PHILIPS

Physical Unclonable Functions (PUF) for IP Protection on FPGA

Sandeep S. Kumar*

Joint work with

Jorge Guajardo Merchan *, Roel Maes†, Geert-Jan Schrijen ** and Pim Tuyls **

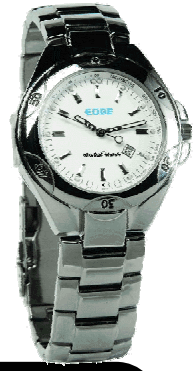
* Philips Research Europe, Eindhoven, The Netherlands

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

† Katholieke Universiteit Leuven, ESAT/COSIC, Leuven, Belgium

Contents

Intellectual Property Theft

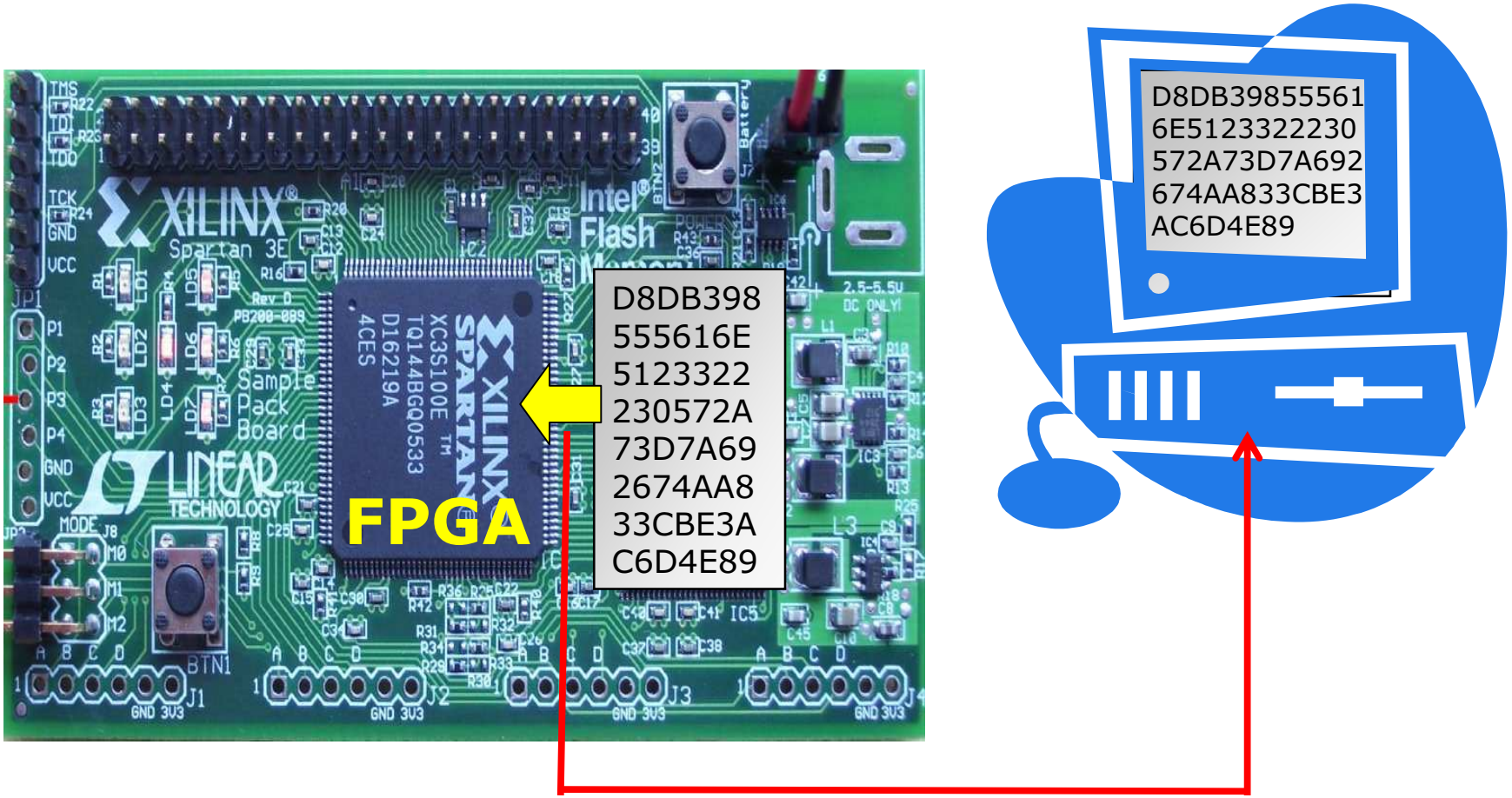


- Annual value of trade in fake goods: $400 Billion
  - Spare parts
  - Clothing
  - Perfumes
  - Medicines
  - Audio & video
  - Software
  - Electronic Designs

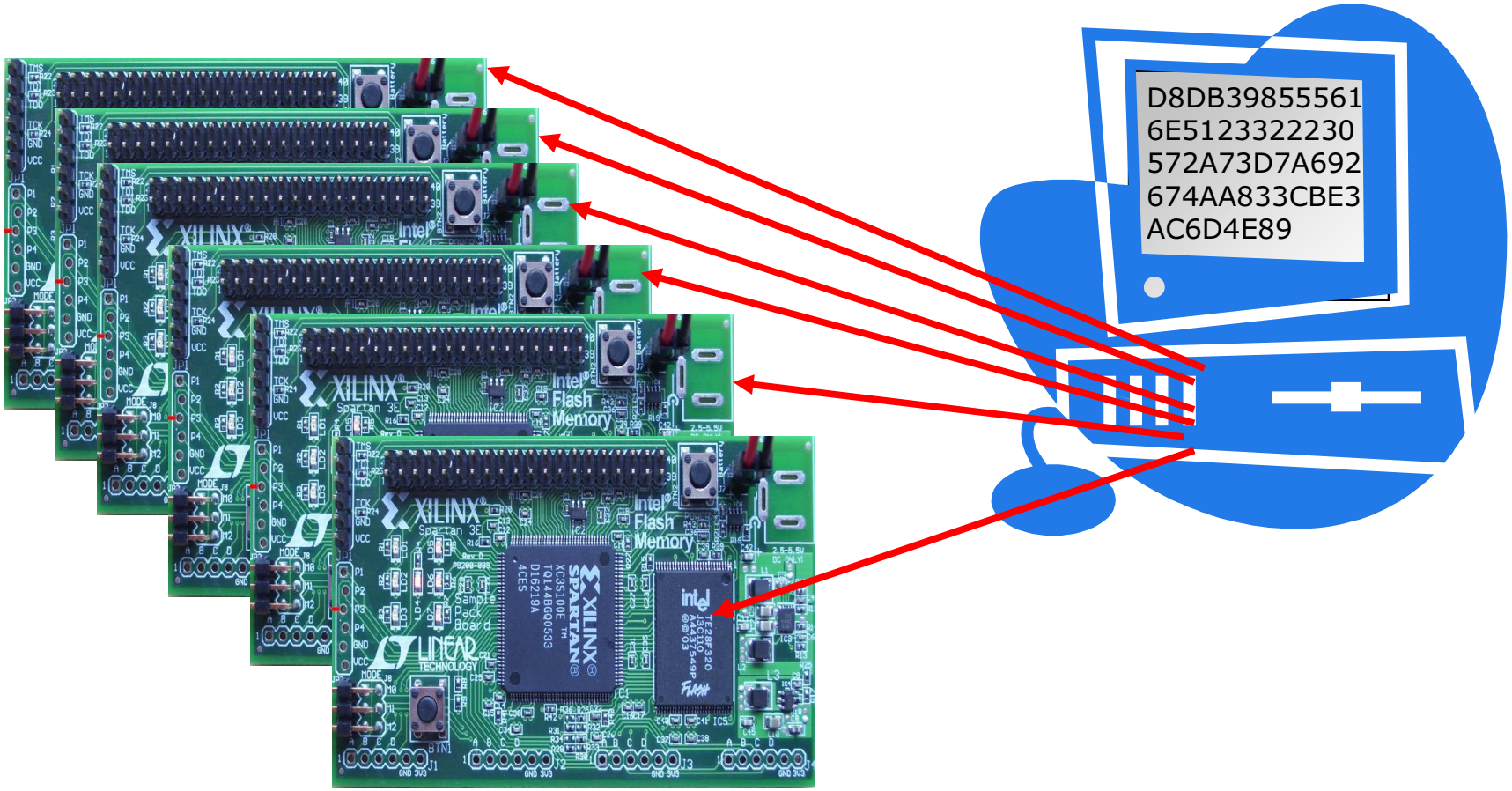
10% of all High Tech Products sold are Counterfeit!

