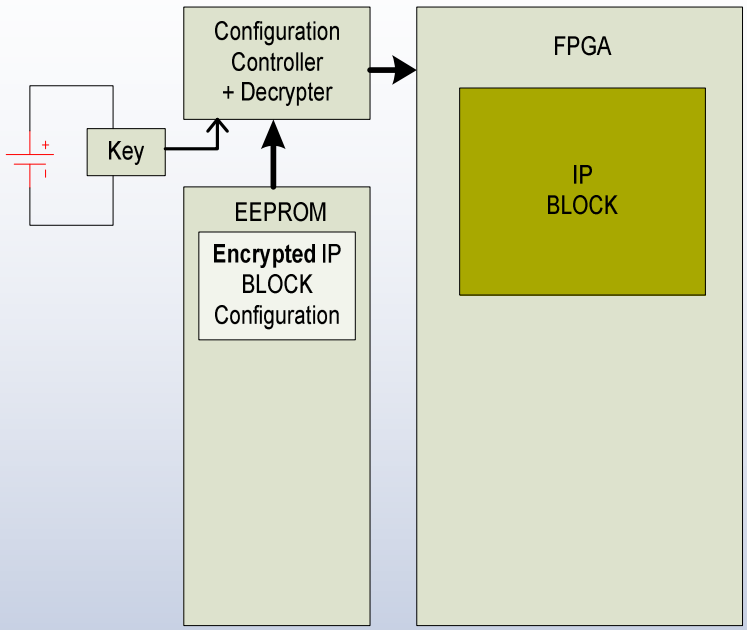
SRAM based FPGA: configuration

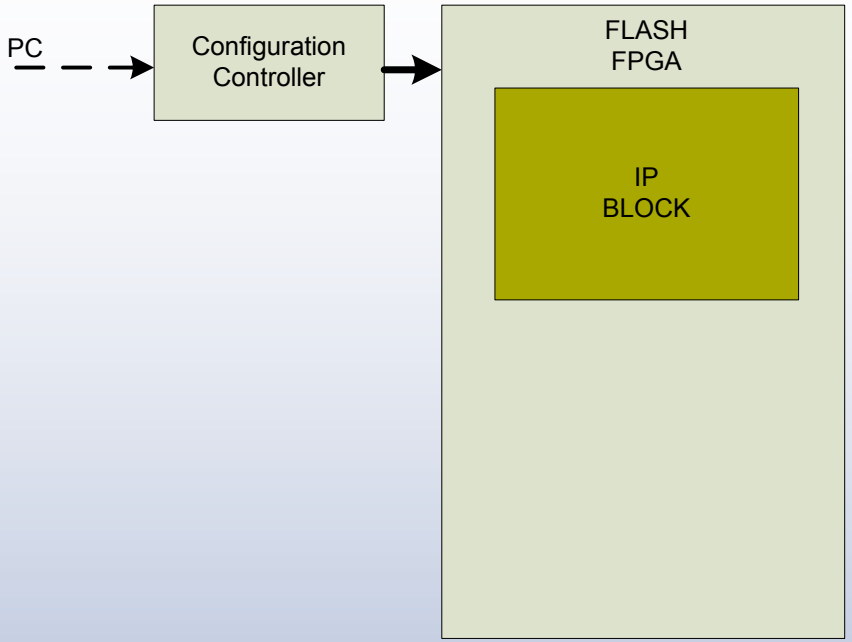


FPGA Design Cloning



Available Solutions





Option 1

- Encrypted IP configuration file
- External battery to store Key

Option 2

- Use flash based FPGA
- Cannot be updated in the field

Option 3

- Use a PUF
- Need two components:
  - Randomness source
  - Fuzzy extractor

Contents

Physical Unclonable Function

- **PUF = Physical Unclonable Function:** Derive strings from a complex physical system that is inherently unclonable
  - Easy to evaluate (by probing the physical system)
  - Inherently tamper resistant
  - Manufacturer not-reproducible
  - PUFs can be used as a source of a large amount of unclonable secret key material

