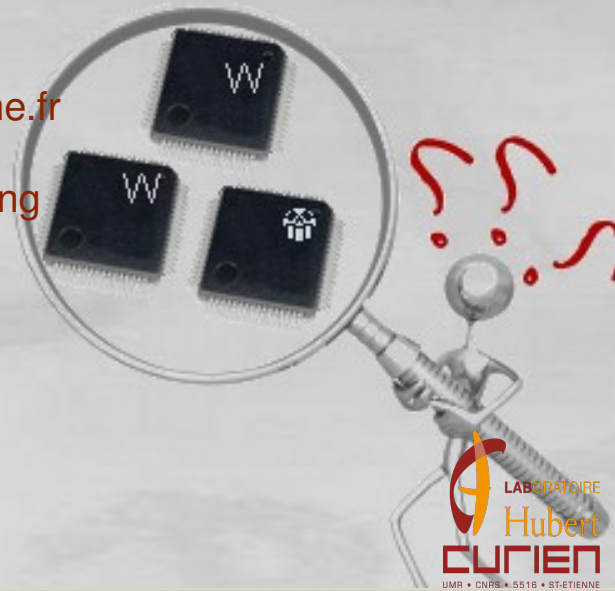
IP Watermark Verification Based on Power Consumption Analysis

Cédric Marchand[1], Lilian Bossuet[1], Edward Jung[2]

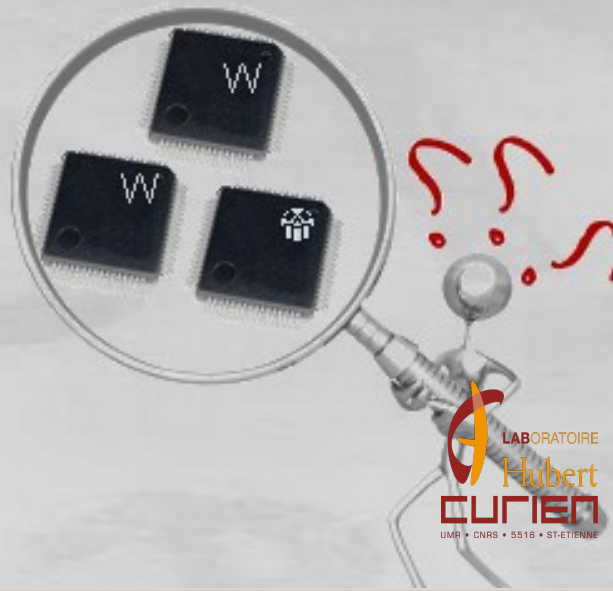
[1]Laboratoire Hubert Curien, UMR CNRS 5516
University of Lyon
Saint-Etienne, France
{cedric.marchand,lilian.bossuet}@univ-st-etienne.fr

[2]School of Computing and Software Engineering
Southern Polytechnic State University
GA, USA
ejung@spsu.edu

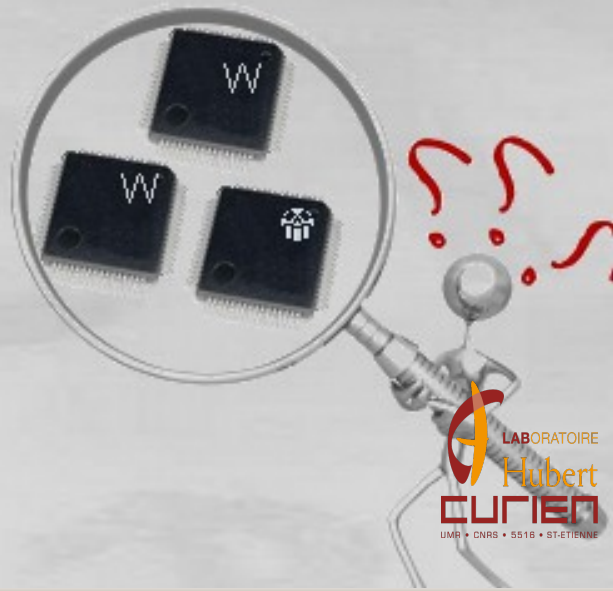
July 1, 2014



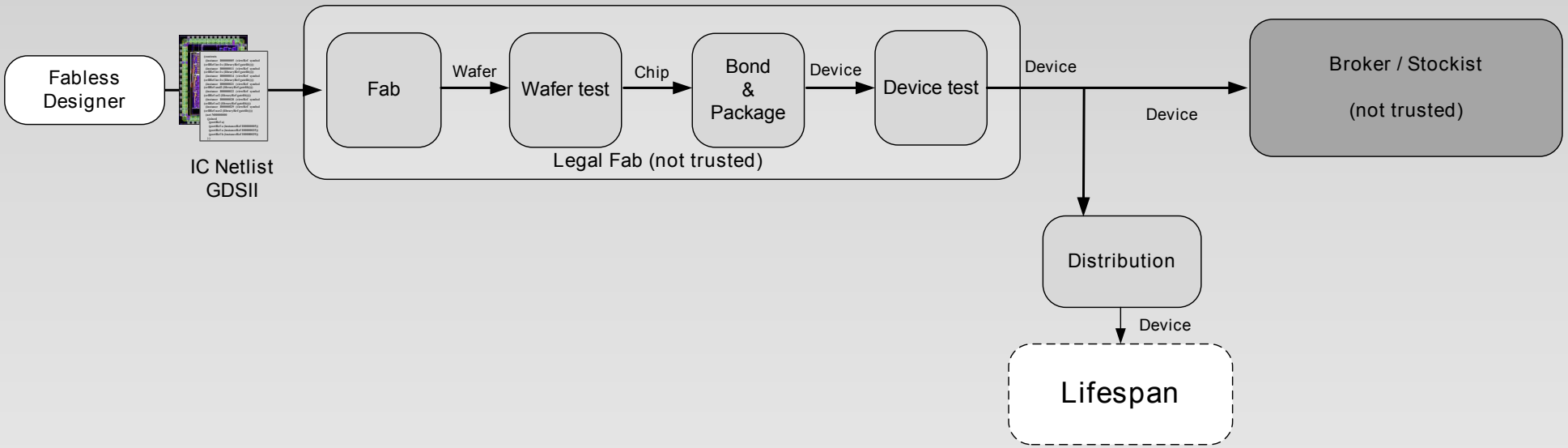
Outline



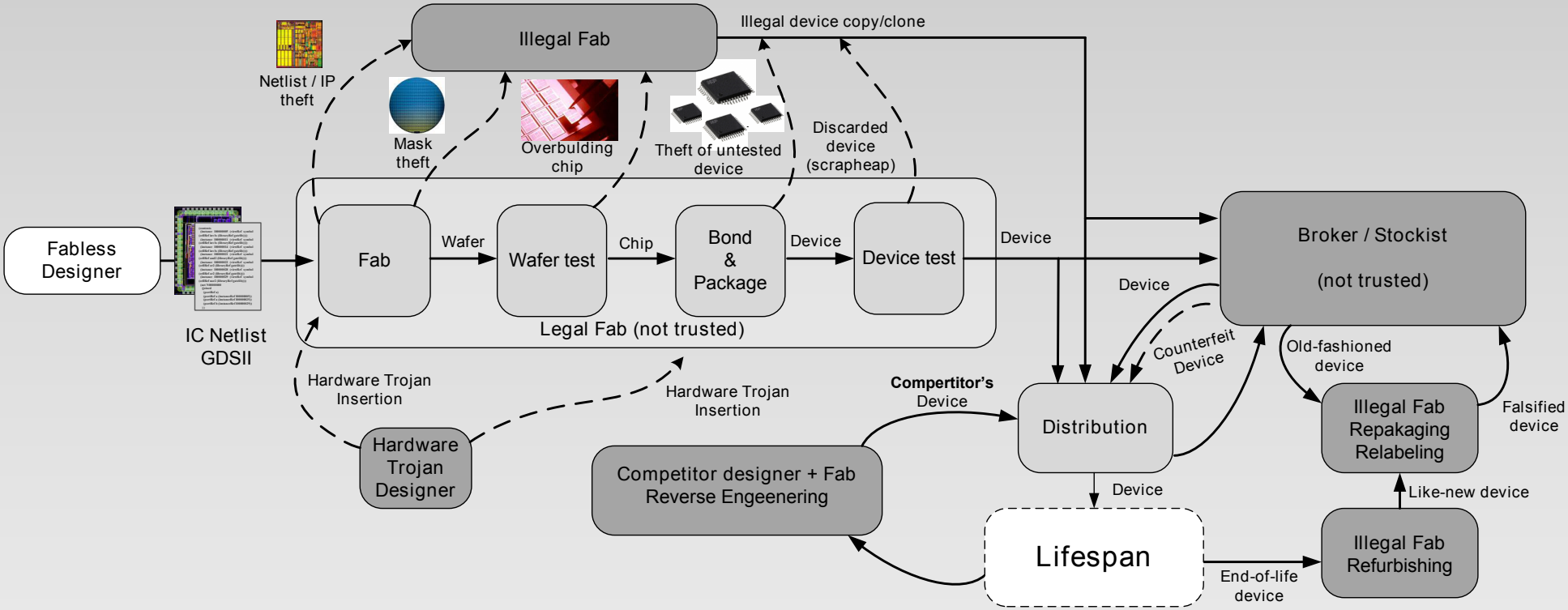
Outline



IC Model


Fabless Designer
IC Netlist GDSII
Fab
Wafer
Wafer test
Chip
Bond & Package
Device
Device test
Legal Fab (not trusted)
Device
Broker / Stockist
(not trusted)
Device
Distribution
Device
Lifespan