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

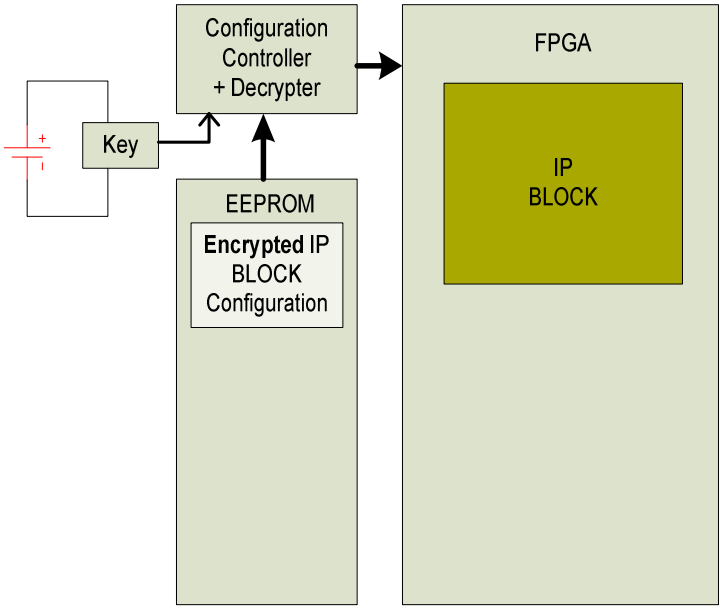
Problem: FPGA Design Cloning

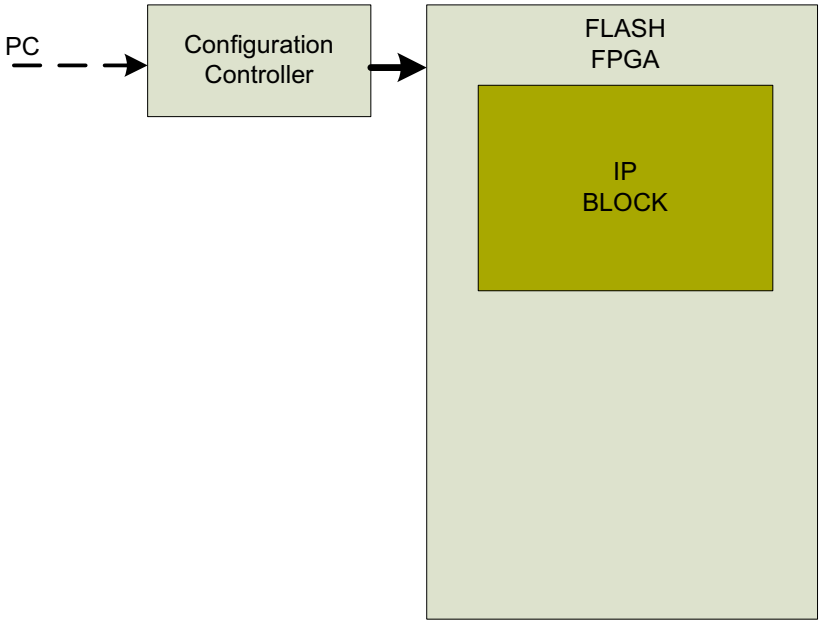


Problem: FPGA Design Cloning



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

generate and store secret keys in a secure and inexpensive way

Option 3

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

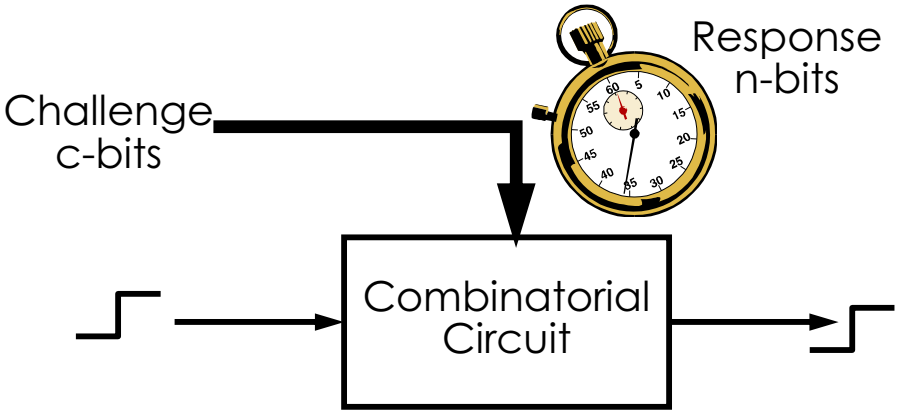
Contents

Physical Unclonable Functions (PUF)

Inherently unclonable physical structures due to random process variations

(no two ICs even when identically built are perfectly identical)

- Process variation is an inherent component of fabrication process
- Hard to remove or predict even by manufacturer
- Relative variation increases as the fabrication process advances



IC with Delay PUF

IC with SRAM PUF

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
- 2008 ….

