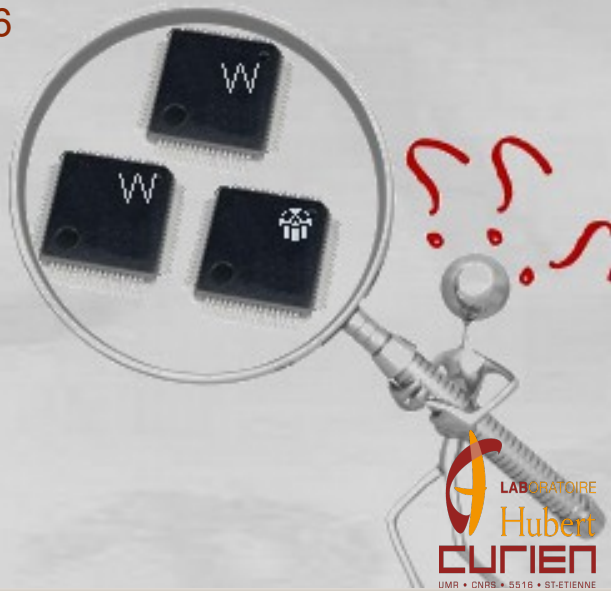
IP Watermark Verification Based on Power Consumption Analysis

Cédric Marchand

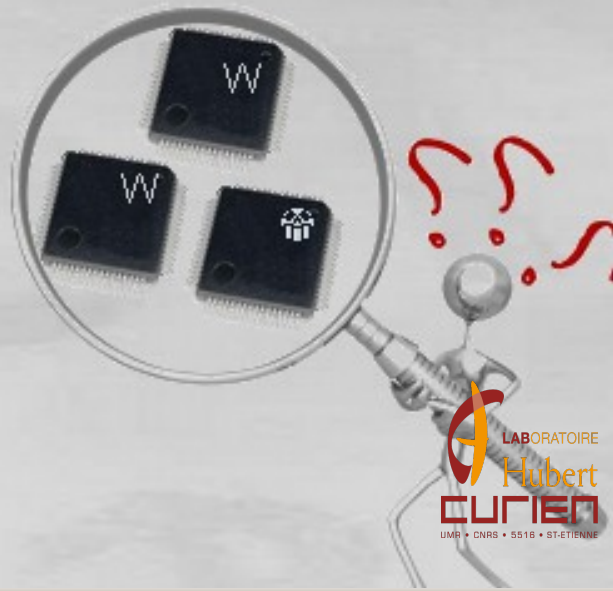
Laboratoire Hubert Curien, UMR CNRS 5516
University of Lyon
Saint-Etienne France