IC Threats Model



Fight these threats by designing SALWARES

SALutary hardWARES: SALWARES

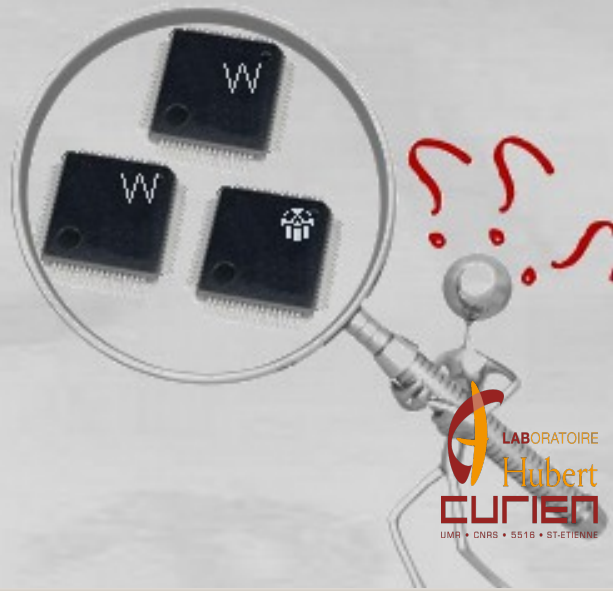
Salutary hardware (SALWARE) is a (small piece of) hardware system, hardly detectable (from the attacker point of view), hardly circumvented (from the attacker point of view), inserted in an integrated circuit or an IP, used to provide intellectual property information and/or to remotely activate the integrated circuit or IP after manufacture and/or during use.

Fight these threats by designing SALWARES

Example of well-known SALWARES

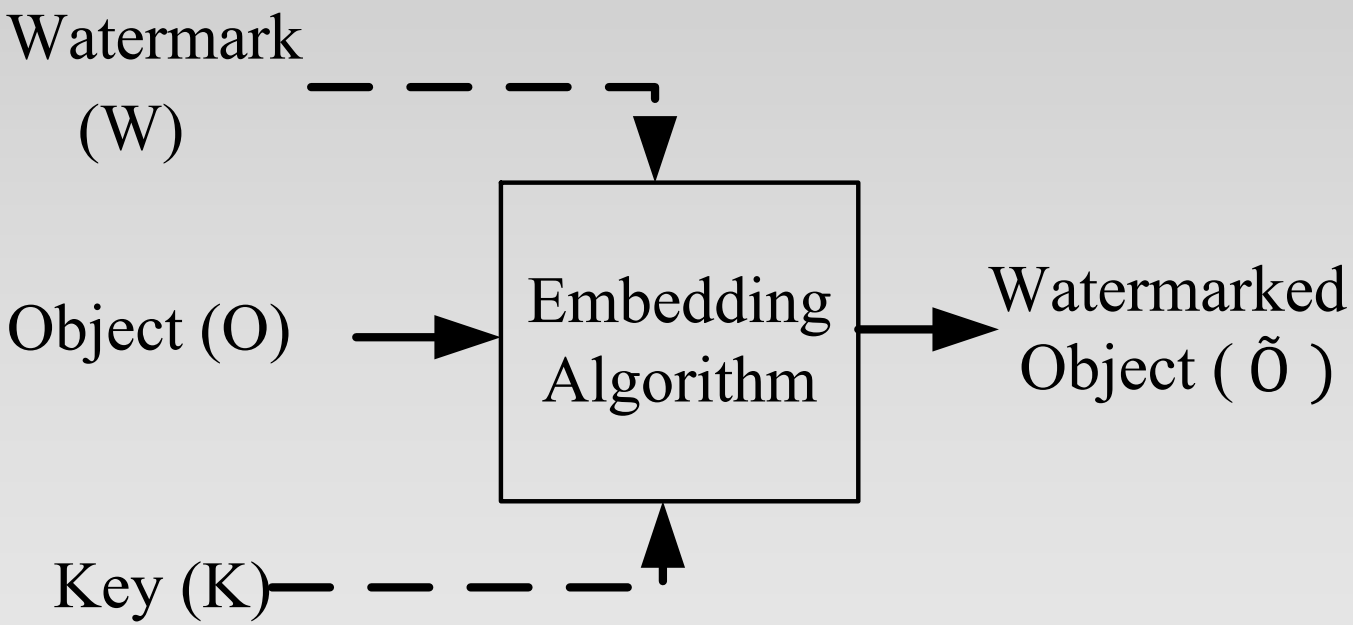
- Physical Unclonable Function for authentication
- Memory encryption, Logic encryption
- Hardware metering, IC metering
- Remote activation
- IP Watermarking

Outline



Watermarking In General

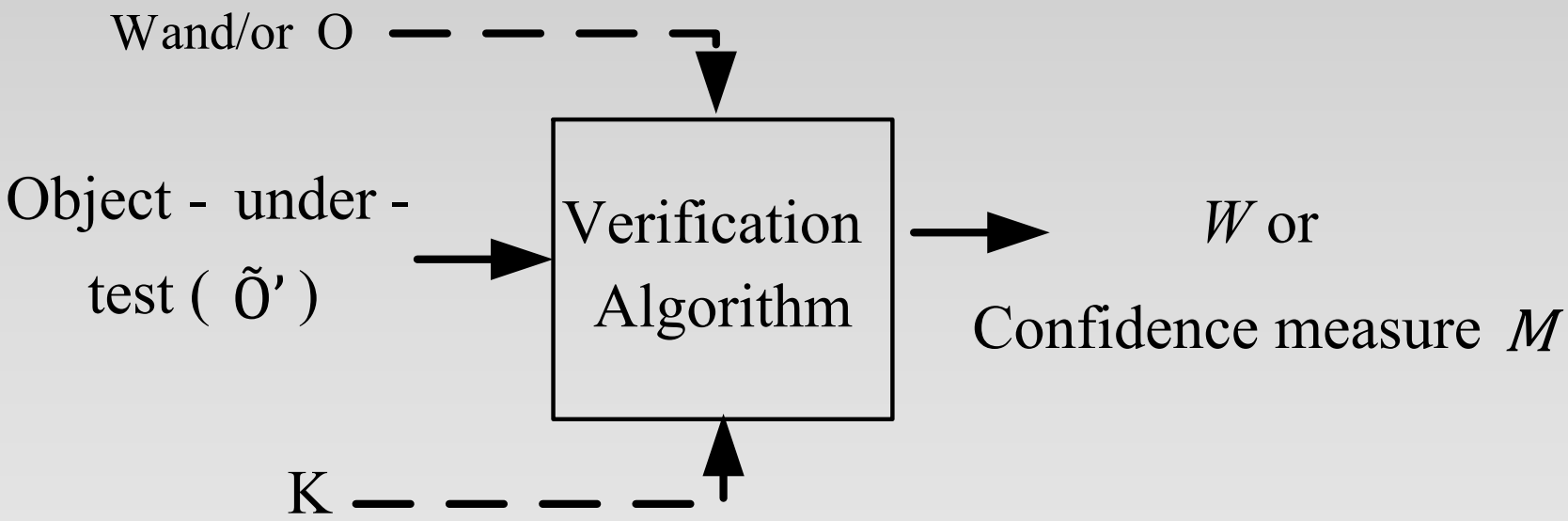
Embedding Process



Watermark embedding scheme.