Physical Unclonable Functions (PUF)

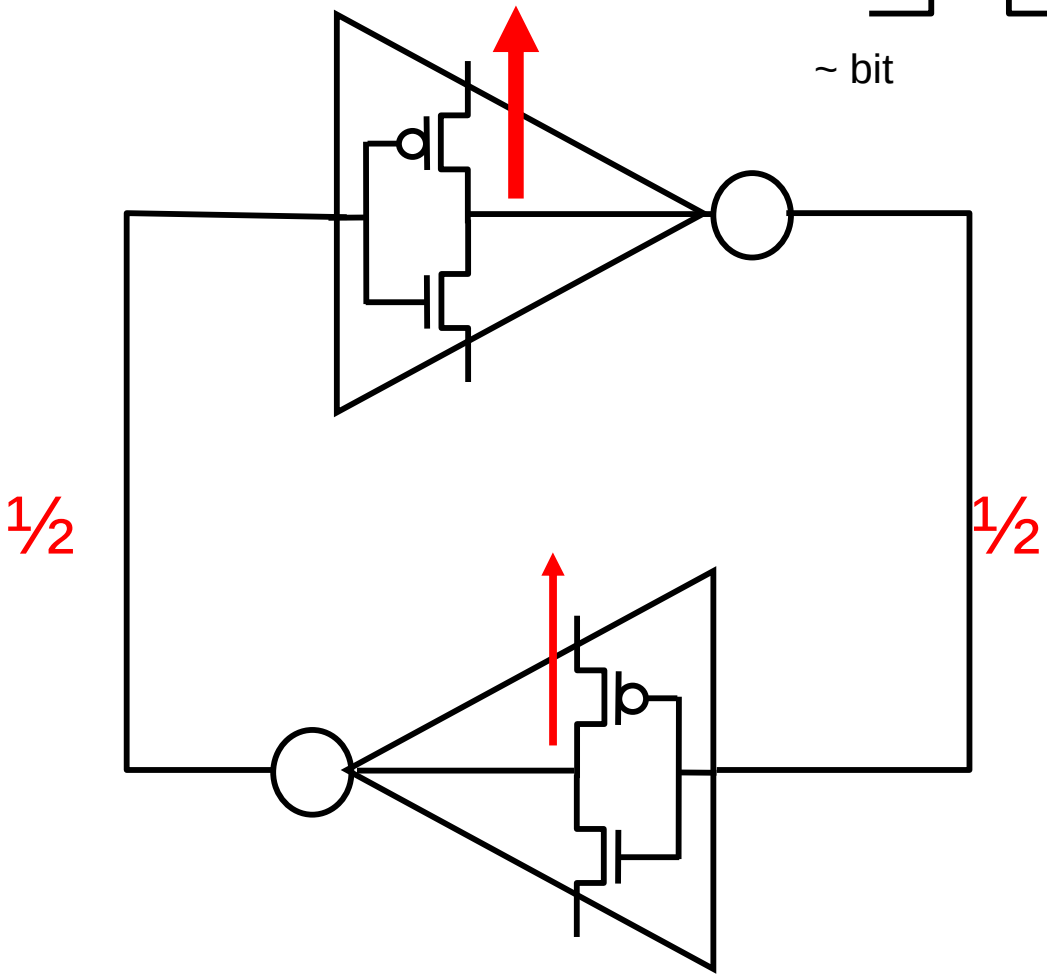
Properties:

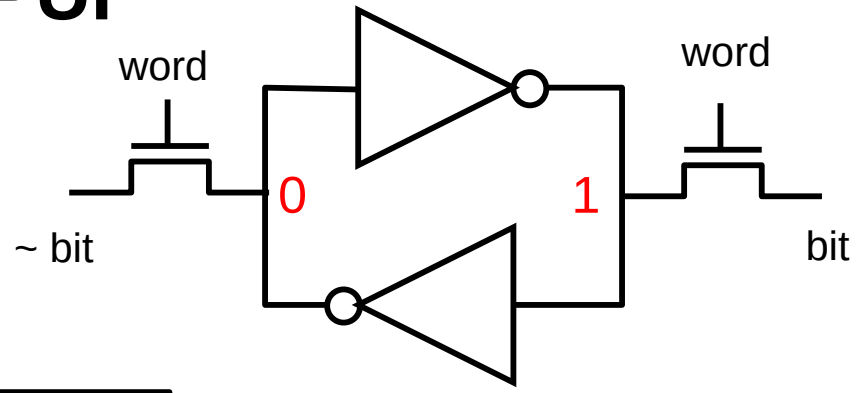
- Easy to evaluate: Challenges-Responses
- Inherently tamper evident
- Manufacturer non-reproducible
- Source of a large amount of unclonable secret key material

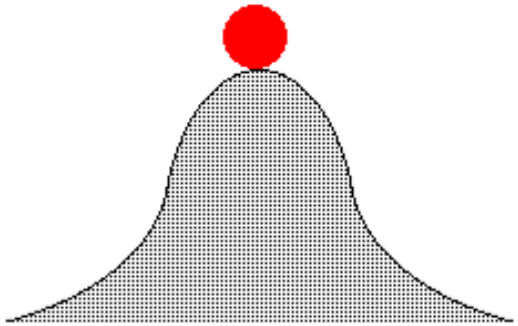
PUF can generate a unique secret key

- Highly securely: volatile secrets, no need for tamper-proof hardware
- Inexpensively: no special fabrication technique, intrinsic