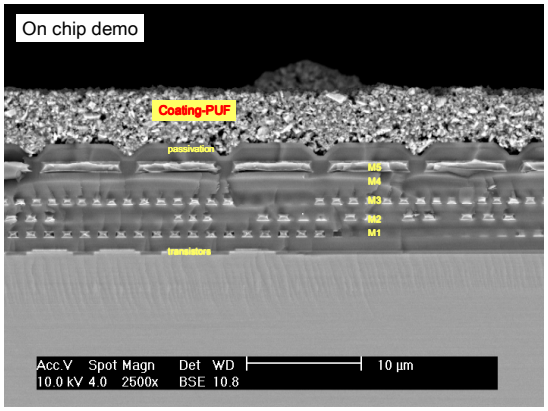
- **Unclonable**
  - Hard to make a physical clone
  - Hard to make a mathematical model that simulates the behavior of the physical structure

- **Practicality Requirements**
  - Easy to challenge the source
  - Cheap and easy integrable on an IC
  - Excellent mechanical and chemical properties

A Bit of History

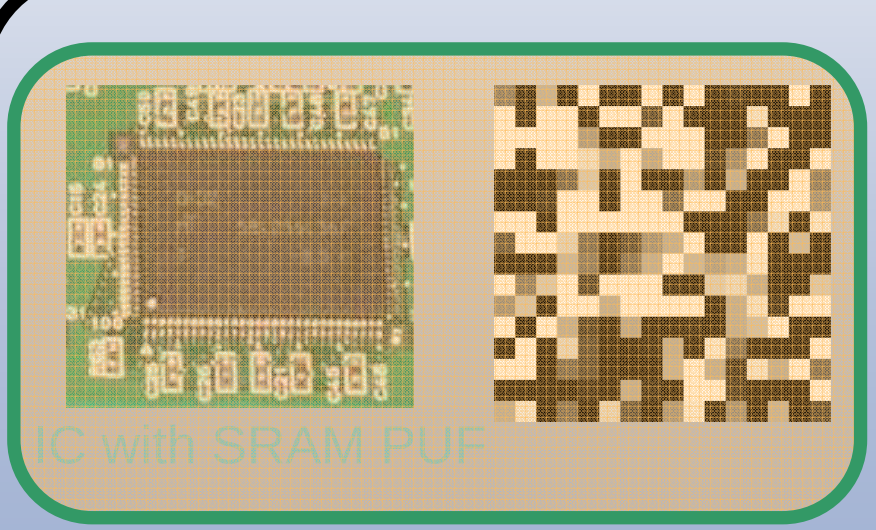
- 2001 Pappu et al. - Physical Random Functions (Optical PUFs) MIT Ph.D. Thesis, and Science 2002
- 2002 Gassend et al., Su et al. – IC PUFs (Delay PUF) CCS 2002, ACSAC 2002
- 2002 Kean, Encryption for IP Protection on FPGAs, FPGA 2002
- 2006 Simpson and Schaumont (Protocols for IP Protection based on the usage of PUFs) CHES 2006
- 2006 Tuyls et al. (Coating PUF), CHES 2006
- 2007 Guajardo et al. PK-based protocols for IP Protection based on intrinsic PUFs, FPL 2007
- 2007 Guajardo et al. FPGA Intrinsic PUFs and their Use in IP Protection, CHES 2007 & This work