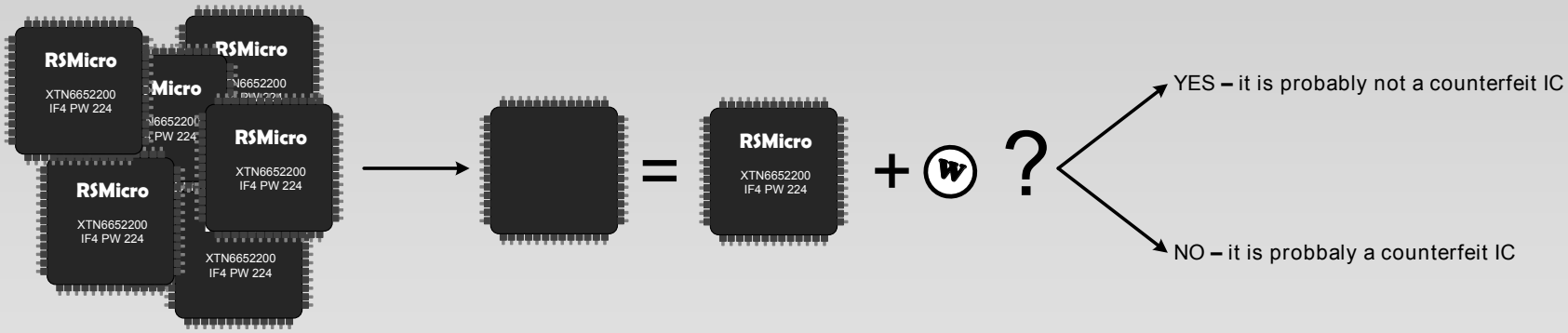
Watermarking In General

Verification Process

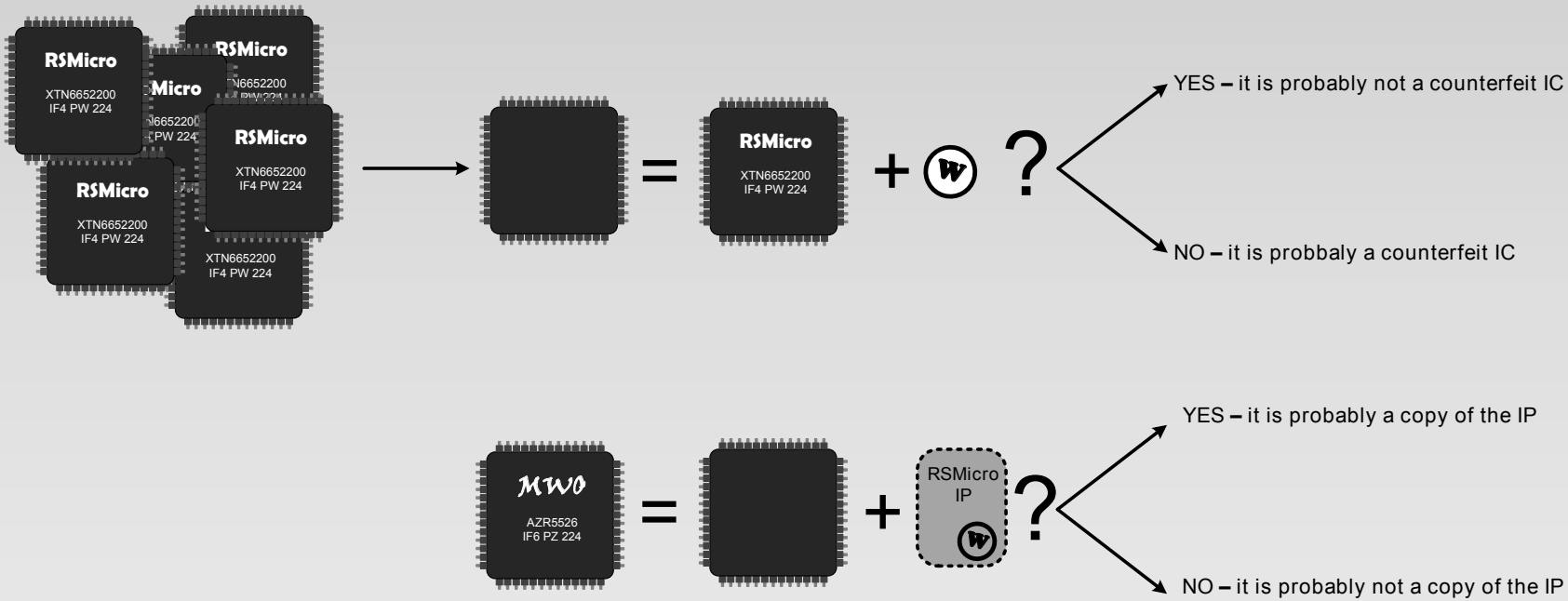


Watermark detecting scheme.

IP Watermarking, why ?



IP Watermarking, why ?



IP Watermarking, how ?

It possible to insert a watermark at different level [1]

Example of Watermarking techniques for IPs

- Physical-level: Constraints based watermarking (map and fitter)
- Structural level: Constraints based watermarking (synthesis)
- Algorithm-level: Extract properties by design
- Behavioral-level : FSM Watermarking

[1] NIE, Tingyuan. Performance Evaluation for IP Protection Watermarking Techniques.

IP Watermarking, how ?

It possible to insert a watermark at different level [1]

Example of Watermarking techniques for IPs

- Physical-level: Constraints based watermarking (map and fitter)
- Structural level: Constraints based watermarking (synthesis)
- Algorithm-level: Extract properties by design
- **Behavioral-level : FSM Watermarking**

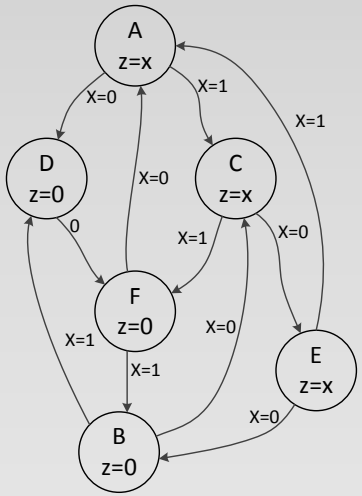
[1] NIE, Tingyuan. Performance Evaluation for IP Protection Watermarking Techniques.

FSM Watermarking

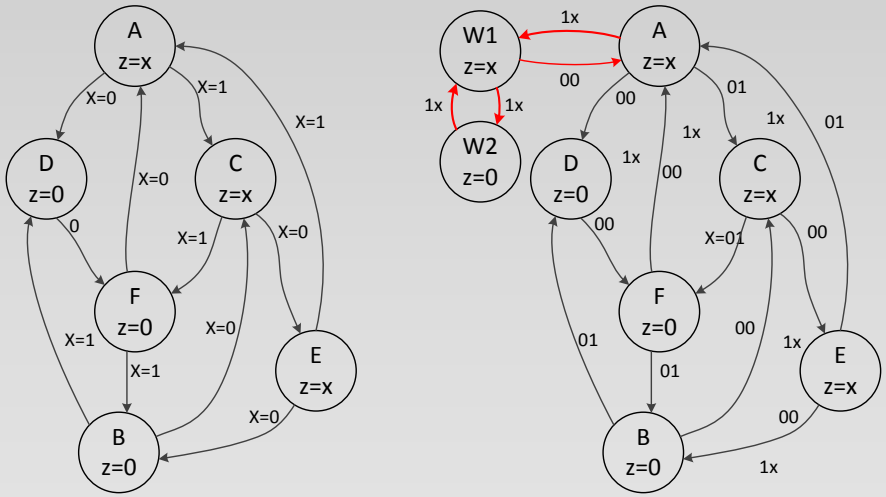
It is the method the most studied to insert a watermark inside digital and synchronous IPs because :

