

# PHILIPS

## Anti-Counterfeiting Technology based on Physical Unclonable Functions

Pim Tuyls

Philips Research Eindhoven  
The Netherlands  
Pim.tuyls@philips.com

## Contents

Introduction and Motivation

Models & Attacks

Physical Unclonable Functions

Secure Key Storage

IP Protection



## Contents

Introduction and Motivation

Models & Attacks

Physical Unclonable Functions

Secure Key Storage

IP Protection



## Erosion of the Value

**They are likely to be Counterfeited!**

- Revenue Losses
- Threat to the economy



## Protection Against Counterfeiting

- **Level 0: No Protection**
- **Level 1: Protection with human verifiable marks**
  - Hologram
  - Visual Label
- **Level 2: Protection with Technology that has to be verified by a “simple” device**
  - ICs in Embedded Devices: RFID-Tags, Smart-Cards,..
  - Ultraviolet
  - ....
- **Level 3: Protection with Technology for which very special equipment is needed**
  - E.g. in a central bank



## Embedded Devices



- “Everywhere”
- Fall Easily in hostile hands
  - Attacker can apply cryptographic attacks
  - Attacker can also apply physical attacks

# Contents

Introduction and Motivation

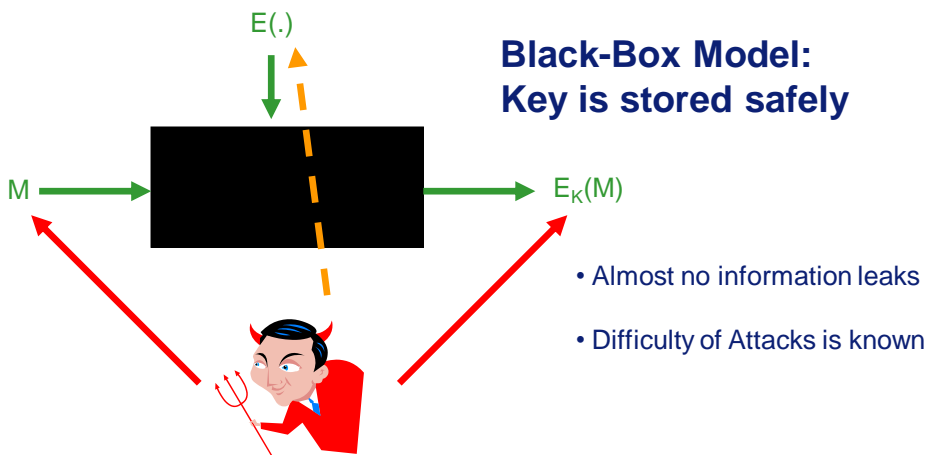
Models & Attacks

Physical Unclonable Functions

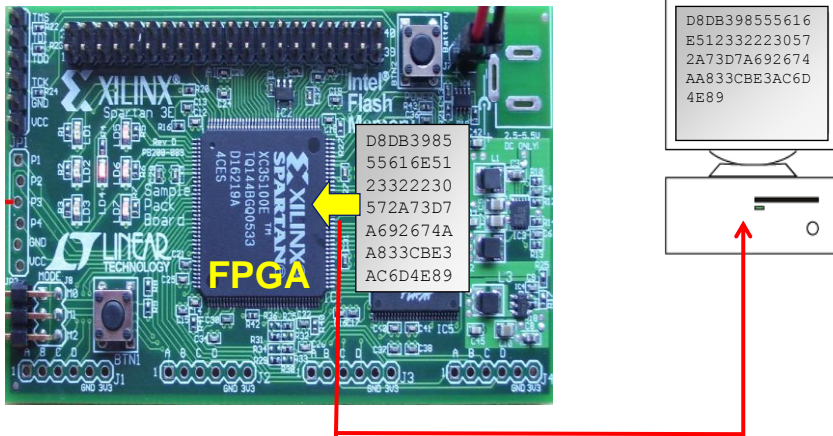
Secure Key Storage

IP Protection

# Classical Crypto

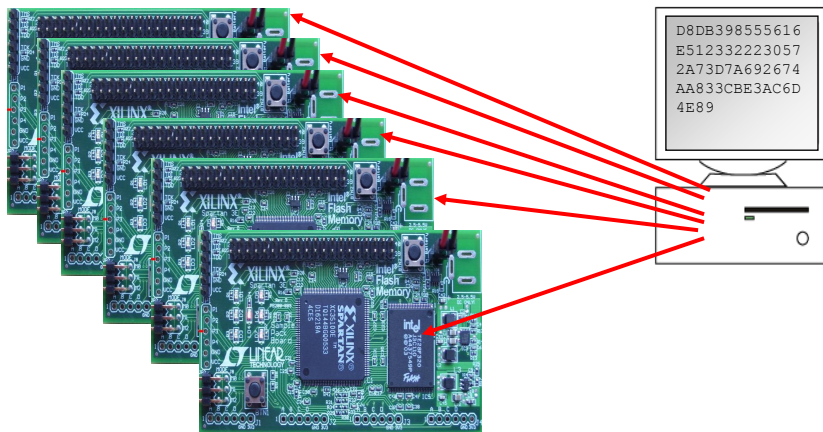


## Cloning: FPGA design cloning



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

## FPGA design cloning



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007



## Invasive vs Non-Invasive Attacks

### Definition

An *invasive* physical attack is an attack where the attacker physically breaks into the device by modifying its structure