cedric.marchand@univ-st-etienne.fr

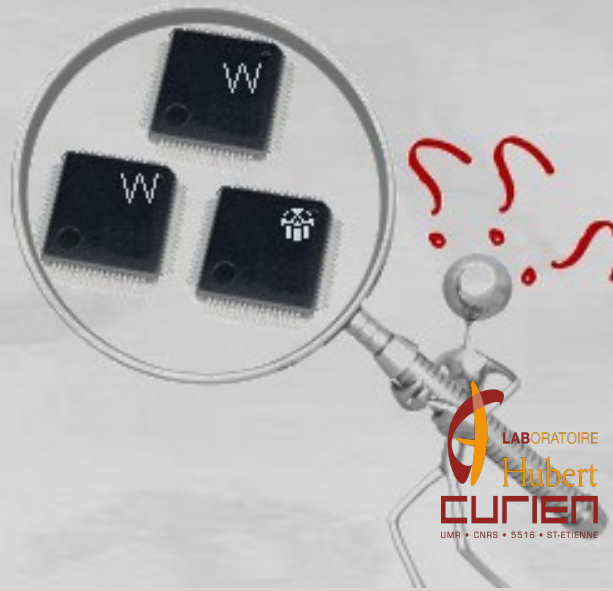
June 17, 2014



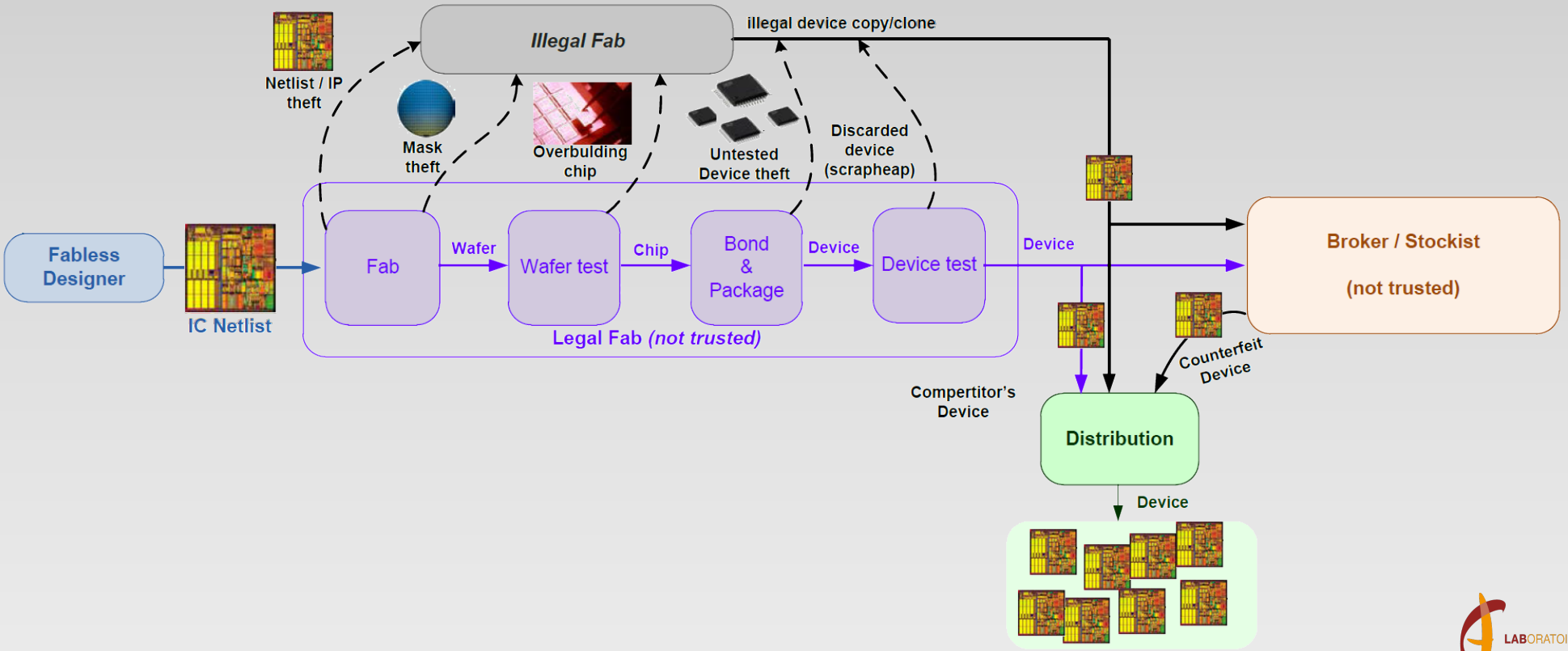
Outline



Outline



IC Threats Model



Consequences

Example of Consequences of these threats

IP theft, Mask theft, Overbuilding chips: Loss of money

Competitor clone devices: Loss of money

Untested devices: Loss of money and reputation

Discarded devices: Loss of money and reputation

Old devices reuse: Loss of money and reputation

In the worst case

In the case of security critical systems, use a counterfeit device could lead to very serious consequences.

Fight these threats by designing SALWARES

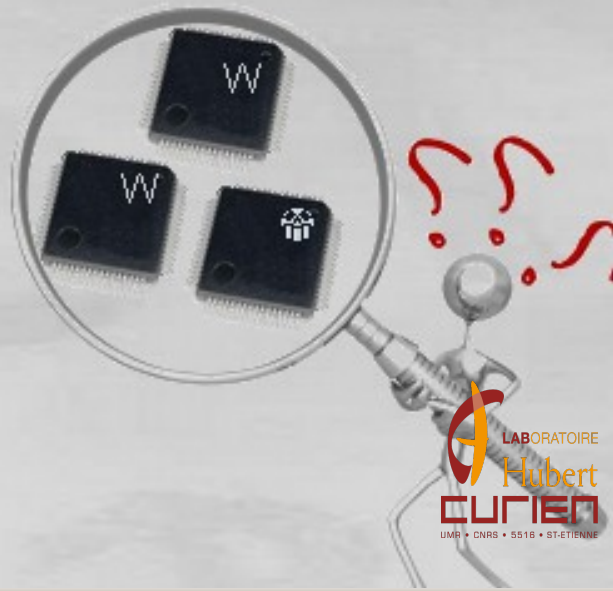
SALutary hardWARES: SALWARES

SALWARES use the same strategies and means as malwares but bring protection to the devices instead of malicious effect.

Example of well-known SALWARES

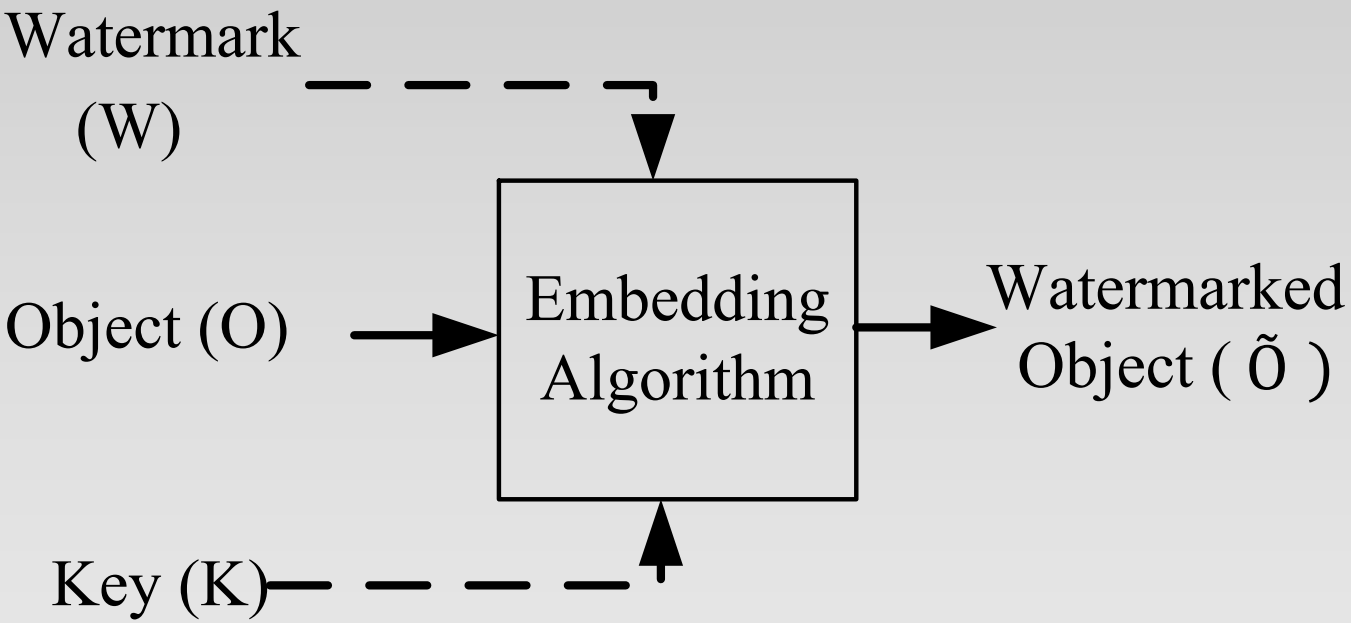
- Physical Unclonable Function for authentication
- Memory encryption, Logic encryption
- Hardware metering, IC metering
- Remote activation
- IP Watermarking