1. Most of this kind of IPs contains a FSM,
2. The FSM of an IP is difficult to modify without damage the IP.

Example of techniques



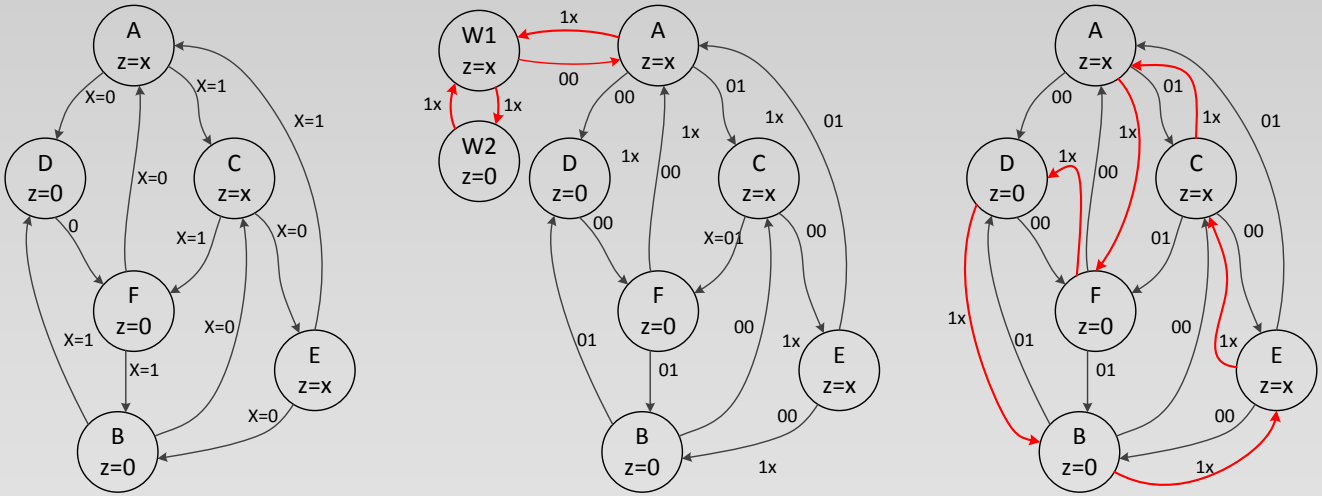
Example of techniques



FSM watermarking techniques

- Add dummy nodes to the FSM

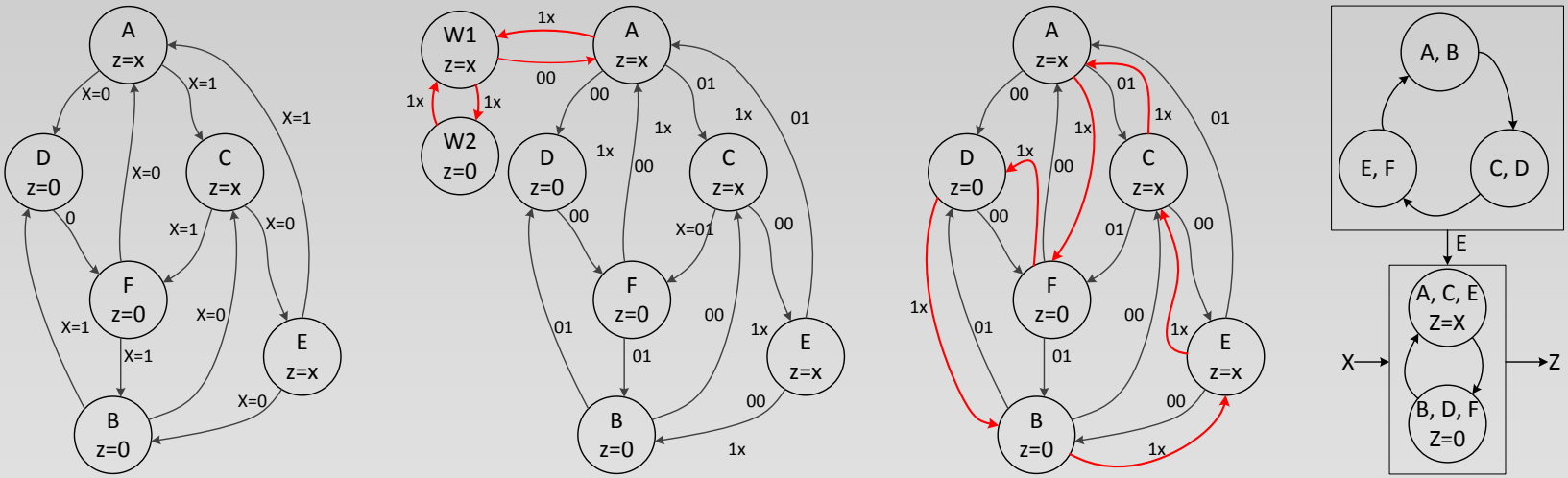
Example of techniques



FSM watermarking techniques

- Add dummy nodes to the FSM
- Add dummy transitions to the FSM

Example of techniques



FSM watermarking techniques

- Add dummy nodes to the FSM
- Add dummy transitions to the FSM
- Design the FSM to extract a specific property

Verification of the Watermark ?

In the case of FSM watermarking, the verification can be difficult and may need:

- An access to a state register
- To reveal explicitly the watermark sequence

Verification of the Watermark ?

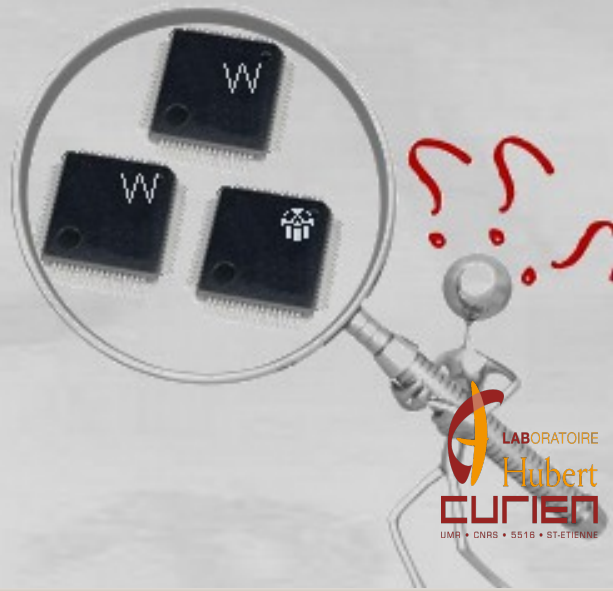
In the case of FSM watermarking, the verification can be difficult and may need:

- An access to a state register
- To reveal explicitly the watermark sequence

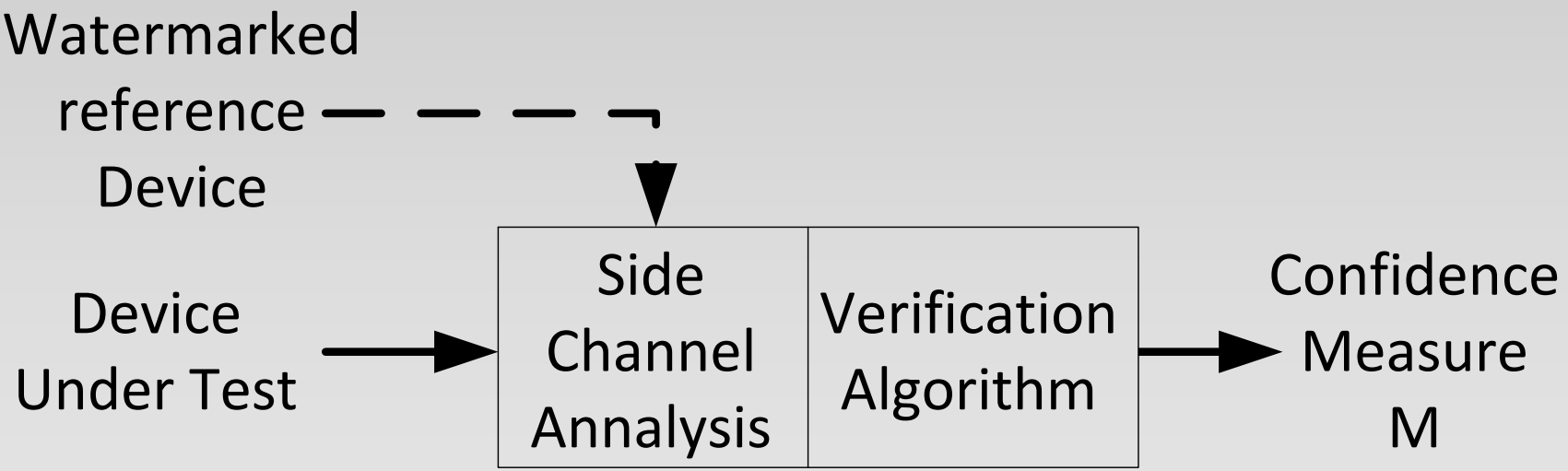
Challenge

- Find a general way to extract FSM watermark without reveal information about the original IP.

Outline



Scenario of Watermark Verifcation



Watermark detecting scheme.