An *non-invasive* physical attack is an attack where the attacker physically breaks into the device without modifying its structure

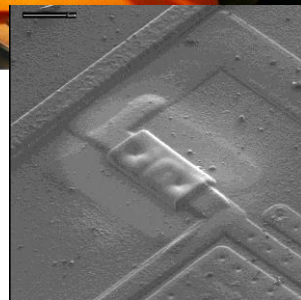
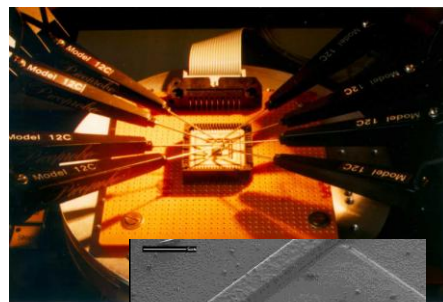


## Invasive Attacks

- Micro Probing
- Focused Ion Beams
- Chemical
- Mechanical
- Etching

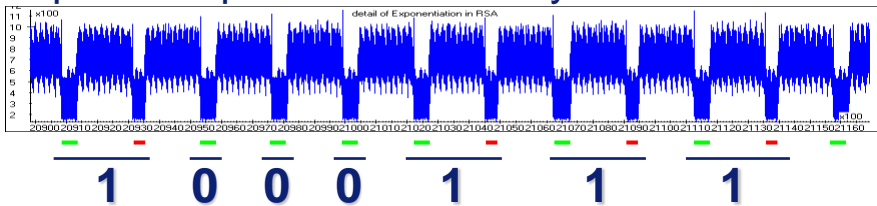
### Reference:

*Advances in Smart Card Security*  
Marc Witteman, TNO



## Non-Invasive Attacks

- Side Channel Attacks
  - Timing Analysis
  - Power Analysis
  - Electromagnetic Radiation
- Fault Induction (light, X-ray, power glitch)
- Optical Inspection of Memory



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

13

## Impact

- Not in the black-box situation
- Need for:
  - Read-Proof Hardware
  - Tamper-Proof Hardware
- New Methods & Models
  - Combine Physics & Crypto

Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

14



## Contents

Introduction and Motivation

Models & Attacks

Physical Unclonable Functions

Secure Key Storage

IP Protection



## New Approach for Secure Key Storage

### Principles:

1. Do **not** store a key in digital form
2. Generate the key **only when needed**
  - Physical Source
3. **Delete** the key



## Hardware Requirements

### Security Requirements:

1. Physical Inscrutability (opaqueness)
2. Unclonability
  1. Physical Unclonability
  2. Mathematical Unclonability
3. Tamper evident

### Practicality Requirements:

1. Easy to challenge the source
2. Cheap and easy integratable on an IC
3. Excellent mechanical and chemical properties



## Physical Unclonable Function

### Physical Unclonable Function (PUF):

Inherently unclonable Physical Structure  
(due to process variations) satisfying:

- Easy to evaluate: Challenges-Responses
- Inherently tamper evident
- Inseparably bound to the object
- Manufacturer not-reproducible
- Source of a large amount of unclonable secret key material

# Hard Problem

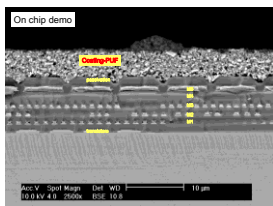
## Making a Random PUF



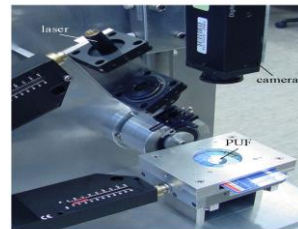
## Making/Modelling a Specific PUF



# Examples



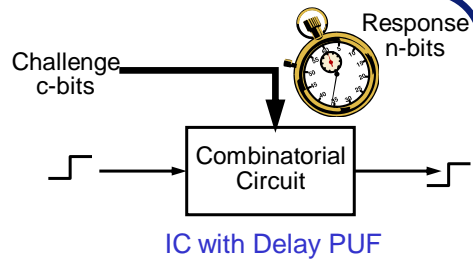
Optical PUF  
IC with Coating PUF



Intrinsic Identifier



IC with SRAM PUF



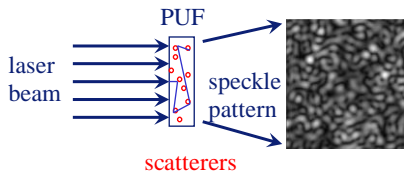
IC with Delay PUF

# Information Content of a PUF (Response)

## Optical PUF [FC05]

$$H(R) \propto \frac{A\ell}{\lambda^2 d} \log \frac{\pi N_{\text{photons}}}{N_{\text{modes}}}$$

≈ 10<sup>7</sup> bits

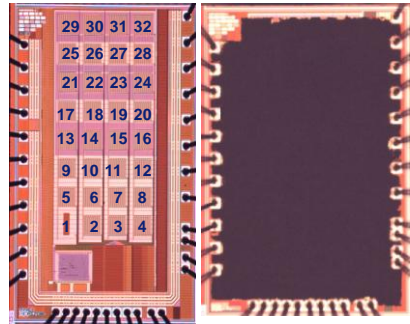


Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

## Coating PUF [JAP06]

$$H = \log \left[ \frac{\sqrt{2\pi\epsilon} A \epsilon_0}{\sigma_N d} \sqrt{\frac{q(1-q)}{Ad/s^3} \frac{|\epsilon_1^{-1} - \epsilon_2^{-1}|}{[(1-q)\epsilon_1^{-1} + q\epsilon_2^{-1}]^2}} \right]$$

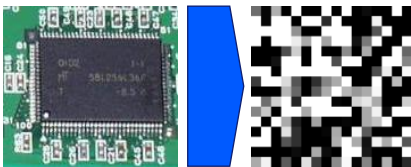
≈ 6.6 bits/sensor



21

# Information Content of a PUF Response II

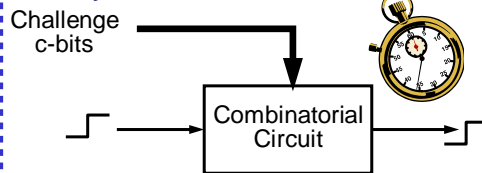
## S-RAM PUF



H(R)=95% S-RAM Size

Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

## Delay PUF

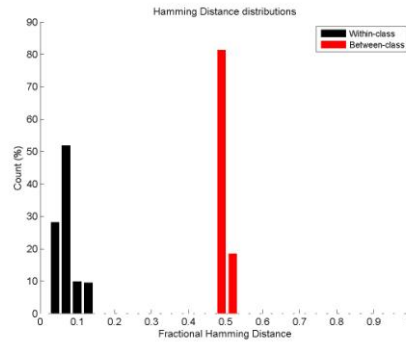
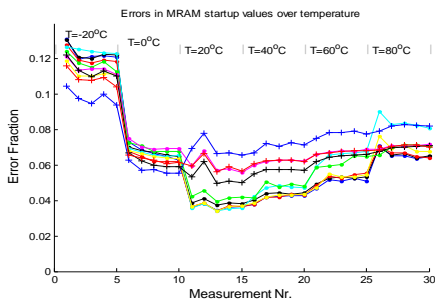