Outline



Watermarking In General

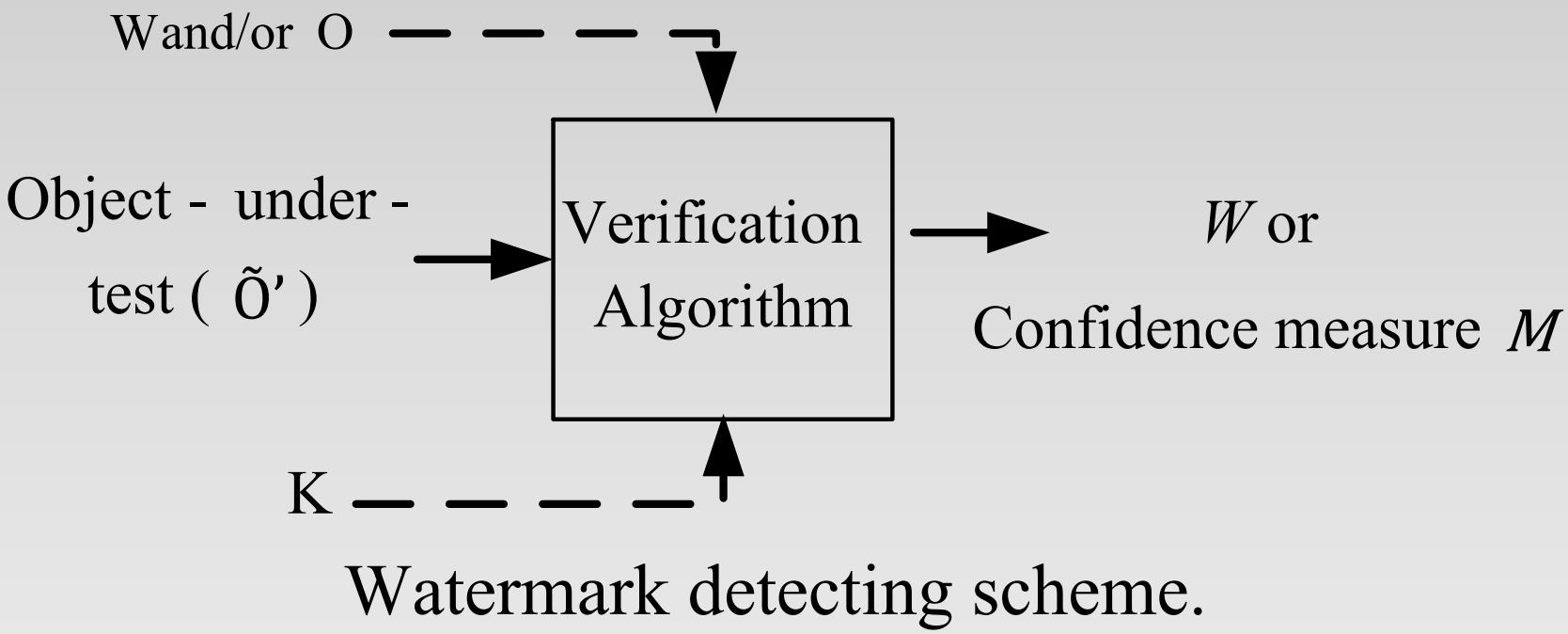
Embedding Process



Watermark embedding scheme.

Watermarking In General

Verification Process



Watermark detecting scheme.

IP Watermarking

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

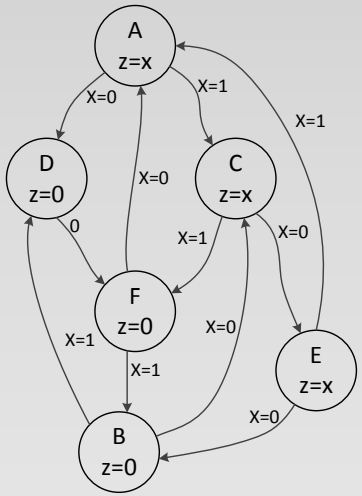
[1] NIE, Tingyuan. Performance Evaluation for IP Protection Watermarking Techniques.

FSM Watermarking

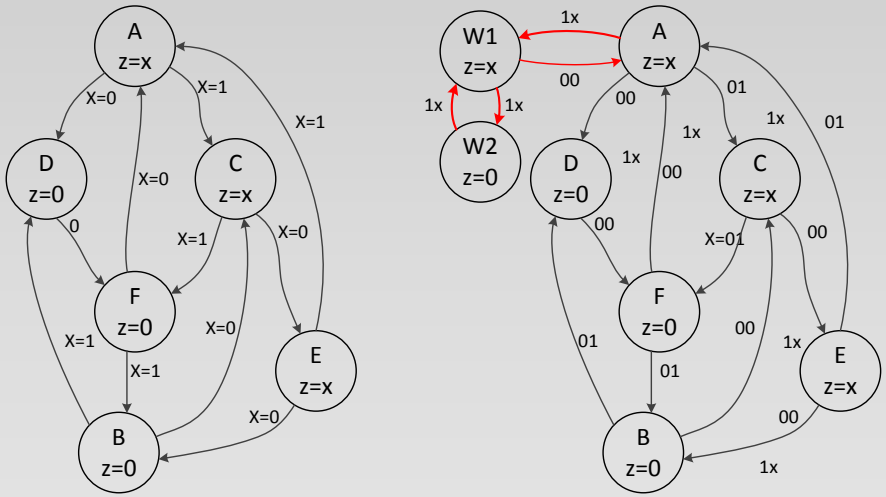
It is the method the most studied to insert a watermark inside digital and synchronous IPs because :