Scenario of Watermark Verifcation

Requirements

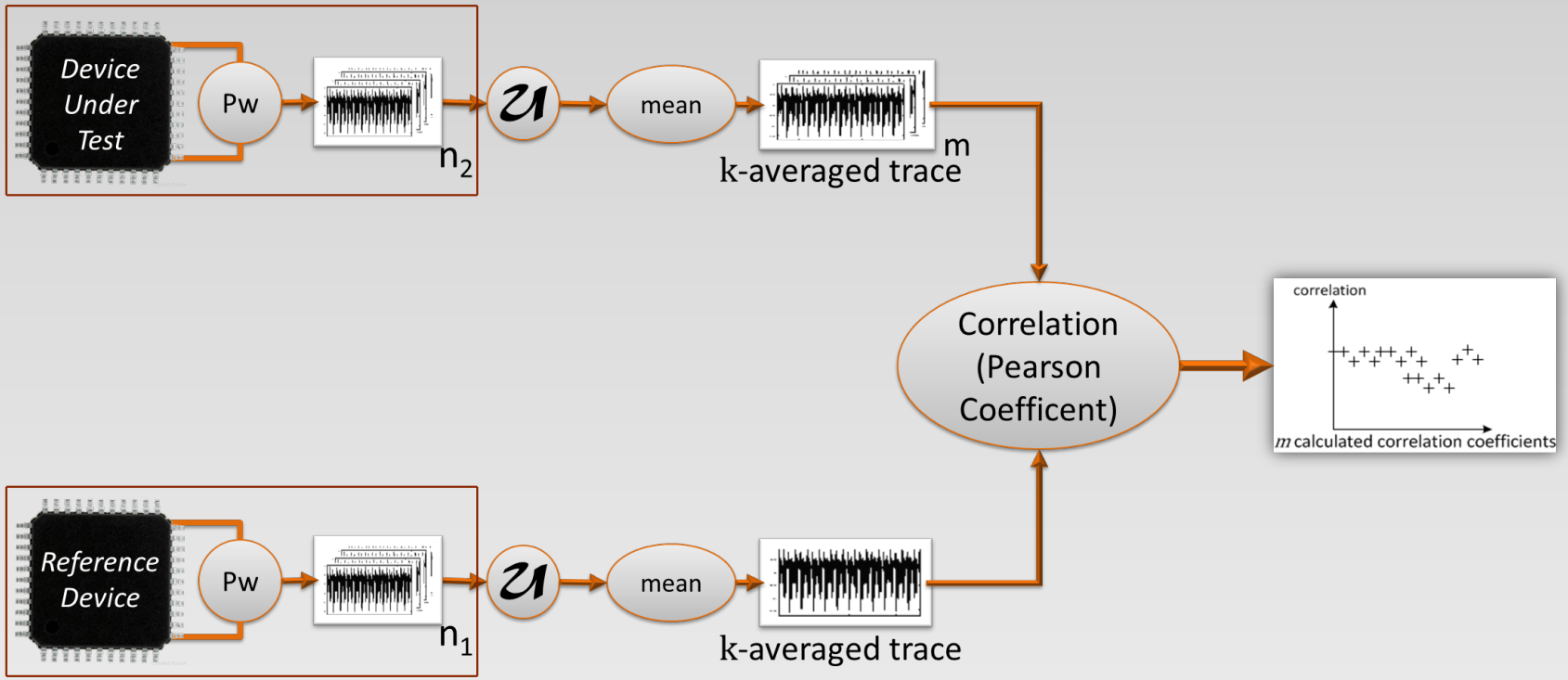
- One device containing the original watermarked IP (Reference Device)
- A set of Device Under Test (DUT)