H(R) ≈ 10 bits

22



## Inter-Class; Intra-Class and Temp Performance Of S-RAM PUFs

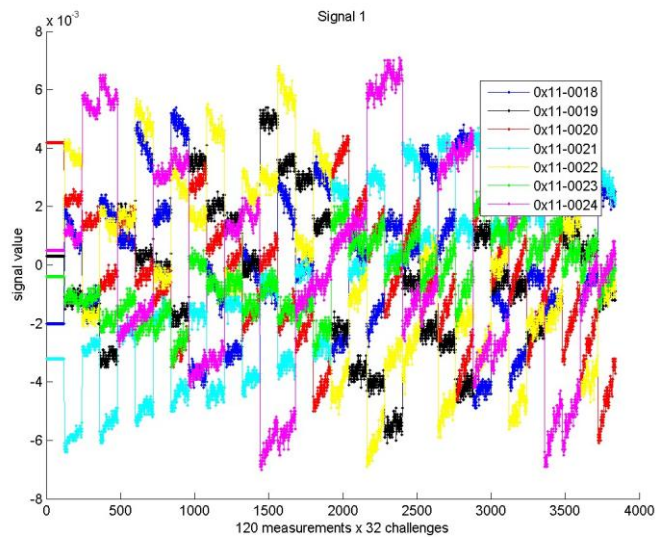


Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

23



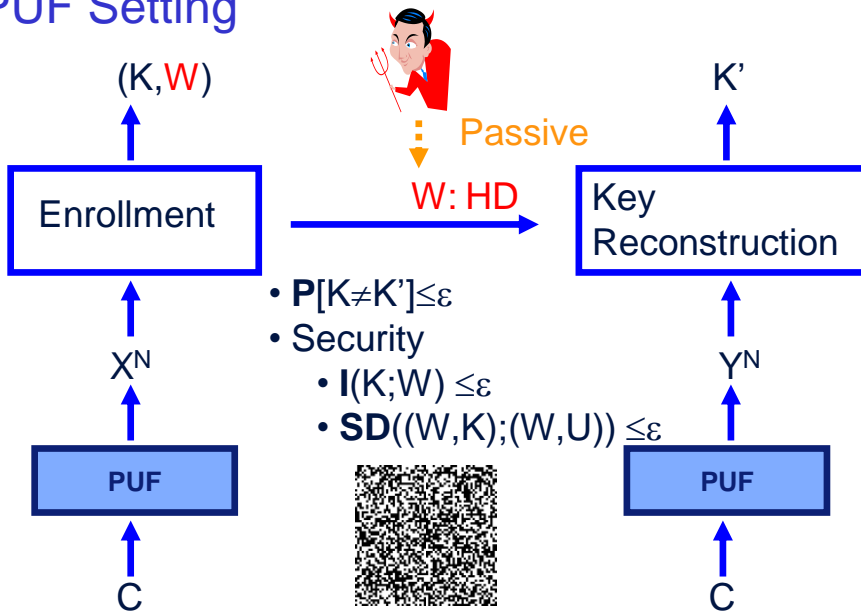
## Delay PUFs: Temperature Influence



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

24

## PUF Setting



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

25

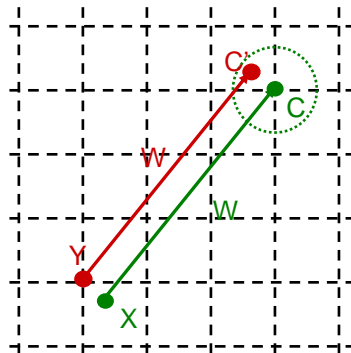
## Key Extraction from Noisy Data: Idea

- Grid points represent ECC Code words
- Enrollment**
- Random codeword  $C(S)$  is chosen
  - Response  $X$  is measured
  - Helper data  $W$  is generated (difference between  $X$  and  $C$ ) and stored in EEPROM