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

Example of techniques



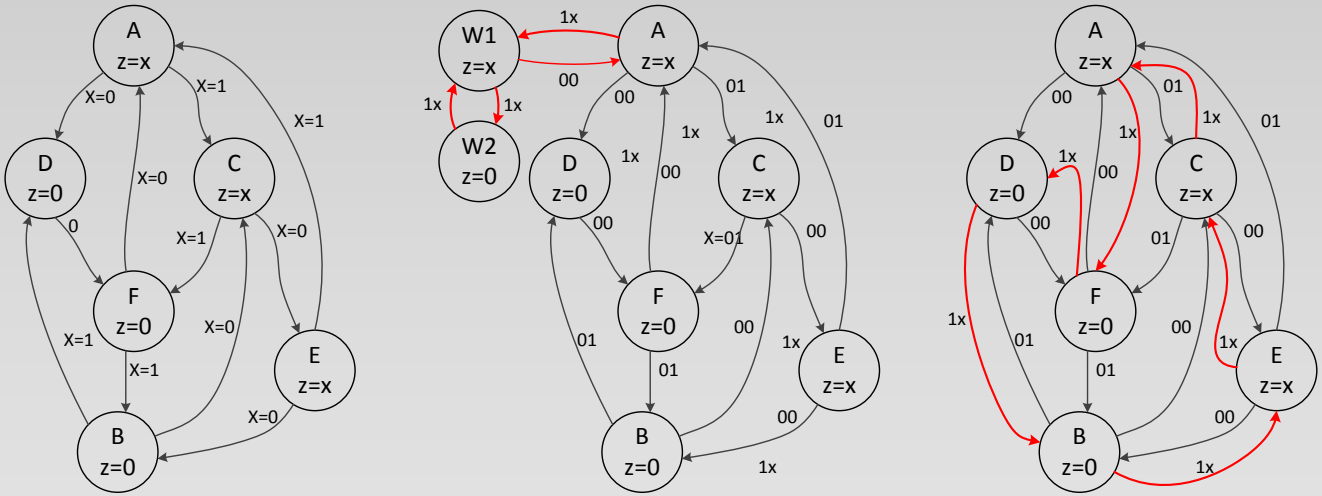
Example of techniques



FSM watermarking techniques

- Add new nodes to the FSM

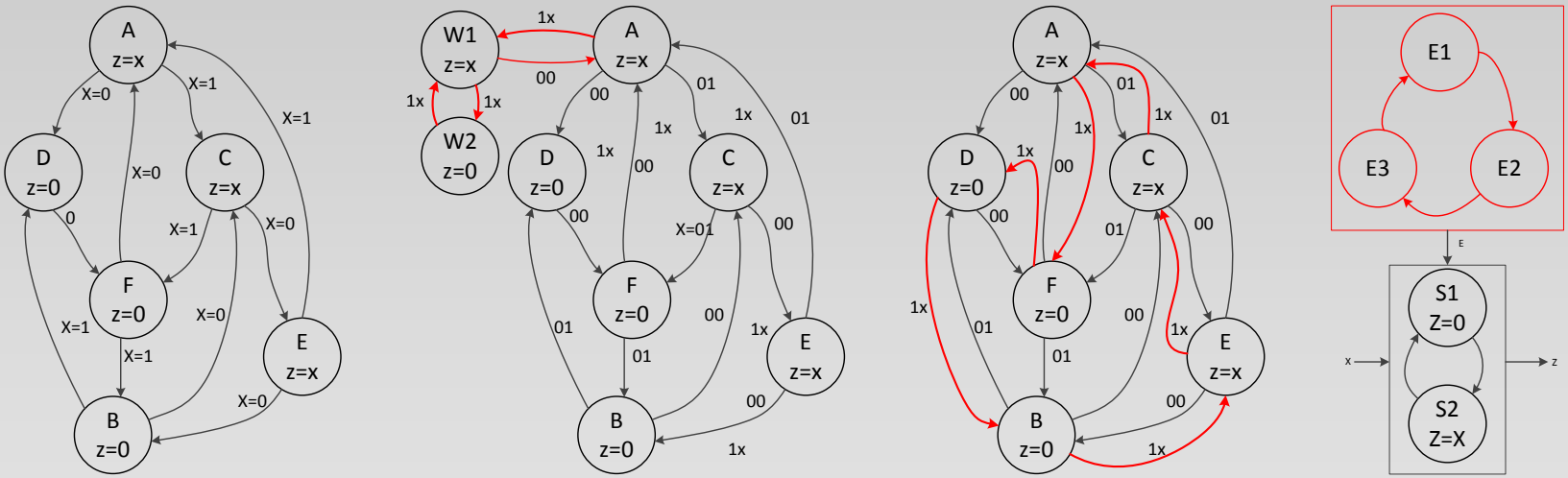
Example of techniques



FSM watermarking techniques

- Add new nodes to the FSM
- Add new transitions to the FSM

Example of techniques



FSM watermarking techniques

- Add new nodes to the FSM
- Add new 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 ?