Examples

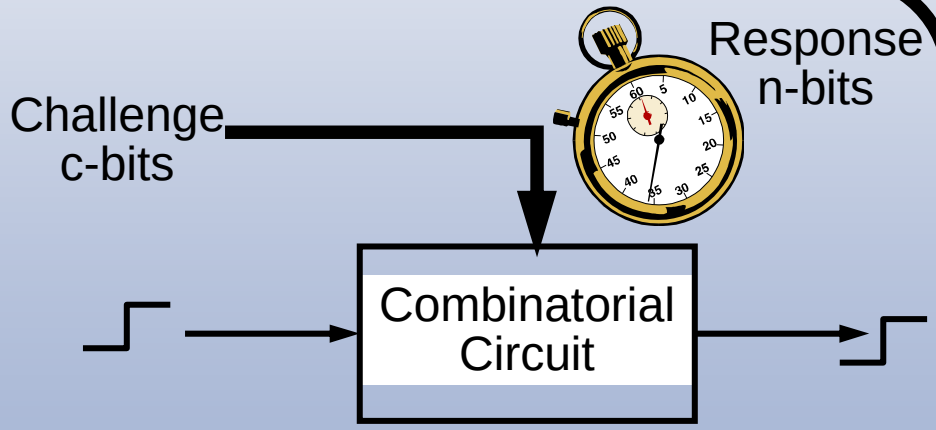


IC with Coating PUF

Intrinsic Identifier

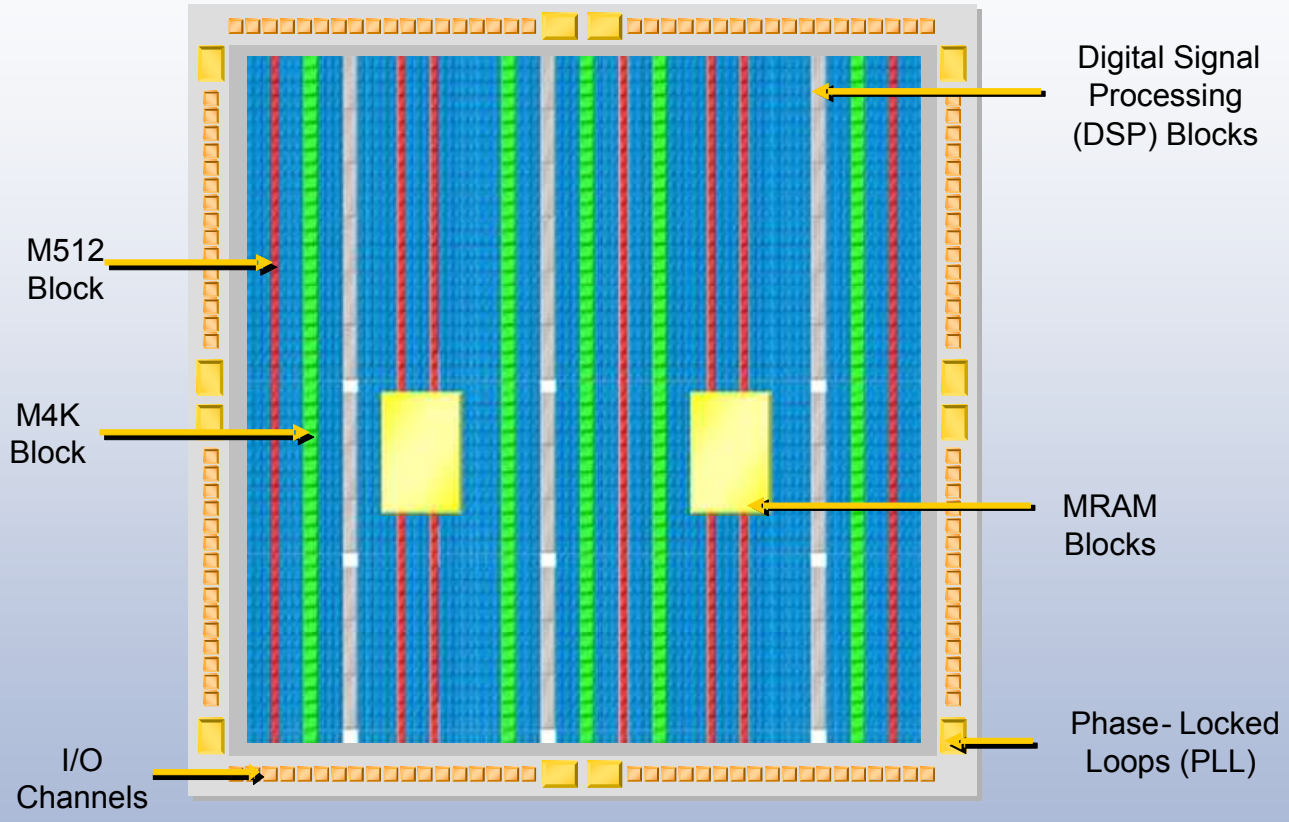


IC with SRAM PUF