Un-initialized S-RAM PUF

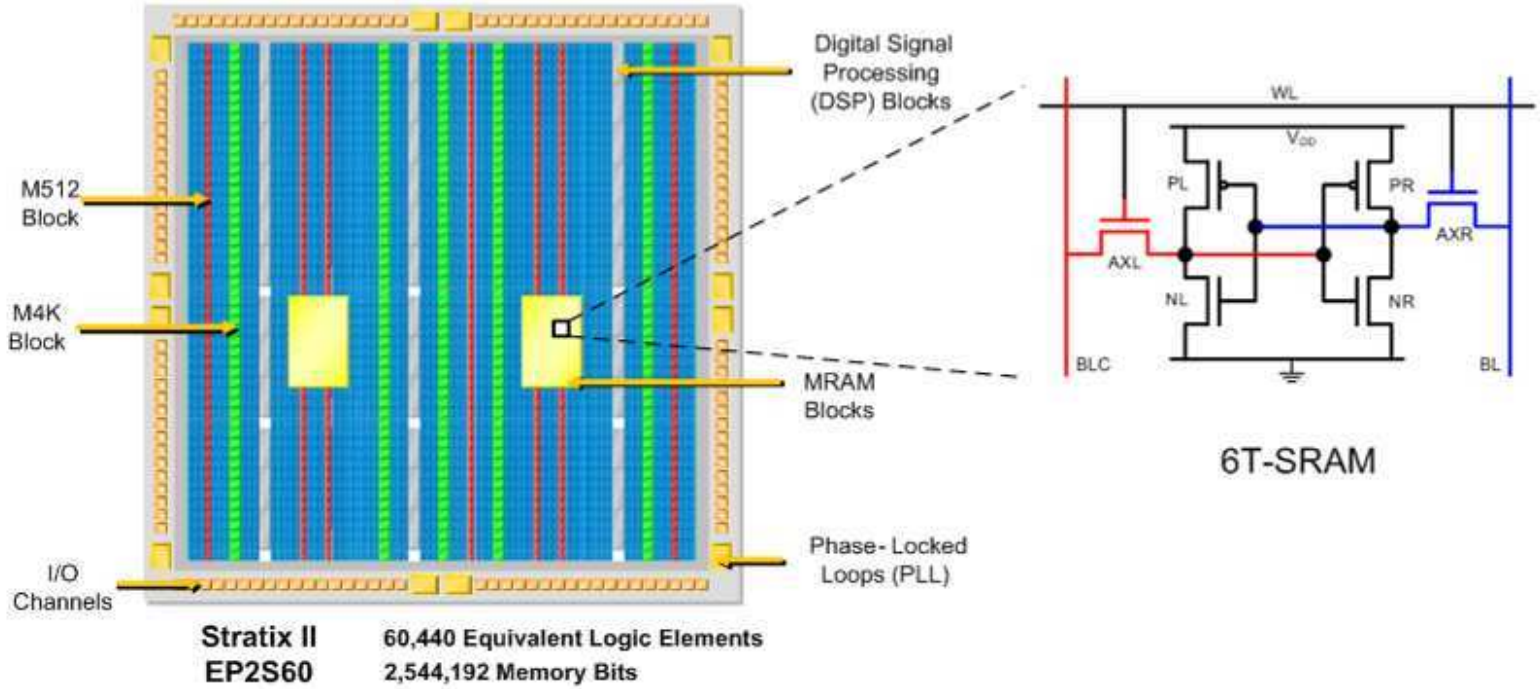






ball at the top of a hill

FPGA Floorplan



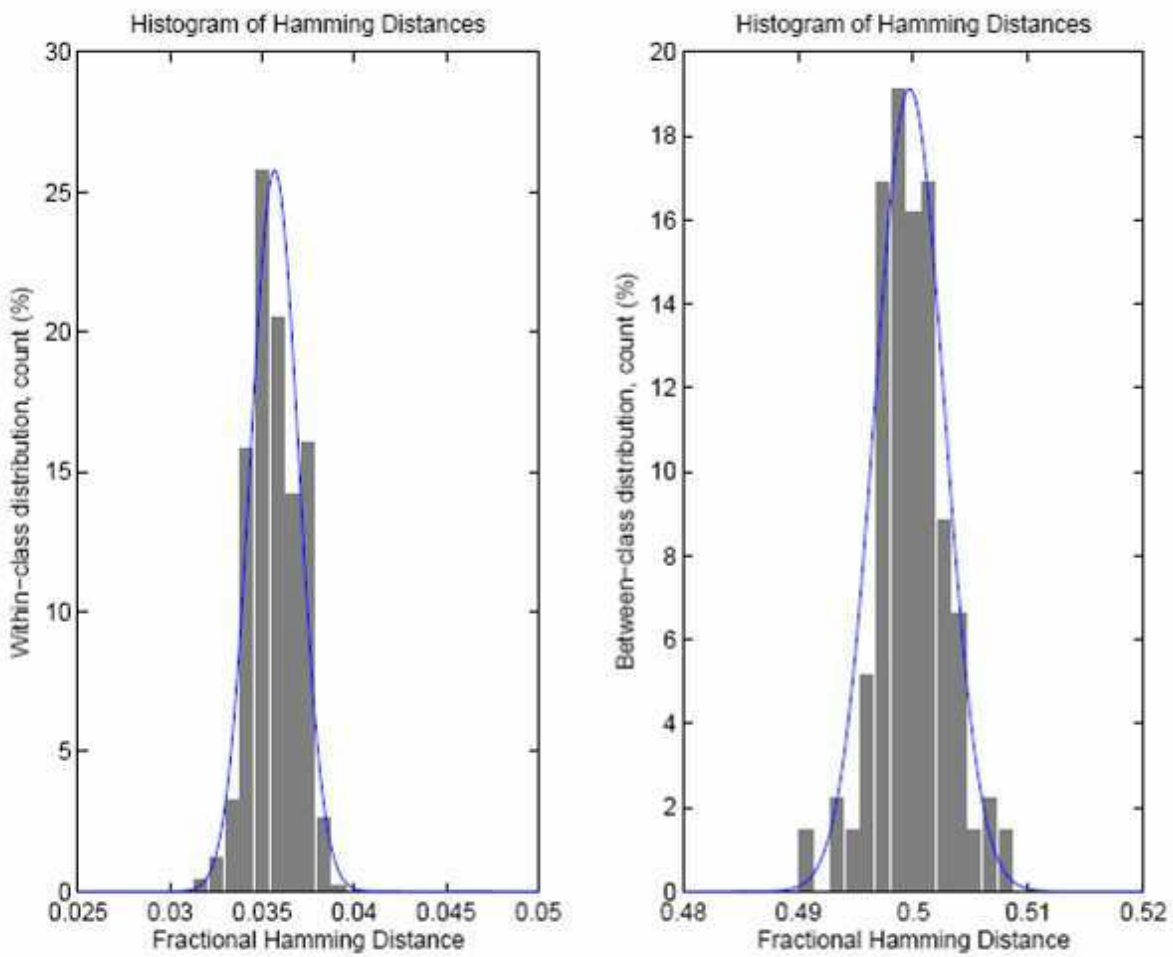
Noise over repeated measurements over a large temperature range

PUF validation

Measurements done at various environmental conditions (temperature, frequency, core voltage..etc)