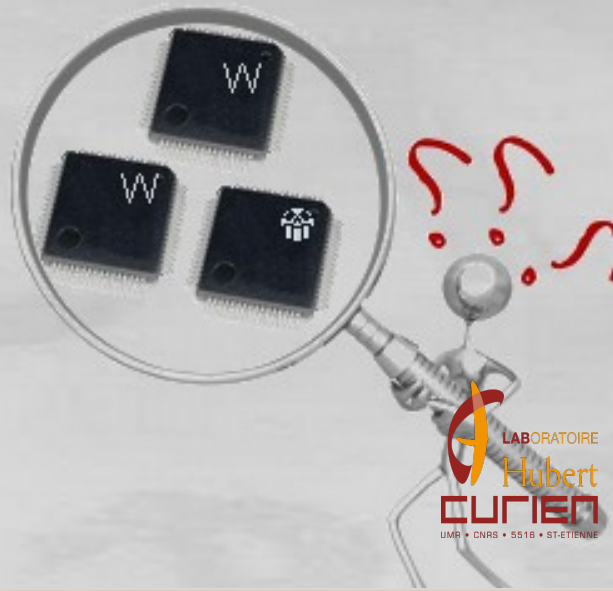
In the case of FSM watermarking, the verification can be difficult and may need:

- 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

Requirements

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

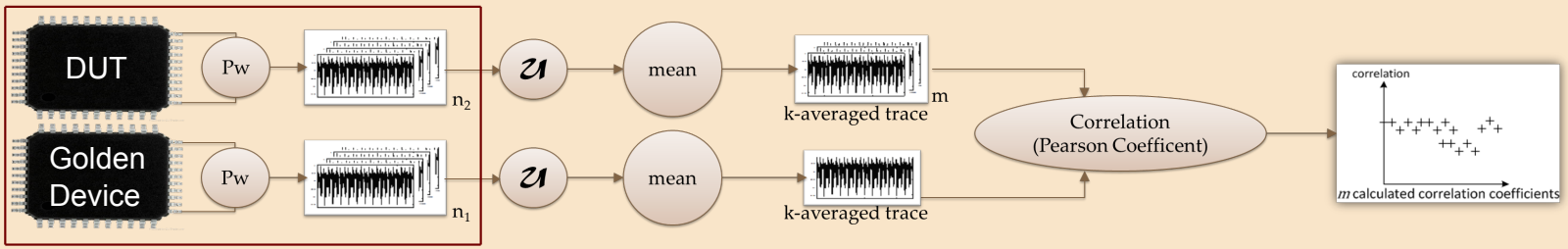
Objectives

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

Verification flow

A correlation computation process is defined with 3 functions for the verification flow of the Watermark of the IP.

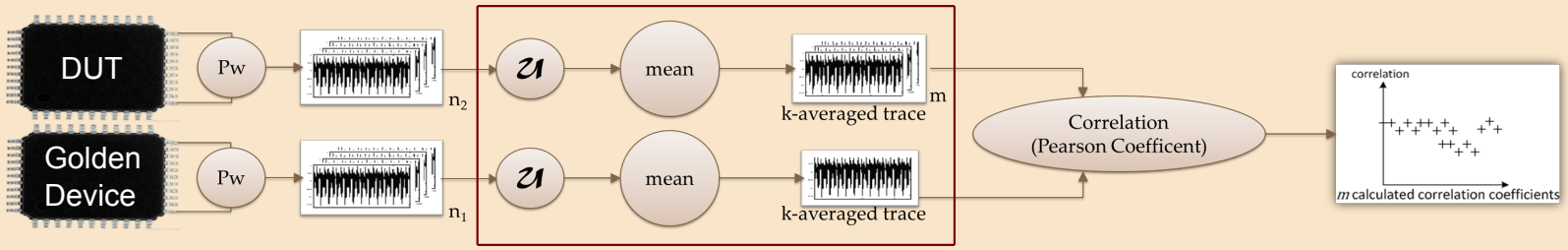
Function 1: Power acquisition



Verification flow

A correlation computation process is defined with 3 functions for the verification flow of the Watermark of the IP.

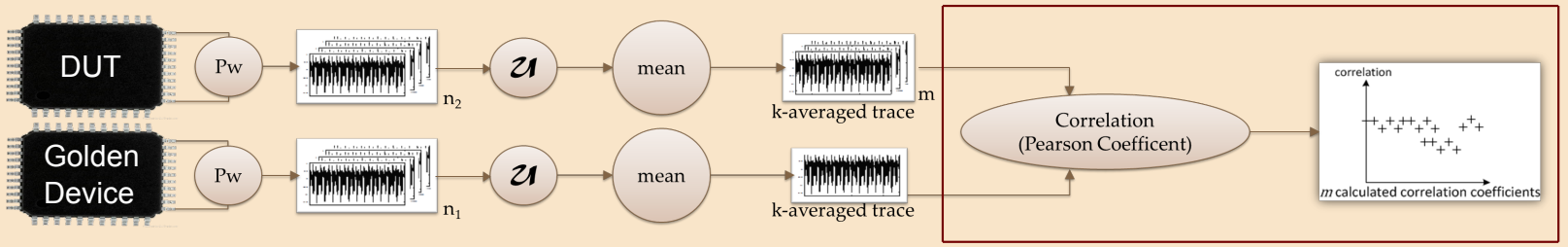
Function 2: Random selection ($\mathfrak{U}$) and mean



Verification flow

A correlation computation process is defined with 3 functions for the verification flow of the Watermark of the IP.