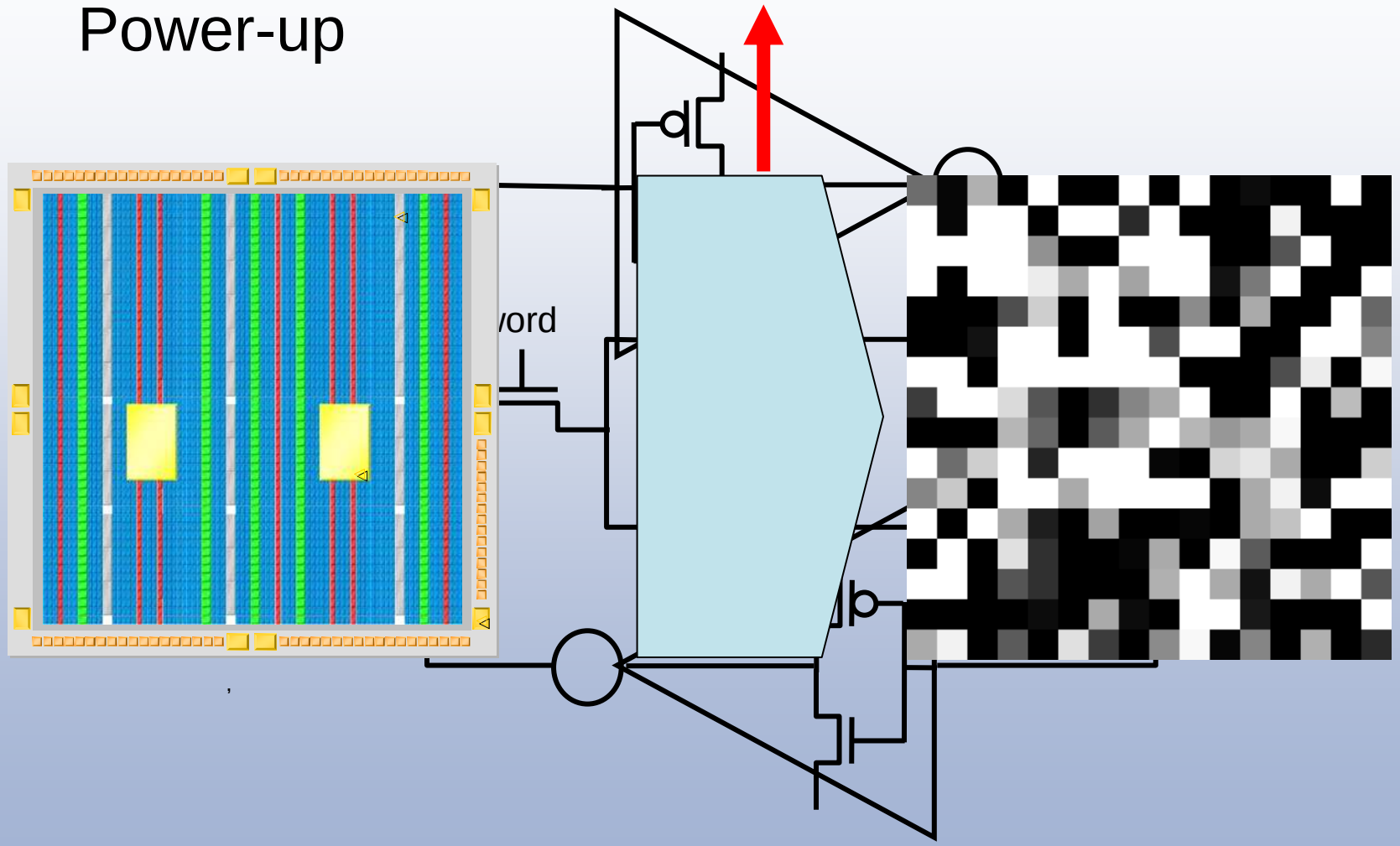
IC with Delay PUF

Modern FPGA Floorplan



S-RAM PUF

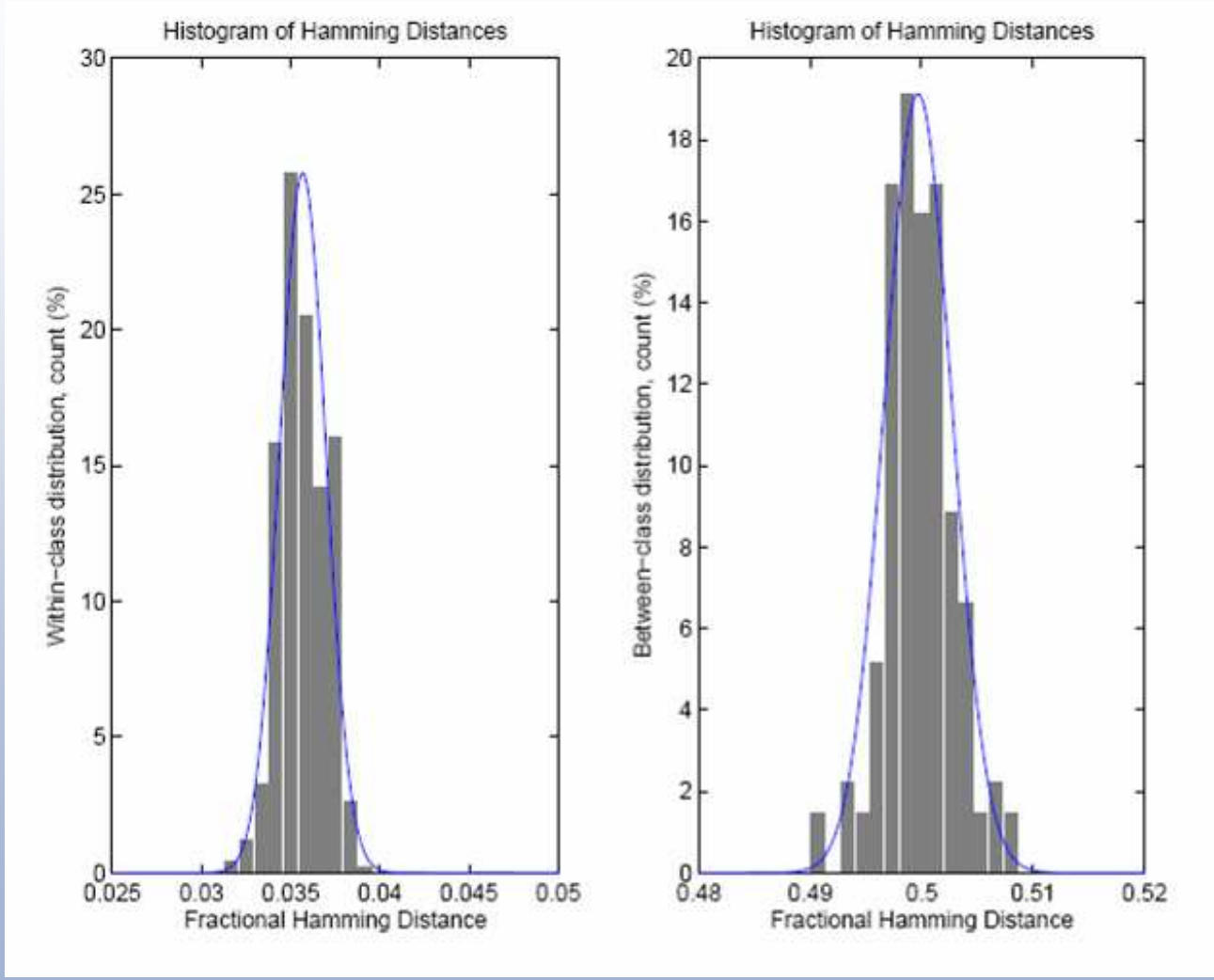
Power-up



Noise over repeated measurements over a large temperature range