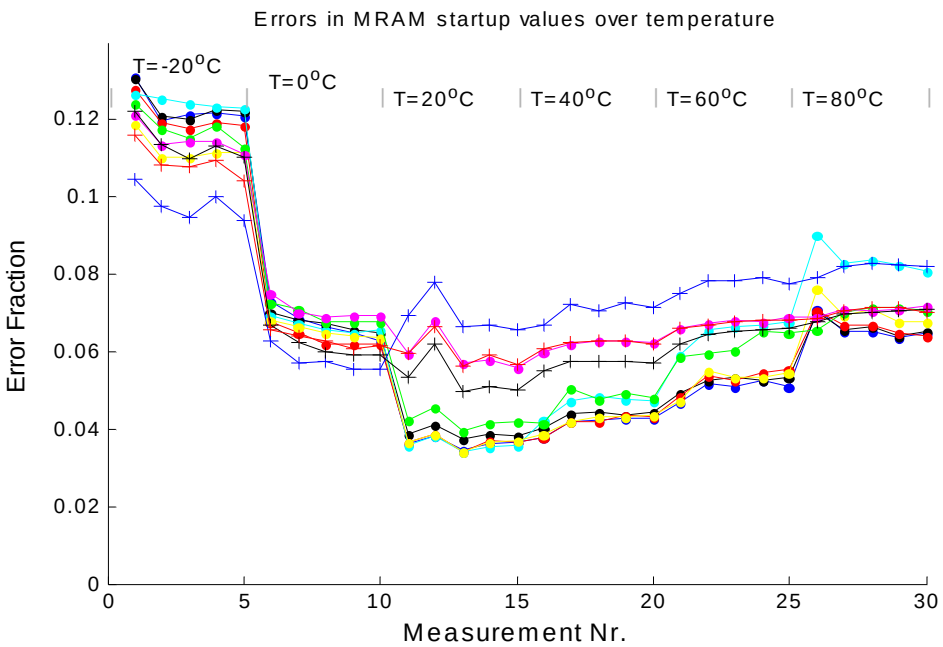
- **Reliability**:
  - Intra-chip variations: how many bits are different between two measurements *on the same device*
  - Ideally should be 0%
- **Security**
  - Inter-chip variations: how many bits are different between measurements *on two different devices*
  - Ideally close to 50%

Histogram of Inter-class and Intra-class differences



Properties

- Randomness
- Noise



Entropy: 95%

Fuzzy Extractor Needed:
- **Error Correction**
- **Randomness Extraction**

Key Extraction from Noisy Data: Idea

Grid points represent ECC Code words

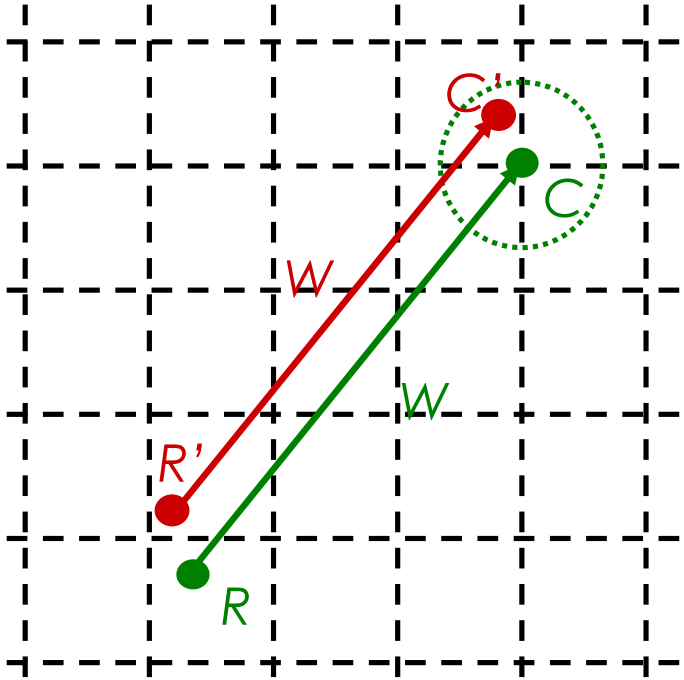
Assumption: Response *R* uniformly random

Enrollment

- Random codeword *C* is chosen
- PUF Response *R* is measured
- Helper data *W* is generated (difference between *R* and C) and stored
- $K \leftarrow h_i(R)$ $(K,W) \leftarrow \mathbf{Gen}(R)$

Key Reconstruction

- PUF response *R'* is noisy
- $R'+W=C'$
- $C=Decode(C')$
- $C+W=R$ $K \leftarrow \mathbf{Rep}(R,W)$



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

Enrollment Phase

HWM **TTP** **IPP**

$\{\{C1,R1\}, \ldots \{Cn,Rn\}\}$ →

Online Phase

SYS **TTP** **IPP**

$ID_{SW} \| ID_{HW}$ →

ID_{SW} →

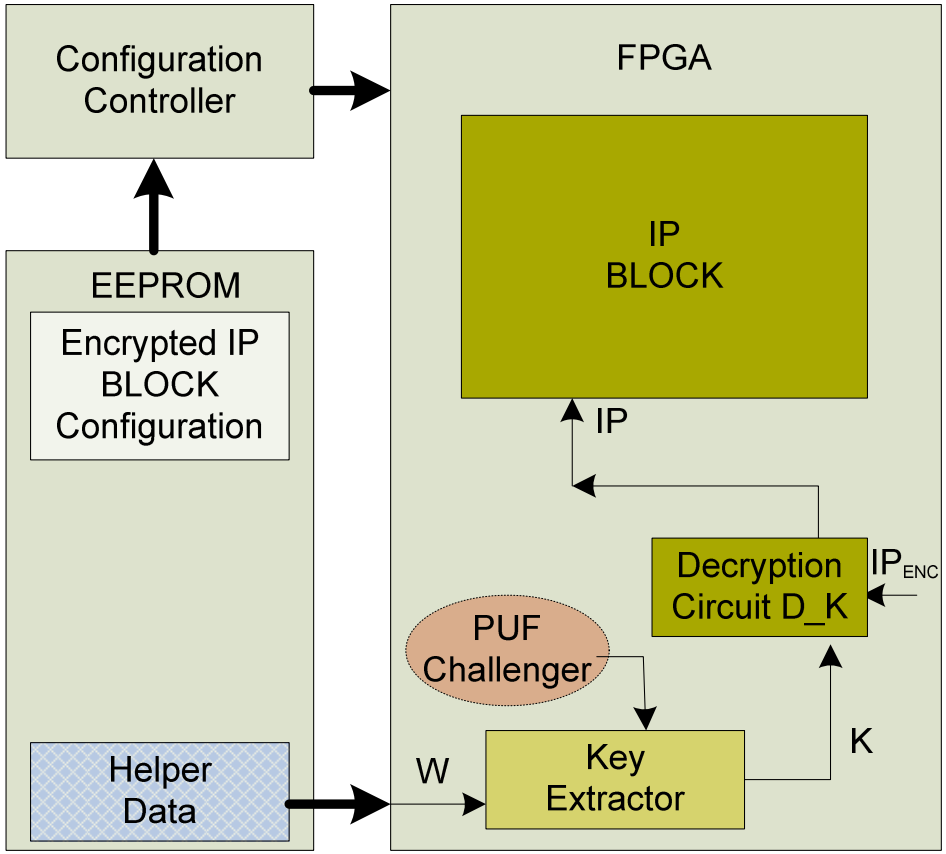
← SW

$D \leftarrow Enc_{R1}(SW \| ID_{SW})$

Offline Phase

← $C_1 \| C_2 \| D \| MAC_{R2}(C1 \| C2 \| D)$

PUF based Solution

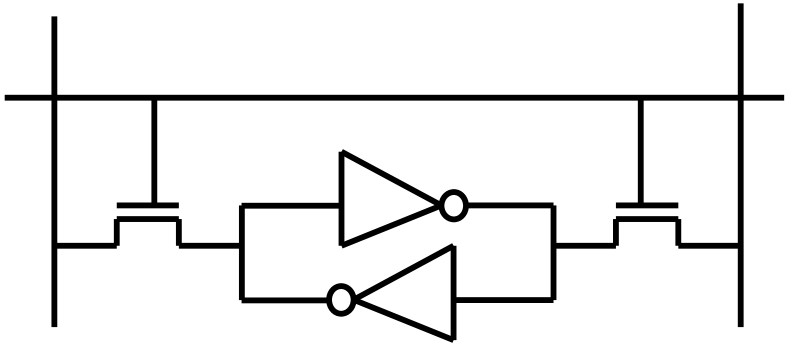


- Intrinsic PUF
- Helper Data dependent on the specific FPGA chip

One Catch!