Function 3: Correlation



Parameters and Choice

Correlation process parameters

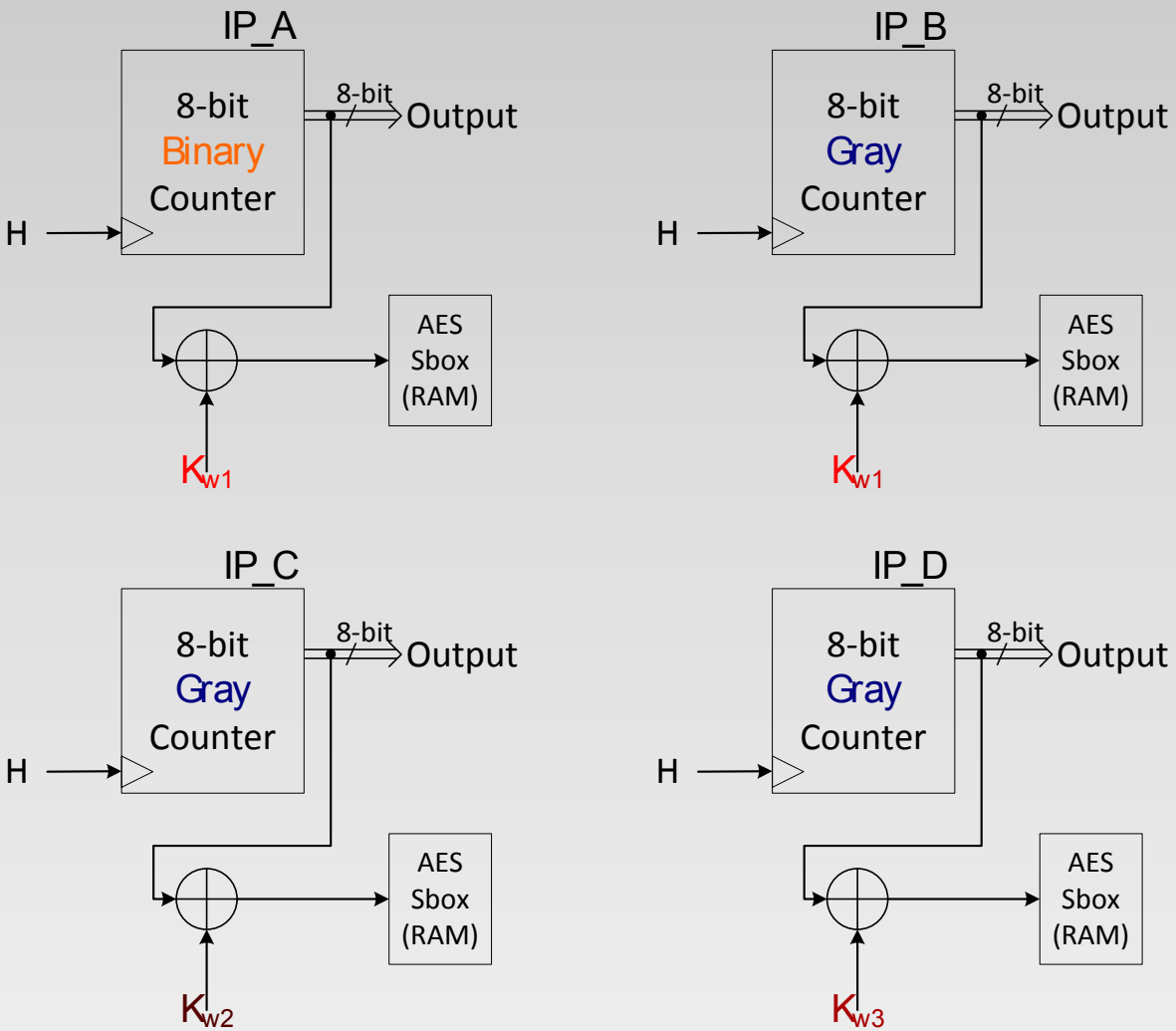
- n_1 : the number of power traces taken over the Golden Device
- n_2 : the number of power traces taken over the DUT
- k : the number of averaged traces
- m : the number of correlation coefficient computed