Objectives

- Find which are the devices which contain the watermark IP among the DUTs

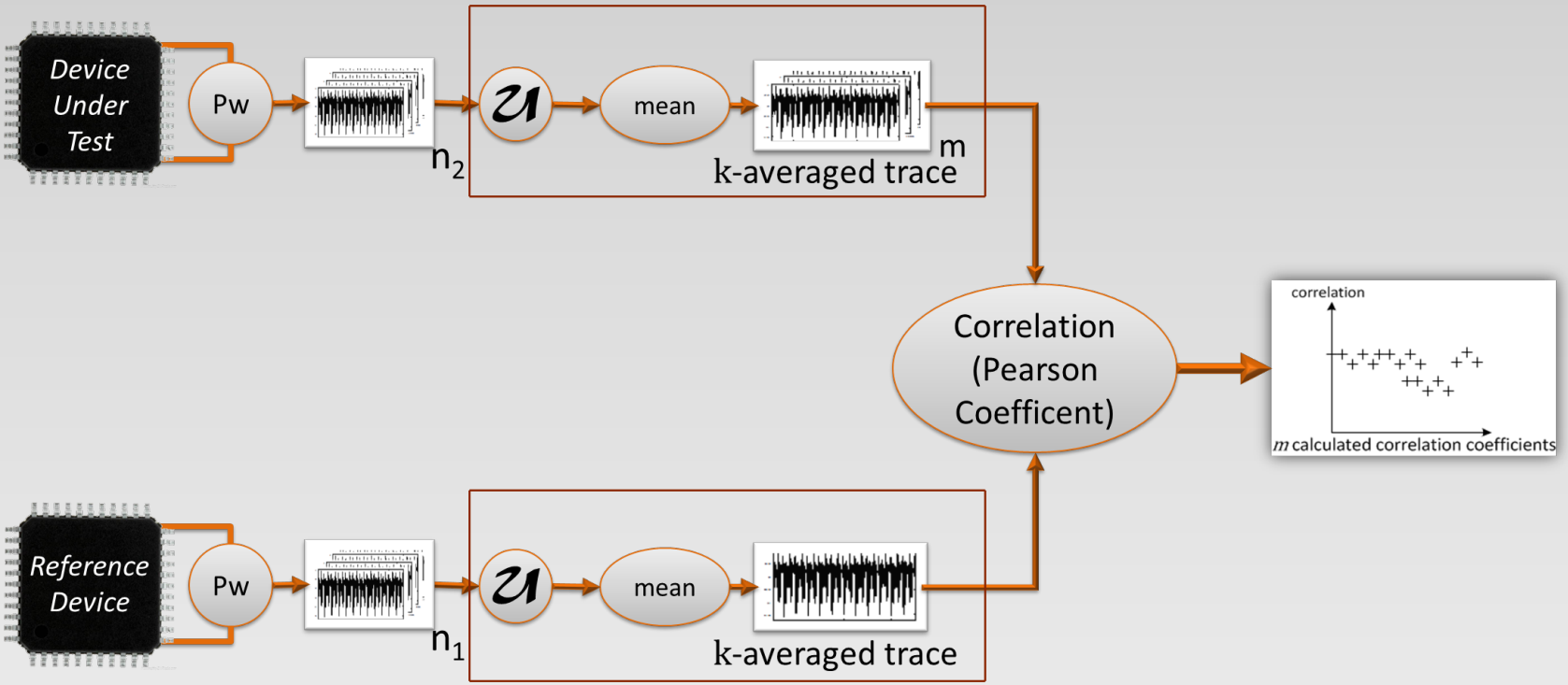
Verification flow

Function 1: Power acquisition



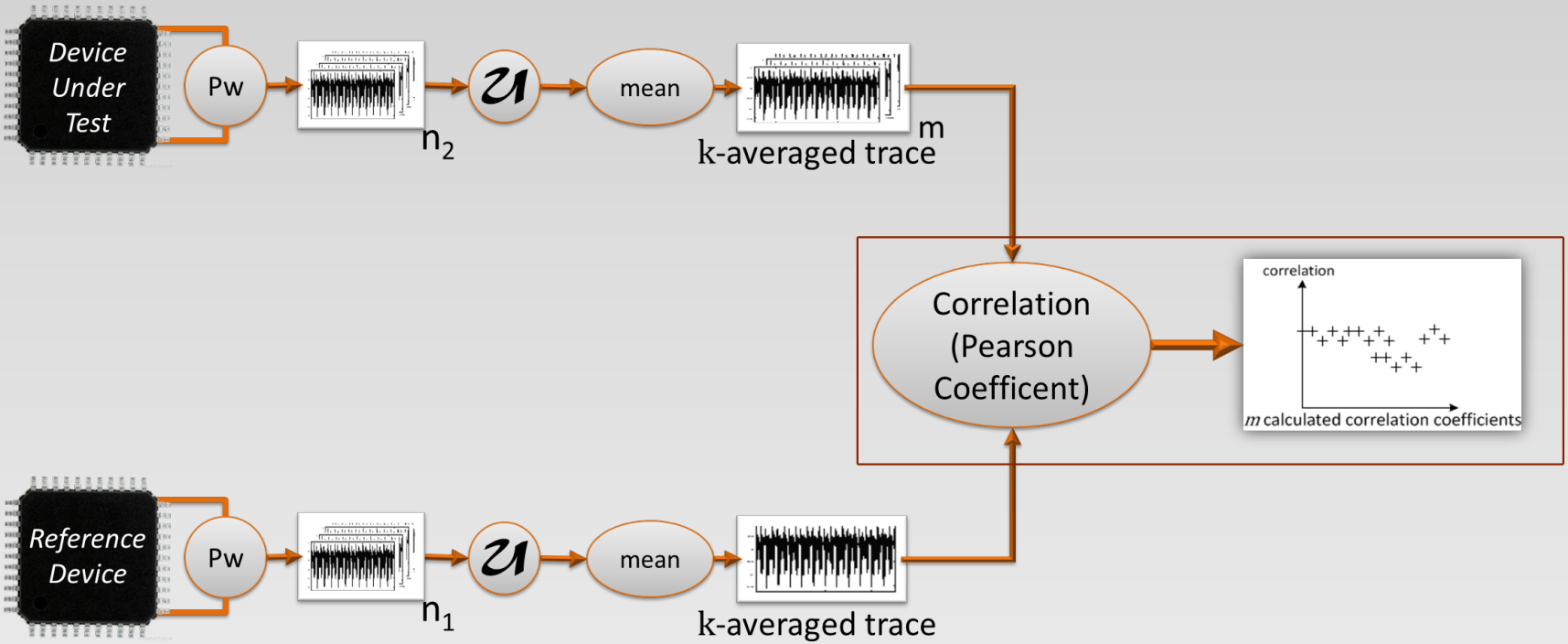
Verification flow

Function 2: Random selection ($\mathfrak{U}$) and mean



Verification flow

Function 3: Correlation



Parameters and Choice

Correlation process parameters

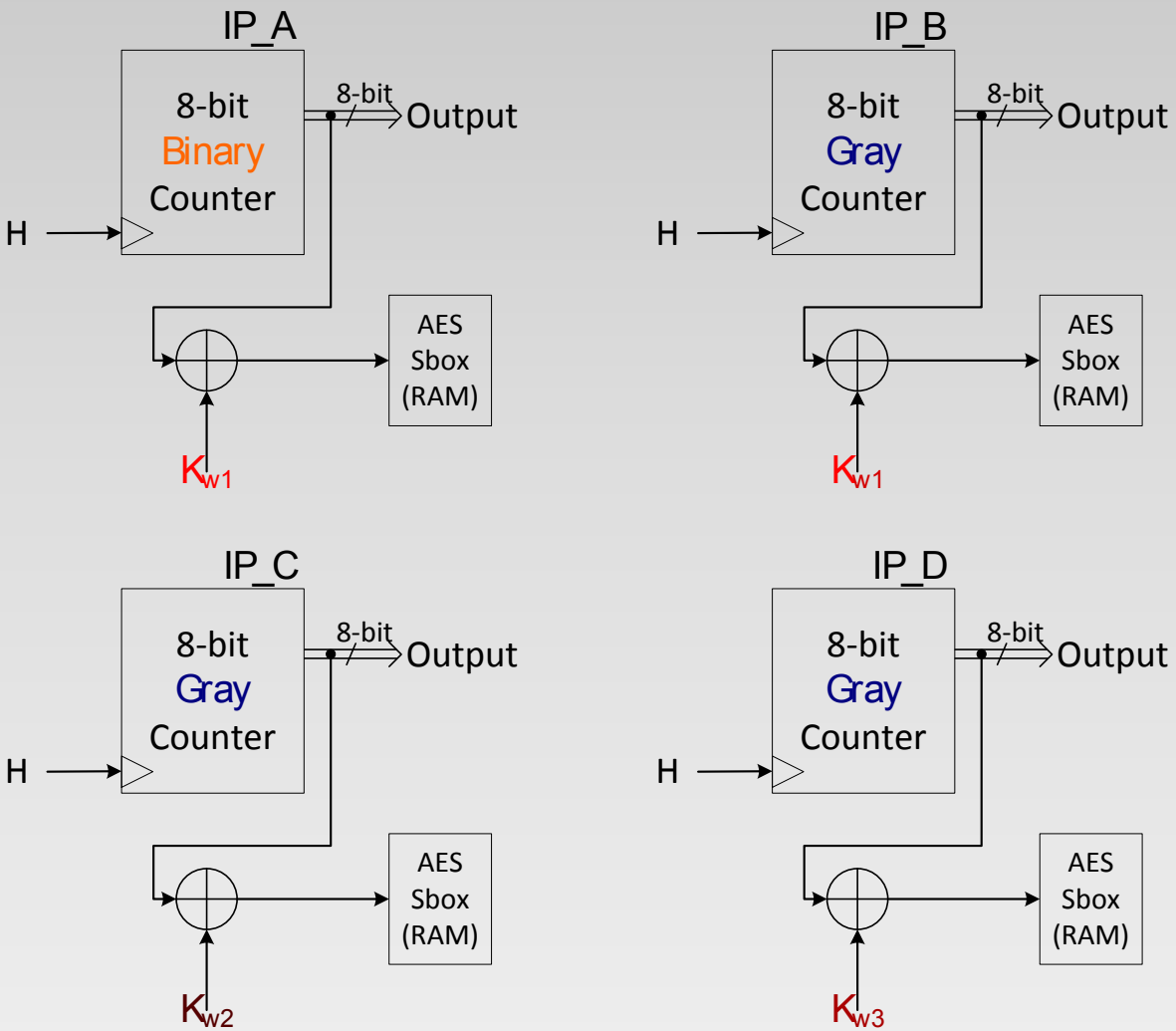
- n_1 : the number of power traces taken over the Reference Device
- n_2 : the number of power traces taken over the DUT
- k : the number of averaged traces
- m : the number of correlation coefficient computed

Requirements for these parameters

- $n_1 \geq k$
- $n_2 \geq k \times m$

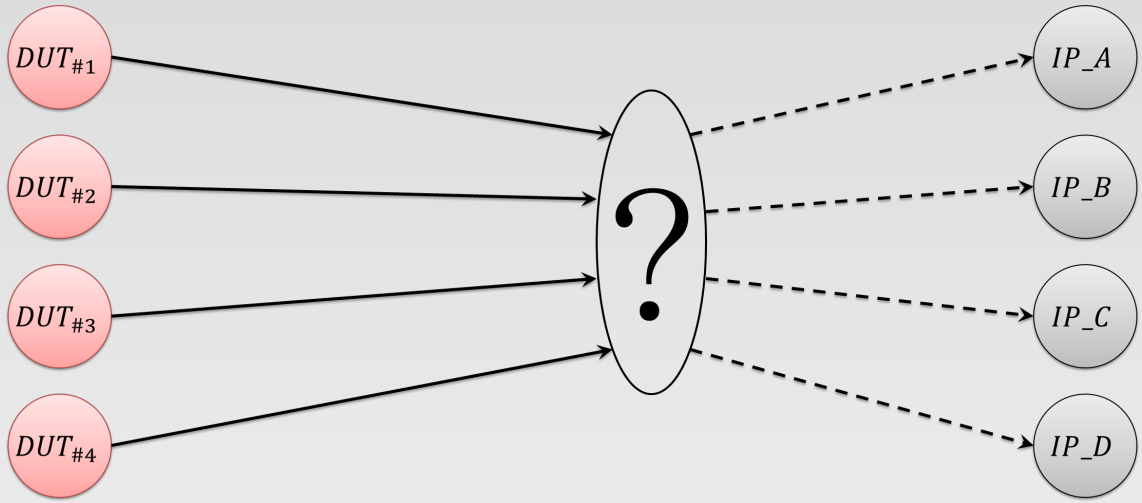
Computation time increases with m
Measurement time with k