**Assumption:** Response  $X$  uniformly random

**Key Reconstruction**

- $Y$  is noisy response
- $Y + W = C'$
- $S' = \text{DEC}(C')$



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

26



## Two Cases

### Discrete Case

PUFs with a discrete

Response:

- S-RAM PUFs

### Uncountable Case

PUFs where the responses belong to an uncountable space

- Optical PUFs: speckle patterns
- Coating PUFs: Capacitance values
- Delay PUFs: timing values



## General Construction: Discrete Case

Two Phases:

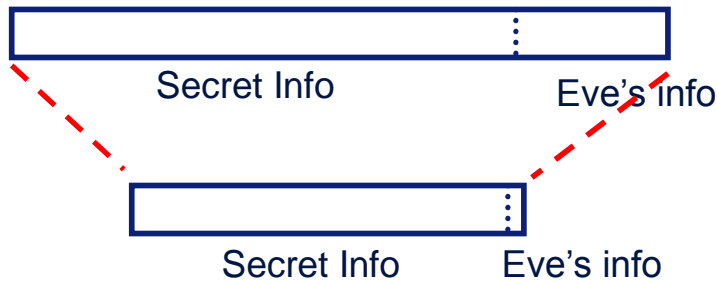
- Information Reconciliation (IR)
  - Performs error correction
  - Leaks information
  - Does not lead to a secure key
  - First set of helper data:  $W_1$
- Privacy Amplification
  - Turns the string after IR into a secure key
  - Second set of helper data:  $W_2$

## Universal Hashing

A class  $\mathcal{H}$  of functions  $\mathcal{A} \rightarrow \mathcal{B}$  is 2-universal if for all distinct  $a_1, a_2 \in \mathcal{A}$  and all  $b_1, b_2 \in \mathcal{B}$

$$\mathbb{P}[h(a_1) = b_1 \quad \text{and} \quad h(a_2) = b_2] = \frac{1}{|\mathcal{B}|^2}$$

for randomly chosen  $h$ .



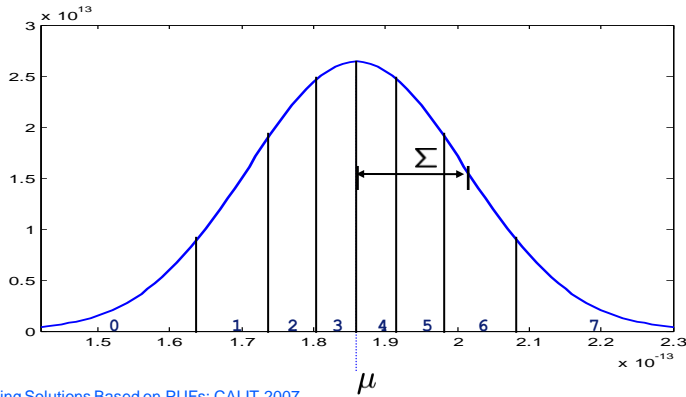
## PUFs with Uncountable Response

Two Step Approach:

- Quantisation Step:
  - Turn analog  $\rightarrow$  Discrete values with Uniform Distribution
- Discrete Fuzzy Extractor
  - Information Reconciliation
  - Privacy Amplification

## Uniformly Distributed Keys

- Quantization with equiprobable intervals

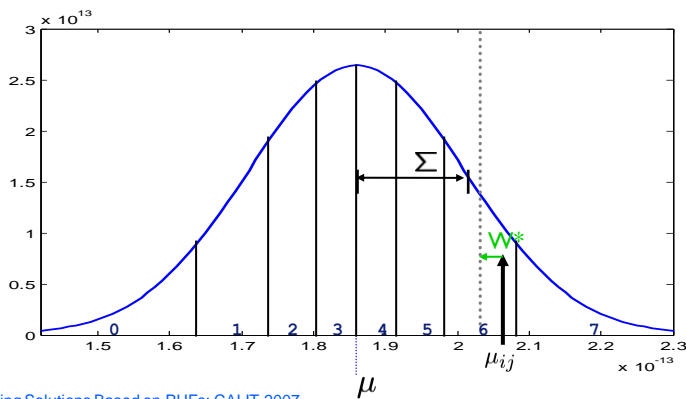


Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

31

## Achieving Robustness (I)

- Define helper-data  $W^*$  that shifts measurements to the center of a quantization interval.