Requirements for these parameters

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

Computation time increases with m
Measurement time with k

Designed IPs



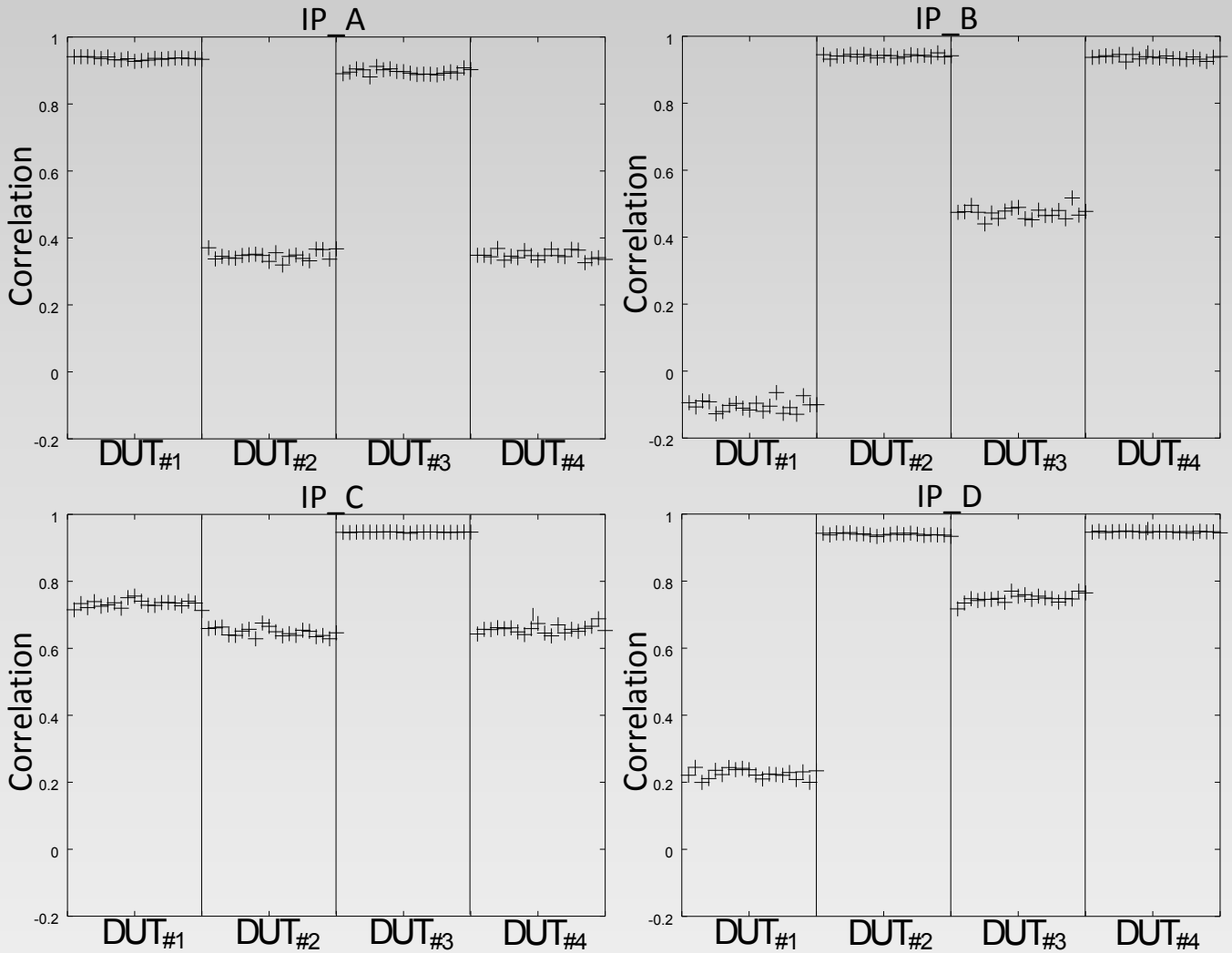
Experimental Setup

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

Correlation computation parameters

- $k = 50$
- $m = 20$
- $n_1 = 400$
- $n_2 = 10000$

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

Confidence distance: Δ_{mean} and Δ_v

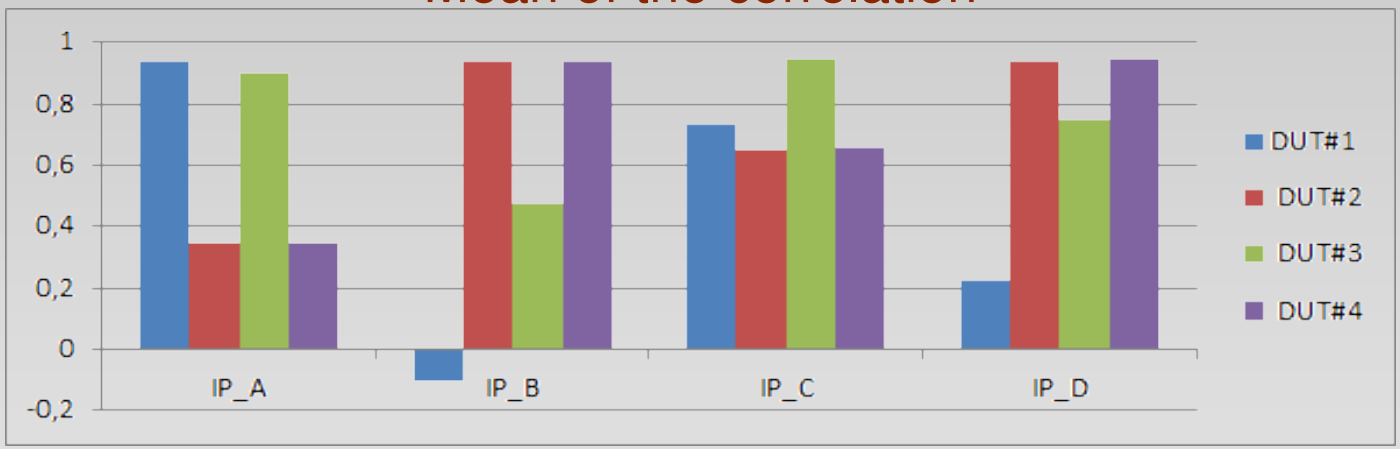
Indicates the effectiveness of each distiguisher in percentage.
2 functions are defined to create these indicators:

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

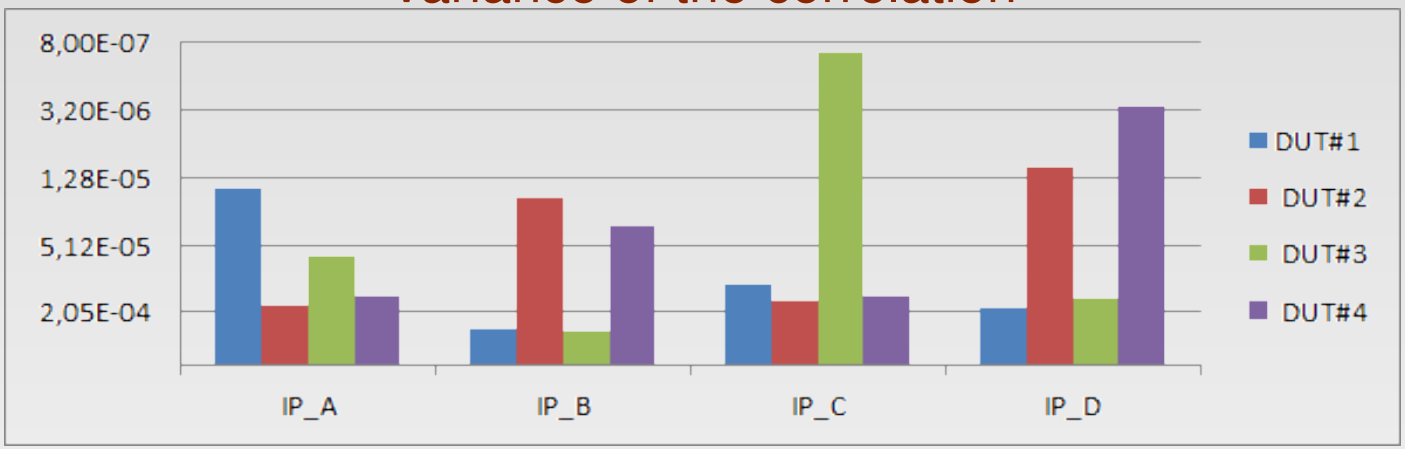
$$\Delta_v(X) = 100 \times \left[1 - \frac{min(\{v(\mathcal{C}_{X,y,k,m}), y \in \{1,2,3,4\}\})}{min_2(\{v(\mathcal{C}_{X,y,k,m}), y \in \{1,2,3,4\}\})}\right]$$