Worst Case IPs

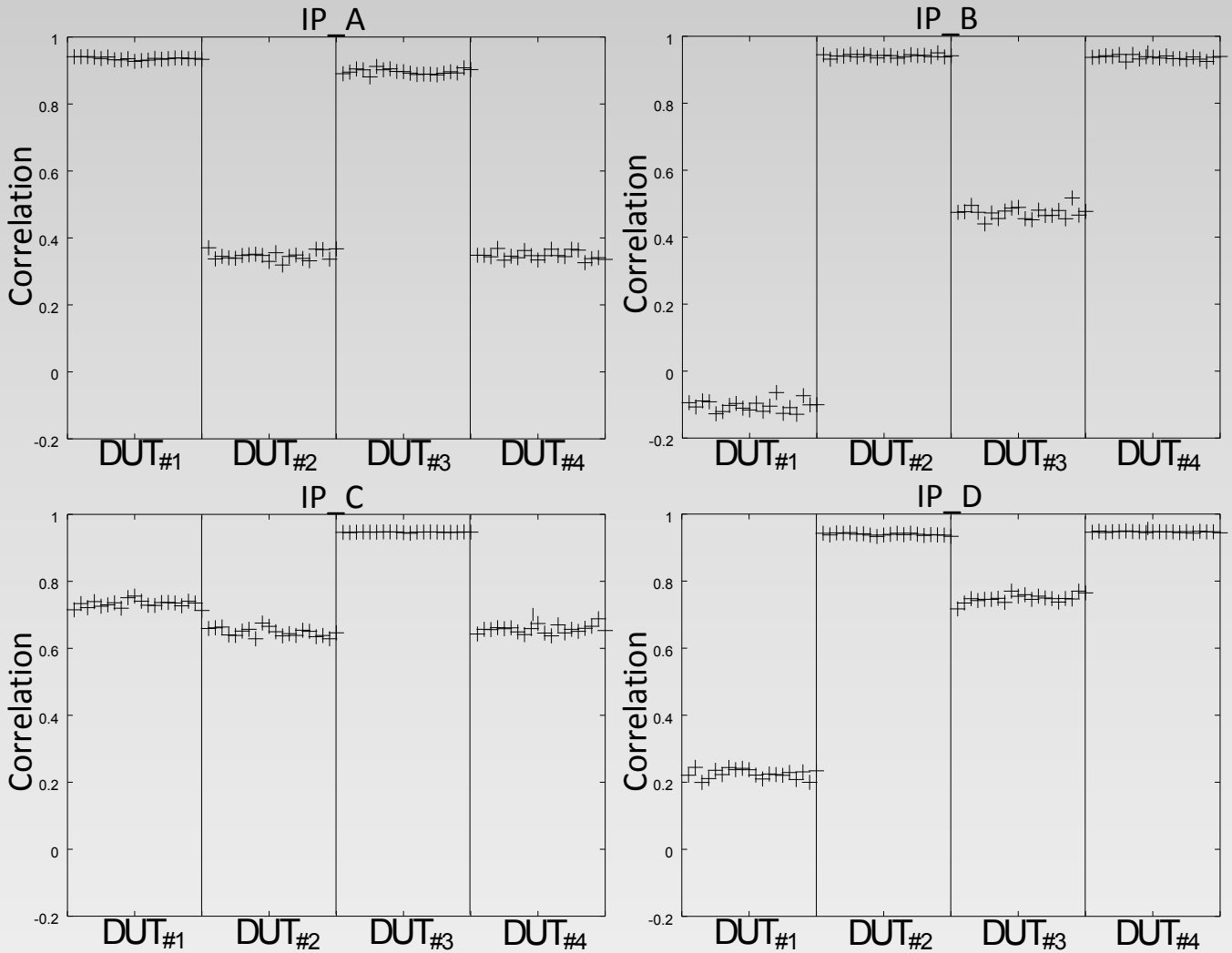


Experiment

- Implement the four IPs in 4 Altera Cyclone III FPGAs gives the four Reference Devices (IP_A, IP_B, IP_C, IP_D)
- Implement the 4 IPs in four **other** Cyclone III FPGAs creates four $DUTs(DUT_{\#1}, DUT_{\#2}, DUT_{\#3}, DUT_{\#4})$



Result of the Correlation Computation



Analysis (1/2)

Choice of the Distinguishers and Definition

Two Distinguishers

- The Means of the correlation : $\overline{C_{X,y,k,m}}$
- The Variance of the correlation : $v(C_{X,y,k,m})$

Confidence distance: Δ_{mean} and Δ_v

Indicates the effectiveness of each distiguisher in percentage.
2 functions are defined to create these indicators:

- $max_2(E)$ give the second highest value of a set E
- $min_2(E)$ give the second lowest value of a set E

$$\Delta_{mean}(X) = 100 \times \left[1 - \frac{max_2(\{\overline{C_{X,y,k,m}}, y \in \{1,2,3,4\}\})}{max(\{\overline{C_{X,y,k,m}}, y \in \{1,2,3,4\}\})}\right]$$

Analysis (1/2)

Choice of the Distinguishers and Definition

Two Distinguishers

- The Means of the correlation : $\overline{C_{X,y,k,m}}$
- The Variance of the correlation : $v(C_{X,y,k,m})$

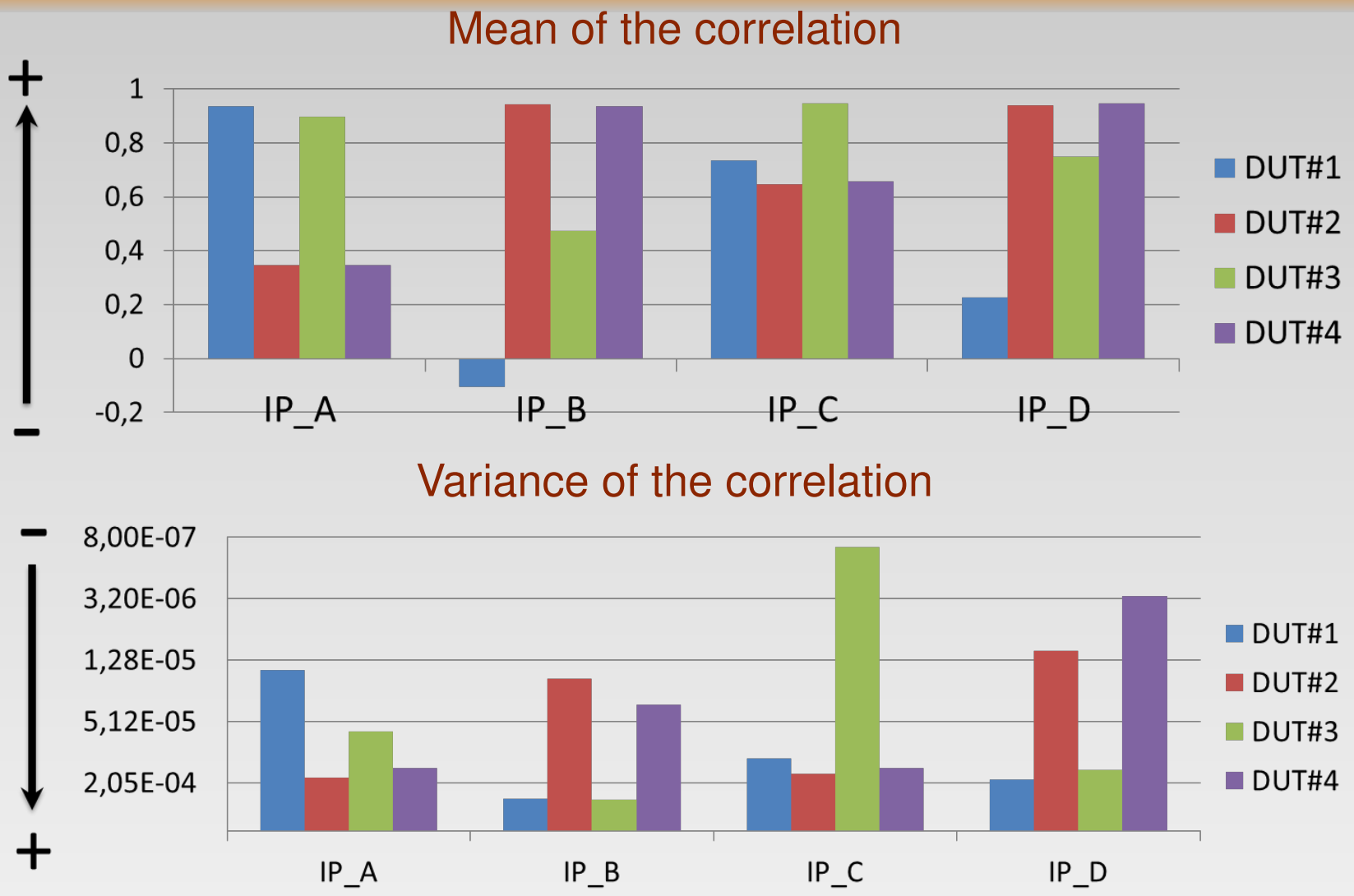
Confidence distance: Δ_{mean} and Δ_v

Indicates the effectiveness of each distiguisher in percentage.
2 functions are defined to create these indicators:

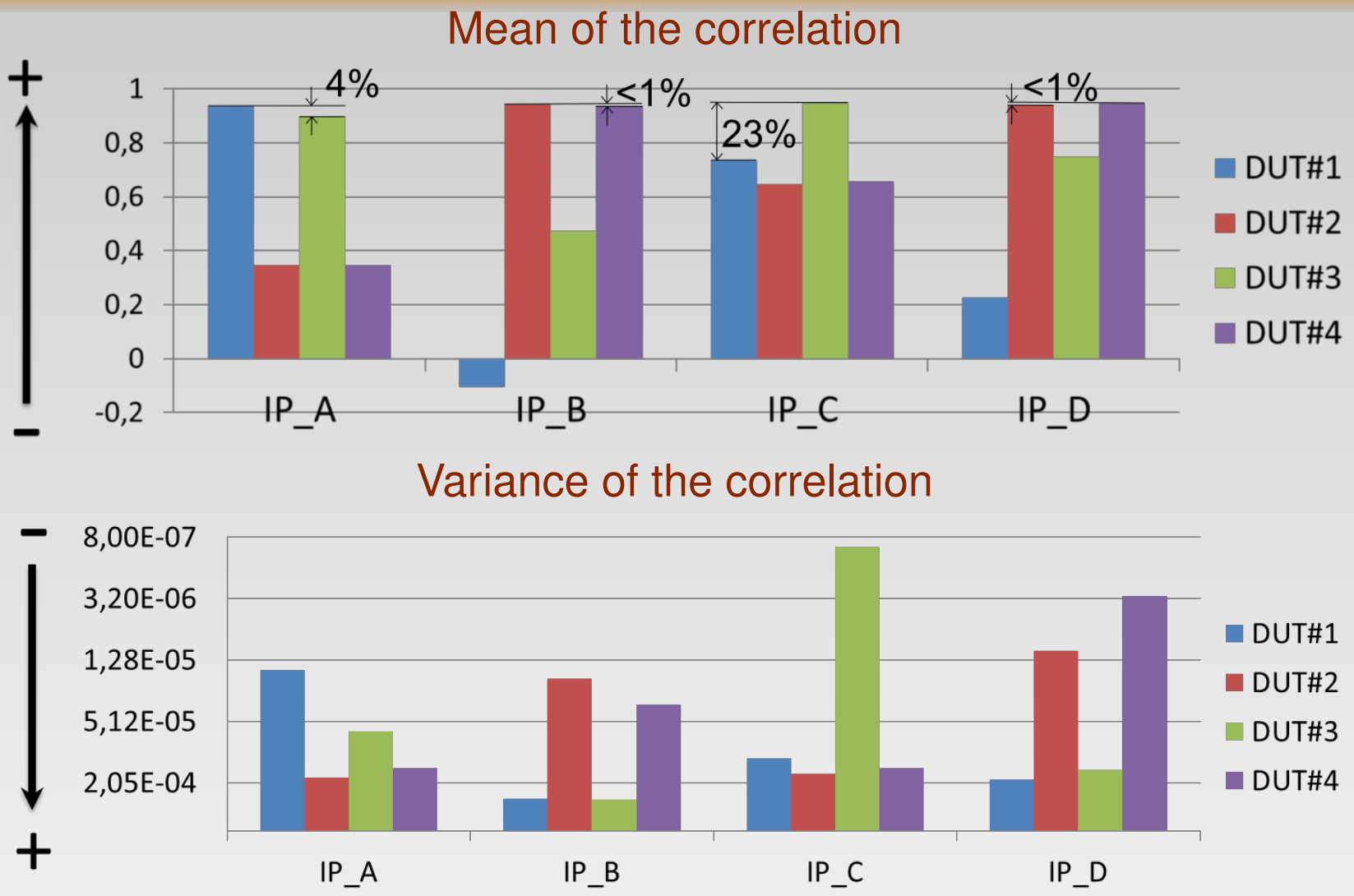
- $max_2(E)$ give the second highest value of a set E
- $min_2(E)$ give the second lowest value of a set E