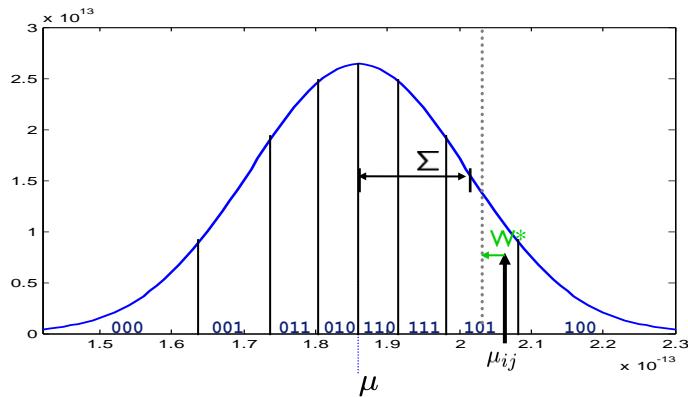


Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

32

## Achieving Robustness (II)

- Assign bits to quantization intervals according to a Gray-code.



- Last Step: Apply a Discrete FE

## Contents

Introduction and Motivation

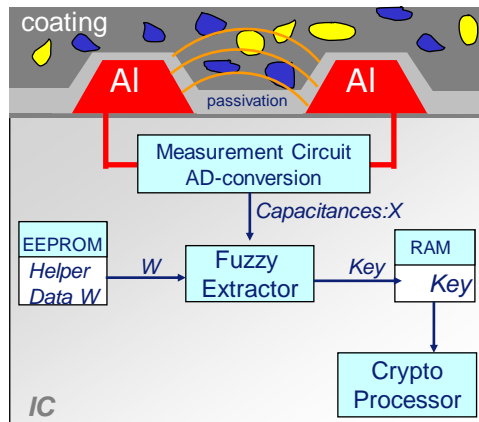
Model & Attacks

Physical Unclonable Functions

Secure Key Storage

IP Protection

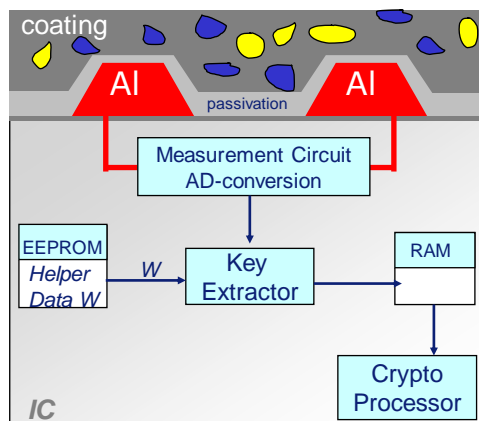
## Key Storage with (Coating) PUF



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

35

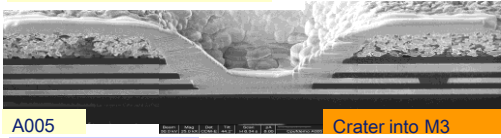
## Key Storage with (Coating) PUF



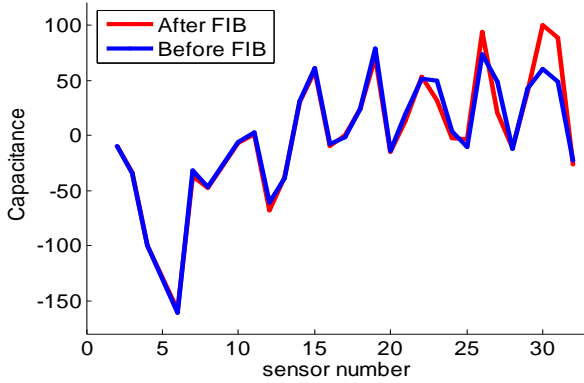
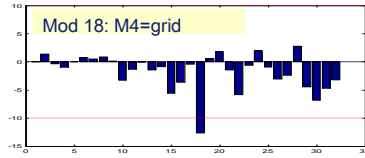
Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