Analysis (2/2)
Results

Mean of the correlation

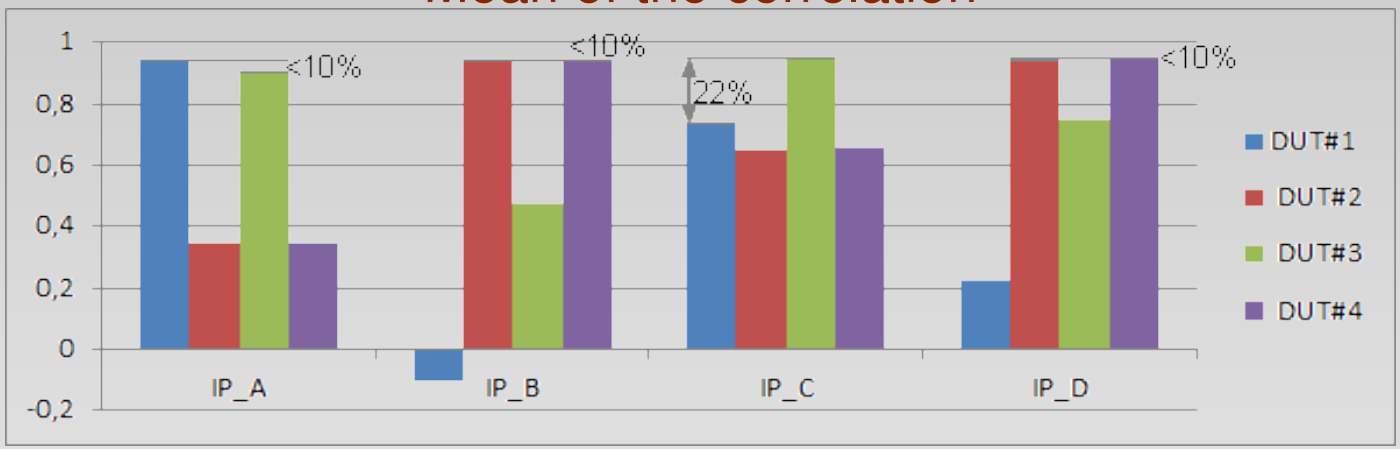


Variance of the correlation

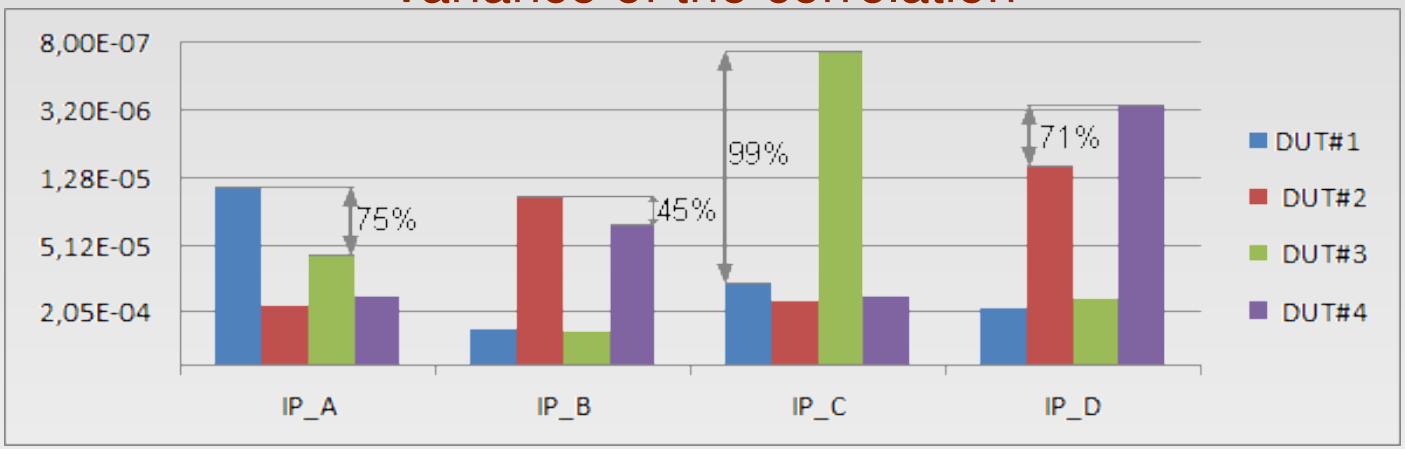


Analysis (2/2)
Results

Mean of the correlation



Variance of the correlation



Conclusion

Verification Algorithm

- Can be applied to verify FSM watermarked IPs
- Insensitive to the Cmos process variations
- The variance of the correlation is a better distinguisher than the mean for the decision

Thank you for your attention

Questions ?

Work accepted to the conference socc2014, to reference it:
C. Marchand, L. Bossuet, and E. Jung, “Ip watermark verification based on power consumption analysis”, in SoCC. IEEE, 2014.