$$\Delta_v(X) = 100 \times \left[1 - \frac{min(\{v(C_{X,y,k,m}), y \in \{1,2,3,4\}\})}{min_2(\{v(C_{X,y,k,m}), y \in \{1,2,3,4\}\})}\right]$$

Analysis (2/2)
Results

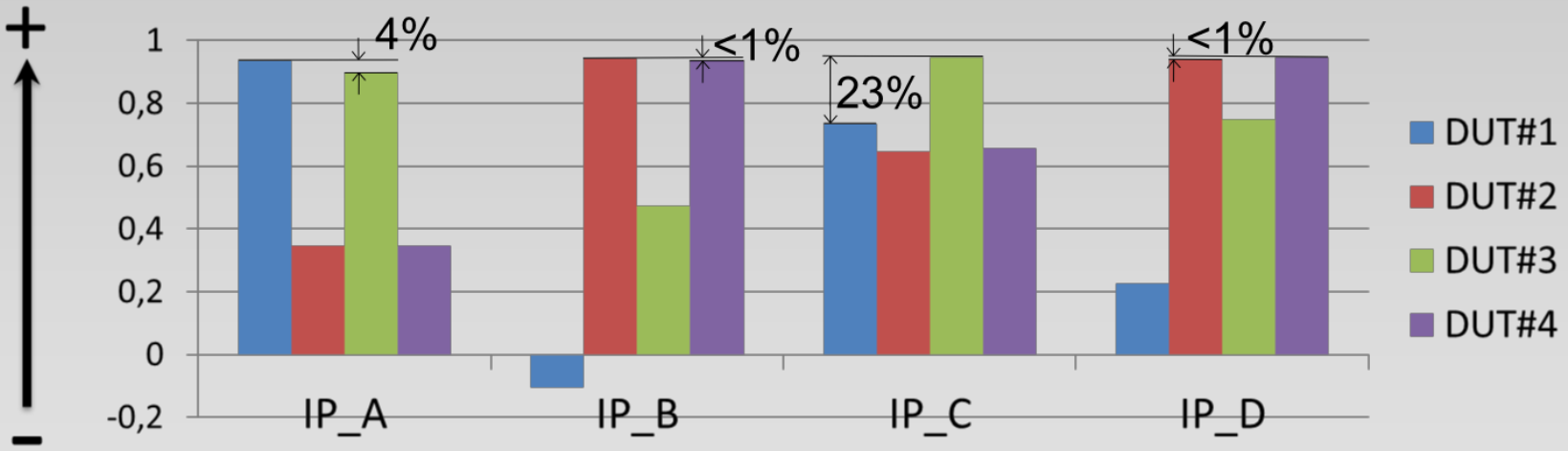


Analysis (2/2)
Results

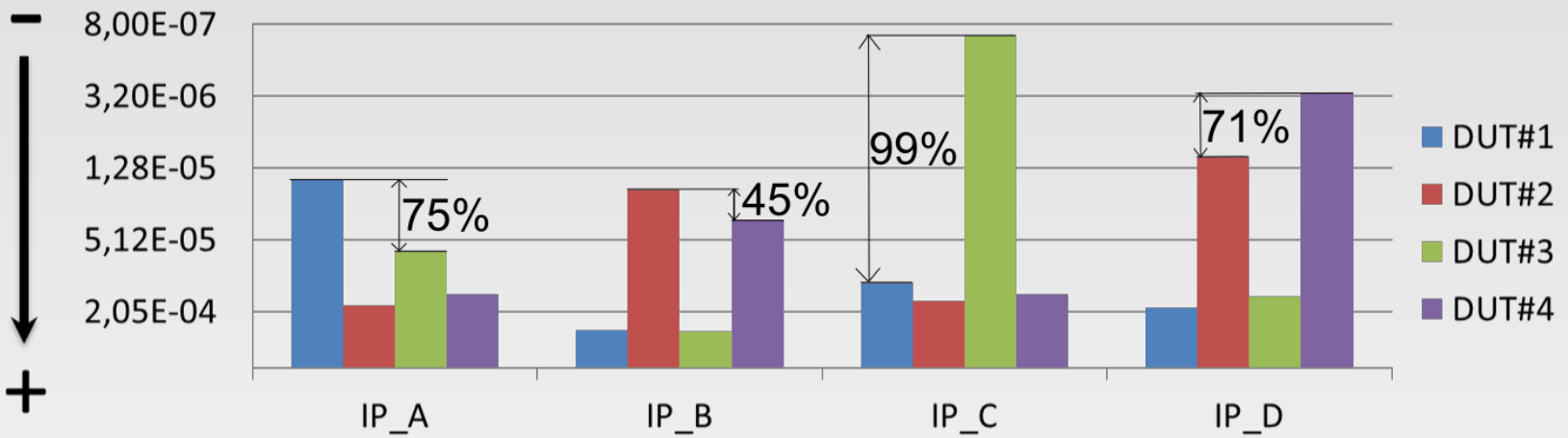


Analysis (2/2)
Results

Mean of the correlation



Variance of the correlation



Conclusion

The proposed verification algorithm :

- Can be applied to verify FSM watermarked IPs
- Insensitive to the CMOS process variations
- The variance of the correlation is better than the mean

Future Works

Future Works

- Replace the reference device by a model
- try to verify IP watermark with more noise

Publication

C. Marchand, L. Bossuet, and E. Jung,
"IP Watermark Verification Based on Power Consumption Analysis",
in IEEE System on Chip Conference 2014.

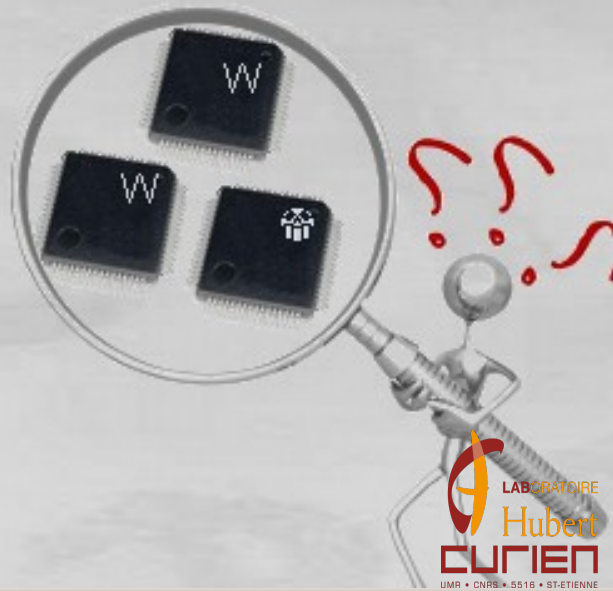
LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE

SALWARE
French ANR Project

PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR
ANR

Thank you for your attention

Questions ?



LABORATOIRE Hubert CURIEN
UMR • CNRS • 5516 • ST-ETIENNE