36

Craters: 10  $\mu\text{m}$  x 10  $\mu\text{m}$



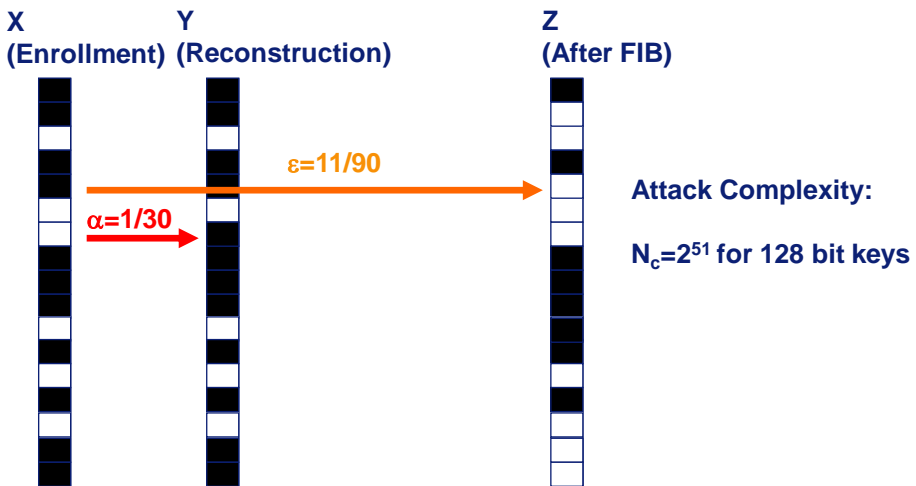
3.0-3.5 coating



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

37

## Key Damage: Experiments

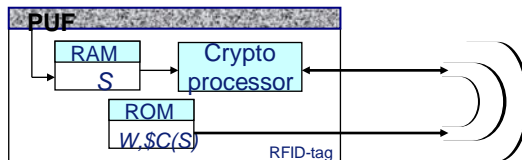


Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

38

## Application: RFID Tags for Anti-Counterfeiting

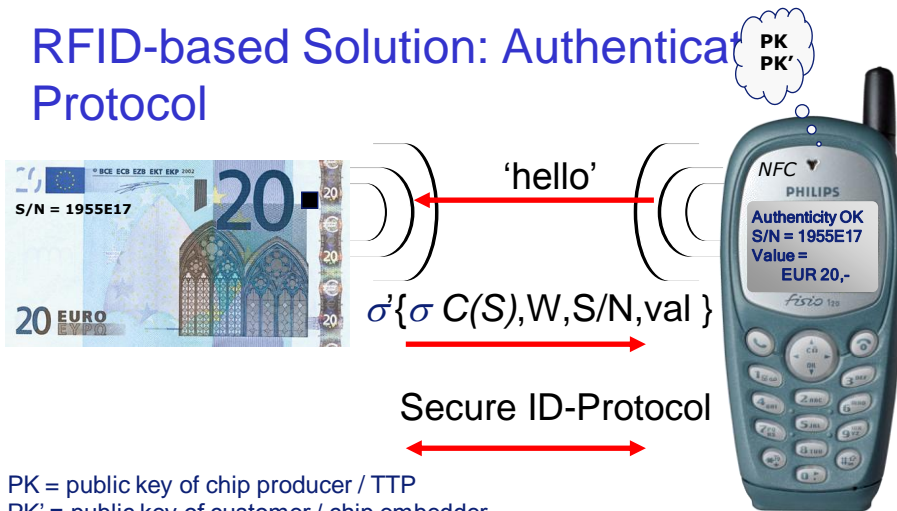
- RFID-tag equipped (e.g. covered) with a PUF
- A unique, secret bit-string  $S$  is derived from the PUF together with HD:  $W$
- Reference information  $\sigma(C(S))$ : *commitment to  $S$ , signed by TTP and stored in ROM.*



Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

39

## RFID-based Solution: Authentication Protocol



PK = public key of chip producer / TTP  
 PK' = public key of customer / chip embedder  
 S/N = serial number