Problem:

- Not all FPGAs contain uninitialized SRAM memory
- Startup = power down + power up



Solution:

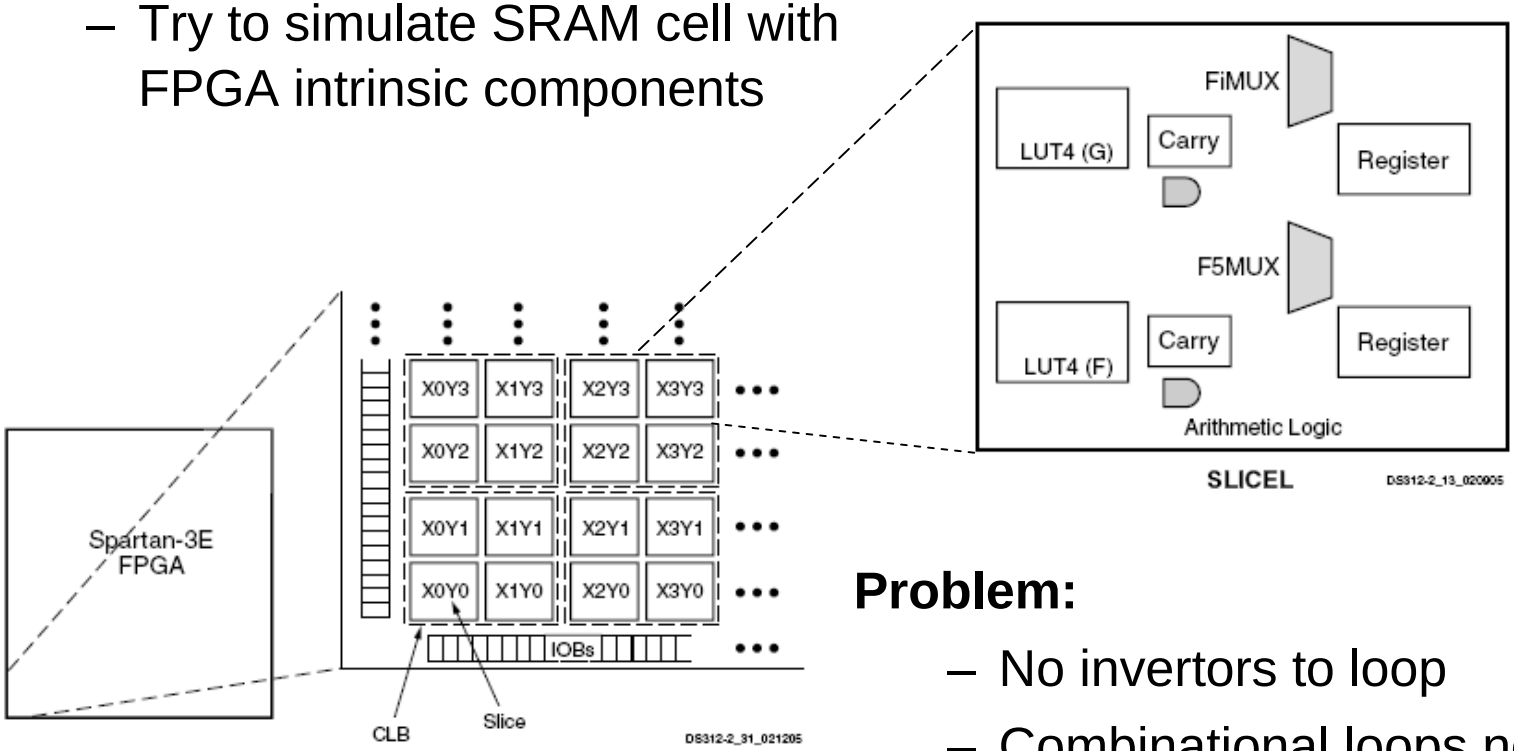
- Try to simulate SRAM cell with FPGA intrinsic components

Contents

Configurable Logic Blocks (CLB)

Solution:

– Try to simulate SRAM cell with FPGA intrinsic components

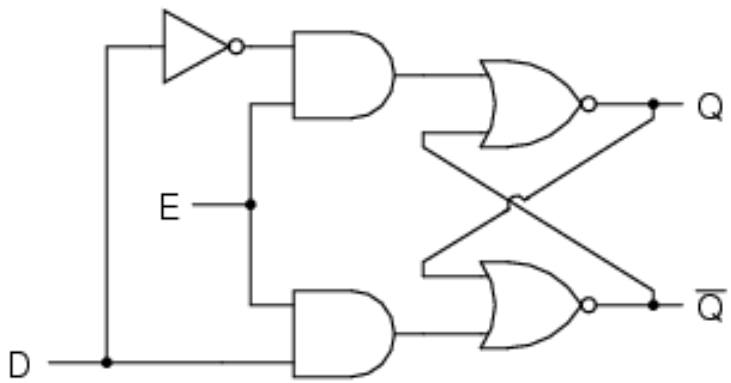


Problem:

– No invertors to loop

– Combinational loops not supported

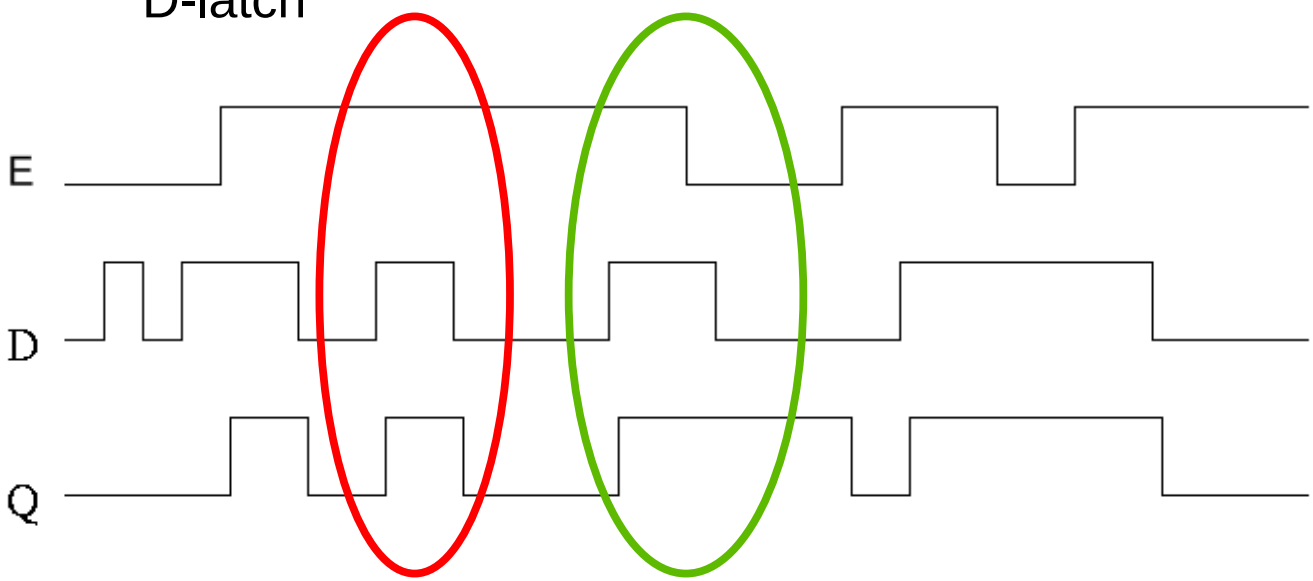
D-Latch operation



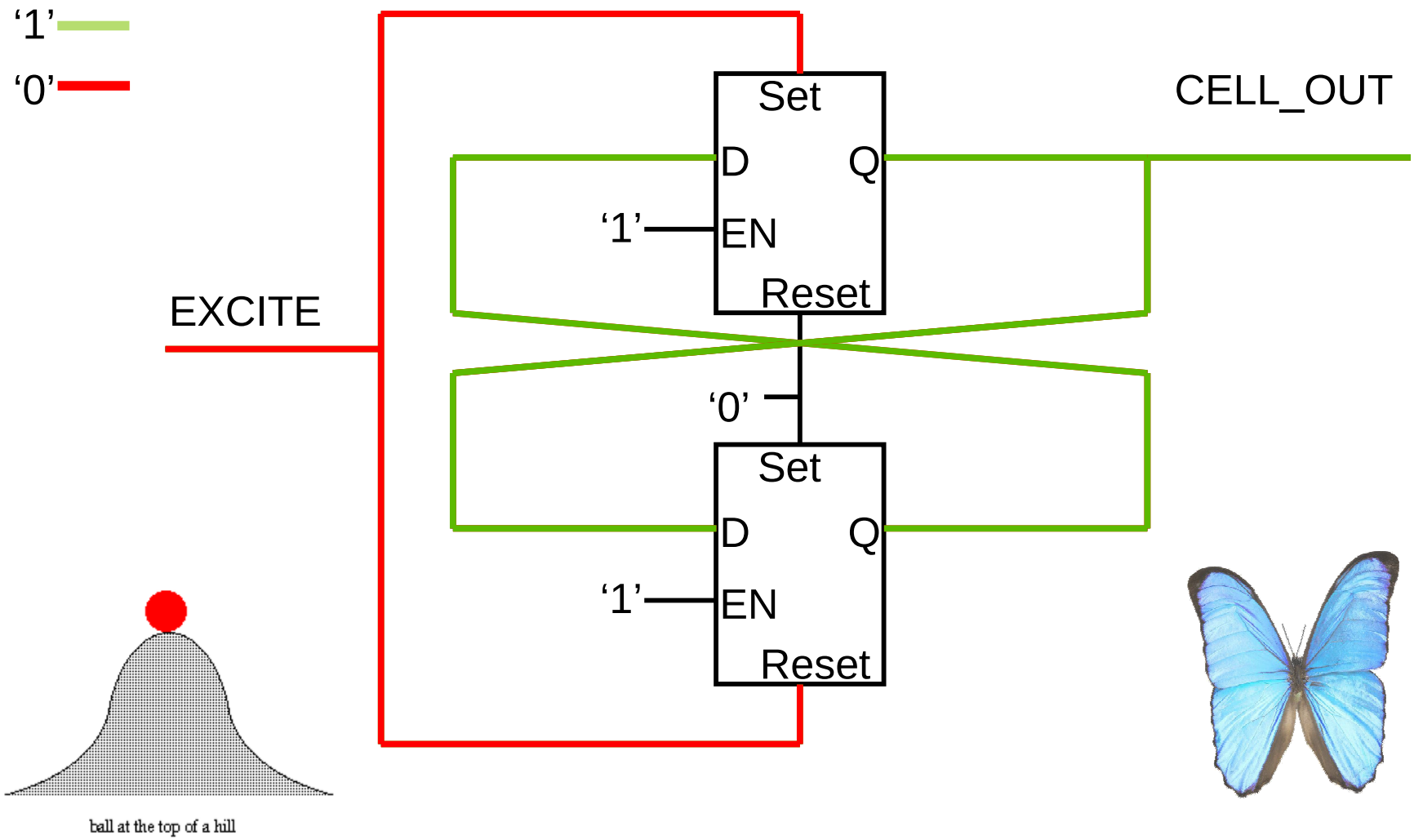
D-latch

Solution:

– Trick FPGA to use latches as combinational circuits

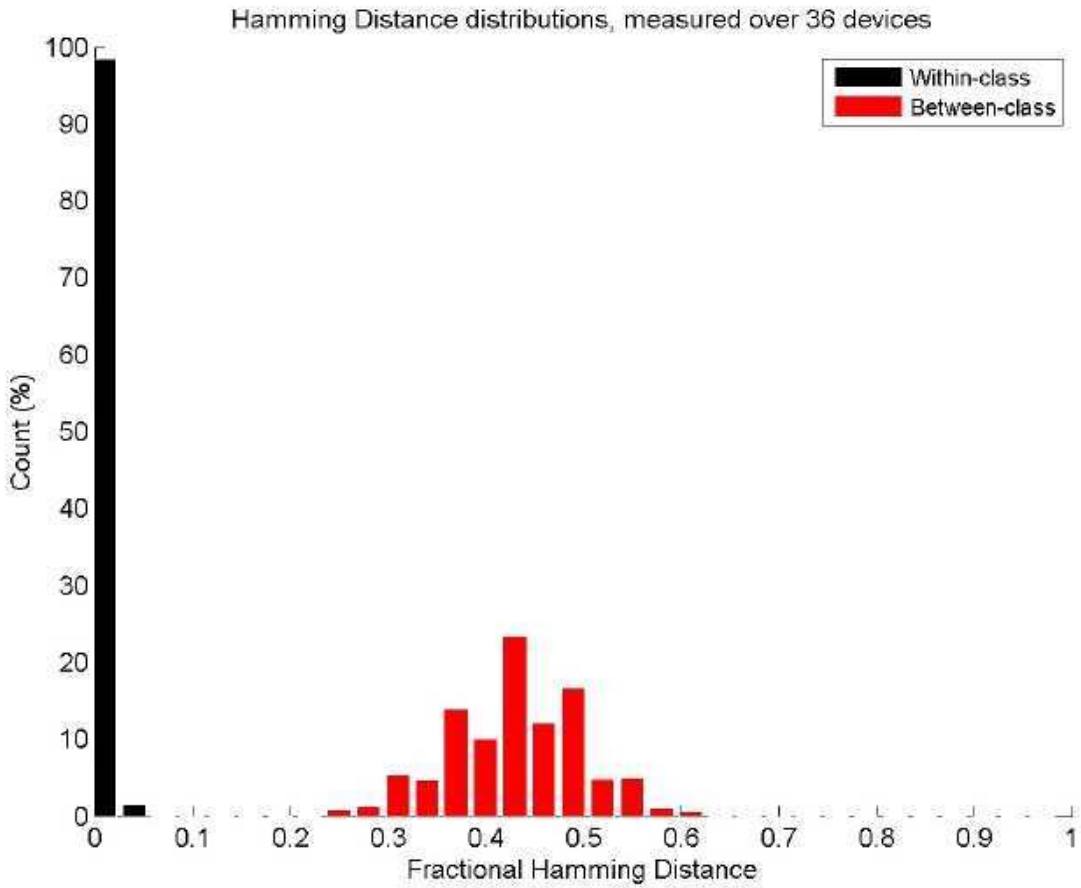


Butterfly-PUF-cell



Properties & Environmental Tests

- Good identification capabilities
  - 64 BPUF cells, we can derive an identifier for the FPGA requiring 130 slices for a full entropy 50-bit identifier

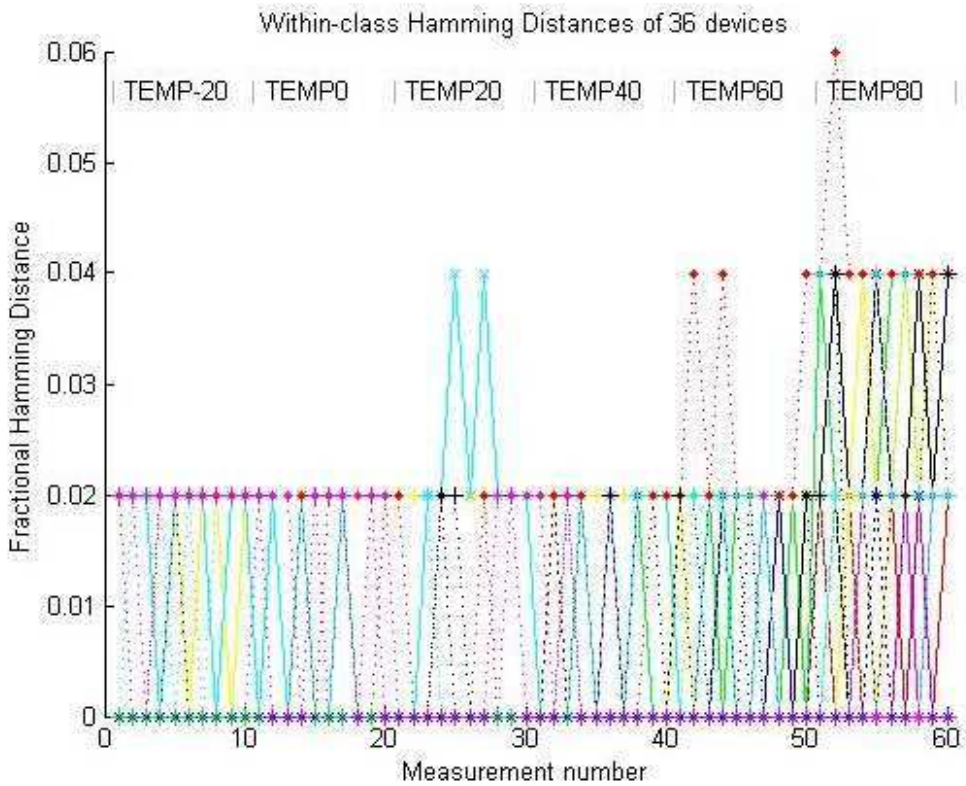


Properties & Environmental Tests

- Good performance in desired temperature range (-20˚C to +80˚C)
- Other Tests: varying operating frequency (50 Mhz to 120 MHz) and FPGA core voltage

Fuzzy extractor to take care of noise in PUF response

Assuming a 0.78 bits of entropy for every BPUF output bit, we would need about 1500 Butterfly PUF cells to derive a uniformly distributed random 128-bit key with a failure rate of 10^{-6}



Past & Future of PUF Research

Interesting because of Unclonability and Randomness property Intrinsic in them

IC Identification

- B. Gassend, D. E. Clarke, M. van Dijk, and S. Devadas. Silicon physical unknown functions. *ACM Conference on Computer and Communications Security — CCS 2002*.

IP protection in FPGAs

- E. Simpson and P. Schaumont. Offline Hardware/Software Authentication for Reconfigurable Platforms. *Cryptographic Hardware and Embedded Systems — CHES 2006*.
- J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls. FPGA Intrinsic PUFs and Their Use for IP Protection. *Cryptographic Hardware and Embedded Systems — CHES 2007.*
- J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls. Physical Unclonable Functions and Public Key Crypto for FPGA IP Protection. *2007 International Conference on Field Programmable Logic and Applications — FPL 2007.*

Remote service and Feature activation

- J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls. Brand and IP Protection with Physical Unclonable Functions. *IEEE International Symposium on Circuits and Systems — ISCAS 2008*.

Secret-Key storage

- P. Tuyls, G.-J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, and R. Wolters. Read-Proof Hardware from Protective Coatings. *Cryptographic Hardware and Embedded Systems — CHES 2006.*

Authentication via challenge-response protocols

- R. S. Pappu. *Physical one-way functions*. PhD thesis, Massachusetts Institute of Technology, March 2001.

Key Distribution in wireless sensor networks

- J. Guajardo, S. S. Kumar, and P. Tuyls. Key Distribution for Wireless Sensor Networks and Physical Unclonable Functions. Secure Component and System Identification — SECSI 2008.

Trusted computing

- D. Schellekens, P. Tuyls, and B. Preneel. Embedded Trusted Computing without Non-Volatile Memory. *TRUST Conference 2008.*

New PUF constructions

- DAC 2007 & ISCAS 2008

Thanks & Questions

?

sandeep.kumar@philips.com