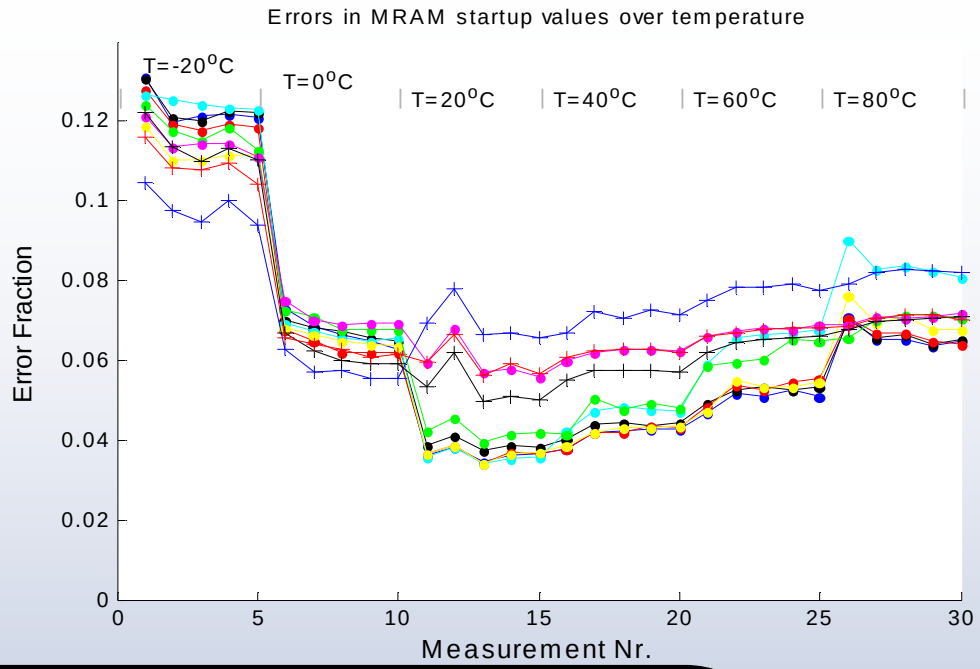
~ 14% errors

Histogram of Inter-class and Intra-class differences



Properties

- Randomness
- Noise



Properties:

- **Entropy: 95%**
- **Secrecy Rate: 76%**

Fuzzy Extractor Needed:

- **Error Correction**
- **Randomness Extraction**

Contents

How do we put everything together?

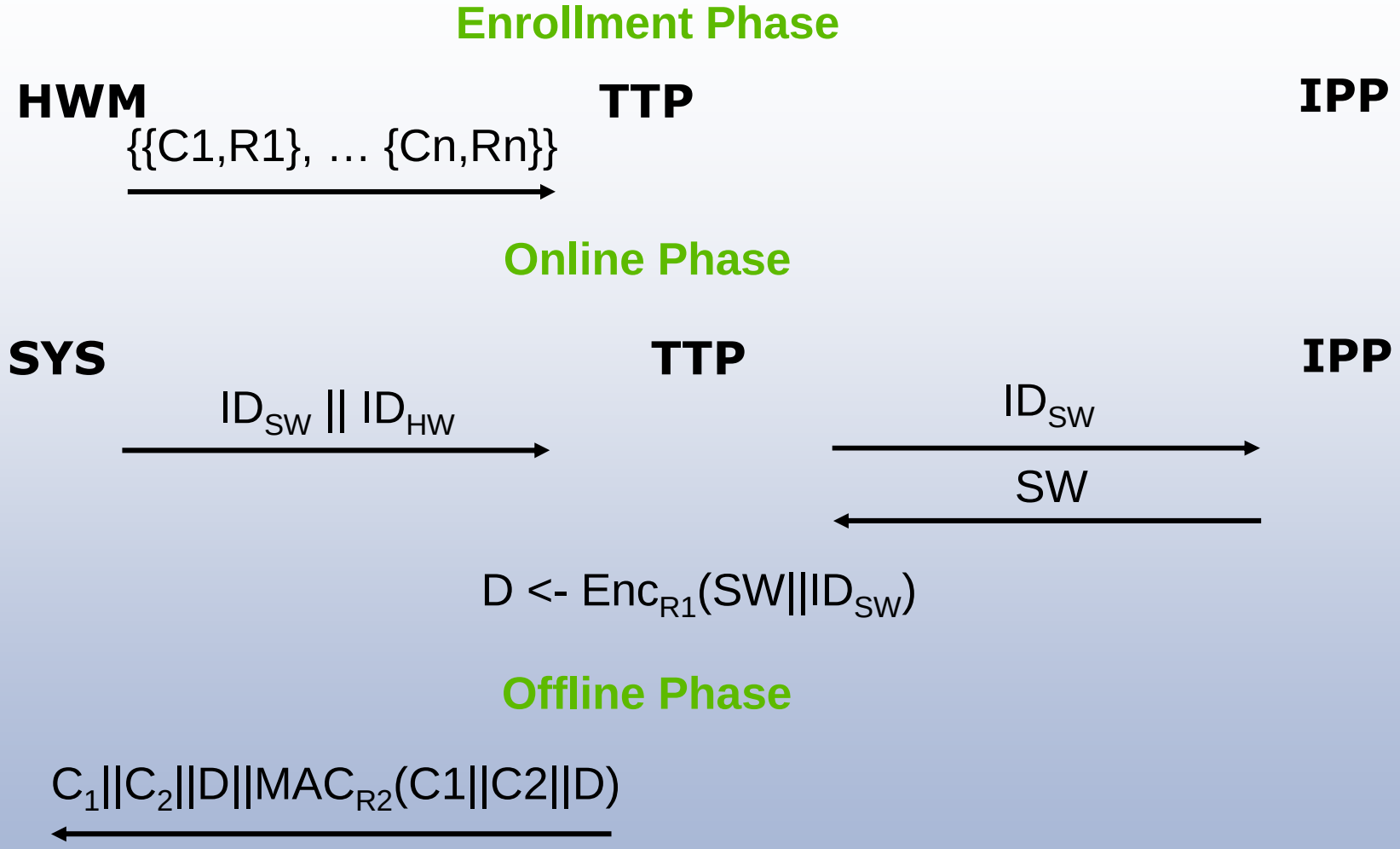
Notation:

- TTP (Trusted Third Party), SYS (System Integrator), IPP (IP Provider), HWM (Hardware Manufacturer)

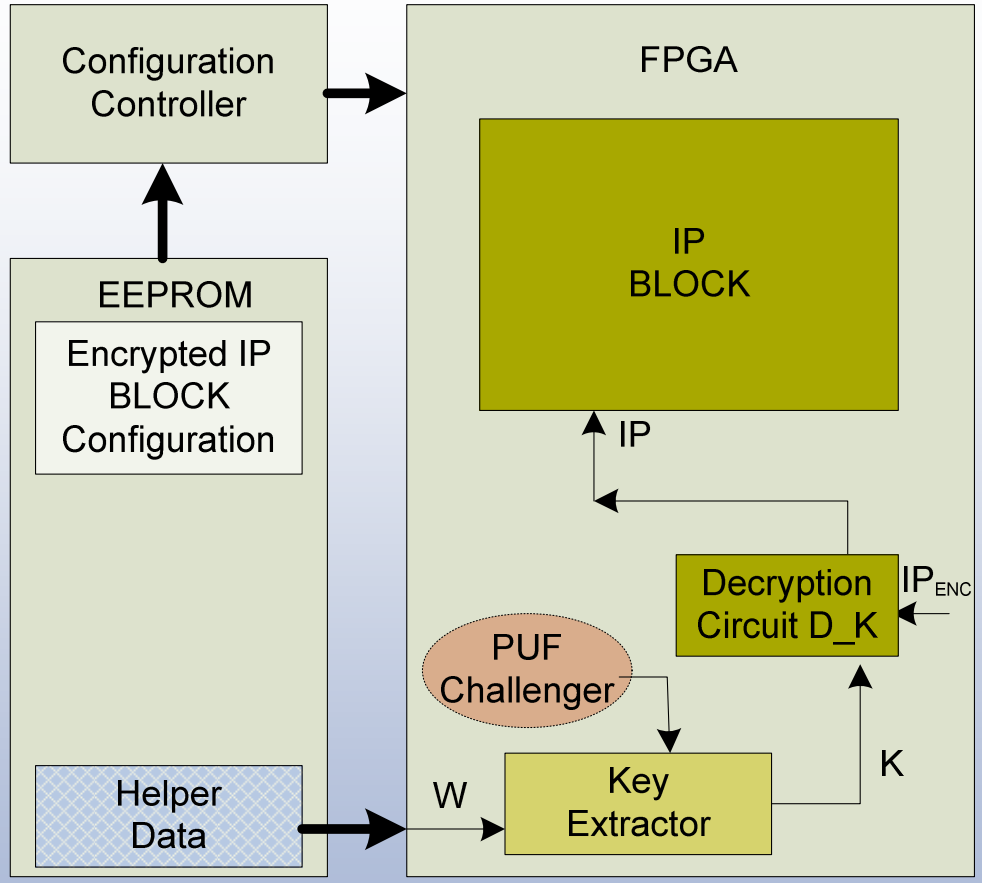
Assumptions:

- Semantically secure encryption scheme
- Honest but curious model
- In the symmetric-key setting, possible constructions for encryption+authentication:
  - $Enc_{K1}(M)||MAC_{K2}(M)$, MAC-then-Encrypt, Encrypt-then-MAC
- PUF and encryption modules assumed to be on the FPGA
- PUF responses are only available inside the FPGA
- Secure and authenticated channels SYS-TTP and TTP-IPP during enrollment and online phase

Protocol for IP Protection on FPGAs



PUF based Solution



- Intrinsic PUF
- Helper Data dependent on the specific FPGA chip

Contents

Conclusions

- New PUF intrinsic to the FPGA with good statistical properties and robustness to environmental conditions.
- New protocol(s) for IP protection on FPGAs
- In the future,
  - Other Intrinsic PUFs
  - Complexity of fuzzy extractors
  - Limit the use of FPGA resources.
  - Reliability: Guaranteeing a low failure rate under all kinds of circumstances.


PHILIPS