Anti-Counterfeiting Solutions Based on PUFs; CALIT 2007

40



# Contents

Introduction and Motivation

Physical Unclonable Functions

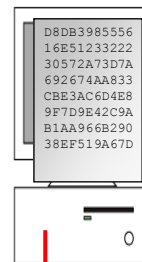
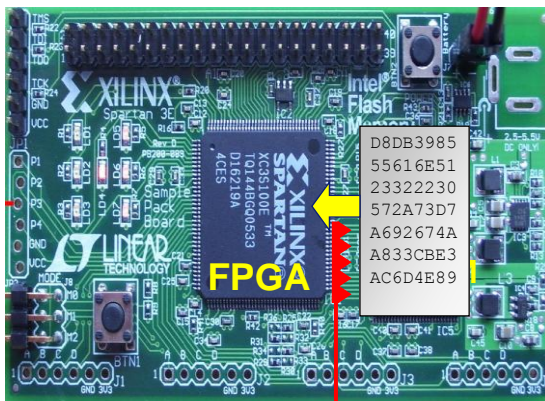
Helper Data and Fuzzy Extractors

Secure Key Storage

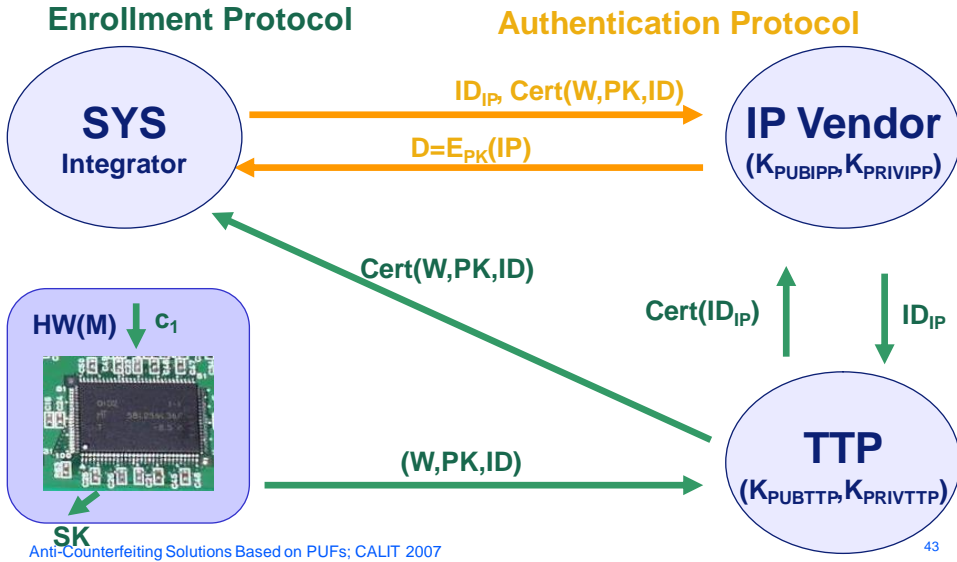
IP Protection



# IP Theft: Bit stream Cloning of SRAM-FPGAs

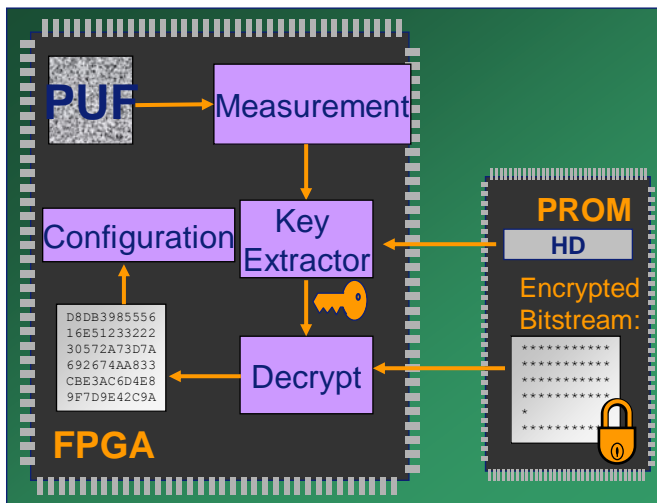


# Secure IP Trading Protocol



43

# FPGA Bitstream Encryption with PUFs



44

